亚马逊云科技

用户指南

# Amazon Simple Storage Service



API 版本 2006-03-01

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

# Amazon Simple Storage Service: 用户指南

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Amazon Web Services 文档中描述的 Amazon Web Services 服务或功能可能因区域而异。要查看适用于中国区域的差异，请参阅 中国的 Amazon Web Services 服务入门 (PDF)。

# Table of Contents

什么是 Amazon S3？ ..... 1
Amazon S3 的功能 ..... 1
存储类 ..... 1
存储管理 ..... 2
访问管理和安全性 ..... 2
数据处理 ..... 3
存储日志记录和监控 ..... 3
分析和见解 ..... 4
强一致性 ..... 4
Amazon S3 的工作原理 ..... 5
存储桶 ..... 5
对象 ..... 7
键 ..... 8
S3 版本控制 ..... 8
版本 ID ..... 8
存储桶策略 ..... 8
S3 接入点 ..... 9
访问控制列表（ACL） ..... 9
区域 ..... 9
Amazon S3 数据一致性模型 ..... 10
并发应用程序 ..... 11
相关服务 ..... 12
访问 Amazon S3 ..... 13
Amazon Web Services Management Console ..... 13
Amazon Command Line Interface ..... 13
Amazon SDK ..... 13
Amazon S3 REST API ..... 14
为 Amazon S3 支付费用 ..... 14
PCI DSS 合规性 ..... 15
入门 ..... 16
设置 ..... 16
注册 Amazon Web Services 账户 ..... 17
保护 IAM 用户 ..... 17
步骤 1：创建存储桶 ..... 18

步骤 2：上传对象 ..... 23
步骤 3：下载对象 ..... 24
使用 S3 控制台 ..... 24
步骤 4：复制对象 ..... 25
步骤 5：删除对象和存储桶 ..... 26
删除对象 ..... 27
清空存储桶 ..... 27
删除存储桶 ..... 28
后续步骤 ..... 28
了解常见使用案例 ..... 29
控制对存储桶和对象的访问 ..... 29
保护和监控存储 ..... 30
用 Amazon S3 进行开发 ..... 30
从教程中学习 ..... 31
探索培训和支持 ..... 33
使用通用存储桶 ..... 34
通用存储桶概述 ..... 35
通用存储桶概述 ..... 35
常见通用存储桶模式 ..... 36
权限 ..... 36
管理对通用存储桶的公共访问权限 ..... 37
通用存储桶配置 ..... 38
通用存储桶操作 ..... 40
通用存储桶性能监控 ..... 40
常见的存储桶模式 ..... 41
多租户通用存储桶模式 ..... 42
按用途划分的存储桶模式 ..... 42
命名规则 ..... 43
通用存储桶命名规则 ..... 44
通用存储桶名称示例 ..... 45
最佳实践 ..... 46
创建在存储桶名称中使用 GUID 的存储桶 ..... 47
配额、局限性和限制 ..... 48
存储桶配额 ..... 48
对象和存储桶限制 ..... 49
存储桶命名规则 ..... 49

访问存储桶 ..... 49
..... 49
通用存储桶的虚拟托管 ..... 52
创建通用存储桶 ..... 60
通用存储桶设置 ..... 60
查看存储桶属性 ..... 73
列出存储桶 ..... 75
清空通用存储桶 ..... 81
清空配置了 Amazon CloudTrail 的通用存储桶 ..... 83
删除通用存储桶 ..... 83
适用于 Amazon S3 的 Mountpoint ..... 88
安装 Mountpoint ..... 89
配置和使用 Mountpoint ..... 92
Mountpoint 故障排除 ..... 95
适用于 Amazon S3 的存储浏览器 ..... 96
使用适用于 S3 的存储浏览器 ..... 97
安装适用于 S3 的存储浏览器 ..... 98
设置适用于 S3 的存储浏览器 ..... 98
配置适用于 S3 的存储浏览器 ..... 110
适用于 S3 的存储浏览器故障排除 ..... 111
配置 Transfer Acceleration ..... 112
为什么要使用 Transfer Acceleration？ ..... 112
使用 Transfer Acceleration 的要求 ..... 112
入门 ..... 114
启用 Transfer Acceleration ..... 115
速度比较工具 ..... 122
使用申请方付款 ..... 123
申请方付款的费用支付方式 ..... 124
配置申请方付款 ..... 124
检索 requestPayment 配置 ..... 126
从申请方付款桶中下载对象 ..... 127
使用对象 ..... 129
对象概述 ..... 130
子资源 ..... 131
为对象命名 ..... 131
选择对象键名称 ..... 132

对象键命名准则 ..... 133
使用元数据 ..... 136
系统定义的对象元数据 ..... 137
用户定义的对象元数据 ..... 139
编辑对象元数据 ..... 141
加快数据发现速度 ..... 144
上传对象 ..... 177
上传对象 ..... 178
防止上传具有相同键名称的对象 ..... 190
使用分段上传 ..... 190
提出有条件请求 ..... 259
如何根据元数据检索或复制对象 ..... 260
如何防止对象覆盖 ..... 261
复制、移动和重命名对象 ..... 271
复制对象 ..... 274
移动对象 ..... 283
重命名对象 ..... 284
下载对象 ..... 285
下载对象 ..... 286
下载多个对象 ..... 288
下载对象的一部分 ..... 290
从另一个 Amazon Web Services 账户下载对象 ..... 290
下载归档对象 ..... 291
根据元数据下载对象 ..... 292
下载对象故障排查 ..... 292
在 Amazon S3 中检查对象完整性 ..... 292
使用支持的校验和算法 ..... 293
完整对象和复合校验和类型 ..... 294
使用完整对象校验和进行分段上传 ..... 296
使用分段级校验和进行分段上传 ..... 296
校验和操作 ..... 297
在上传对象时使用 Content-M5 ..... 305
使用 Content-MD5 和 ETag 验证上传的对象 ..... 305
使用尾随校验和 ..... 306
删除对象 ..... 311
删除对象之前应考虑的最佳实践 ..... 311

从启用版本控制的存储桶中删除对象 ..... 312
从已暂停版本控制的存储桶中删除对象 ..... 313
从不受版本控制的存储桶中删除对象 ..... 313
从启用了 MFA 的存储桶中删除对象 ..... 313
删除单个对象 ..... 313
删除多个对象 ..... 324
组织和列出对象 ..... 327
使用前缀 ..... 328
列出对象 ..... 329
使用文件夹 ..... 332
查看对象属性 ..... 336
使用标签对于对象进行分类 ..... 337
使用预签名 URL 下载和上传对象 ..... 349
谁可以创建预签名 URL ..... 350
预签名 URL 的到期时间 ..... 351
限制预签名 URL 功能 ..... 351
使用预签名 URL 共享对象 ..... 353
使用预签名 URL 上传对象 ..... 356
转换对象 ..... 359
创建对象 Lambda 接入点 ..... 361
使用 Amazon S3 对象 Lambda 接入点 ..... 373
安全注意事项 ..... 377
编写 Lambda 函数 ..... 383
使用 Amazon 构建的函数 ..... 413
S3 对象 Lambda 的最佳实践和指南 ..... 415
S3 对象 Lambda 教程 ..... 417
S3 对象 Lambda 故障排除 ..... 449
批量执行对象操作 ..... 449
批量操作基础知识 ..... 450
S3 批量操作教程 ..... 451
授予权限 ..... 451
创建任务 ..... 461
支持的操作 ..... 482
管理任务 ..... 519
跟踪任务状态和完成报告 ..... 523
使用标签 ..... 536

使用批量操作管理对象锁定 ..... 551
教程：对视频进行批量转码 ..... 575
排查批量操作问题 ..... 613
就地查询数据 ..... 615
要求和限制 ..... 615
构建请求 ..... 616
错误 ..... 617
S3 Select 示例 ..... 617
SQL 参考 ..... 621
使用目录存储桶 ..... 660
目录存储桶名称 ..... 660
目录 ..... 661
键名称 ..... 661
访问权限管理 ..... 661
目录存储桶配额 ..... 662
创建和使用目录存储桶 ..... 662
目录存储桶的应用场景 ..... 663
高性能工作负载 ..... 663
数据驻留工作负载 ..... 700
目录存储桶的差异 ..... 711
目录存储桶的差异 ..... 712
目录存储桶支持的 API 操作 ..... 713
目录存储桶不支持的 Amazon S3 功能 ..... 714
目录存储桶的联网 ..... 716
了解如何查看、监控和管理 SageMaker 端点。 ..... 716
配置 VPC 网关端点 ..... 716
目录存储桶命名规则 ..... 717
查看属性 ..... 718
管理存储桶策略 ..... 718
添加存储桶策略 ..... 719
查看存储桶策略 ..... 722
删除存储桶策略 ..... 722
清空目录存储桶 ..... 723
删除目录存储桶 ..... 724
列出目录存储桶 ..... 727
确定您是否可以访问存储桶 ..... 729

使用目录桶中的对象 ..... 730
将对象导入到目录存储桶 ..... 731
使用 S3 生命周期 ..... 732
对 S3 Express One Zone 使用批量操作 ..... 745
向对象追加数据 ..... 747
上传对象 ..... 749
复制对象 ..... 779
删除对象 ..... 784
下载对象 ..... 788
生成预签名 URL 以共享对象 ..... 791
检索对象元数据 ..... 791
列出对象 ..... 792
目录存储桶的安全性 ..... 792
数据保护和加密 ..... 793
对请求进行身份验证和授权 ..... 813
安全最佳实践 ..... 845
使用目录存储桶的接入点 ..... 849
命名规则、限制和局限性 ..... 849
引用目录存储桶的接入点 ..... 851
接入点对象操作 ..... 851
配置 IAM 策略 ..... 852
监控和日志记录 ..... 857
创建目录存储桶的接入点 ..... 858
管理接入点 ..... 860
使用 Amazon CloudTrail 对目录存储桶进行日志记录 ..... 869
目录存储桶的 CloudTrail 管理事件 ..... 869
目录存储桶的 CloudTrail 数据事件 ..... 870
..... 871
优化目录存储桶性能 ..... 878
使用基于会话的身份验证 ..... 878
其他 S3 校验和最佳实践 ..... 878
使用最新版本的 Amazon SDK 和通用运行时库 ..... 879
使用目录存储桶进行开发 ..... 879
目录存储桶的区域和可用区端点 ..... 879
使用 S3 控制台、Amazon CLI 和 Amazon SDK 处理目录存储桶 ..... 880
目录存储桶 API 操作 ..... 881

使用 Amazon S3 表类数据存储服务和表存储桶 ..... 884
S3 表类数据存储服务的功能 ..... 884
相关服务 ..... 885
教程：S3 表类数据存储服务入门 ..... 886
步骤 1：创建表存储桶并将其与 Amazon 分析服务集成 ..... 887
步骤 2：创建表命名空间和表 ..... 888
（可选）步骤 3：授予对表的 Lake Formation 权限 ..... 890
步骤 4：在 Athena 中使用 SQL 查询数据 ..... 891
表存储桶 ..... 892
表存储桶命名规则 ..... 893
创建表存储桶 ..... 895
删除表存储桶 ..... 897
查看表存储桶详细信息 ..... 898
管理策略 ..... 898
S3 表类数据存储服务维护 ..... 899
S3 表类数据存储服务维护任务状态 ..... 899
表存储桶维护 ..... 900
表维护 ..... 902
注意事项和限制 ..... 904
命名空间 ..... 906
创建命名空间 ..... 907
删除命名空间 ..... 908
表 ..... 909
创建表 ..... 910
删除表 ..... 915
管理策略 ..... 915
访问表 ..... 917
通过 Amazon SageMaker 智能湖仓集成访问表 ..... 917
直接访问表 ..... 918
将 S3 表类数据存储服务与 Amazon 分析服务结合使用 ..... 919
使用 Amazon Glue Iceberg REST 端点访问表 ..... 931
使用 Amazon S3 表类数据存储服务 Iceberg REST 端点访问表 ..... 935
使用客户端目录访问表 ..... 941
Amazon Athena ..... 943
Amazon Redshift ..... 945
Amazon EMR ..... 945

QuickSight ..... 949
Amazon Data Firehose ..... 951
Amazon Glue ETL ..... 958
Amazon Web Services 区域、端点和配额 ..... 969
S3 表类数据存储服务 Amazon Web Services 区域和端点 ..... 969
S3 表类数据存储服务配额 ..... 974
S3 表类数据存储服务的安全性 ..... 975
加密 ..... 976
访问权限管理 ..... 988
VPC 连接 ..... 1007
限制和局限性 ..... 1010
使用 Amazon CloudTrail 对 S3 表类数据存储服务进行日志记录 ..... 1011
S3 表类数据存储服务的 CloudTrail 管理事件 ..... 1011
S3 表类数据存储服务的 CloudTrail 数据事件 ..... 1012
CloudTrail 日志示例 ..... 1013
访问控制 ..... 1017
S3 资源 ..... 1017
身份 ..... 1021
存储桶拥有者或资源拥有者 ..... 1023
访问管理工具 ..... 1023
操作 ..... 1028
访问管理使用案例 ..... 1029
访问管理故障排除 ..... 1035
Identity and Access Management (IAM) ..... 1036
受众 ..... 1037
使用身份进行身份验证 ..... 1037
使用策略管理访问 ..... 1039
Amazon S3 如何与 IAM 配合使用 ..... 1041
请求授权 ..... 1065
S3 API 操作所需的权限 ..... 1073
策略和权限 ..... 1103
存储桶策略 ..... 1107
基于身份的策略 ..... 1148
使用策略的演练 ..... 1181
将服务相关角色用于 Amazon S3 Storage Lens 存储统计管理工具 ..... 1216
Amazon S3 身份和访问问题排查 ..... 1220

Amazon 托管式策略 ..... 1239
使用通用存储桶的接入点 ..... 1241
命名规则、限制和局限性 ..... 1242
引用接入点 ..... 1244
接入点兼容性 ..... 1247
配置 IAM 策略 ..... 1248
监控和日志记录 ..... 1255
创建通用存储桶的接入点 ..... 1257
管理接入点 ..... 1263
使用接入点 ..... 1267
使用 S3 Access Grants 管理访问权限 ..... 1278
S3 Access Grants 的概念 ..... 1279
S3 Access Grants 和公司目录身份 ..... 1283
开始使用 S3 Access Grants ..... 1291
使用 S3 访问权限管控实例 ..... 1292
使用 S3 访问权限管控位置 ..... 1304
在 S3 访问权限管控中处理授权 ..... 1325
使用访问授权获取 S3 数据 ..... 1337
S3 Access Grants 跨账户访问 ..... 1350
将 Amazon 标签与 S3 Access Grants 配合使用 ..... 1362
S3 Access Grants 限制 ..... 1364
S3 Access Grants 集成 ..... 1366
使用 ACL 管理访问 ..... 1368
ACL 概念 ..... 1369
配置 ACL ..... 1384
策略示例 ..... 1401
阻止公有访问 ..... 1405
屏蔽公共访问权限设置 ..... 1407
在接入点上执行屏蔽公共访问权限操作 ..... 1410
“公有”的含义 ..... 1410
使用适用于 S3 的 IAM Access Analyzer 查看公有存储桶 ..... 1413
权限 ..... 1414
配置屏蔽公共访问权限 ..... 1414
配置账户设置 ..... 1415
配置存储桶和接入点设置 ..... 1417
查看存储桶访问 ..... 1420

适用于 S3 的 IAM Access Analyzer 提供哪些信息？ ..... 1421
启用适用于 S3 的 IAM Access Analyzer ..... 1422
阻止所有公有访问 ..... 1422
查看和更改桶访问权限 ..... 1423
对存储桶结果进行归档 ..... 1425
激活已归档的存储桶结果 ..... 1425
查看结果详细信息 ..... 1425
下载适用于 S3 的 IAM Access Analyzer 报告 ..... 1426
验证存储桶所有权 ..... 1426
何时使用存储桶拥有者条件 ..... 1427
验证存储桶拥有者 ..... 1427
示例 ..... 1428
限制和局限性 ..... 1431
控制对象所有权 ..... 1431
对象所有权设置 ..... 1432
通过禁用 ACL 引起的更改 ..... 1434
禁用 ACL 的先决条件 ..... 1435
Object Ownership 权限 ..... 1435
禁用所有新存储桶的 ACL ..... 1435
复制和 Object Ownership ..... 1436
设置对象所有权 ..... 1436
禁用 ACL 的先决条件 ..... 1437
创建存储桶 ..... 1451
设置对象所有权 ..... 1459
查看 Object Ownership 设置 ..... 1462
禁用所有新存储桶的 ACL ..... 1464
故障排除 ..... 1466
安全性 ..... 1469
安全最佳实践 ..... 1471
Amazon S3 安全最佳实践 ..... 1471
Amazon S3 监控和审计最佳实践 ..... 1476
监控数据安全 ..... 1479
数据保护 ..... 1481
数据加密 ..... 1482
服务器端加密 ..... 1484
使用客户端加密 ..... 1571

互联网络流量隐私 ..... 1571
服务与本地客户端和应用之间的流量 ..... 1572
同一区域中 Amazon 资源之间的流量 ..... 1572
适用于 Amazon S3 的 Amazon PrivateLink ..... 1572
合规性验证 ..... 1588
故障恢复能力 ..... 1589
备份加密 ..... 1591
基础设施安全性 ..... 1592
配置和漏洞分析 ..... 1593
访问权限管理 ..... 1593
数据保护 ..... 1596
在区域内和跨区域复制对象 ..... 1597
为什么使用复制？ ..... 1598
何时使用跨区域复制 ..... 1599
何时使用同区域复制 ..... 1600
何时使用双向复制 ..... 1600
何时使用 S3 分批复制 ..... 1600
工作负载要求和实时复制 ..... 1601
复制了什么内容？ ..... 1602
复制的要求和注意事项 ..... 1605
设置实时复制 ..... 1608
管理或暂停实时复制 ..... 1693
复制现有对象 ..... 1694
对复制进行问题排查 ..... 1706
监控进度并获取状态 ..... 1713
管理多区域流量 ..... 1731
创建多区域接入点 ..... 1732
配置多区域接入点 ..... 1740
使用多区域接入点 ..... 1743
保留对象的多个版本 ..... 1787
不受版本控制、启用了版本控制和已暂停版本控制的存储桶 ..... 1788
将 S3 版本控制与 S3 生命周期结合使用 ..... 1789
S3 版本控制 ..... 1789
在存储桶上启用版本控制 ..... 1793
配置 MFA 删除 ..... 1798
使用启用版本控制的对象 ..... 1800

使用已暂停版本控制的对象 ..... 1828
版本控制故障排除 ..... 1832
锁定对象 ..... 1836
S3 对象锁定的工作原理 ..... 1837
对象锁定注意事项 ..... 1840
配置对象锁定 ..... 1845
备份数据 ..... 1854
成本优化 ..... 1856
账单和使用率报告 ..... 1856
使用成本分配标签 ..... 1857
账单报告 ..... 1859
使用情况报告 ..... 1861
了解账单和使用率报告 ..... 1863
Amazon S3 错误响应的账单计费 ..... 1884
了解和管理存储类 ..... 1898
经常访问的对象 ..... 1898
自动优化访问模式不断变化或未知的数据 ..... 1899
不经常访问的对象 ..... 1900
极少访问的对象 ..... 1902
Amazon S3 on Outposts ..... 1903
比较存储类 ..... 1903
设置对象的存储类 ..... 1904
存储类分析 ..... 1908
使用 Amazon S3 Intelligent-Tiering 管理存储成本 ..... 1914
Amazon S3 Glacier 存储类 ..... 1925
使用归档的对象 ..... 1930
管理生命周期 ..... 1941
管理对象的完整生命周期 ..... 1943
转换对象 ..... 1944
即将过期的对象 ..... 1951
设置生命周期配置 ..... 1953
使用其他存储桶配置 ..... 1971
配置 S3 生命周期事件通知 ..... 1973
生命周期配置元素 ..... 1975
生命周期配置冲突 ..... 1990
S3 生命周期配置的示例 ..... 1995

排查生命周期问题 ..... 2009
日志记录和监控 ..... 2015
监控工具 ..... 2018
自动化工具 ..... 2018
手动工具 ..... 2018
日志记录选项 ..... 2019
使用 Cloudtrail 进行日志记录 ..... 2021
将 CloudTrail 日志与 Amazon S3 服务器访问日志和 CloudWatch Logs 结合使用 ..... 2023
使用 Amazon S3 SOAP API 调用进行 CloudTrail 跟踪 ..... 2023
CloudTrail 事件 ..... 2024
示例日志文件 ..... 2036
启用 CloudTrail ..... 2040
识别 S3 请求 ..... 2043
记录服务器访问 ..... 2050
如何启用日志传送？ ..... 2050
日志对象密钥格式 ..... 2052
如何传输日志？ ..... 2053
最大努力服务器日志传输 ..... 2054
存储桶日志记录状态更改将逐渐生效 ..... 2054
启用服务器访问日志记录 ..... 2055
日志格式 ..... 2076
删除日志文件 ..... 2090
识别 S3 请求 ..... 2090
排查服务器访问日志记录问题 ..... 2098
使用 CloudWatch 监控指标 ..... 2100
指标与维度 ..... 2102
访问 CloudWatch 指标 ..... 2118
CloudWatch 指标配置 ..... 2119
Amazon S3 事件通知 ..... 2127
概述 ..... 2127
通知类型和目标 ..... 2129
使用 SQS、SNS 和 Lambda ..... 2135
使用 EventBridge ..... 2161
可视化存储活动和用量 ..... 2170
S3 Storage Lens 存储统计管理工具指标和功能 ..... 2171
了解 S3 Storage Lens 存储统计管理工具 ..... 2173

指标词汇表 ..... 2182
设置权限 ..... 2213
使用 S3 Storage Lens 存储统计管理工具 ..... 2216
查看存储指标 ..... 2254
使用组织 ..... 2305
使用 Storage Lens 组 ..... 2315
对数据进行编目和分析 ..... 2357
Amazon S3 清单存储桶 ..... 2358
清单列表 ..... 2358
配置 Amazon S3 清单 ..... 2363
查找清单 ..... 2371
设置清单完成通知 ..... 2375
使用 Athena 查询清单 ..... 2376
将空版本 ID 字符串转换为空字符串 ..... 2381
使用“对象 ACL”字段 ..... 2384
优化性能 ..... 2386
Amazon S3 的性能准则 ..... 2387
衡量性能 ..... 2387
水平扩展 ..... 2388
使用字节范围提取 ..... 2388
重试请求 ..... 2388
在同一区域中结合 Amazon S3 和 Amazon EC2 ..... 2389
使用 Transfer Acceleration 最大限度地减少延迟 ..... 2389
使用最新的 Amazon SDK ..... 2389
Amazon S3 的性能设计规律 ..... 2389
缓存频繁访问的内容 ..... 2390
延迟敏感型应用程序的超时和重试 ..... 2390
水平扩缩和请求并行化 ..... 2391
加快地理位置分散的数据传输速度 ..... 2392
托管静态网站 ..... 2393
网站端点 ..... 2393
网站端点示例 ..... 2395
添加 DNS 别名记录 ..... 2395
将自定义域与 Route 53 结合使用 ..... 2396
网站端点和 REST API 端点之间的主要区别 ..... 2396
启用网站托管 ..... 2397

配置索引文档 ..... 2401
索引文档和文件夹 ..... 2402
配置索引文档 ..... 2403
配置自定义错误文档 ..... 2404
Amazon S3 HTTP 响应代码 ..... 2404
配置自定义错误文档 ..... 2406
设置访问网站的权限 ..... 2407
步骤 1：编辑 S3 阻止公有访问设置 ..... 2408
步骤 2：添加存储桶策略 ..... 2409
对象访问控制列表 ..... 2411
记录 Web 流量 ..... 2412
配置重定向 ..... 2413
重新导向请求至另一个主机 ..... 2413
配置重新导向规则 ..... 2414
重新导向对于对象的请求 ..... 2421
使用 CORS ..... 2423
跨源资源共享：使用案例场景 ..... 2423
Amazon S3 如何评估针对存储桶的 CORS 配置？ ..... 2424
对象 Lambda 接入点如何支持 CORS ..... 2424
CORS 配置的元素 ..... 2424
配置 CORS ..... 2430
测试 CORS ..... 2438
CORS 问题排查 ..... 2440
静态网站教程 ..... 2445
托管视频流 ..... 2446
配置静态网站 ..... 2462
在中国托管 Amazon S3 静态网站 ..... 2470
使用自定义域配置静态网站 ..... 2475
从 Amazon S3 将静态网站部署到 Amplify ..... 2497
配额 ..... 2500
增加配额 ..... 2500
参考 ..... 2501
文档历史记录 ..... 2502
早期更新 ..... 2534

# 什么是 Amazon S3？

Amazon Simple Storage Service（Amazon S3）是一种对象存储服务，提供行业领先的可扩展性、数据可用性、安全性和性能。各种规模和行业的客户都可以使用 Amazon S3 存储和保护任意数量的数据，用于数据湖、网站、移动应用程序、备份和恢复、归档、企业应用程序、IoT 设备和大数据分析。Amazon S3 提供了管理功能，使您可以优化、组织和配置对数据的访问，以满足您的特定业务、组织和合规性要求。

> **Note**
>
> 有关将 Amazon S3 Express One Zone 存储类与目录存储桶配合使用的更多信息，请参阅S3 Express One Zone和使用目录存储桶。

主题


- Amazon S3 的功能
- Amazon S3 的工作原理
- Amazon S3 数据一致性模型
- 相关服务
- 访问 Amazon S3
- 为 Amazon S3 支付费用
- PCI DSS 合规性


# Amazon S3 的功能

## 存储类

Amazon S3 提供一系列适合不同使用案例的存储类。例如，您可以将任务关键型生产数据存储在 S3 Standard 或 S3 Express One Zone 中以便频繁访问，将不经常访问的数据存储在 S3 Standard-IA 或 S3 One Zone-IA 中，并在 S3 Glacier Instant Retrieval、S3 Glacier Flexible Retrieval、和 S3 Glacier Deep Archive 中以极低的成本归档数据。

Amazon S3 Express One Zone 是高性能的单区 Amazon S3 存储类，专门用于为延迟要求极高的应用程序提供稳定的毫秒级数据访问。S3 Express One Zone 是目前具有极低延迟的云对象存储类，相比

S3 Standard，其数据访问速度要快 10 倍，且请求成本低 50%。S3 Express One Zone 是第一种可以在其中选择单个可用区的 S3 存储类，您可以选择将您的对象存储与计算资源联合托管在一个位置，从而提供尽可能高的访问速度。此外，为了进一步提高访问速度并支持每秒数十万个请求，数据存储在新的存储桶类型中：Amazon S3 目录存储桶。有关更多信息，请参阅S3 Express One Zone和使用目录存储桶。

您可以在 S3 Intelligent-Tiering 中存储具有不断变化或未知访问模式的数据，该分层可在访问模式发生变化时自动在四个访问层之间移动数据，从而优化存储成本。这四个访问层包括两个低延迟访问层（针对频繁和不频繁访问进行了优化），以及两个为异步访问很少访问的数据而设计的 opt-in archive 访问层。

有关更多信息，请参阅 了解和管理 Amazon S3 存储类。

## 存储管理

Amazon S3 具有存储管理功能，您可以使用这些功能来管理成本、满足法规要求、减少延迟并保存数据的多个不同副本以满足合规性要求。

- S3 生命周期 - 配置生命周期配置以管理您的对象，并在整个生命周期内经济高效地存储这些对象。您可以将对象转换为其他 S3 存储类，也可以使其生命周期结束的对象过期。
- S3 对象锁定 - 可以在固定的时间段内或无限期地阻止删除或覆盖 Amazon S3 对象。可以使用对象锁定来帮助您满足需要一次写入多次读取（WORM）存储的法规要求，或只是添加另一个保护层来防止对象被更改和删除。
- S3 复制 - 将对象及其各自的元数据和对象标签复制到同一或不同的 Amazon Web Services 区域 目标存储桶中的一个或多个目标存储桶，以减少延迟、合规性、安全性和其他使用案例。
- S3 批量操作 - 通过单个 S3 API 请求或在 Amazon S3 控制台中单击几次，大规模管理数十亿个对象。您可以使用批量操作来执行诸如复制、调用 Amazon Lambda 函数和恢复数百万或数十亿对象这样的操作。

## 访问管理和安全性

Amazon S3 提供了用于审核和管理对存储桶和对象的访问的功能。默认情况下，S3 存储桶和对象都是私有的。您只能访问您创建的 S3 资源。要授予支持您特定使用案例的细粒度资源权限或审核 Amazon S3 资源的权限，您可以使用以下功能。

- S3 阻止公有访问 - 阻止对 S3 存储桶和对象的公有访问。默认情况下，“屏蔽公共访问权限”设置在存储桶级别处于开启状态。我们建议您将所有“屏蔽公共访问权限”设置保持为启用状态，除非您知道您

需要为您的特定使用案例关闭其中一个或多个设置。有关更多信息，请参阅 为 S3 存储桶配置屏蔽公共访问权限设置。

- Amazon Identity and Access Management（IAM）– IAM 是一种 Web 服务，可帮助您安全地控制对 Amazon 资源（包括 Amazon S3 资源）的访问。借助 IAM，您可以集中管理控制用户可访问哪些 Amazon 资源的权限。可以使用 IAM 来控制谁通过了身份验证（准许登录）并获得授权（具有相应权限）来使用资源。
- 存储桶策略 - 使用基于 IAM 的策略语言为 S3 存储桶及其中的对象配置基于资源的权限。
- Amazon S3 接入点 – 使用专用访问策略配置命名网络端点，以便大规模管理对 Amazon S3 中共享数据集的访问。
- 访问控制列表（ACL）- 向授权用户授予单个存储桶和对象的读写权限。作为一般规则，我们建议您使用基于 S3 资源的策略（存储桶策略和接入点策略）或 IAM 用户策略进行访问控制，而不是 ACL。策略是一种简化、更灵活的访问控制选项。借助存储桶策略和接入点策略，您可以定义广泛适用于针对 Amazon S3 资源的所有请求的规则。有关何时使用 ACL 而不是基于资源的策略或 IAM 用户策略的特定情况的更多信息，请参阅使用 ACL 管理访问。
- S3 对象所有权 – 获取存储桶中每个对象的所有权，从而简化对存储在 Amazon S3 中的数据的访问管理。S3 对象所有权是 Amazon S3 存储桶级别的设置，您可以使用该设置来禁用或启用 ACL。默认情况下，ACL 处于禁用状态。禁用 ACL 后，存储桶拥有者拥有存储桶中的所有对象，并使用访问管理策略来专门管理对数据的访问权限。
- 适用于 S3 的 IAM Access Analyzer - 评估和监控您的 S3 存储桶访问策略，确保这些策略仅提供对 S3 资源的预期访问权限。

## 数据处理

要转换数据并触发工作流以大规模自动执行各种其他处理活动，您可以使用以下功能。

- S3 Object Lambda - 您可以将自己的代码添加到 S3 GET、HEAD 和 LIST 请求中，以便在数据返回到应用程序时修改和处理数据。筛选行、动态调整图像大小、编辑机密数据等。
- 事件通知 - 当您的 S3 资源进行更改时，触发使用 Amazon Simple Notification Service (Amazon SNS)、Amazon Simple Queue Service (Amazon SQS) 和的工作流程和 Amazon Lambda。

## 存储日志记录和监控

Amazon S3 提供日志记录和监控工具，您可以使用这些工具来监控和控制 Amazon S3 资源的使用情况。更多信息，请参阅监控工具。

自动监控工具

- Amazon S3 的 Amazon CloudWatch 指标- 跟踪 S3 资源的运行状况，并在估计费用达到用户定义的阈值时配置计费警报。
- Amazon CloudTrail - 在 Amazon S3 中记录用户采取的行动、角色或 Amazon Web Services 服务。CloudTrail 日志为您提供了 S3 存储桶级别和对象级操作的详细 API 跟踪。

手动监控工具

- 服务器访问日志- 详细地记录对存储桶提出的各种请求。您可以使用服务器访问日志对许多使用案例进行安全和访问审计，了解客户群或了解您的 Amazon S3 账单。
- Amazon Trusted Advisor - 通过使用 Amazon 最佳实践检查以确定优化 Amazon 基础架构、提高安全性和性能、降低成本以及监控服务配额。然后，您可以按照建议优化服务和资源。

## 分析和见解

Amazon S3 提供的功能可帮助您了解存储使用情况，从而使您能够更好地了解、分析和大规模优化存储。

- Amazon S3 Storage Lens - 了解、分析和优化您的存储。S3 Storage Lens 存储统计管理工具提供了超过 60 个使用率和活动指标以及交互式控制面板，用于汇总整个组织、特定客户、Amazon Web Services 区域、存储桶或前缀的数据。
- 存储类分析- 分析存储访问模式，以决定何时需要将数据移动到更经济高效的存储类。
- 带清单报告的 S3 清单- 审核和报告对象及其相应的元数据，并配置其他 Amazon S3 功能，在清单报告中采取措施。例如，您可以报告对象的复制和加密状态。有关清单报告中每个对象可用的所有元数据的列表，请参阅 Amazon S3 清单。

## 强一致性

Amazon S3 为所有 Amazon Web Services 区域 中的 Amazon S3 存储桶中对象的 PUT 和 DELETE 请求提供了强大的先写后读一致性。这个行为既适用于到新对象的写入，也适用于覆盖现有对象的 PUT 和 DELETE。此外，针对 Amazon S3 Select、Amazon S3 访问控制列表 (ACL)、Amazon S3 对象标签和对象元数据（例如 HEAD 对象）的读取操作具有严格一致性。有关更多信息，请参阅 Amazon S3 数据一致性模型。

# Amazon S3 的工作原理

Amazon S3 是一种对象存储服务，可将数据作为对象、层次结构数据或表数据存储在存储桶中。对象指的是一个文件和描述该文件的任何元数据。存储桶是对象的容器。

要将数据存储在 Amazon S3 中，您需要先创建存储桶，然后指定存储桶名称和 Amazon Web Services 区域。然后，您将数据作为 Amazon S3 中的对象上传到该存储桶。每个对象都带有密钥（或键名称），它是存储桶中对象的唯一标识符。

S3 提供了一些功能，您可以配置这些功能以支持您的特定使用案例。例如，您可以使用 S3 版本控制将对象的多个版本保持在同一个存储桶中，这允许您恢复意外删除或覆盖的对象。

存储桶及其中的对象是私有的，只有在您明确授予访问权限时才可以访问。您可以使用存储桶策略、Amazon Identity and Access Management（IAM）策略、访问控制列表（ACL）和 S3 接入点管理访问。

主题

- 存储桶
- 对象
- 键
- S3 版本控制
- 版本 ID
- 存储桶策略
- S3 接入点
- 访问控制列表（ACL）
- 区域

## 存储桶

Amazon S3 支持三种类型的存储桶：通用存储桶、目录存储桶和表存储桶。每种类型的存储桶都为不同的应用场景提供了一组独特的功能。

通用存储桶：建议将通用存储桶用于大多数应用场景和访问模式，它们是最初的 S3 存储桶类型。通用存储桶是存储在 Amazon S3 中的对象的容器，您可以在存储桶中和跨所有存储类（S3 Express One Zone 除外）存储任意数量的对象，因此，您可以跨多个可用区以冗余方式存储对象。有关更多信息，请参阅创建、配置和使用 Amazon S3 通用存储桶。

> **Note**
>
> 默认情况下，所有通用存储桶都是私有的。但是，您可以授予对通用存储桶的公共访问权限。您可以在存储桶、前缀（文件夹）或对象标签级别控制对通用存储桶的访问权限。有关更多信息，请参阅 Amazon S3 中的访问控制。

目录存储桶：建议用于低延迟应用场景和数据驻留应用场景。默认情况下，在 Amazon Web Services 账户中最多可以创建 100 个目录存储桶，并且对目录存储桶中可以存储的对象数量没有限制。目录存储桶将对象组织到层次结构目录（前缀）中，而不是通用存储桶的扁平存储结构。此存储桶类型没有前缀限制，单个目录可以水平扩展。有关更多信息，请参阅使用目录存储桶。

- 对于低延迟应用场景，您可以在单个 Amazon 可用区中创建目录存储桶来存储数据。可用区中的目录存储桶支持 S3 Express One Zone 存储类。使用 S3 Express One Zone，您的数据将冗余地存储在单个可用区中的多个设备上。如果您的应用程序注重性能，并且受益于个位数毫秒的 PUT 和 GET 延迟，则建议使用 S3 Express One Zone 存储类。要了解有关在可用区中创建目录存储桶的更多信息，请参阅高性能工作负载。
- 对于数据驻留应用场景，您可以在单个 Amazon 专用本地区域（DLZ）中创建目录存储桶来存储数据。在专用本地区域中，您可以创建 S3 目录存储桶来将数据存储在特定的数据边界中，这有助于支持您的数据驻留和隔离应用场景。Local Zones 中的目录存储桶支持 S3 One Zone-Infrequent Access（S3 One Zone-IA；Z-IA）存储类。要了解有关在本地区域中创建目录存储桶的更多信息，请参阅数据驻留工作负载。

> **Note**
>
> 默认情况下，目录存储桶会禁用所有公共访问权限。此行为不可更改。您无法授予对存储在目录存储桶中的对象的访问权限。您只能授予对目录存储桶的访问权限。有关更多信息，请参阅对请求进行身份验证和授权。

表存储桶：建议用于存储表数据，例如每日购买交易、流传感器数据或广告展示次数。表数据以列和行表示数据，就像在数据库表中一样。表存储桶提供针对分析和机器学习工作负载进行优化的 S3 存储，其功能旨在持续提高查询性能并降低表的存储成本。S3 表类数据存储服务专为以 Apache Iceberg 格式存储表数据而构建。您可以使用常用的查询引擎（包括 Amazon Athena、Amazon Redshift 和 Apache Spark）在 S3 表类数据存储服务中查询表数据。默认情况下，每个 Amazon Web Services 区域、每个 Amazon Web Services 账户最多可以创建 10 个表存储桶，每个表存储桶最多可以创建 10000 个表。有关更多信息，请参阅使用 S3 表类数据存储服务和表存储桶。

> **Note**
>
> 所有表存储桶和表都是私有的，不能使之成为公有的。只有被明确授予访问权限的用户才可以访问这些资源。要授予访问权限，您可以对表存储桶和表使用基于 IAM 资源的策略，并对用户和角色使用基于 IAM 身份的策略。有关更多信息，请参阅 S3 表类数据存储服务的安全性。

### 关于所有存储桶类型的附加信息

创建存储桶时，您可以输入存储桶名称，然后选择Amazon Web Services 区域存储桶将驻留的位置。创建存储桶后，无法更改存储桶或区域的名称。存储桶名称必须遵循以下存储桶命名规则：

- 通用存储桶命名规则
- 目录存储桶命名规则
- 表存储桶命名规则

存储桶还：

- 在最高级别组织 Amazon S3 命名空间。对于通用存储桶，此命名空间为 S3。对于目录存储桶，此命名空间为 s3express。对于表存储桶，此命名空间为 s3tables。
- 标识负责存储和数据传输费用的账户。
- 用作使用情况报告的聚合单元。

## 对象

对象是 Amazon S3 中存储的基础实体。对象由对象数据和元数据组成。元数据是一组描述对象的名称-值对。这些对值包括一些默认元数据（如上次修改日期）和标准 HTTP 元数据（如 Content-Type）。您还可以在存储对象时指定自定义元数据。

每个对象都储存在一个存储桶中。例如，如果名为 photos/puppy.jpg 的对象存储在美国西部（俄勒冈州）区域的 amzn-s3-demo-bucket 通用存储桶中，则可使用 URL https://amzn-s3-demo-bucket.s3.us-west-2.amazonaws.com/photos/puppy.jpg 对该对象进行寻址。有关更多信息，请参阅访问存储桶。

存储桶中的对象由密钥（名称）和版本 ID唯一标识（如果在存储桶上启用了 S3 版本控制）。有关对象的更多信息，请参阅 Amazon S3 对象概述。

## 键

对象密钥（或密钥名称）是指存储桶中对象的唯一标识符。存储桶内的每个对象都只能有一个键。存储桶、对象密钥和可选版本 ID 的组合（如果为存储桶启用了 S3 版本控制）唯一标识每个对象。因此，您可以将 Amazon S3 看作“存储桶 + 键 + 版本”与对象本身之间的基本数据映射。

将 Web 服务端点、存储桶名称、密钥和版本（可选）组合在一起，可唯一地寻址 Amazon S3 中的每个对象。例如，在 URL `https://amzn-s3-demo-bucket.s3.us-west-2.amazonaws.com/photos/puppy.jpg` 中，*`amzn-s3-demo-bucket`* 是存储桶的名称，`photos/puppy.jpg` 是密钥。

有关对象键的更多信息，请参阅 为 Amazon S3 对象命名。

## S3 版本控制

您可以使用 S3 版本控制功能将对象的多个变量保留在同一存储桶中。使用 S3 版本控制功能，您可以保留、检索和恢复存储桶中的各个版本。您能够轻松从用户意外操作和应用程序故障中恢复数据。

有关更多信息，请参阅 使用 S3 版本控制保留对象的多个版本。

## 版本 ID

在存储桶中启用 S3 版本控制时，Amazon S3 会为添加到存储桶中的每个对象生成唯一的版本ID。启用版本控制时存在于存储桶中的对象的版本 ID 为`null`。如果使用其他操作修改这些（或任何其他）对象，例如 CopyObject 和 PutObject 时，新对象将获得唯一的版本 ID。

有关更多信息，请参阅 使用 S3 版本控制保留对象的多个版本。

## 存储桶策略

存储桶策略是基于资源的 Amazon Identity and Access Management (IAM) 策略，您可以使用该策略向存储桶及其中对象授予访问权限。只有存储桶拥有者才能将策略与存储桶关联。附加到存储桶的权限适用于存储桶拥有者拥有的存储桶中所有对象。存储桶策略的大小限制为 20 KB。

存储桶策略使用基于 JSON 的访问策略语言，该语言是跨平台的标准语言 Amazon。您可以使用存储桶策略添加或拒绝存储桶中对象的权限。存储桶策略根据策略中的元素允许或拒绝请求，包括请求者、S3 操作、资源以及请求的方面或条件（例如，用于发出请求的 IP 地址）。例如，您可以创建一个存储桶策略，该策略授予跨账户将对象上传到 S3 存储桶的权限，同时确保存储桶拥有者对上传的对象拥有完全控制权。有关更多信息，请参阅 Amazon S3 存储桶策略的示例。

在存储桶策略中，您可以在 Amazon 资源名称（ARN）和其他值上使用通配符来授予对对象子集的权限。例如，您可以控制对以通用前缀或以给定扩展名结尾的对象组的访问，例如 `.html`。

## S3 接入点

Amazon S3 接入点被命名为网络端点，其专用访问策略描述了如何使用该端点访问数据。接入点附加到通用存储桶或目录存储桶，您可以使用这些存储桶来执行 S3 对象操作（如 GetObject 和 PutObject）。接入点可简化对 Amazon S3 中的共享数据集的大规模数据访问管理。

每个接入点都有自己的接入点策略。您还可以为每个接入点配置阻止公有访问设置。为了限制 Amazon S3 数据访问提供网络，您可以将任何接入点配置为仅接受来自私有云（VPC）的请求。

有关通用存储桶的接入点的更多信息，请参阅通过接入点管理对通用存储桶中共享数据集的访问。有关目录存储桶的接入点的更多信息，请参阅通过接入点管理对目录存储桶中共享数据集的访问权限。

## 访问控制列表（ACL）

您可以使用 ACL 向已授权的用户授予对单个通用存储桶和对象的读写权限。每个通用存储桶和对象都有一个作为子资源附加到它的 ACL。ACL 定义了哪些 Amazon Web Services 账户 或组将被授予访问权限以及访问的类型。ACL 是一种访问控制机制，其早于 IAM。有关 ACL 的更多信息，请参阅 访问控制列表 (ACL) 概述。

S3 对象所有权是 Amazon S3 存储桶级别的设置，您可以使用该设置来控制上传到存储桶的对象的所有权和禁用或启用 ACL。默认情况下，对象所有权设为强制存储桶拥有者设置，并且所有 ACL 均处于禁用状态。禁用 ACL 后，存储桶拥有者拥有存储桶中的所有对象，并使用访问管理策略来专门管理对这些对象的访问权限。

Amazon S3 中的大多数现代使用案例不再需要使用 ACL。我们建议您将 ACL 保持为禁用状态，除非有需要单独控制每个对象的访问权限的特殊情况。禁用 ACL 后，您可以使用策略来控制对存储桶中所有对象的访问权限，无论是谁将对象上传到您的存储桶。有关更多信息，请参阅 为您的存储桶控制对象所有权和禁用 ACL。 。

## 区域

您可以选择一个 Amazon Web Services 区域 供 Amazon S3 存储您创建的存储桶。您可以选择一个区域，以便优化延迟、尽可能降低成本或满足法规要求。存储在 Amazon Web Services 区域 中的对象永远不会离开该区域，除非显式地将它们传输或复制到另一个区域。例如，在欧洲（爱尔兰）区域存储的对象将一直留在欧洲。

> **Note**
>
> 您只能在已为账户启用的 Amazon Web Services 区域 中访问 Amazon S3 及其功能。有关启用区域以创建和管理 Amazon 资源的更多信息，请参阅《Amazon Web Services 一般参考》中的管理 Amazon Web Services 区域。

有关 Amazon S3 区域和端点的列表，请参阅《Amazon Web Services 一般参考》中的区域和端点。

# Amazon S3 数据一致性模型

Amazon S3 为所有 Amazon Web Services 区域 中的 Amazon S3 存储桶中对象的 PUT 和 DELETE 请求提供了强大的先写后读一致性。此行为既适用于对新对象的写入，也适用于覆盖现有对象的 PUT 请求和 DELETE 请求。此外，Amazon S3 Select、Amazon S3访问控制列表 (ACL)、Amazon S3对象标记和对象元数据（例如，HEAD对象）上的读取操作非常一致。

单个键的更新是原子更新。例如，如果您从一个线程对现有密钥执行 PUT 请求，并同时从另一个线程对同一密钥执行 GET 请求，则您将获得旧数据或新数据，但绝不会获得部分或损坏的数据。

Amazon S3 通过在 Amazon 数据中心内的多个服务器之间复制数据，从而实现高可用性。如果 PUT 请求成功，则数据已安全存储。在收到成功的 PUT 响应后启动的任何读取（GET 或 LIST 请求）都将返回 PUT 请求写入的数据。以下是此行为的示例：

- 这是一个过程，它将一个新对象写入 Amazon S3，并立即列出其存储桶内的密钥。新对象显示在列表中。
- 这是一个过程，会替换一个现有的对象，并立即尝试读取此对象。Amazon S3 返回新数据。
- 这是一个过程，会删除一个现有的对象，并立即尝试读取此对象。Amazon S3 不会返回任何数据，因为对象已被删除。
- 这是一个过程，会删除一个现有的对象，并立即列出其存储桶内的键。该对象不会显示在列表中。

> **Note**
>
> - Amazon S3 不支持对并发写入器进行对象锁定。如果同时对同一键发出两个 PUT 请求，则以带有最新时间戳的请求为准。如果这会导致问题，您需要在应用程序中创建对象锁定机制。

- 更新是基于键的。无法跨键值实现原子更新。例如，无法根据一个键值的更新对另一个键值进行更新，除非将此功能设计到应用程序中。

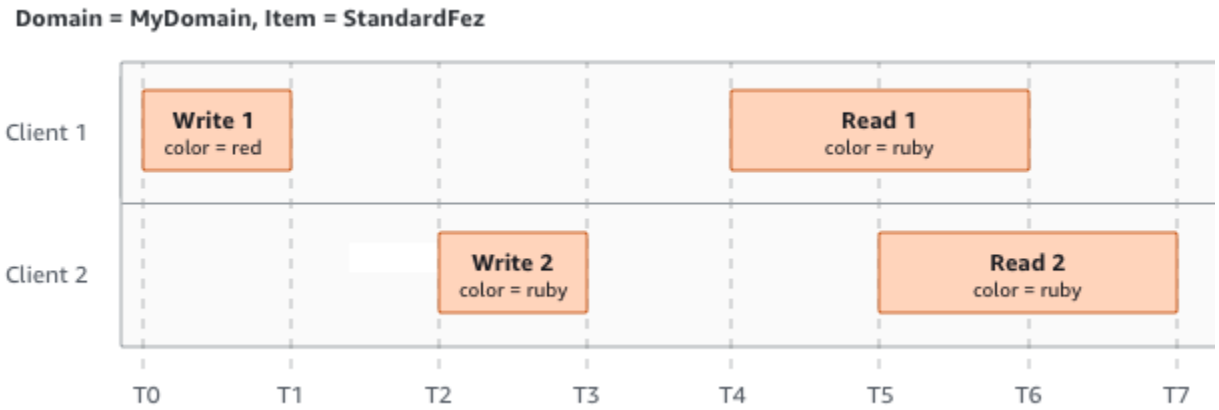
存储桶配置具有最终一致性模型。具体而言，这意味着：

- 如果您删除存储桶，然后立即列出所有存储桶，则所删除的存储桶可能仍会显示在列表中。
- 如果您首次对存储桶启用版本控制，则可能需要很短的时间即可完全传播更改。我们建议您在启用版本控制后等待 15 分钟，然后再对存储桶中的对象发出写入操作（PUT 或 DELETE 请求）。

## 并发应用程序

本部分提供了当多个客户端向同一项目写入时，Amazon S3 应采取的行为示例。

在本示例中，W1 (写入 1) 和 W2 (写入 2) 会在 R1 (读取 1) 和 R2 (读取 2) 启动之前完成。由于 S3 具有严格一致性，因此 R1 和 R2 都会返回 `color = ruby`。




在下一个示例中，W2 不会在 R1 启动之前完成。因此，R1 可能会返回 `color = ruby` 或 `color = garnet`。但是，由于 W1 和 W2 在 R2 开始之前完成，因此 R2 会返回 `color = garnet`。




在上一个示例中，W2 在 W1 收到确认之前开始。因此，这些写入被视为并发写入。Amazon S3 在内部使用 last-writer-wins 语义来确定哪个写入优先。但是，由于网络延迟等各种因素，无法预测 Amazon S3 接收请求的顺序和应用程序接收确认的顺序。例如，W2 可能由同一区域中的 Amazon EC2 实例启动，而 W1 可能由距离更远的主机启动。确定最终值的最佳方法是在确认两次写入操作后执行读取。




# 相关服务

将数据加载到 Amazon S3 中之后，您可以将数据用于其他 Amazon 服务。以下是您可能最常用使用的服务：

- Amazon Elastic Compute Cloud (Amazon EC2) – 在 Amazon Web Services 云中提供安全可扩展的计算容量。使用 Amazon EC2 可避免前期的硬件投入，因此您能够更快地开发和部署应用程序。您可以使用 Amazon EC2 启动所需数量的虚拟服务器，配置安全性和联网以及管理存储。

- Amazon EMR – 帮助企业、研究人员、数据分析师和开发人员轻松、经济实惠地处理海量数据。Amazon EMR 使用 Amazon EC2 和 Amazon S3 的 Web 规模基础设施上运行的托管 Hadoop 框架。
- AmazonSnow 系列 - 帮助那些需要在严格、非数据中心环境中以及在缺乏一致网络连接的位置运行操作的客户。您可以使用 Amazon Snow Family 设备可在本地经济高效地访问 Amazon Web Services 云 在互联网连接可能不是一个选项的地方。
- Amazon Transfer Family - 为使用安全外壳 (SSH) 文件传输协议 (SFTP)、通过 SSL (FTPS) 的文件传输协议 (FTPS) 和文件传输协议 (FTP) 直接进出 Amazon S3 或 Amazon Elastic File System (Amazon EFS) 的文件传输提供完全托管支持。

# 访问 Amazon S3

您可以通过以下任何方式使用 Amazon S3：

## Amazon Web Services Management Console

控制台是基于 Web 的用户界面，用于管理 Amazon S3 和 Amazon 资源。如果您已注册 Amazon Web Services 账户 账户，您可以通过登录 Amazon Web Services Management Console 并从 Amazon Web Services Management Console 主页中选择 S3 来访问 Amazon S3 控制台。

## Amazon Command Line Interface

可以使用 Amazon 命令行工具，在系统的命令行中发出命令来执行 Amazon （包括 S3）任务。

Amazon Command Line Interface (Amazon CLI) 针对大量 Amazon Web Services 服务 提供了相关命令。Amazon CLI 在 Windows、macOS 和 Linux 上受支持。要开始使用，请参阅 Amazon Command Line Interface 用户指南。有关 Amazon S3 命令的更多信息，请参阅 Amazon CLI 一般参考中的 s3api 和 s3control。

## Amazon SDK

Amazon 提供的 SDK（软件开发工具包）包含各种编程语言和平台（Java、Python、Ruby、.NET、iOS、Android 等）的库和示例代码。Amazon SDK 提供便捷的方式来创建对 S3 和 Amazon 的编程访问。Amazon S3 是一项 REST 服务。您可以使用 Amazon SDK 库向 Amazon S3 发送请求，该库包装了底层 Amazon S3 REST API 并简化了编程任务。例如，SDK 负责计算签名、加密签名请求、管理错误和自动重试请求等任务。有关 Amazon SDK 的信息（包括如何下载及安装），请参阅 适用于 Amazon 的工具 。

与 Amazon S3 的每一次交互都是经身份验证的或匿名的。如果您使用 Amazon SDK，库根据您提供的密钥计算用于身份验证的签名。有关如何向 Amazon S3 发出请求的更多信息，请参阅 Making requests。

## Amazon S3 REST API

Amazon S3 架构的设计与编程语言无关，使用 Amazon 支持的接口来存储和检索对象。您可以访问 S3 和 Amazon 以编程方式使用 Amazon S3 REST API。REST API 是面向 Amazon S3 的 HTTP 接口。借助 REST API，您可以使用标准的 HTTP 请求创建、提取和删除存储桶和对象。

要使用 REST API，您可以借助任何支持 HTTP 的工具包。只要对象是匿名可读的，您甚至可以使用浏览器来提取它们。

REST API 使用标准的 HTTP 标头和状态代码，以使标准的浏览器和工具包按预期工作。在某些区域中，我们向 HTTP 添加了功能 (例如，我们添加了标头来支持访问控制)。在这些情况下，我们已尽最大努力使添加的新功能与标准的 HTTP 使用样式相匹配。

如果您在应用程序中直接调用 REST API，您必须编写代码来计算签名并将它添加到请求中。有关如何向 Amazon S3 发出请求的更多信息，请参阅《Amazon S3 API 参考》中的 Making requests。

> **Note**
>
> HTTP 上的 SOAP API 支持已弃用，但是仍可在 HTTPS 上使用。SOAP 不支持较新的 Amazon S3 特征。我们建议您使用 REST API 或 Amazon SDK。

# 为 Amazon S3 支付费用

Amazon S3 定价的设计可让您不必为应用程序的存储需求制定计划。大多数存储提供商都要求您购买预定量的存储和网络传输容量。在这种情况下，如果超过此容量，就会关闭您的服务或对您收取高额的超容量费用。如果没有超过此容量，又要按全部容量支付使用费用。

Amazon S3 仅按照您的实际使用容量收费，没有任何隐性收费和超容量收费。此模型为您提供了一种可变成本服务，它可以随着您的业务增长而增长，同时为您提供 Amazon 基础架构的成本优势。有关更多信息，请参阅 Amazon S3 定价。

在注册 Amazon 时，将在 Amazon 中为您的 Amazon Web Services 账户 自动注册所有服务，包括 Amazon S3。不过，您只需为使用的服务付费。如果您是 Amazon S3 的新客户，则可以免费开始使用 Amazon S3。有关更多信息，请参阅 Amazon免费套餐。

若要查看您的账单，请转到 Amazon 账单与成本管理 控制台中的账单和成本管理控制面板。要了解关于Amazon Web Services 账户 账单的更多信息，请参阅 Amazon Billing 用户指南。如果您有关于 Amazon 账单和 Amazon Web Services 账户的问题，请联系 Amazon 支持。

# PCI DSS 合规性

Amazon S3 支持由商家或服务提供商处理、存储和传输信用卡数据，而且已经验证符合支付卡行业 (PCI) 数据安全标准 (DSS)。有关 PCI DSS 的更多信息，包括如何请求 Amazon PCI Compliance Package 的副本，请参阅 PCI DSS 第 1 级。

# Amazon S3 入门

您可以通过使用存储桶和对象来开始使用 Amazon S3。存储桶是对象的容器。对象指的是一个文件和描述该文件的任何元数据。

要在 Amazon S3 中存储对象，您需要创建存储桶，然后将该对象上传到存储桶。当对象位于存储桶时，您可以将其打开、下载并移动它。当您不再需要对象或存储桶时，可以清理您的资源。

使用 Amazon S3，您只需按实际用量付费。有关 Amazon S3 特征和定价的更多信息，请参阅 Amazon S3。如果您是 Amazon S3 的新客户，则可以免费开始使用 Amazon S3。有关更多信息，请参阅 Amazon 免费套餐。

> **Note**
>
> 有关将 Amazon S3 Express One Zone 存储类与目录存储桶配合使用的更多信息，请参阅S3 Express One Zone和使用目录存储桶。

视频：Amazon S3 入门

先决条件

开始之前，请确认您已完成设置 Amazon S3中的步骤。

## 设置 Amazon S3

在注册 Amazon 时，将在 Amazon 中为您的 Amazon Web Services 账户 自动注册所有服务，包括 Amazon S3。您只需为使用的服务付费。

使用 Amazon S3，您只需按实际用量付费。有关 Amazon S3 特征和定价的更多信息，请参阅 Amazon S3。如果您是 Amazon S3 的新客户，则可以免费开始使用 Amazon S3。有关更多信息，请参阅 Amazon 免费套餐。

要设置 Amazon S3，请使用以下部分中的步骤。

注册 Amazon 并设置 Amazon S3 时，您可以选择在 Amazon Web Services Management Console 中更改显示语言。有关更多信息，请参阅《Amazon Web Services Management Console 入门指南》中的更改 Amazon Web Services Management Console 的语言。

主题


- 注册 Amazon Web Services 账户
- 保护 IAM 用户


## 注册 Amazon Web Services 账户

如果您还没有 Amazon Web Services 账户，请完成以下步骤来创建一个。

注册 Amazon Web Services 账户

1. 打开 https://portal.aws.amazon.com/billing/signup。
2. 按照屏幕上的说明操作。

   在注册时，将接到电话，要求使用电话键盘输入一个验证码。

   当您注册 Amazon Web Services 账户 时，系统将会创建一个 Amazon Web Services 账户根用户。根用户有权访问该账户中的所有 Amazon Web Services 服务和资源。作为最佳安全实践，请为用户分配管理访问权限，并且只使用根用户来执行需要根用户访问权限的任务。

注册过程完成后，Amazon 会向您发送一封确认电子邮件。在任何时候，您都可以通过转至 https://aws.amazon.com/ 并选择我的账户来查看当前的账户活动并管理您的账户。

## 保护 IAM 用户

注册 Amazon Web Services 账户 后，启用多重身份验证（MFA）保护您的管理用户。有关说明，请参阅《IAM 用户指南》中的 为 IAM 用户启用虚拟 MFA 设备（控制台）。

要授予其他用户访问您的 Amazon Web Services 账户资源的权限，请创建 IAM 用户。为了保护您的 IAM 用户，请启用 MFA 并仅向 IAM 用户授予执行任务所需的权限。

有关创建和保护 IAM 用户的更多信息，请参阅《IAM 用户指南》中的以下主题：

- 在您的 Amazon Web Services 账户中创建 IAM 用户
- 适用于 Amazon 资源的访问权限管理
- 基于 IAM 身份的策略示例

# 步骤 1：创建您的第一个 S3 存储桶

注册 Amazon 后，您即可使用 Amazon Web Services Management Console 在 Amazon S3 中创建存储桶了。Amazon S3 中的每个对象都存储在存储桶中。必须先创建一个存储桶，然后才能在 Amazon S3 中存储数据。

> **Note**
>
> 有关将 Amazon S3 Express One Zone 存储类与目录存储桶配合使用的更多信息，请参阅S3 Express One Zone和使用目录存储桶。

> **Note**
>
> 您无需为创建存储桶付费。只有将对象存储到存储桶中以及从存储桶传入和传出对象才需要付费。仿照本指南中的示例操作产生的费用非常少（不到 1 USD）。有关存储费用的更多信息，请参阅 Amazon S3 定价。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在页面顶部的导航栏中，选择当前所显示 Amazon Web Services 区域的名称。接下来，选择要在其中创建存储桶的区域。

   > **Note**
   >
   > - 存储桶创建后，便无法再更改其区域。
   > - 要最大程度地减少延迟和成本以及满足法规要求，请选择一个靠近您的区域。在某一区域存储的对象将一直留在该区域，除非您特意将其转移到其他区域。有关 Amazon S3 Amazon Web Services 区域的列表，请参阅《Amazon Web Services 一般参考》中的 Amazon Web Services 服务 端点。
3. 在左侧导航窗格中，选择通用存储桶。
4. 选择创建存储桶。此时将打开创建存储桶页面。
5. 对于存储桶名称，请输入存储桶的名称。

   存储桶名称必须满足以下要求：

- 在分区中是唯一的。分区是区域的分组。Amazon 目前有三个分区：aws（商用区域）、aws-cn（中国区域）和 aws-us-gov（Amazon GovCloud (US) Regions）。
- 长度必须介于 3 到 63 个字符之间。
- 只能由小写字母、数字、句点 (.) 和连字符 (-) 组成。为了获得最佳兼容性，我们建议您避免在存储桶名称中使用句点 (.)，但仅用于静态网站托管的存储桶除外。
- 以字母或数字开头和结尾。
- 有关存储桶命名规则的完整列表，请参阅通用存储桶命名规则。

> **Important**
>
> - 创建存储桶后，便无法更改其名称。
> - 请勿在存储桶名称中包含敏感信息。存储桶名称会显示在指向存储桶中的对象的 URL 中。

6. （可选）在常规配置下，您可以选择将现有存储桶的设置复制到新存储桶。如果您不想复制现有存储桶的设置，请跳到下一步。

> **Note**
>
> 此选项：
>
> - 在 Amazon CLI 中不可用，仅在 Amazon S3 控制台中可用
> - 不会将存储桶策略从现有存储桶复制到新存储桶

要复制现有存储桶的设置，请在从现有存储桶复制设置下，选择选择存储桶。将打开选择存储桶窗口。找到包含您要复制的设置的存储桶，然后选择选择存储桶。选择存储桶窗口关闭，而创建存储桶窗口重新打开。

在从现有存储桶复制设置下，您现在将看到您选择的存储桶的名称。新存储桶的设置现在与您选择的存储桶的设置相匹配。如果要移除复制的设置，请选择恢复默认设置。在创建存储桶页面上查看其余的存储桶设置。如果您不想进行任何更改，可以跳到最后一步。

7. 在 Object Ownership（对象所有权）下方，要禁用或启用 ACL，并控制上传到存储桶中的对象的所有权，请选择以下设置之一：

已禁用 ACL

- 强制存储桶拥有者（默认）：ACL 已禁用，存储桶拥有者自动拥有并完全控制通用存储桶中的每个对象。ACL 不再影响对 S3 通用存储桶中数据的访问权限。存储桶专门使用策略来定义访问控制。

  默认情况下，ACL 处于禁用状态。Amazon S3 中的大多数现代使用案例不再需要使用 ACL。我们建议您将 ACL 保持为禁用状态，除非有必须单独控制每个对象的访问权限的特殊情况。有关更多信息，请参阅 为您的存储桶控制对象所有权和禁用 ACL。。

已启用 ACL

- Bucket owner preferred（首选存储桶拥有者）— 存储桶拥有者拥有并完全控制其他账户使用 `bucket-owner-full-control` 标准 ACL 写入存储桶的新对象。

  如果应用首选存储桶拥有者设置，以要求所有 Amazon S3 上传都包含 `bucket-owner-full-control` 标准 ACL，则可以添加存储桶策略，该策略只允许使用此 ACL 上传对象。
- 对象编写者— 该 Amazon Web Services 账户上传对象拥有该对象，对其拥有完全控制权，并且可以通过 ACL 授予其他用户访问该对象的权限。

> **Note**
>
> 默认设置为强制存储桶拥有者。要应用默认设置并将 ACL 保持为禁用状态，只需要 `s3:CreateBucket` 权限。要启用 ACL，您必须具有 `s3:PutBucketOwnershipControls` 权限。

8. 在此存储桶的屏蔽公共访问权限设置中，请选择要应用于存储桶的屏蔽公共访问权限设置。

默认情况下，启用所有四个“屏蔽公共访问权限”设置。我们建议您将所有设置保持为启用状态，除非您知道您需要为您的特定使用案例关闭其中一个或多个设置。有关屏蔽公共访问权限的更多信息，请参阅阻止对您的 Amazon S3 存储的公有访问。

> **Note**
>
> 要启用所有“屏蔽公共访问权限”设置，只需要 `s3:CreateBucket` 权限。要关闭任何“屏蔽公共访问权限”设置，您必须拥有 `s3:PutBucketPublicAccessBlock` 权限。

9. （可选）默认情况下，存储桶版本控制处于禁用状态。版本控制是在相同的存储桶中保留对象的多个变量的方法。对于 存储桶中存储的每个对象，您可以使用版本控制功能来保留、检索和还原它们的各个版本。使用版本控制能够更加轻松地从用户意外操作和应用程序故障中恢复数据。有关版本控制的更多信息，请参阅使用 S3 版本控制保留对象的多个版本。

   要在存储桶上启用版本控制，请选择启用。

10. （可选）在 Tags（标签）下，您可以选择向存储桶添加标签。利用 Amazon 成本分配功能，可以使用存储桶标签来对存储桶的使用计费添加注释。一个标签即为一个键值对，用于表示用户分配给存储桶的标记。有关更多信息，请参阅 the section called “使用成本分配标签”。

    要添加存储桶标签，请输入 Key（键），并（可选）输入 Value（值），然后选择 Add Tag（添加标签）。

11. 要配置默认加密，请在加密类型下，选择以下选项之一：

    - 具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）
    - 具有 Amazon Key Management Service 密钥的服务器端加密（SSE-KMS）
    - 具有 Amazon Key Management Service（Amazon KMS）密钥的双层服务器端加密（DSSE-KMS）

    > **Important**
    >
    > 如果您将 SSE-KMS 或 DSSE-KMS 选项用于默认加密配置，则您将受到 Amazon KMS 的每秒请求数（RPS）配额限制。有关 Amazon KMS 限额以及如何请求增加限额的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的限额。

    通过将具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）用作基本加密配置级别，对存储桶和新对象进行加密。有关默认加密的更多信息，请参阅为 Amazon S3 存储桶设置默认服务器端加密行为。有关 SSE-S3 的更多信息，请参阅使用具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）。

    有关使用服务器端加密对数据进行加密的更多信息，请参阅the section called “数据加密”。

12. 如果您选择具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）或具有 Amazon Key Management Service（Amazon KMS）密钥的双层服务器端加密（DSSE-KMS），请执行以下操作：

    a. 在 Amazon KMS 密钥下，通过以下方式之一指定您的 KMS 密钥：

- 要从可用的 KMS 密钥列表中进行选择，请选择从您的 Amazon KMS keys 密钥中进行选择，并从可用密钥的列表中选择您的 KMS 密钥。

  Amazon 托管式密钥 (aws/s3) 和您的客户自主管理型密钥都显示在此列表中。有关客户自主管理型密钥的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的客户密钥和 Amazon 密钥。
- 要输入 KMS 密钥 ARN，请选择输入 Amazon KMS key ARN，然后在显示的字段中输入您的 KMS 密钥 ARN。
- 要在 Amazon KMS 控制台中创建新的客户自主管理型密钥，请选择创建 KMS 密钥。

  有关创建 Amazon KMS key 的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的创建密钥。

> **Important**
>
> 您只能使用与存储桶所在相同的 Amazon Web Services 区域中可用的 KMS 密钥。Amazon S3 控制台仅列出与存储桶位于同一区域中的前 100 个 KMS 密钥。要使用未列出的 KMS 密钥，您必须输入 KMS 密钥 ARN。如果您希望使用由其它账户拥有的 KMS 密钥，则必须首先有权使用该密钥，然后必须输入相应的 KMS 密钥 ARN。有关 KMS 密钥的跨账户权限的更多信息，请参阅《Amazon Key Management Service Developer Guide》中的 Creating KMS keys that other accounts can use。有关 SSE-KMS 的更多信息，请参阅 使用 Amazon KMS (SSE-KMS) 指定服务器端加密。有关 DSSE-KMS 的更多信息，请参阅the section called “双层服务器端加密（DSSE-KMS）”。
>
> 在 Amazon S3 中使用 Amazon KMS key 进行服务器端加密时，您必须选择对称加密 KMS 密钥。Amazon S3 仅支持对称加密 KMS 密钥，而不支持非对称 KMS 密钥。有关更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的确定对称和非对称 KMS 密钥。

b. 将存储桶配置为使用 SSE-KMS 进行默认加密时，还可以使用 S3 存储桶密钥。S3 存储桶密钥可通过减少从 Amazon S3 到 Amazon KMS 的请求流量，降低加密成本。有关更多信息，请参阅 使用 Amazon S3 存储桶密钥降低 SSE-KMS 的成本。DSSE-KMS 不支持 S3 存储桶密钥。

默认情况下，S3 存储桶密钥在 Amazon S3 控制台中处于启用状态。我们建议将 S3 存储桶密钥保留为启用状态以降低成本。要为存储桶禁用 S3 存储桶密钥，请在存储桶密钥下选择禁用。

13. （可选）S3 对象锁定有助于保护新对象不被删除或覆盖。有关更多信息，请参阅 使用对象锁定以锁定对象。如果要启用 S3 对象锁定，请执行以下操作：

    a. 选择高级设置。

    > **Important**
    >
    > 启用对象锁定会自动为存储桶启用版本控制。启用并成功创建存储桶后，还必须在存储桶的属性选项卡上配置对象锁定默认保留设置和法定保留设置。

    b. 如果要启用对象锁定，请选择 Enable（启用），阅读出现的警告，并予以确认。

    > **Note**
    >
    > 要创建启用了对象锁定的存储桶，您必须具有以下权限：`s3:CreateBucket`、`s3:PutBucketVersioning` 和 `s3:PutBucketObjectLockConfiguration`。

14. 选择创建存储桶。

您已在 Amazon S3 中完成存储桶创建。

下一步

要将对象添加到您的存储桶，请参阅步骤 2：将对象上传到存储桶。

## 步骤 2：将对象上传到存储桶

在 Amazon S3 中创建存储桶后，您就可以将对象上传到存储桶了。对象可以是任何类型的文件：文本文件、图片、视频等等。

> **Note**
>
> 有关将 Amazon S3 Express One Zone 存储类与目录存储桶配合使用的更多信息，请参阅 S3 Express One Zone 和 使用目录存储桶。

将对象上传到存储桶

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets (存储桶) 列表中，选择要将对象上传到的存储桶的名称。
3. 在存储桶的对象选项卡上，选择上传。
4. 在文件和文件夹下，选择添加文件。
5. 选择要上传的文件，然后选择打开。
6. 选择上传。

您已成功将对象上传到存储桶。

后续步骤

要查看您的对象，请参阅 步骤 3：下载对象。

# 步骤 3：下载对象

当您将对象上传到存储桶后，您可以查看有关对象的信息并将对象下载到本地计算机上。

> **Note**
>
> 有关将 Amazon S3 Express One Zone 存储类与目录存储桶配合使用的更多信息，请参阅 S3 Express One Zone 和 使用目录存储桶。

## 使用 S3 控制台

本部分介绍如何使用 Amazon S3 控制台从 S3 存储桶下载对象。

> **Note**
>
> - 一次只能下载一个对象。

- 如果您使用 Amazon S3 控制台下载对象的键名以句点 (.) 结尾，则该句点将从下载对象的键名中删除。要保留所下载对象名称末尾的句点，您必须使用 Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 Amazon S3 REST API。

从 S3 存储桶下载对象

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶或目录存储桶。
3. 在存储桶列表中，选择要从中下载对象的存储桶的名称。
4. 您可以使用以下任一方式从 S3 存储桶下载对象：
   - 选中对象旁边的复选框，然后选择下载。如果您要将对象下载到特定文件夹，请在操作菜单中，选择下载为。
   - 如果要下载对象的特定版本，请打开显示版本（位于搜索框旁边）。选中所需对象版本旁边的复选框，然后选择下载。如果您要将对象下载到特定文件夹，请在操作菜单中，选择下载为。

您已成功下载您的对象。

下一步

要在 Amazon S3 中复制并粘贴对象，请参阅步骤 4：将对象复制到文件夹。

## 步骤 4：将对象复制到文件夹

您已向存储桶添加一个对象并已下载该对象。现在，您可以创建一个文件夹，复制对象并将其粘贴到此文件夹中。

> **Note**
>
> 有关将 Amazon S3 Express One Zone 存储类与目录存储桶配合使用的更多信息，请参阅S3 Express One Zone和使用目录存储桶。

将对象复制到文件夹中

1. 在存储桶列表中，选择您的存储桶名称。
2. 选择创建文件夹并配置新文件夹：
   a. 输入文件夹名称（例如，`favorite-pics`）。
   b. 对于文件夹加密设置，选择禁用。
   c. 选择保存。
3. 导航到包含待复制对象的 Amazon S3 存储桶或文件夹。
4. 选中要复制的对象名称左侧的复选框。
5. 选择操作，然后从显示的选项列表中选择复制。

   或者，从右上角的选项中选择复制。
6. 选择目标文件夹：
   a. 选择浏览 S3。
   b. 选择文件夹名称左侧的选项按钮。

      要导航到文件夹并选择子文件夹作为目标，请选择文件夹名称。
   c. 选择选择目标。

   目标文件夹的路径显示在目标框中。在目标中，您可以依次输入目标路径，例如 s3://*bucket-name*/*folder-name*/。
7. 在右下角，选择复制。

   Amazon S3 会将对象复制到目标文件夹。

后续步骤

要删除 Amazon S3 中的对象和存储桶，请参阅步骤 5：删除对象和存储桶。

# 步骤 5：删除对象和存储桶

当您不再需要对象或存储桶时，我们建议您删除它们以防止发生进一步的费用。如果您将此入门演练作为练习完成，并且不打算使用您的存储桶或对象，我们建议您删除存储桶和对象，从而不再产生费用。

在删除存储桶之前，请清空存储桶或删除存储桶中的对象。删除对象和存储桶后，它们将不再可用。

如果要继续使用相同的存储桶名称，我们建议您删除对象或清空存储桶，但不要删除存储桶。删除存储桶后，该名称可供重复使用。但是，在您有机会重复使用此名称之前，其他 Amazon Web Services 账户可能会创建具有相同名称的存储桶。

> **Note**
>
> 有关将 Amazon S3 Express One Zone 存储类与目录存储桶配合使用的更多信息，请参阅S3 Express One Zone和使用目录存储桶。

主题


- 删除对象
- 清空存储桶
- 删除存储桶


## 删除对象

如果您希望选择要删除的对象而不清空存储桶中的所有对象，则可以删除单个对象。

1. 在存储桶列表中，选择要从中删除对象的存储桶的名称。
2. 选择您要删除的对象。
3. 从右上角的选项中选择删除。
4. 在删除对象页面上，键入 **`delete`** 以确认删除您的对象。
5. 选择删除对象。

## 清空存储桶

如果您计划删除存储桶，则必须首先清空存储桶，这会删除存储桶中的所有对象。

清空存储桶

1. 在存储桶列表中，选择要清空的存储桶，然后选择清空。
2. 要确认您要清空存储桶并删除其中的所有对象，请在 Empty bucket（清空存储桶）中，键入 **`permanently delete`**。

> **Important**
>
> 无法撤消清空存储桶操作。当正在执行清空存储桶操作时添加到存储桶的对象将被删除。

3. 要清空存储桶并删除其中的所有对象，并选择 Empty（清空）。

   Empty bucket: Status（清空存储桶：状态）页面打开，您可以使用该页面来查看失败和成功的对象删除操作的摘要。

4. 要返回到存储桶列表，请选择退出。

## 删除存储桶

清空存储桶或从存储桶中删除所有对象后，您可以删除存储桶。

1. 要删除存储桶，请在存储桶列表中选择该存储桶。
2. 选择删除。
3. 要确认删除，请在 Delete bucket（删除存储桶）中，键入存储桶的名称。

> **Important**
>
> 无法撤消删除存储桶的操作。存储桶名称是唯一的。如果您删除存储桶，则其他 Amazon 用户可以使用该名称。如果您希望继续使用相同的存储桶名称，请不要删除该存储桶。相反，清空并保留存储桶。

4. 要删除您的存储桶，请选择删除存储桶。

# 后续步骤

在前面的示例中，您了解了如何执行一些基本的 Amazon S3 任务。

下列主题介绍了各种可促使您深入了解 Amazon S3，进而在应用程序中实施服务的方式。

> **Note**
>
> 有关将 Amazon S3 Express One Zone 存储类与目录存储桶配合使用的更多信息，请参阅S3 Express One Zone和使用目录存储桶。

主题


- 了解常见使用案例
- 控制对存储桶和对象的访问
- 保护和监控存储
- 用 Amazon S3 进行开发
- 从教程中学习
- 探索培训和支持


## 了解常见使用案例

您可以使用 Amazon S3 支持您的具体使用案例。Amazon 解决方案库和 Amazon 博客提供了具体使用案例的信息和教程。以下是 Amazon S3 的一些常见使用案例：

- Backup and storage（备份和存储）- 使用 Amazon S3 存储管理功能来管理成本、满足法规要求、减少延迟并保存多个不同的数据拷贝以满足合规性要求。
- 应用程序托管 - 部署、安装和管理可靠、高度可扩展和低成本的 Web 应用程序。例如，可以配置您的 Amazon S3 存储桶来承载一个静态网站。有关更多信息，请参阅 使用 Amazon S3 托管静态网站。
- 媒体托管 - 构建托管视频、照片或音乐上载和下载的高可用性基础设施。
- 软件传输 - 托管可供客户下载的软件应用程序。

## 控制对存储桶和对象的访问

Amazon S3 提供了各种安全功能和工具。有关概述，请参阅Amazon S3 中的访问控制。

默认情况下，S3 存储桶和对象都是私有的。您只能访问您创建的 S3 资源。您可以使用以下功能授予支持具体使用案例的细粒度资源权限，或审核您的 Amazon S3 资源的权限。

- S3 阻止公有访问 - 阻止对 S3 存储桶和对象的公有访问。默认情况下，“屏蔽公共访问权限”设置在存储桶级别处于开启状态。
- Amazon Identity and Access Management（IAM）身份 – 使用 IAM 或 Amazon IAM Identity Center 在 Amazon Web Services 账户 中创建 IAM 身份，以管理对 Amazon S3 资源的访问。例如，您可以将 IAM 用于 Amazon S3，以控制用户或用户组对您的 Amazon Web Services 账户拥有 Amazon S3 存储桶的访问类型。有关 IAM 身份和最佳实践的更多信息，请参阅《IAM 用户指南》中的 IAM 身份（用户、用户组和角色）。

- 桶策略 - 使用基于 IAM 的策略语言为 S3 桶及其中的对象配置基于资源的权限。
- 访问控制列表（ACL）- 向授权用户授予单个存储桶和对象的读写权限。作为一般规则，我们建议您使用基于 S3 资源的策略（存储桶策略和接入点策略）或 IAM 用户策略进行访问控制，而不是 ACL。策略是一种简化、更灵活的访问控制选项。借助存储桶策略和接入点策略，您可以定义广泛适用于针对 Amazon S3 资源的所有请求的规则。有关何时使用 ACL 而不是基于资源的策略或 IAM 用户策略的特定情况的更多信息，请参阅Amazon S3 的身份和访问管理。
- S3 对象所有权 – 获取存储桶中每个对象的所有权，从而简化对存储在 Amazon S3 中的数据的访问管理。S3 对象所有权是 Amazon S3 存储桶级别的设置，您可以使用该设置来禁用或启用 ACL。默认情况下，ACL 处于禁用状态。禁用 ACL 后，存储桶拥有者拥有存储桶中的所有对象，并使用访问管理策略来专门管理对数据的访问权限。
- 适用于 S3 的 IAM Access Analyzer - 评估和监控您的 S3 存储桶访问策略，确保这些策略仅提供对 S3 资源的预期访问权限。

## 保护和监控存储

- 保护存储 - 在 Amazon S3 中创建存储桶和上传对象后，可以保护对象存储。例如，可以使用 S3 版本控制、S3 复制和多区域接入点失效转移控制来进行灾难恢复，使用 Amazon Backup 来备份数据，使用 S3 对象锁定来设置保留期，防止删除和覆盖，并满足合规性要求。
- 监控存储 - 监控是保持 Amazon S3 和您的 Amazon 解决方案的可靠性、可用性和性能的重要方面。您可以监控存储活动和成本。我们推荐您从 Amazon 解决方案的所有方面收集监控数据，更轻松地调试出现的多点故障。

  还可以使用 Amazon S3 中的分析和见解来了解、分析和优化存储使用情况。例如，使用 Amazon S3 Storage Lens 存储统计管理工具 了解、分析和优化存储。S3 Storage Lens 存储统计管理工具提供了超过 29 个使用和活动指标以及交互式仪表板，聚合整个组织、特定账户、区域、存储桶或前缀的数据。使用存储类分析来分析存储访问模式，决定何时需要将数据移动到更经济高效的存储类。要管理成本，可以使用 S3 生命周期。

## 用 Amazon S3 进行开发

Amazon S3 是一项 REST 服务。您可以使用 REST API 或 Amazon SDK 库（打包了底层 Amazon S3 REST API 以简化编程任务），向 Amazon S3 发送请求。您也可以使用 Amazon Command Line Interface (Amazon CLI) 调用Amazon S3 API。有关更多信息，请参阅《Amazon S3 API 参考》中的 Making requests。

Amazon S3 REST API 是面向 Amazon S3 的 HTTP 接口。借助 REST API，您可以使用标准的 HTTP 请求创建、提取和删除存储桶和对象。要使用 REST API，您可以借助任何支持 HTTP 的工具包。只要对象是匿名可读的，您甚至可以使用浏览器来提取它们。有关更多信息，请参阅《Amazon S3 API 参考》中的 Developing with Amazon S3。

我们提供以下资源来帮助您使用所选的语言创建应用程序：

Amazon CLI

您可以使用 Amazon CLI 访问 Amazon S3 功能。要下载和配置 Amazon CLI，请参阅《Amazon S3 API 参考》中的 Developing with Amazon S3 using the Amazon CLI。

Amazon CLI 提供两个层级的命令来访问 Amazon S3：高级别（s3）命令和 API 级别（s3api 和 `s3control`）命令。高级 S3 命令构成简化了常见任务的执行，如创建、操作和删除对象及存储桶。s3api 和 s3control 命令提供对所有 Amazon S3 API 操作的直接访问，您可以使用它们执行单凭高级别命令无法完成的高级操作。

有关 Amazon S3 的列表 Amazon CLI 命令，请参见 s3、s3api 和 s3control。

Amazon SDK 和 Explorer

使用 Amazon S3 开发应用程序时，您可以使用 Amazon SDK。Amazon SDK 包装了底层 REST API，可以简化您的编程任务。还提供 Amazon Mobile SDK 和 Amplify JavaScript 库，用于使用 Amazon 构建互连移动和 Web 应用程序。

除了 Amazon SDK 外，Amazon Explorer 也适用于 Visual Studio 和 Eclipse for Java IDE。在此情况下，可以将 SDK 和 Explorer 捆绑在一起作为 Amazon 工具包。

有关更多信息，请参阅《Amazon S3 API 参考》中的 Developing with Amazon S3 using the Amazon SDKs。

示例代码和库

Amazon 开发人员中心和 Amazon 示例代码目录会特别针对 Amazon S3 编写示例代码和库。您可以运用这些代码示例了解 Amazon S3 API 的实施。您也可以查看 Amazon 简单存储服务 API 参考，了解 Amazon S3 API 操作的详细信息。

## 从教程中学习

开始使用分步教程，了解有关 Amazon S3 的更多信息。这些教程适用于实验室类型环境，使用了虚构的公司名称、用户名称等。其目的在于提供一般性指导。在未进行仔细审核并进行改进以满足组织环境的独特需求的情况下，这些过程不适合在您的生产环境中直接使用。

## 入门

- 教程：使用 Amazon S3 存储和检索文件
- 教程：开始使用 S3 Intelligent-Tiering
- 教程：开始使用 Amazon S3 Glacier 存储类

## 优化存储成本

- 教程：开始使用 S3 Intelligent-Tiering
- 教程：开始使用 Amazon S3 Glacier 存储类
- 教程：使用 S3 Storage Lens 存储统计管理工具优化成本和了解使用情况

## 管理存储

- 教程：Amazon S3 多区域接入点入门
- 教程：使用 S3 批量复制来复制 Amazon S3 存储桶中的现有对象

## 托管视频和网站

- 教程：使用 Amazon S3、Amazon CloudFront 和 Amazon Route 53 托管点播流视频
- 教程：在 Amazon S3 上配置静态网站
- 教程：使用注册到 Route 53 的自定义域配置静态网站

## 处理数据

- 教程：使用 S3 对象 Lambda 转换应用程序的数据
- 教程：使用 S3 对象 Lambda 和 Amazon Comprehend 检测和修订 PII 数据
- 教程：使用 S3 对象 Lambda 在检索图像时对其动态加水印
- 教程：使用 S3 批量操作对视频进行批量转码

## 保护数据

- 教程：使用额外的校验和检查 Amazon S3 中数据的完整性
- 教程：使用 S3 复制在 Amazon Web Services 区域内和区域之间复制数据

- 教程：使用 S3 版本控制、S3 对象锁定和 S3 复制保护 Amazon S3 上的数据免遭意外删除或应用程序错误
- 教程：使用 S3 批量复制来复制 Amazon S3 存储桶中的现有对象

## 探索培训和支持

您可以向 Amazon 专家学习，提高您的技能并获得专家协助，实现您的目标。

- 培训 - 培训资源提供了学习 Amazon S3 的实践方法。有关更多信息，请参阅 Amazon 培训和认证和 Amazon 线上技术讲座。
- 论坛 - 您可以在论坛中查看帖子，了解使用 Amazon S3 的优势和局限。您也可以发布问题。有关更多信息，请参阅论坛。
- 技术支持 - 如果有其他问题，请联系技术支持。

# 创建、配置和使用 Amazon S3 通用存储桶

要将数据存储在 Amazon S3 中，您需要使用称为存储桶和对象的资源。存储桶是对象的容器。对象指的是一个文件和描述该文件的任何元数据。

要将对象存储在 Amazon S3 中，您需要创建存储桶，然后将该对象上传到存储桶。当对象位于存储桶时，您可以将其打开、下载并移动它。当您不再需要对象或存储桶时，可以清理您的资源。

本节中的主题概述了在 Amazon S3 中使用通用存储桶。它们包括有关命名、创建、访问和删除通用存储桶的信息。有关查看或列出存储桶中对象的更多信息，请参阅 组织、列出和处理对象。

Amazon S3 存储桶有几种类型。在创建存储桶之前，请确保选择最适合应用程序和性能要求的存储桶类型。有关各种存储桶类型以及每种类型的相应用例的更多信息，请参阅存储桶。

> **Note**
>
> 有关将 Amazon S3 Express One Zone 存储类与目录存储桶配合使用的更多信息，请参阅 S3 Express One Zone 和使用目录存储桶。

> **Note**
>
> 使用 Amazon S3，您只需按实际用量付费。有关 Amazon S3 特征和定价的更多信息，请参阅 Amazon S3。如果您是 Amazon S3 的新客户，则可以免费开始使用 Amazon S3。有关更多信息，请参阅 Amazon 免费套餐。

主题


- 通用存储桶概述
- 在 Amazon S3 上构建应用程序的常见通用存储桶模式
- 通用存储桶命名规则
- 通用存储桶配额、限制和局限性
- 访问 Amazon S3 通用存储桶
- 创建通用存储桶
- 查看 S3 通用存储桶的属性
- 列出 Amazon S3 通用存储桶

- 清空通用存储桶
- 删除通用存储桶
- 使用适用于 Amazon S3 的 Mountpoint
- 使用适用于 Amazon S3 的存储浏览器
- 使用 Amazon S3 Transfer Acceleration 配置快速、安全的文件传输
- 使用申请方付款通用存储桶进行存储传输和使用

# 通用存储桶概述

要向 Amazon S3 上传数据（照片、视频、文档等），您必须首先在其中一个 Amazon Web Services 区域 中创建 S3 存储桶。

Amazon S3 存储桶有几种类型。在创建存储桶之前，请确保选择最适合应用程序和性能要求的存储桶类型。有关各种存储桶类型以及每种类型的相应用例的更多信息，请参阅存储桶。

以下各节提供了有关通用存储桶的更多信息，包括存储桶命名规则、配额和存储桶配置详细信息。有关与 Amazon S3 存储桶相关的限制和局限性的列表，请参阅通用存储桶配额、限制和局限性。

主题

- 通用存储桶概述
- 常见通用存储桶模式
- 权限
- 管理对通用存储桶的公共访问权限
- 通用存储桶配置选项
- 通用存储桶操作
- 通用存储桶性能监控

## 通用存储桶概述

每个对象都储存在一个存储桶中。例如，如果名为 `photos/puppy.jpg` 的对象存储在美国西部（俄勒冈州）区域的 `amzn-s3-demo-bucket` 通用存储桶中，则可使用 URL `https://amzn-s3-demo-bucket.s3.us-west-2.amazonaws.com/photos/puppy.jpg` 对该对象进行寻址。有关更多信息，请参阅访问存储桶。

- 只能从美国东部（弗吉尼亚州北部）查看和管理商业区域的通用存储桶配额。

- 只能从中国（北京）区域查看和管理中国区域的通用存储桶配额。
- 只能从 Amazon GovCloud（美国西部）查看和管理 Amazon GovCloud (US) 的通用存储桶配额。

对于实施，存储桶和对象是 Amazon 资源，而 Amazon S3 提供 API 供您管理资源。例如，您可以使用 Amazon S3 API 创建存储桶并上传对象。您还可以使用 Amazon S3 控制台执行这些操作。该控制台使用 Amazon S3 API 将请求发送到 Amazon S3。

本节介绍如何使用通用存储桶。有关使用对象的信息，请参阅 Amazon S3 对象概述。

Amazon S3 支持全局通用存储桶，这意味着每个存储桶名称在分区内的所有 Amazon Web Services 区域、所有 Amazon Web Services 账户中都必须是唯一的。分区是一组区域。Amazon 目前有三个分区：`aws`（标准区域）、`aws-cn`（中国区域）和 `aws-us-gov`（Amazon GovCloud (US)）。

在创建通用存储桶之后，该存储桶的名称不能被同一分区中的另一个 Amazon Web Services 账户使用，直到删除该存储桶。不应依赖特定的存储桶命名约定来实现可用性或安全验证。有关存储桶命名指南，请参阅通用存储桶命名规则。

Amazon S3 在指定的区域中创建存储桶。为减少延迟、最大限度地降低成本或满足法规要求，请选择地理上靠近您的任何 Amazon Web Services 区域。例如，如果您位于欧洲，您可能会发现在欧洲（爱尔兰）或欧洲（法兰克福）区域创建存储桶十分有利。有关 Amazon S3 区域的列表，请参阅《Amazon 一般参考》中的区域和终端节点。

> **Note**
>
> 属于您在特定 Amazon Web Services 区域 中创建的存储桶的对象永远不会离开该区域，除非您明确将其传输到另一个区域。例如，在欧洲（爱尔兰）区域存储的对象将一直留在该区域。

## 常见通用存储桶模式

在 Amazon S3 上构建应用程序时，您可以使用唯一的通用存储桶来分隔不同的数据集或工作负载。根据您的应用场景，使用通用存储桶有不同的设计模式和最佳实践。有关更多信息，请参阅 在 Amazon S3 上构建应用程序的常见通用存储桶模式。

## 权限

可以使用Amazon Web Services 账户根用户凭证来创建通用存储桶并执行任何其它 Amazon S3 操作。但是，我们建议您不要使用 Amazon Web Services 账户 的根用户凭证发出请求，例如创建存储

桶。而是创建一个 Amazon Identity and Access Management (IAM) 用户，并向该用户授予完全访问权限 (用户在默认情况下没有任何权限)。

这些用户称为管理员。您可以使用管理员用户凭证而不是您账户的根用户凭证来与 Amazon 交互和执行任务，例如创建存储桶，创建用户和授予他们权限。

有关更多信息，请参阅《Amazon 一般参考》中的 Amazon Web Services 账户根用户 凭证和 IAM 用户凭证以及《IAM 用户指南》中的 IAM 中的安全最佳实践。

创建资源的 Amazon Web Services 账户 拥有该资源。例如，如果您在 Amazon Web Services 账户 中创建一个 IAM 用户并向该用户授予创建存储桶的权限，则该用户可以创建存储桶。但该用户不拥有存储桶；该存储桶属于用户所属的 Amazon Web Services 账户 所有。用户需要资源拥有者提供其他权限来执行任何其他存储桶操作。有关为您的 Amazon S3 资源管理权限的更多信息，请参阅Amazon S3 的身份和访问管理。

## 管理对通用存储桶的公共访问权限

通过存储桶策略和/或访问控制列表（ACL）授予对通用存储桶和对象的公共访问权限。为了帮助您管理对 Amazon S3 资源的公有访问，Amazon S3 提供屏蔽公共访问权限的设置。Amazon S3 屏蔽公共访问权限设置可以覆盖 ACL 和存储桶策略，以便您可以对这些资源的公有访问实施统一限制。您可以将屏蔽公共访问权限设置应用于您的账户中的单个存储桶或所有存储桶。

为确保所有 Amazon S3 通用存储桶和对象都屏蔽了公共访问权限，在创建新的存储桶时，默认情况下会启用“屏蔽公共访问权限”的所有四个设置。我们建议也为您的账户启用“屏蔽公共访问权限”的所有四个设置。这些设置阻止所有当前和将来的存储桶的所有公有访问。

在应用这些设置之前，请确认您的应用程序在没有公有访问的情况下能够正常工作。如果您需要对存储桶或对象进行某种级别的公共访问，例如，要按照使用 Amazon S3 托管静态网站中所述托管静态网站，则可以自定义各个设置以符合您的存储使用案例要求。有关更多信息，请参阅 阻止对您的 Amazon S3 存储的公有访问。

但是，我们建议将“屏蔽公共访问权限”保留为启用状态。如果要将所有四个“屏蔽公共访问权限”设置保持为启用状态并托管静态网站，则可以使用 Amazon CloudFront 来源访问控制（OAC）。Amazon CloudFront 提供了设置安全静态网站所需的功能。Amazon S3 静态网站仅支持 HTTP 端点。Amazon CloudFront 使用 Amazon S3 的持久存储，同时提供额外的安全标头，如 HTTPS。HTTPS 通过加密正常 HTTP 请求并防范常见的网络攻击来增强安全性。

有关更多信息，请参阅《Amazon CloudFront 开发人员指南》中的安全静态网站入门。

> **Note**
>
> 如果您在列出通用存储桶及其公有访问权限设置时看到 `Error`，则您可能不具备所需的权限。确保您已将以下权限添加到您的用户或角色策略：
>
> ```
> s3:GetAccountPublicAccessBlock
> s3:GetBucketPublicAccessBlock
> s3:GetBucketPolicyStatus
> s3:GetBucketLocation
> s3:GetBucketAcl
> s3:ListAccessPoints
> s3:ListAllMyBuckets
> ```
>
> 在极少数情况下，请求也可能因 Amazon Web Services 区域中断而失败。

## 通用存储桶配置选项

Amazon S3 支持各种供您用于配置通用存储桶的选项。例如，您可以配置存储桶用于网站托管、添加配置以管理存储桶中对象的生命周期以及配置存储桶以记录对存储桶的所有访问。Amazon S3 支持供您存储和管理存储桶配置信息的子资源。您可以使用 Amazon S3 API 创建和管理这些子资源。但是，还可以使用控制台或 Amazon SDK。

> **Note**
>
> 还有对象级配置。例如，可以通过特定于该对象的配置访问控制列表 (ACL) 来配置对象级权限。

这些称为子资源，因为它们存在于特定存储桶或对象的上下文中。下表列出使您可以管理特定于存储桶的配置的子资源。

| 子资源 | 描述 |
| --- | --- |
| cors（跨源资源共享） | 您可以配置存储桶以便允许跨源请求。<br><br>有关更多信息，请参阅 使用跨源资源共享 (CORS)。 |
| 事件通知 | 您可以使存储桶向您发送特定存储桶事件的通知。 |

| 子资源 | 描述 |
| --- | --- |
| | 有关更多信息，请参阅 Amazon S3 事件通知。 |
| 生命周期 | 您可以为存储桶中明确定义了生命周期的对象定义生命周期规则。例如，您可以定义一个规则以在创建一年之后存档对象，或在创建 10 年之后删除对象。<br><br>有关更多信息，请参阅 管理对象的生命周期。 |
| 位置 | 创建存储桶时，请指定需要 Amazon S3 在其中创建存储桶的 Amazon Web Services 区域。Amazon S3 将此信息存储在位置子资源中并提供 API 用于检索此信息。 |
| 日志记录 | 日志记录使您可以跟踪针对存储桶的访问请求。每个访问日志记录都提供有关单个访问请求的详细信息，如请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果有）。访问日志信息可能在安全和访问审核方面十分有用。它还可以帮助您了解您的客户群并了解您的 Amazon S3 账单。<br><br>有关更多信息，请参阅 使用服务器访问日志记录来记录请求。 |
| 对象锁定 | 要使用 S3 对象锁定，您必须为存储桶启用它。您还可以选择配置将应用于存储桶中放置的新对象的默认保留模式和保留期限。<br><br>有关更多信息，请参阅 使用对象锁定以锁定对象。 |
| 策略 和 ACL（访问控制列表） | 所有资源（如存储桶和对象）在默认情况下为私有。Amazon S3 支持存储桶策略和访问控制列表（ACL）选项，供您用于授予和管理存储桶级权限。Amazon S3 将权限信息存储在策略 和 acl 子资源中。<br><br>有关更多信息，请参阅 Amazon S3 的身份和访问管理。 |
| 复制 | 复制是在相同或跨不同 Amazon Web Services 区域 中的存储桶自动、异步地复制对象。有关更多信息，请参阅 在区域内和跨区域复制对象。 |
| requestPayment | 默认情况下，创建存储桶的 Amazon Web Services 账户（存储桶拥有者）支付从存储桶进行的下载。存储桶拥有者可以使用此子资源指定对请求下载的人员收取下载费用。Amazon S3 提供了一个 API，用于管理此子资源。<br><br>有关更多信息，请参阅 使用申请方付款通用存储桶进行存储传输和使用。 |

| 子资源 | 描述 |
| --- | --- |
| 标记 | 您可以向存储桶添加成本分配标签以便对 Amazon 成本进行分类和跟踪。Amazon S3 提供标记 子资源以对存储桶上的标签进行存储和管理。通过使用应用于您存储桶的标签，Amazon 可生成成本分配报告，其中按标签汇总了使用情况和成本。<br><br>有关更多信息，请参阅 Amazon S3 的账单和使用情况报告。 |
| 传输加速 | Transfer Acceleration 可在您的客户端与 S3 存储桶之间实现快速、轻松、安全的远距离文件传输。Transfer Acceleration 利用 Amazon CloudFront 中的全球分布式边缘站点。<br><br>有关更多信息，请参阅 使用 Amazon S3 Transfer Acceleration 配置快速、安全的文件传输。 |
| 版本控制 | 版本控制可帮助恢复意外覆盖和删除。<br><br>我们建议将版本控制作为从错误删除或覆盖恢复对象的最佳实践。<br><br>有关更多信息，请参阅 使用 S3 版本控制保留对象的多个版本。 |
| 网站 | 您可以配置存储桶以便用于静态网站托管。Amazon S3 通过创建网站 子资源来存储此配置。<br><br>有关更多信息，请参阅 使用 Amazon S3 托管静态网站。 |

## 通用存储桶操作

Amazon S3 的高可用性设计主要关注获取、放置、列出和删除操作。由于通用存储桶操作针对集中的全球资源空间进行，因此我们建议不要在应用程序的高可用性代码路径上创建、删除或配置存储桶。最好是在单独的初始化或设置不常运行的例程时创建、删除或配置存储桶。

## 通用存储桶性能监控

当您的关键应用程序和业务流程依赖于 Amazon 资源时，监控系统并获取其警报非常重要。监控数据有助于维护 Amazon S3 和 Amazon 解决方案的可靠性、可用性和性能。可以使用多项 Amazon 服务来收集和汇总 S3 存储桶的指标和日志。

根据您的用例，您可以选择最适合贵组织需求的 Amazon 服务，来调试问题、监控数据、优化存储成本或解决多点问题。例如：

- 提高使用 S3 的应用程序的性能：设置 CloudWatch 警报以监控存储数据、复制指标或请求指标。
- 要规划存储空间使用、优化存储成本或了解整个组织中有多少存储空间：使用 Amazon S3 Storage Lens 存储统计管理工具。或者，您可以通过启用高级指标并使用详细的状态代码指标来获取成功或失败请求的计数，使用 S3 Storage Lens 存储统计管理工具提高数据性能。
- 要统一查看运营状况：将 S3 Storage Lens 存储统计管理工具使用情况和活动指标发布到 Amazon CloudWatch 控制面板。

> **Note**
>
> Amazon CloudWatch 发布选项可用于升级到高级指标和建议的 S3 Storage Lens 存储统计管理工具。您可以在 S3 Storage Lens 存储统计管理工具中为新的或现有的仪表板配置启用 CloudWatch 发布选项。

- 要获取用户、角色或 Amazon 服务所执行操作的记录：设置 Amazon CloudTrail logs。还可以使用 Amazon CloudTrail 日志将 Amazon S3 的 API 调用作为事件进行查看。
- 要接收有关 S3 存储桶中何时发生特定事件的通知：设置 Amazon S3 事件通知。
- 要获取向 S3 存储桶发出的请求的详细记录：设置 S3 访问日志。

有关可用于监控数据的所有不同 Amazon 服务的列表，请参阅 Amazon S3 中的日志记录和监控。

# 在 Amazon S3 上构建应用程序的常见通用存储桶模式

在 Amazon S3 上构建应用程序时，您可以使用唯一的通用存储桶来分隔不同的数据集或工作负载。当您构建为最终用户或不同用户组服务的应用程序时，请使用我们的最佳实践设计模式来构建能够充分利用 Amazon S3 功能和可扩展性的应用程序。

> **Important**
>
> 我们建议您创建不可预测的通用存储桶名称。除非您已经创建了存储桶，否则不要编写假定您所选存储桶名称可用的代码。创建不可预测的存储桶名称的一种方法是，在您的存储桶名称后附加一个全局唯一标识符（GUID），例如 `amzn-s3-demo-bucket-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`。有关通用存储桶命名规则的更多信息，请参阅通用存储桶命名规则。

主题


- 多租户通用存储桶模式
- 按用途划分的存储桶模式


## 多租户通用存储桶模式

使用多租户存储桶，您可以为团队或工作负载创建单个通用存储桶。您可以使用唯一的 S3 前缀来组织存储在存储桶中的对象。前缀是对象键名称开头的一串字符串。前缀可以是任意长度，取决于对象键名称的最大长度（1024 个字节）。您可以把前缀视为一种以类似于目录的方式组织数据的方式。但是，前缀不是目录。

例如，要存储关于城市的信息，您可以按大陆、按国家/区域，然后按省份或州来进行组织。因为这些名称通常不包含标点符号，您可以使用斜杠 (/) 作为分隔符。以下示例展示了如何使用斜杠（/）作为分隔符，通过大陆、国家/地区，然后是省份或州来组织城市名称的前缀。

- Europe/France/NouvelleA-Aquitaine/Bordeaux
- North America/Canada/Quebec/Montreal
- North America/USA/Washington/Bellevue
- North America/USA/Washington/Seattle

当通用存储桶内有数百个唯一的数据集时，这种模式可以很好地扩展。使用前缀，您可以轻松地对这些数据集进行组织和分组。

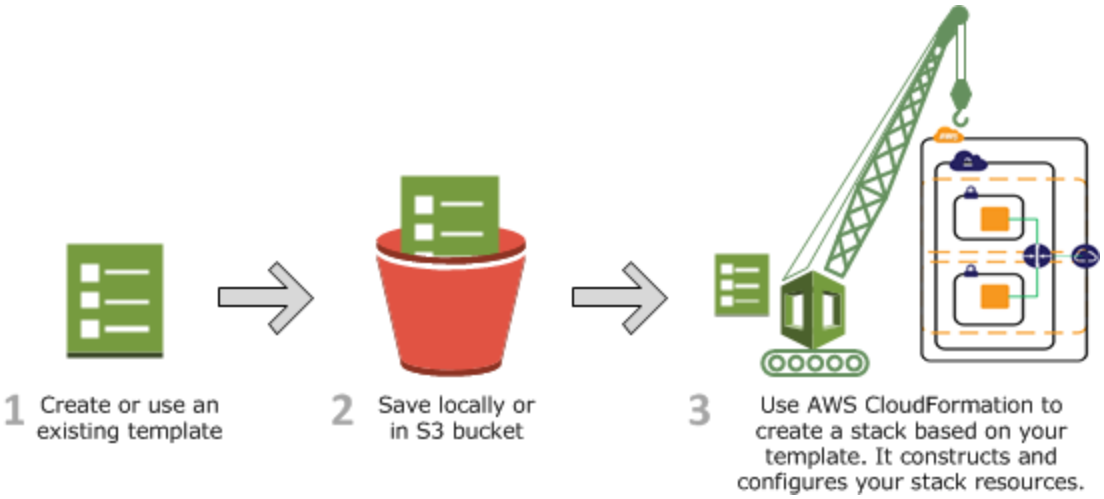
但是，多租户通用存储桶模式的一个潜在缺点是，许多 S3 存储桶级别的功能（例如默认存储桶加密、S3 版本控制和 S3 申请方付款）是在存储桶级别而不是在前缀级别设置的。如果多租户存储桶中的不同数据集具有独特的要求，而您无法在前缀级别配置许多 S3 存储桶级别功能，那么您可能很难为每个数据集指定正确的设置。此外，在多租户存储桶中，当您试图了解与特定前缀相关的存储、请求和数据传输时，成本分配可能会变得复杂。

## 按用途划分的存储桶模式

使用按用途划分的存储桶模式，您可以为每个不同的数据集、最终用户或团队创建一个通用存储桶。由于您可以为每个存储桶配置 S3 存储桶级别的功能，因此您可以使用此模式来配置唯一的存储桶级别设置。例如，您可以按照针对每个存储桶中的数据集自定义的方式，来配置默认存储桶加密、S3 版本控制和 S3 申请方付款等功能。为每个不同的数据集、最终用户或团队使用一个存储桶，还有助于简化访问管理和成本分配策略。

这种策略的一个潜在缺点是，您可能需要管理数千个存储桶。所有 Amazon Web Services 账户的默认配额均为 10000 个通用存储桶。可以通过提交增加配额请求来增加账户的存储桶配额。要请求提高通用存储桶的配额，请访问服务配额控制台。

要管理您的按用途划分的存储桶模式，并简化您的基础设施管理，可以使用 Amazon CloudFormation。您可以为您的模式创建自定义 Amazon CloudFormation 模板，该模板已经定义了 S3 通用存储桶所需的所有设置，以便您可以轻松部署和跟踪对基础设施的任何更改。有关更多信息，请参阅《Amazon CloudFormation User Guide》中的 AWS::S3::Bucket。




# 通用存储桶命名规则

创建通用存储桶时，请务必考虑存储桶名称的长度、有效字符、格式和唯一性。以下各节提供有关通用存储桶命名的信息，包括命名规则、最佳实践，以及创建名称包含全局唯一标识符（GUID）的通用存储桶的示例。

有关对象键名称的信息，请参阅创建对象键名称。

要创建通用存储桶，请参阅the section called “创建通用存储桶”。

主题


- 通用存储桶命名规则
- 通用存储桶名称示例
- 最佳实践
- 创建在存储桶名称中使用 GUID 的存储桶

# 通用存储桶命名规则

以下命名规则适用于通用存储桶。

- 存储桶名称必须介于 3（最少）到 63（最多）个字符之间。
- 存储桶名称只能由小写字母、数字、句点 (.) 和连字符 (-) 组成。
- 存储桶名称必须以字母或数字开头和结尾。
- 存储桶名称不得包含两个相邻的句点。
- 存储桶名称不得采用 IP 地址格式（例如 `192.168.5.4`）。
- 存储桶名称不得以前缀 `xn--` 开头。
- 存储桶名称不得以前缀 `sthree-` 开头。
- 存储桶名称不得以前缀 `amzn-s3-demo-` 开头。
- 存储桶名称不得以后缀 `-s3alias` 结尾。此后缀是为接入点别名预留的。有关更多信息，请参阅 通用存储桶的接入点别名。
- 存储桶名称不得以后缀 `--ol-s3` 结尾。此后缀是为对象 Lambda 接入点别名预留的。有关更多信息，请参阅 如何为您的 S3 存储桶对象 Lambda 接入点使用存储桶式别名。
- 存储桶名称不得以后缀 `.mrap` 结尾。此后缀预留用于多区域接入点名称。有关更多信息，请参阅 命名 Amazon S3 多区域接入点的规则。
- 存储桶名称不得以后缀 `--x-s3` 结尾。此后缀预留用于目录存储桶。有关更多信息，请参阅 目录存储桶命名规则。
- 存储桶名称不得以后缀 `--table-s3` 结尾。此后缀预留用于 S3 表类数据存储服务存储桶。有关更多信息，请参阅 Amazon S3 表存储桶、表和命名空间命名规则。
- 与 Amazon S3 Transfer Acceleration 一起使用的存储桶在其名称中不能有句点 (.)。有关 Transfer Acceleration 的更多信息，请参阅使用 Amazon S3 Transfer Acceleration 配置快速、安全的文件传输。

> **Important**
>
> - 存储桶名称在分区内所有 Amazon Web Services 区域中的所有 Amazon Web Services 账户间必须是唯一的。分区是区域的分组。Amazon 目前有三个分区：`aws`（商用区域）、`aws-cn`（中国区域）和 `aws-us-gov`（Amazon GovCloud (US) 区域）。
> - 存储桶名称不能被同一分区中的另一个 Amazon Web Services 账户使用，直到存储桶被删除。删除存储桶后，请注意，同一分区中的另一个 Amazon Web Services 账户可以使用相

同的存储桶名称来表示新存储桶，因此可能会收到针对已删除存储桶的请求。如果需要防止出现这种情况，或者如果您希望继续使用相同的存储桶名称，请不要删除该存储桶。我们建议您清空并保留存储桶，同时根据需要阻止任何存储桶请求。对于不再活跃使用的存储桶，我们建议清空存储桶中的所有对象，以最大限度地降低成本，同时保留存储桶本身。

- 创建通用存储桶时，您可以选择存储桶名称和要在其中创建存储桶的 Amazon Web Services 区域。在创建通用存储桶后，将无法再更改其名称或区域。
- 请勿在存储桶名称中包含敏感信息。存储桶名称会显示在指向存储桶中的对象的 URL 中。

> **Note**
>
> 2018 年 3 月 1 日之前，在美国东部（弗吉尼亚北部）区域中创建的存储桶的名称最多可包含 255 个字符，并且包括大写字母和下划线。自 2018 年 3 月 1 日起，美国东部（弗吉尼亚北部）中的新存储桶必须符合在所有其他区域中应用的相同规则。

## 通用存储桶名称示例

以下存储桶名称显示了在通用存储桶名称中支持使用哪些字符的示例：a-z、0-9 和连字符 (-)。此处使用 `amzn-s3-demo-` 保留前缀仅用于说明目的。由于它是保留前缀，因此您无法创建以 `amzn-s3-demo-` 开头的存储桶名称。

- `amzn-s3-demo-bucket1-a1b2c3d4-5678-90ab-cdef-example11111`
- `amzn-s3-demo-bucket`

以下示例存储桶名称是有效的，但不推荐用于除静态网站托管以外的其它用途，因为它们包含句点 (.)：

- `example.com`
- `www.example.com`
- `my.example.s3.bucket`

以下示例存储桶名称无效：

- `amzn_s3_demo_bucket`（包含下划线）
- `AmznS3DemoBucket`（包含大写字母）

- amzn-s3-demo-bucket-（以 amzn-s3-demo- 前缀开头，并以连字符结尾）
- example..com（连续包含两个句点）
- 192.168.5.4（与 IP 地址的格式相匹配）

## 最佳实践

命名通用存储桶时，请考虑以下存储桶命名最佳实践。

选择不可能导致命名冲突的存储桶命名方案

如果应用程序自动创建了存储桶，请选择不可能导致命名冲突的存储桶命名方案。确保存储桶名称已被使用时，您的应用程序逻辑会选择其他存储桶名称。

将全局唯一标识符（GUID）附加到存储桶名称

我们建议您创建不可预测的存储桶名称。除非您已经创建了存储桶，否则不要编写假定您所选存储桶名称可用的代码。创建不可预测的存储桶名称的一种方法是，在存储桶名称后附加一个全局唯一标识符（GUID），例如 amzn-s3-demo-bucket-a1b2c3d4-5678-90ab-cdef-example11111。有关更多信息，请参阅 the section called “创建在存储桶名称中使用 GUID 的存储桶”。

避免在存储桶名称中使用句点 (.)

为了获得最佳兼容性，我们建议您避免在存储桶名称中使用句点 (.)，但仅用于静态网站托管的存储桶除外。如果您在存储桶名称中包含句点，则无法通过 HTTPS 使用虚拟托管类型寻址，除非您执行自己的证书验证。用于存储桶虚拟托管的安全证书不适用于其名称中带有句点的存储桶。

此限制不会影响用于静态网站托管的存储桶，因为静态网站托管只能通过 HTTP 提供。有关虚拟主机式寻址的更多信息，请参阅通用存储桶的虚拟托管。有关静态网站托管的更多信息，请参阅使用 Amazon S3 托管静态网站。

选择一个相关的名称

为存储桶命名时，我们建议您选择与您或您的业务相关的名称。避免使用与其他人关联的名称。例如，避免在存储桶名称中使用 AWS 或 Amazon。

不要为了重新使用存储桶名称而删除存储桶

如果存储桶为空，您可以将其删除。删除存储桶后，该名称可供重复使用。但是，不能保证您能够立即重新使用该名称或完全可以重新使用该名称。删除存储桶后，可能需要一段时间才能重新使用该名

称。此外，在您重新使用此名称之前，其它 Amazon Web Services 账户可能会创建具有相同名称的存储桶。

删除通用存储桶后，请注意，同一分区中的另一个 Amazon Web Services 账户可以使用相同的存储桶名称来表示新存储桶，因此可能会收到针对已删除通用存储桶的请求。如果需要防止出现这种情况，或者如果您希望继续使用相同的通用存储桶名称，请不要删除该通用存储桶。我们建议您清空并保留存储桶，同时根据需要阻止任何存储桶请求。

## 创建在存储桶名称中使用 GUID 的存储桶

以下示例向您展示了如何创建在存储桶名称末尾使用 GUID 的通用存储桶。

使用 Amazon CLI

以下 Amazon CLI 示例在美国西部（北加利福尼亚）区域 (us-west-1) 中创建一个通用存储桶，示例存储桶名称使用了全局唯一标识符（GUID）。要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3api create-bucket \
    --bucket amzn-s3-demo-bucket1$(uuidgen | tr -d - | tr '[:upper:]' '[:lower:]' ) \
    --region us-west-1 \
    --create-bucket-configuration LocationConstraint=us-west-1
```

使用适用于 Java 的 Amazon SDK

以下示例向您展示了如何使用适用于 Java 的 Amazon SDK，在美国东部（弗吉尼亚州北部）区域 (us-east-1) 中创建在存储桶名称末尾使用 GUID 的存储桶。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。有关其他 Amazon SDK 的信息，请参阅在 Amazon 上构建的工具。

```
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.Bucket;
import com.amazonaws.services.s3.model.CreateBucketRequest;

import java.util.List;
import java.util.UUID;

public class CreateBucketWithUUID {
    public static void main(String[] args) {
```

```
        final AmazonS3 s3 =
 AmazonS3ClientBuilder.standard().withRegion(Regions.US_EAST_1).build();
        String bucketName = "amzn-s3-demo-bucket" +
 UUID.randomUUID().toString().replace("-", "");
        CreateBucketRequest createRequest = new CreateBucketRequest(bucketName);
        System.out.println(bucketName);
        s3.createBucket(createRequest);
    }
}
```

# 通用存储桶配额、限制和局限性

Amazon S3 通用存储桶归创建它的 Amazon Web Services 账户所有。存储桶所有权不可转移到其他账户。

## 存储桶配额

默认情况下，每个 Amazon Web Services 账户可以创建多达 10000 个通用存储桶。要请求增加通用存储桶的配额，请访问服务配额控制台。

**Important**

我们强烈建议仅使用分页 `ListBuckets` 请求。只有设置为默认通用存储桶配额 10000 的 Amazon Web Services 账户，才支持未分页的 `ListBuckets` 请求。如果您批准的通用存储桶配额超过 10000，则必须发送分页 `ListBuckets` 请求以列出您账户的存储桶。对于通用存储桶配额大于 10000 的 Amazon Web Services 账户，所有未分页的 `ListBuckets` 请求都将遭拒绝。

**Note**

必须使用以下 Amazon Web Services 区域来查看 Amazon Web Services 账户中的配额、存储桶利用率或者请求增加通用存储桶。

- 只能从美国东部（弗吉尼亚州北部）查看和管理商业区域的通用存储桶配额。
- 只能从中国（北京）区域查看和管理中国区域的通用存储桶配额。
- 只能从 Amazon GovCloud（美国西部）查看和管理 Amazon GovCloud (US) 的通用存储桶配额。

有关服务配额的信息，请参阅《Amazon Web Services 一般参考》中的 Amazon service quotas。

## 对象和存储桶限制

没有最大存储桶大小，对存储桶中可存储的项目数也没有限制。您可以在单个存储桶中存储所有对象，也可以在多个存储桶中组织它们。但是，您无法从其他存储桶中创建存储桶。

## 存储桶命名规则

创建存储桶时，您可以选择存储桶名称和要在其中创建存储桶的 Amazon Web Services 区域。创建存储桶后，便无法再更改其名称或区域。有关存储桶命名的更多信息，请参阅 通用存储桶命名规则。

# 访问 Amazon S3 通用存储桶

您可以使用 Amazon S3 控制台、Amazon Command Line Interface、Amazon SDK 或 Amazon S3 REST API 访问 Amazon S3 通用存储桶。访问 S3 通用存储桶的每种方法都支持特定的应用场景。有关更多信息，请参阅以下部分。

主题

- 使用案例
- Amazon S3 控制台
- Amazon CLI
- Amazon SDK
- Amazon S3 REST API

## 使用案例

根据您的 Amazon S3 通用存储桶的应用场景，建议使用不同方法来访问存储桶中的底层数据。以下列表包括访问数据的常见应用场景。

- 静态网站 – 您可以使用 Amazon S3 托管静态网站。在此应用场景中，您可以配置 S3 通用存储桶，使其功能与网站相似。要了解有关在 Amazon S3 上托管网站的步骤的示例，请参阅教程：在 Amazon S3 上配置静态网站。

  要托管启用了“屏蔽公共访问权限”等安全设置的静态网站，建议使用带来源访问控制（OAC）的 Amazon CloudFront，并实施其它安全标头，例如 HTTPS。有关更多信息，请参阅安全静态网站入门。

> **Note**
>
> Amazon S3 针对静态网站访问支持虚拟托管类型和路径类型 URL。由于可以使用路径类型和虚拟托管类型 URL 访问存储桶，因此，建议您使用符合 DNS 标准的存储桶名称创建存储桶。有关更多信息，请参阅 通用存储桶配额、限制和局限性。

- 共享数据集：在 Amazon S3 上扩展时，通常会采用多租户模式，即在共享通用存储桶中为不同的最终客户或业务部门分配唯一前缀。通过使用 Amazon S3 接入点，您可以将一个大型存储桶策略划分为每个需要访问共享数据集的应用程序的独立接入点策略。这种方法可以更轻松地专注于为一个应用程序构建正确的访问策略，而不中断任何其它应用程序在共享数据集中的操作。有关更多信息，请参阅 通过接入点管理对通用存储桶中共享数据集的访问。
- 高吞吐量工作负载：适用于 Amazon S3 的 Mountpoint 是一款高吞吐量开源文件客户端，用于将 Amazon S3 通用存储桶作为本地文件系统进行挂载。借助 Mountpoint，您的应用程序可以通过文件系统操作（例如打开和读取）访问存储在 Amazon S3 中的对象。Mountpoint 会自动将这些操作转换为 S3 对象 API 调用，让您的应用程序能够通过文件接口访问 Amazon S3 的弹性存储和吞吐量。有关更多信息，请参阅 使用适用于 Amazon S3 的 Mountpoint。
- 多区域应用程序：Amazon S3 多区域接入点提供了一个全局端点，应用程序可以使用该端点来满足来自位于多个 Amazon Web Services 区域中的 S3 通用存储桶的请求。您可以使用多区域接入点通过单个区域中使用的相同架构构建多区域应用程序，然后在世界任何地方运行这些应用程序。多区域接入点不是通过公共互联网发送请求，而是提供内置的网络韧性，加速向 Amazon S3 发送基于互联网的请求。有关更多信息，请参阅 使用多区域接入点管理多区域流量。
- Secure Shell（SSH）文件传输协议（SFTP）：如果您尝试通过互联网安全地传输敏感数据，则可以将支持 SFTP 的服务器与 Amazon S3 通用存储桶结合使用。Amazon SFTP 是一种网络协议，支持 SSH 的完全安全和身份验证功能。使用此协议，您可以对用户身份、权限和密钥进行精细控制，也可以使用 IAM 策略来管理访问权限。要将支持 SFTP 的服务器与您的 Amazon S3 存储桶相关联，请务必先创建支持 SFTP 的服务器。然后设置用户账户，并将服务器与 Amazon S3 通用存储桶关联。有关此过程的介绍，请参阅 Amazon 博客中的 Amazon Transfer for SFTP – Fully Managed SFTP Service for Amazon S3。

## Amazon S3 控制台

控制台是基于 Web 的用户界面，用于管理 Amazon S3 和 Amazon 资源。使用 Amazon S3 控制台，您可以轻松访问存储桶并修改存储桶属性。您还可以使用控制台 UI 执行大多数存储桶操作，而不必编写任何代码。

如果您已注册 Amazon Web Services 账户，您可以通过登录 Amazon S3 控制台并从 Amazon S3 控制台主页中选择 S3 来访问 Amazon S3 控制台。您也可以使用此链接直接访问 https://console.aws.amazon.com/s3/。

## Amazon CLI

可以使用 Amazon CLI，在系统的命令行中发出命令或构建脚本来执行 Amazon（包括 S3）任务。例如，如果您需要访问多个存储桶，则可以使用 Amazon CLI 自动执行常见任务和重复任务，从而节省时间。随着组织的扩大，常见操作的可脚本化和可重复性是经常考虑的因素。

Amazon CLI 针对大量 Amazon Web Services 服务 提供了相关命令。Amazon CLI 在 Windows、macOS 和 Linux 上受支持。要开始使用，请参阅 Amazon Command Line Interface 用户指南。有关 Amazon S3 命令的更多信息，请参阅 Amazon CLI 一般参考中的 s3api 和 s3control。

## Amazon SDK

Amazon 提供的 SDK（软件开发工具包）包含各种编程语言和平台（Java、Python、Ruby、.NET、iOS、Android 等）的库和示例代码。Amazon SDK 提供便捷的方式来创建对 S3 和 Amazon 的编程访问。Amazon S3 是一项 REST 服务。您可以使用 Amazon SDK 库向 Amazon S3 发送请求，该库包装了底层 Amazon S3 REST API 并简化了编程任务。例如，SDK 负责计算签名、加密签名请求、管理错误和自动重试请求等任务。有关 Amazon SDK 的信息（包括如何下载及安装），请参阅 适用于 Amazon 的工具 。

与 Amazon S3 的每一次交互都是经身份验证的或匿名的。如果您使用 Amazon SDK，库根据您提供的密钥计算用于身份验证的签名。有关如何向 Amazon S3 发出请求的更多信息，请参阅 Making requests。

## Amazon S3 REST API

Amazon S3 架构的设计与编程语言无关，使用 Amazon 支持的接口来存储和检索对象。您可以访问 S3 和 Amazon 以编程方式使用 Amazon S3 REST API。REST API 是面向 Amazon S3 的 HTTP 接口。借助 REST API，您可以使用标准的 HTTP 请求创建、提取和删除存储桶和对象。

要使用 REST API，您可以借助任何支持 HTTP 的工具包。只要对象是匿名可读的，您甚至可以使用浏览器来提取它们。

REST API 使用标准的 HTTP 标头和状态代码，以使标准的浏览器和工具包按预期工作。在某些区域中，我们向 HTTP 添加了功能 (例如，我们添加了标头来支持访问控制)。在这些情况下，我们已尽最大努力使添加的新功能与标准的 HTTP 使用样式相匹配。

如果您在应用程序中直接调用 REST API，您必须编写代码来计算签名并将它添加到请求中。有关如何向 Amazon S3 发出请求的更多信息，请参阅《Amazon S3 API 参考》中的 Making requests。

## 通用存储桶的虚拟托管

虚拟托管是指从单个 Web 服务器为多个网站提供服务的做法。区分 Amazon S3 REST API 请求中的站点的一种方法是通过使用请求-URI 的显式主机名，而不只是 URI 的路径名称部分。普通的 Amazon S3 REST 请求使用“请求-URI”路径的第一个斜杠分隔部分指定存储桶。相反，您可以通过使用 HTTP `Host` 标头，在 REST API 调用中使用 Amazon S3 虚拟托管对通用存储桶进行寻址。事实上，Amazon S3 会将 `Host` 解释为可在 `https://`*`bucket-name`*`.s3.`*`region-code`*`.amazonaws.com` 上自动访问大多数存储桶（对于有限类型的请求）。有关 Amazon S3 区域和端点的完整列表，请参阅《Amazon Web Services 一般参考》中的 Amazon S3 端点和限额。

虚拟托管还有其他好处。通过使用注册域名来命名您的存储桶，并将该名称设为 Amazon S3 的 DNS 别名，您可以完全自定义 Amazon S3 资源的 URL，例如：`http://my.`*`bucket-name`*`.com/`。您还可以发布到存储桶的虚拟服务器的“根目录”。此功能很重要，因为许多现有应用程序在此标准位置搜索文件。例如，`favicon.ico`、`robots.txt` 和 `crossdomain.xml` 都应可在根目录下找到。

> **Important**
>
> 当通过 SSL 使用虚拟托管类型通用存储桶时，SSL 通配符证书仅匹配不包含句点 (`.`) 的存储桶。要解决此问题，请使用 HTTP 或编写自己的证书验证逻辑。有关更多信息，请参阅 Amazon 新闻博客 上的 Amazon S3 路径弃用计划。

主题


- 路径类型请求
- 虚拟托管类型请求
- HTTP Host 标头桶规范
- 示例
- 使用 CNAME 记录自定义 Amazon S3 URL
- 如何将主机名与 Amazon S3 桶关联
- 限制
- 向后兼容性

## 路径类型请求

目前，Amazon S3 在所有 Amazon Web Services 区域中同时支持虚拟托管类型和路径类型 URL 访问。但是，路径类型 URL 将来会停用。有关更多信息，请参阅下面的重要提示。

在 Amazon S3 中，路径类型 URL 使用以下格式：

```
https://s3.region-code.amazonaws.com/bucket-name/key-name
```

例如，如果您在美国西部（俄勒冈）区域中创建一个名为 amzn-s3-demo-bucket1 的存储桶，并希望访问该存储桶中的 puppy.jpg 对象，则可使用以下路径类型 URL：

```
https://s3.us-west-2.amazonaws.com/amzn-s3-demo-bucket1/puppy.jpg
```

> **Important**
>
> 更新（2020 年 9 月 23 日）– 为确保客户有时间转换到虚拟托管类型 URL，我们决定推迟弃用路径类型 URL。有关更多信息，请参阅 Amazon 新闻博客中的 Amazon S3 路径弃用计划 – 案例的其余部分。

> **Warning**
>
> 托管将通过 Web 浏览器访问的网站内容时，请避免使用路径样式 URL，因为这可能会干扰浏览器的同源安全模型。要托管网站内容，我们建议您使用 S3 网站端点或 CloudFront 分配。有关更多信息，请参阅网站端点和《Amazon 透视指导模式》中的将基于 React 的单页应用程序部署到 Amazon S3 和 CloudFront。

## 虚拟托管类型请求

在虚拟托管类型 URI 中，存储桶名称是 URL 中域名的一部分。

Amazon S3 虚拟托管类型 URL 使用以下格式：

```
https://bucket-name.s3.region-code.amazonaws.com/key-name
```

在此示例中，amzn-s3-demo-bucket1 为存储桶名称，美国西部（俄勒冈）为区域，puppy.png 为密钥名称：

```
https://amzn-s3-demo-bucket1.s3.us-west-2.amazonaws.com/puppy.png
```

## HTTP **Host** 标头桶规范

只要您的 GET 请求不使用 SSL 终端节点，您就可以通过使用 HTTP Host 标头为请求指定存储桶。REST 请求中的 Host 标头解释如下：

- 如果 Host 标头被省略，或其值为 s3.*region-code*.amazonaws.com，则该请求的存储桶将是请求-URI 的第一个斜杠分隔的部分，而且该请求的键将是请求-URI 的其余部分。这是常用方法，如本部分第一个和第二个示例所示。省略 Host 标头仅对于 HTTP 1.0 请求有效。
- 否则，如果 Host 标头的值以 .s3.*region-code*.amazonaws.com 结尾，则存储桶名称是 Host 标头值中从开头到 .s3.*region-code*.amazonaws.com 的部分。该请求的键值为“Request-URI”。此解释将存储桶公开为 .s3.*region-code*.amazonaws.com 的子域，如本部分第三和第四个示例所示。
- 否则，请求的存储桶是 Host 标头的小写值，请求的键值是“Request-URI”。如果注册的 DNS 名称与桶名称相同，并且已将该名称配置为 Amazon S3 的规范名称 (CNAME) 别名，则此解释很有用。注册域名和配置 CNAME DNS 记录的过程不在本指南的范围内，但本节中的最后一个示例展示了结果。

## 示例

本节提供示例 URL 和请求。

Example – 路径类型 URL 和请求

此示例使用以下内容：

- 存储桶名称 – example.com
- 区域 – 美国东部（弗吉尼亚北部）
- 键名 – homepage.html

URL 如下：

```
http://s3.us-east-1.amazonaws.com/example.com/homepage.html
```

请求如下：

```
GET /example.com/homepage.html HTTP/1.1
Host: s3.us-east-1.amazonaws.com
```

具有 HTTP 1.0 且省略 Host 标头的请求如下：

```
GET /example.com/homepage.html HTTP/1.0
```

有关 DNS 兼容名称的信息，请参阅限制。有关密钥的更多信息，请参阅密钥。

Example – 虚拟托管类型 URL 和请求

此示例使用以下内容：

- 桶名称 - amzn-s3-demo-bucket1
- 区域 – 欧洲（爱尔兰）
- 键名 - homepage.html

URL 如下：

```
http://amzn-s3-demo-bucket1.s3.eu-west-1.amazonaws.com/homepage.html
```

请求如下：

```
GET /homepage.html HTTP/1.1
Host: amzn-s3-demo-bucket1.s3.eu-west-1.amazonaws.com
```

Example – CNAME 别名方法

要使用此方法，您必须将 DNS 名称配置为 *bucket-name*.s3.us-east-1.amazonaws.com 的 CNAME 别名。有关更多信息，请参阅 使用 CNAME 记录自定义 Amazon S3 URL。

此示例使用以下内容：

- 存储桶名称 – example.com
- 键名称 - homepage.html

URL 如下：

```
http://www.example.com/homepage.html
```

示例如下：

```
GET /homepage.html HTTP/1.1
Host: www.example.com
```

## 使用 CNAME 记录自定义 Amazon S3 URL

根据您的需要，您可能不希望 s3.*region-code*.amazonaws.com 显示在网站或服务中。例如，如果您在 Amazon S3 上托管网站映像，您可能会首选 http://images.example.com/，而不是 http://images.example.com.s3.us-east-1.amazonaws.com/。具有 DNS 兼容名称的任何存储桶都可按以下方式引用： http://*BucketName*.s3.*Region*.amazonaws.com/[*Filename*]，例如 http://images.example.com.s3.us-east-1.amazonaws.com/mydog.jpg。通过使用 CNAME，您可以将 images.example.com 映射到 Amazon S3 主机名，使上面的 URL 变成 http://images.example.com/mydog.jpg。

存储桶名称必须与 CNAME 相同。例如，如果您创建一个 CNAME 以将 images.example.com 映射到 images.example.com.s3.us-east-1.amazonaws.com，则 http://images.example.com/filename 和 http://images.example.com.s3.us-east-1.amazonaws.com/filename 两者将相同。

CNAME DNS 记录应将您的域名别名设置为适当的虚拟托管类型主机名。例如，如果存储桶名称和域名是 images.example.com 而存储桶位于美国东部（弗吉尼亚北部）区域中，则 CNAME 记录的别名应为 images.example.com.s3.us-east-1.amazonaws.com。

```
images.example.com CNAME    images.example.com.s3.us-east-1.amazonaws.com.
```

Amazon S3 使用主机名来确定存储桶名称。所以 CNAME 和存储桶名称必须相同。例如，假定您配置了 www.example.com 作为 www.example.com.s3.us-east-1.amazonaws.com 的别名记录。当您访问http://www.example.com时，Amazon S3 会收到如以下所示的请求：

Example

```
GET / HTTP/1.1
Host: www.example.com
Date: date
Authorization: signatureValue
```

Amazon S3 仅查看原始主机名 www.example.com 且不知道用于解决请求的 CNAME 映射。

您可以在 CNAME 别名中使用任何 Amazon S3 端点。例如，s3.ap-southeast-1.amazonaws.com 可用于 CNAME 别名中。有关端点的更多信息，请参阅《Amazon S3 API Reference》中的 Request endpoints。要使用自定义域创建静态网站，请参阅教程：使用注册到 Route 53 的自定义域配置静态网站。

> **Important**
>
> 将自定义 URL 与 CNAME 结合使用时，您需要确保对于您配置的任何 CNAME 或别名记录都存在匹配的桶。例如，如果您为 www.example.com 和 login.example.com 创建 DNS 条目以使用 S3 发布 Web 内容，将需要同时创建两个桶 www.example.com 和 login.example.com。
>
> 当 CNAME 或别名记录配置为指向没有匹配桶的 S3 端点时，任何 Amazon 用户都可以创建该桶并在配置的别名下发布内容，即使拥有权不同也是如此。
>
> 出于同样的原因，我们建议您在删除桶时更改或移除相应的 CNAME 或别名。

## 如何将主机名与 Amazon S3 桶关联

使用 CNAME 将主机名与 Amazon S3 桶关联

1. 选择属于您控制的域的主机名。

   本示例使用 images 域的 example.com 子域。

2. 创建与主机名匹配的存储桶。

   在本示例中，主机名和存储桶名称是 images.example.com。存储桶名称必须与主机名精确 匹配。

3. 创建一条 CNAME DNS 记录，它将主机名定义为 Amazon S3 桶的别名。

   例如：

   ```
   images.example.com CNAME images.example.com.s3.us-west-2.amazonaws.com
   ```

   > **Important**
   >
   > 出于请求路由原因，CNAME DNS 记录必须严格按照上述示例所示进行定义。否则，它可能显示为正常运行，但将最终导致不可预测的行为。

配置 CNAME DNS 记录的过程取决于您的 DNS 服务器或 DNS 提供商。有关特定信息，请参阅您的服务器文档或与您的供应商联系。

## 限制

SOAP API 不适用于新客户，并将于 2025 年 8 月 31 日接近使用寿命终止（EOL）。我们建议您使用 REST API 或 Amazon 开发工具包。

## 向后兼容性

以下各节介绍了 Amazon S3 向后兼容性的各个方面，这些方面与路径类型和虚拟托管类型 URL 请求相关。

### 传统终端节点

某些区域支持传统终端节点。您可能会在服务器访问日志或 Amazon CloudTrail 日志中看到这些端点。有关更多信息，请查看以下信息。有关 Amazon S3 区域和端点的完整列表，请参阅《Amazon Web Services 一般参考》中的 Amazon S3 端点和限额。

**Important**

尽管您可能会在日志中看到传统终端节点，但我们建议您始终使用标准终端节点语法访问存储桶。

Amazon S3 虚拟托管类型 URL 使用以下格式：

```
https://bucket-name.s3.region-code.amazonaws.com/key-name
```

在 Amazon S3 中，路径类型 URL 使用以下格式：

```
https://s3.region-code.amazonaws.com/bucket-name/key-name
```

### s3-区域

一些较旧的 Amazon S3 区域支持在 `s3` 和区域代码之间包含短划线 (`-`) 而不是点（例如 `s3.us-west-2`）的端点（例如 `s3-us-west-2`）。如果您的存储桶位于这些区域之一，您可能会在服务器访问日志或 CloudTrail 日志中看到以下终端节点格式：

```
https://bucket-name.s3-region-code.amazonaws.com
```

在此示例中，存储桶名称为 amzn-s3-demo-bucket1，区域为美国西部（俄勒冈）：

```
https://amzn-s3-demo-bucket1.s3-us-west-2.amazonaws.com
```

传统全局端点

对于某些区域，可以使用传统全局端点来构建未指定特定于区域的端点的请求。传统全局终端节点如下所示：

```
bucket-name.s3.amazonaws.com
```

在服务器访问日志或 CloudTrail 日志中，您可能会看到使用传统全局终端节点的请求。在此示例中，桶名称为 amzn-s3-demo-bucket1，传统全局端点为：

```
https://amzn-s3-demo-bucket1.s3.amazonaws.com
```

美国东部（弗吉尼亚州北部）的虚拟托管类型请求

原定设置情况下，使用传统全局端点发出的请求会转到美国东部（弗吉尼亚州北部）。因此，传统全局终端节点有时用于替代美国东部（弗吉尼亚北部）的区域终端节点。如果您在美国东部（弗吉尼亚州北部）创建桶并使用全局端点，则原定设置情况下，Amazon S3 会将您的请求路由到此区域。

其他区域的虚拟托管类型请求

传统全局端点也用于其他受支持的区域中的虚拟托管类型请求。当您在 2019 年 3 月 20 日之前发布的区域中创建桶并使用传统全局端点时，Amazon S3 将更新 DNS 记录以将请求重新路由到正确的位置，这可能会花费一些时间。同时，将应用原定设置规则，您的虚拟托管类型请求将转到美国东部（弗吉尼亚州北部）区域。然后，Amazon S3 将使用 HTTP 307 临时重定向将它重定向到正确的区域。

对于在 2019 年 3 月 20 日之后发布的区域中的 S3 桶，DNS 服务器不会将您的请求直接路由到您的桶所在的 Amazon Web Services 区域。它而是会返回 HTTP 400 错误请求错误。有关更多信息，请参阅《Amazon S3 API 参考》中的 Making requests。

路径类型请求

对于美国东部（弗吉尼亚州北部）区域，可以将传统全局端点用于路径类型请求。

对于所有其他区域，路径类型语法要求您在尝试访问存储桶时使用特定于区域的终端节点。如果您尝试访问具有传统全局端点的存储桶或与存储桶所在区域的端点不同的其它端点，您会收到 HTTP

响应代码“301 永久重定向”错误和一条消息（指示您资源的正确 URI）。例如，如果您将 `https://s3.amazonaws.com/bucket-name` 用于在美国西部（俄勒冈州）区域创建的存储桶，您将收到“HTTP 301 永久重定向”错误。

# 创建通用存储桶

要向 Amazon S3 上传数据，您必须首先在其中一个 Amazon Web Services 区域中创建 Amazon S3 通用存储桶。创建存储桶的 Amazon Web Services 账户 拥有该存储桶。创建存储桶时，您必须选择存储桶名称和区域。在创建过程中，您可以选择为存储桶选择其它存储管理选项。

> **Important**
>
> 创建存储桶后，无法更改存储桶名称、存储桶拥有者或区域。有关存储桶命名的更多信息，请参阅 the section called “命名规则”。

默认情况下，每个 Amazon Web Services 账户可以创建多达 10000 个通用存储桶。要请求增加通用存储桶的配额，请访问服务配额控制台。

一个存储桶中可以存储任意数量的对象。有关与 Amazon S3 通用存储桶相关的限制和局限性的列表，请参阅通用存储桶配额、限制和局限性。

## 通用存储桶设置

创建通用存储桶时，可以使用以下设置来控制存储桶行为的各个方面：

- S3 对象所有权：S3 对象所有权是 Amazon S3 存储桶级别的设置，您可以使用该设置来控制上传到存储桶的对象的所有权，并禁用或启用访问控制列表（ACL）。默认情况下，对象所有权设为强制存储桶拥有者设置，并且所有 ACL 均处于禁用状态。禁用 ACL 后，存储桶拥有者拥有存储桶中的每个对象，并使用策略专门管理对数据的访问权限。有关更多信息，请参阅 为您的存储桶控制对象所有权和禁用 ACL。。
- S3 对象锁定：S3 对象锁定有助于在固定的时间长度内或无限期地阻止删除或覆盖 Amazon S3 对象。对象锁定使用一次写入多次读取（WORM）模式存储对象。您可以使用对象锁定来协助满足需要 WORM 存储的法规要求，或用于添加额外的保护层来防止对象被更改和删除。有关更多信息，请参阅 the section called “锁定对象”。

创建通用存储桶后，或者当使用 Amazon S3 控制台创建通用存储桶时，还可以使用以下设置来控制存储桶行为的其它方面：

- S3 屏蔽公共访问权限：S3 屏蔽公共访问权限功能提供接入点、存储桶和账户的设置，有助于您管理对 Amazon S3 资源的公共访问权限。默认情况下，新存储桶、接入点和对象不允许公有访问。但是，用户可以修改存储桶策略、接入点策略或对象权限以允许公有访问。S3 屏蔽公共访问权限设置会覆盖这些策略和权限，以便于您可以限制这些资源的公有访问。有关更多信息，请参阅 the section called “阻止公有访问”。
- S3 版本控制：版本控制是在同一个存储桶中保留对象的多个版本的方法。对于 存储桶中存储的每个对象，您可以使用版本控制功能来保留、检索和还原它们的各个版本。使用版本控制能够轻松从用户意外操作和应用程序故障中恢复数据。默认情况下，对存储桶禁用版本控制。有关更多信息，请参阅 the section called “保留对象的多个版本”。
- 默认加密：可以为存储桶中的所有对象设置默认加密类型。具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）是 Amazon S3 中每个存储桶的基本加密配置级别。上传到 S3 存储桶的所有新对象都将使用 SSE-S3 作为基本加密级别自动进行加密。如果您要使用不同的默认加密类型，则可以使用具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）、具有 Amazon KMS 密钥的双层服务器端加密（DSSE-KMS）或具有客户提供的密钥的服务器端加密（SSE-C）来加密您的数据。有关更多信息，请参阅 为 Amazon S3 存储桶设置默认服务器端加密行为。

可以使用 Amazon S3 控制台、Amazon S3 REST API、Amazon Command Line Interface（Amazon CLI）或 Amazon SDK 来创建通用存储桶。有关创建通用存储桶所需权限的更多信息，请参阅《Amazon Simple Storage Service API Reference》中的 CreateBucket。

如果您在创建 Amazon S3 存储桶时遇到问题，请参阅 Amazon Web Services re:Post 上的我如何解决在创建 Amazon S3 存储桶时出现的错误？

## 使用 S3 控制台

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在页面顶部的导航栏中，选择当前所显示 Amazon Web Services 区域的名称。接下来，选择要在其中创建存储桶的区域。

> **Note**
>
> - 存储桶创建后，便无法再更改其区域。
> - 要最大程度地减少延迟和成本以及满足法规要求，请选择一个靠近您的区域。在某一区域存储的对象将一直留在该区域，除非您特意将其转移到其他区域。有关 Amazon S3

Amazon Web Services 区域的列表，请参阅《Amazon Web Services 一般参考》中的 Amazon Web Services 服务 端点。

3. 在左侧导航窗格中，选择通用存储桶。
4. 选择创建存储桶。此时将打开创建存储桶页面。
5. 对于存储桶名称，请输入存储桶的名称。

   存储桶名称必须满足以下要求：

   - 在分区中是唯一的。分区是区域的分组。Amazon 目前有三个分区：aws（商用区域）、aws-cn（中国区域）和 aws-us-gov（Amazon GovCloud (US) Regions）。
   - 长度必须介于 3 到 63 个字符之间。
   - 只能由小写字母、数字、句点 (.) 和连字符 (-) 组成。为了获得最佳兼容性，我们建议您避免在存储桶名称中使用句点 (.)，但仅用于静态网站托管的存储桶除外。
   - 以字母或数字开头和结尾。
   - 有关存储桶命名规则的完整列表，请参阅通用存储桶命名规则。

   **Important**

   - 创建存储桶后，便无法更改其名称。
   - 请勿在存储桶名称中包含敏感信息。存储桶名称会显示在指向存储桶中的对象的 URL 中。

6. （可选）在常规配置下，您可以选择将现有存储桶的设置复制到新存储桶。如果您不想复制现有存储桶的设置，请跳到下一步。

   **Note**

   此选项：

   - 在 Amazon CLI 中不可用，仅在 Amazon S3 控制台中可用
   - 不会将存储桶策略从现有存储桶复制到新存储桶

要复制现有存储桶的设置，请在从现有存储桶复制设置下，选择选择存储桶。将打开选择存储桶窗口。找到包含您要复制的设置的存储桶，然后选择选择存储桶。选择存储桶窗口关闭，而创建存储桶窗口重新打开。

在从现有存储桶复制设置下，您现在将看到您选择的存储桶的名称。新存储桶的设置现在与您选择的存储桶的设置相匹配。如果要移除复制的设置，请选择恢复默认设置。在创建存储桶页面上查看其余的存储桶设置。如果您不想进行任何更改，可以跳到最后一步。

7. 在 Object Ownership（对象所有权）下方，要禁用或启用 ACL，并控制上传到存储桶中的对象的所有权，请选择以下设置之一：

   已禁用 ACL

   - 强制存储桶拥有者（默认）：ACL 已禁用，存储桶拥有者自动拥有并完全控制通用存储桶中的每个对象。ACL 不再影响对 S3 通用存储桶中数据的访问权限。存储桶专门使用策略来定义访问控制。

     默认情况下，ACL 处于禁用状态。Amazon S3 中的大多数现代使用案例不再需要使用 ACL。我们建议您将 ACL 保持为禁用状态，除非有必须单独控制每个对象的访问权限的特殊情况。有关更多信息，请参阅 为您的存储桶控制对象所有权和禁用 ACL。。

   已启用 ACL

   - Bucket owner preferred（首选存储桶拥有者）— 存储桶拥有者拥有并完全控制其他账户使用 `bucket-owner-full-control` 标准 ACL 写入存储桶的新对象。

     如果应用首选存储桶拥有者设置，以要求所有 Amazon S3 上传都包含 `bucket-owner-full-control` 标准 ACL，则可以添加存储桶策略，该策略只允许使用此 ACL 上传对象。
   - 对象编写者— 该 Amazon Web Services 账户上传对象拥有该对象，对其拥有完全控制权，并且可以通过 ACL 授予其他用户访问该对象的权限。

   > **Note**
   >
   > 默认设置为强制存储桶拥有者。要应用默认设置并将 ACL 保持为禁用状态，只需要 `s3:CreateBucket` 权限。要启用 ACL，您必须具有 `s3:PutBucketOwnershipControls` 权限。

8. 在此存储桶的屏蔽公共访问权限设置中，请选择要应用于存储桶的屏蔽公共访问权限设置。

   默认情况下，启用所有四个“屏蔽公共访问权限”设置。我们建议您将所有设置保持为启用状态，除非您知道您需要为您的特定使用案例关闭其中一个或多个设置。有关屏蔽公共访问权限的更多信息，请参阅阻止对您的 Amazon S3 存储的公有访问。

   > **Note**
   >
   > 要启用所有“屏蔽公共访问权限”设置，只需要 `s3:CreateBucket` 权限。要关闭任何“屏蔽公共访问权限”设置，您必须拥有 `s3:PutBucketPublicAccessBlock` 权限。

9. （可选）默认情况下，存储桶版本控制处于禁用状态。版本控制是在相同的存储桶中保留对象的多个变量的方法。对于 存储桶中存储的每个对象，您可以使用版本控制功能来保留、检索和还原它们的各个版本。使用版本控制能够更加轻松地从用户意外操作和应用程序故障中恢复数据。有关版本控制的更多信息，请参阅使用 S3 版本控制保留对象的多个版本。

   要在存储桶上启用版本控制，请选择启用。

10. （可选）在 Tags（标签）下，您可以选择向存储桶添加标签。利用 Amazon 成本分配功能，可以使用存储桶标签来对存储桶的使用计费添加注释。一个标签即为一个键值对，用于表示用户分配给存储桶的标记。有关更多信息，请参阅 the section called “使用成本分配标签”。

    要添加存储桶标签，请输入 Key（键），并（可选）输入 Value（值），然后选择 Add Tag（添加标签）。

11. 要配置默认加密，请在加密类型下，选择以下选项之一：

    - 具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）
    - 具有 Amazon Key Management Service 密钥的服务器端加密（SSE-KMS）
    - 具有 Amazon Key Management Service（Amazon KMS）密钥的双层服务器端加密（DSSE-KMS）

    > **Important**
    >
    > 如果您将 SSE-KMS 或 DSSE-KMS 选项用于默认加密配置，则您将受到 Amazon KMS 的每秒请求数（RPS）配额限制。有关 Amazon KMS 限额以及如何请求增加限额的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的限额。

通过将具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）用作基本加密配置级别，对存储桶和新对象进行加密。有关默认加密的更多信息，请参阅为 Amazon S3 存储桶设置默认服务器端加密行为。有关 SSE-S3 的更多信息，请参阅使用具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）。

有关使用服务器端加密对数据进行加密的更多信息，请参阅the section called “数据加密”。

12. 如果您选择具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）或具有 Amazon Key Management Service（Amazon KMS）密钥的双层服务器端加密（DSSE-KMS），请执行以下操作：

    a. 在 Amazon KMS 密钥下，通过以下方式之一指定您的 KMS 密钥：

    - 要从可用的 KMS 密钥列表中进行选择，请选择从您的 Amazon KMS keys 密钥中进行选择，并从可用密钥的列表中选择您的 KMS 密钥。

      Amazon 托管式密钥 (aws/s3) 和您的客户自主管理型密钥都显示在此列表中。有关客户自主管理型密钥的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的客户密钥和 Amazon 密钥。
    - 要输入 KMS 密钥 ARN，请选择输入 Amazon KMS key ARN，然后在显示的字段中输入您的 KMS 密钥 ARN。
    - 要在 Amazon KMS 控制台中创建新的客户自主管理型密钥，请选择创建 KMS 密钥。

      有关创建 Amazon KMS key 的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的创建密钥。

> **Important**
>
> 您只能使用与存储桶所在相同的 Amazon Web Services 区域中可用的 KMS 密钥。Amazon S3 控制台仅列出与存储桶位于同一区域中的前 100 个 KMS 密钥。要使用未列出的 KMS 密钥，您必须输入 KMS 密钥 ARN。如果您希望使用由其它账户拥有的 KMS 密钥，则必须首先有权使用该密钥，然后必须输入相应的 KMS 密钥 ARN。有关 KMS 密钥的跨账户权限的更多信息，请参阅《Amazon Key Management Service Developer Guide》中的 Creating KMS keys that other accounts can use。有关 SSE-KMS 的更多信息，请参阅 使用 Amazon KMS (SSE-KMS) 指定服务器端加密。有关 DSSE-KMS 的更多信息，请参阅the section called “双层服务器端加密（DSSE-KMS）”。

在 Amazon S3 中使用 Amazon KMS key 进行服务器端加密时，您必须选择对称加密 KMS 密钥。Amazon S3 仅支持对称加密 KMS 密钥，而不支持非对称 KMS 密钥。有关更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的确定对称和非对称 KMS 密钥。

b. 将存储桶配置为使用 SSE-KMS 进行默认加密时，还可以使用 S3 存储桶密钥。S3 存储桶密钥可通过减少从 Amazon S3 到 Amazon KMS 的请求流量，降低加密成本。有关更多信息，请参阅 使用 Amazon S3 存储桶密钥降低 SSE-KMS 的成本。DSSE-KMS 不支持 S3 存储桶密钥。

默认情况下，S3 存储桶密钥在 Amazon S3 控制台中处于启用状态。我们建议将 S3 存储桶密钥保留为启用状态以降低成本。要为存储桶禁用 S3 存储桶密钥，请在存储桶密钥下选择禁用。

13. （可选）S3 对象锁定有助于保护新对象不被删除或覆盖。有关更多信息，请参阅 使用对象锁定以锁定对象。如果要启用 S3 对象锁定，请执行以下操作：

a. 选择高级设置。

**Important**

启用对象锁定会自动为存储桶启用版本控制。启用并成功创建存储桶后，还必须在存储桶的属性选项卡上配置对象锁定默认保留设置和法定保留设置。

b. 如果要启用对象锁定，请选择 Enable（启用），阅读出现的警告，并予以确认。

**Note**

要创建启用了对象锁定的存储桶，您必须具有以下权限：`s3:CreateBucket`、`s3:PutBucketVersioning` 和 `s3:PutBucketObjectLockConfiguration`。

14. 请选择 Create bucket（创建存储桶）。

## 使用 Amazon 软件开发工具包

使用 Amazon SDK 创建通用存储桶时，您必须先创建一个客户端，然后使用该客户端发送创建存储桶的请求。作为最佳做法，您应在同一 Amazon Web Services 区域 中创建客户端和存储桶。如果您在

创建客户端或存储桶时未指定区域，Amazon S3 将使用默认区域，即美国东部（弗吉尼亚州北部）。如果您想将存储桶的创建限制在特定 Amazon Web Services 区域内，则使用 LocationConstraint 条件键。

要创建客户端来访问双堆栈端点，则必须指定 Amazon Web Services 区域。有关更多信息，请参阅《Amazon S3 API 参考》中的 Using Amazon S3 dual-stack endpoints。有关可用 Amazon Web Services 区域的列表，请参阅《Amazon Web Services 一般参考》中的 Amazon Simple Storage Service endpoints and quotas。

创建客户端时，区域映射到特定于区域的端点。客户端使用此端点与 Amazon S3 进行通信：`s3.region.amazonaws.com`。如果您的区域是在 2019 年 3 月 20 日之后启动的，则您的客户端和存储桶必须位于同一区域。不过，您可以使用美国东部（弗吉尼亚北部）区域中的客户端在 2019 年 3 月 20 日之前启动的任何区域中创建存储桶。有关更多信息，请参阅 传统终端节点。

这些 Amazon SDK 代码示例执行以下任务：

- 通过显式指定 Amazon Web Services 区域创建客户端 – 在本例中，客户端使用 `s3.us-west-2.amazonaws.com` 端点与 Amazon S3 通信。您可以指定任意 Amazon Web Services 区域。有关 Amazon Web Services 区域 的列表，请参阅《Amazon 一般参考》中的区域和端点。
- 通过仅指定存储桶名称来发送创建存储桶请求 – 客户端向 Amazon S3 发送请求，请求在您创建客户端的区域中创建存储桶。
- 检索有关存储桶位置的信息：Amazon S3 将存储桶位置信息存储在与存储桶关联的位置子资源中。

有关其它 Amazon SDK 示例以及其它语言的示例，请参阅《Amazon Simple Storage Service API Reference》中的 Use CreateBucket with an Amazon SDK or CLI。

Java

Example 创建存储桶名称中使用全局唯一标识符（GUID）的存储桶

以下示例向您展示了如何使用适用于 Java 的 Amazon SDK，在美国东部（弗吉尼亚州北部）区域 (us-east-1) 中创建在存储桶名称末尾使用 GUID 的存储桶。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。有关其他 Amazon SDK 的信息，请参阅在 Amazon 上构建的工具。

```
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.Bucket;
```

```
import com.amazonaws.services.s3.model.CreateBucketRequest;

import java.util.List;
import java.util.UUID;

public class CreateBucketWithUUID {
    public static void main(String[] args) {
        final AmazonS3 s3 =
 AmazonS3ClientBuilder.standard().withRegion(Regions.US_EAST_1).build();
        String bucketName = "amzn-s3-demo-bucket" +
 UUID.randomUUID().toString().replace("-", "");
        CreateBucketRequest createRequest = new CreateBucketRequest(bucketName);
        System.out.println(bucketName);
        s3.createBucket(createRequest);
    }
}
```

Example 创建通用存储桶

此示例向您展示如何通过使用适用于 Java 的 Amazon SDK 来创建 Amazon S3 存储桶。有关创建和测试有效示例的说明，请参阅 Amazon SDK for Java 2.x Developer Guide。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.CreateBucketRequest;
import com.amazonaws.services.s3.model.GetBucketLocationRequest;

import java.io.IOException;

public class CreateBucket2 {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
```

```
                    .withRegion(clientRegion)
                    .build();

            if (!s3Client.doesBucketExistV2(bucketName)) {
                // Because the CreateBucketRequest object doesn't specify a region,
 the
                // bucket is created in the region specified in the client.
                s3Client.createBucket(new CreateBucketRequest(bucketName));

                // Verify that the bucket was created by retrieving it and checking
 its
                // location.
                String bucketLocation = s3Client.getBucketLocation(new
 GetBucketLocationRequest(bucketName));
                System.out.println("Bucket location: " + bucketLocation);
            }
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

有关如何创建和测试有效示例的信息，请参阅 Amazon SDK for .NET Version 3 API Reference。

Example

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using Amazon.S3.Util;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
```

```
   class CreateBucketTest
   {
       private const string bucketName = "*** bucket name ***";
       // Specify your bucket region (an example region is shown).
       private static readonly RegionEndpoint bucketRegion =
RegionEndpoint.USWest2;
       private static IAmazonS3 s3Client;
       public static void Main()
       {
           s3Client = new AmazonS3Client(bucketRegion);
           CreateBucketAsync().Wait();
       }

       static async Task CreateBucketAsync()
       {
           try
           {
               if (!(await AmazonS3Util.DoesS3BucketExistAsync(s3Client,
bucketName)))
               {
                   var putBucketRequest = new PutBucketRequest
                   {
                       BucketName = bucketName,
                       UseClientRegion = true
                   };

                   PutBucketResponse putBucketResponse = await
s3Client.PutBucketAsync(putBucketRequest);
               }
               // Retrieve the bucket location.
               string bucketLocation = await FindBucketLocationAsync(s3Client);
           }
           catch (AmazonS3Exception e)
           {
               Console.WriteLine("Error encountered on server. Message:'{0}' when
writing an object", e.Message);
           }
           catch (Exception e)
           {
               Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
           }
       }
       static async Task<string> FindBucketLocationAsync(IAmazonS3 client)
```

```
        {
            string bucketLocation;
            var request = new GetBucketLocationRequest()
            {
                BucketName = bucketName
            };
            GetBucketLocationResponse response = await
 client.GetBucketLocationAsync(request);
            bucketLocation = response.Location.ToString();
            return bucketLocation;
        }
    }
}
```

Ruby

有关如何创建和测试有效示例的信息，请参阅 Amazon SDK for Ruby - Version 3。

Example

```
require 'aws-sdk-s3'

# Wraps Amazon S3 bucket actions.
class BucketCreateWrapper
  attr_reader :bucket

  # @param bucket [Aws::S3::Bucket] An Amazon S3 bucket initialized with a name.
 This is a client-side object until
  #                                  create is called.
  def initialize(bucket)
    @bucket = bucket
  end

  # Creates an Amazon S3 bucket in the specified AWS Region.
  #
  # @param region [String] The Region where the bucket is created.
  # @return [Boolean] True when the bucket is created; otherwise, false.
  def create?(region)
    @bucket.create(create_bucket_configuration: { location_constraint: region })
    true
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't create bucket. Here's why: #{e.message}"
    false
```

```
  end

  # Gets the Region where the bucket is located.
  #
  # @return [String] The location of the bucket.
  def location
    if @bucket.nil?
      'None. You must create a bucket before you can get its location!'
    else
      @bucket.client.get_bucket_location(bucket: @bucket.name).location_constraint
    end
  rescue Aws::Errors::ServiceError => e
    "Couldn't get the location of #{@bucket.name}. Here's why: #{e.message}"
  end
end

# Example usage:
def run_demo
  region = "us-west-2"
  wrapper = BucketCreateWrapper.new(Aws::S3::Bucket.new("amzn-s3-demo-bucket-
#{Random.uuid}"))
  return unless wrapper.create?(region)

  puts "Created bucket #{wrapper.bucket.name}."
  puts "Your bucket's region is: #{wrapper.location}"
end

run_demo if $PROGRAM_NAME == __FILE__
```

## 使用 Amazon CLI

以下 Amazon CLI 示例在美国西部（北加利福尼亚）区域 (us-west-1) 中创建一个通用存储桶，示例存储桶名称使用了全局唯一标识符（GUID）。要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3api create-bucket \
    --bucket amzn-s3-demo-bucket1$(uuidgen | tr -d - | tr '[:upper:]' '[:lower:]' ) \
    --region us-west-1 \
    --create-bucket-configuration LocationConstraint=us-west-1
```

有关更多信息和其它示例，请参阅《Amazon CLI Command Reference》中的 create-bucket。

# 查看 S3 通用存储桶的属性

您可以查看您拥有的任何 Amazon S3 存储桶的属性。这些设置包括：

- 存储桶版本控制：使用版本控制在一个通用存储桶中保留对象的多个版本。默认情况下，将为新存储桶禁用版本控制。有关启用版本控制的信息，请参阅在存储桶上启用版本控制。
- 标签：利用 Amazon 成本分配功能，您可以使用存储桶标签对通用存储桶的使用计费添加注释。一个标签即为一个键值对，用于表示用户分配给存储桶的标记。有关更多信息，请参阅 使用成本分配 S3 存储桶标签。
- Default encryption (默认加密) – 启用默认加密可为您提供自动服务器端加密。Amazon S3 会在将对象保存到磁盘之前对其进行加密，并在下载对象时对其进行解密。有关更多信息，请参阅 为 Amazon S3 存储桶设置默认服务器端加密行为。
- 服务器访问日志记录：使用服务器访问日志记录详细地记录对通用存储桶发出的各种请求。默认情况下，Amazon S3 不会收集服务器访问日志。有关启用服务器访问日志记录的信息，请参阅启用 Amazon S3 服务器访问日志记录。
- Amazon CloudTrail 数据事件 – 使用 CloudTrail 记录数据事件。默认情况下，跟踪不记录数据事件。记录数据事件将收取额外费用。有关更多信息，请参阅《Amazon CloudTrail 用户指南》中的记录数据事件以便跟踪。
- 事件通知：启用特定的 Amazon S3 通用存储桶事件，以便在每次发生这些事件时向目标发送通知消息。有关更多信息，请参阅 使用 Amazon S3 控制台启用和配置事件通知。
- Transfer acceleration（传输加速）– 在您的客户端与 S3 存储桶之间实现快速、轻松和安全的远距离文件传输。有关启用传输加速的信息，请参阅启用和使用 S3 Transfer Acceleration。
- Object Lock (对象锁定) – 使用 S3 对象锁定在固定的时间段内或无限期地阻止删除或覆盖对象。有关更多信息，请参阅 使用对象锁定以锁定对象。
- 申请方付款：如果您希望申请方（而不是通用存储桶拥有者）支付请求和数据传输费用，请启用申请方付款。有关更多信息，请参阅 使用申请方付款通用存储桶进行存储传输和使用。
- Static website hosting (静态网站托管) – 您可以在 Amazon S3 上托管静态网站。有关更多信息，请参阅 使用 Amazon S3 托管静态网站。

您可以使用 Amazon Web Services Management Console、Amazon CLI 或 Amazon SDK 查看存储桶属性

## 使用 S3 控制台

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶或目录存储桶。
3. 在存储桶列表中，选择要查看其属性的存储桶的名称。
4. 选择属性选项卡。
5. 在属性页面上，您可以为存储桶配置上述属性。

## 使用 Amazon CLI

使用 Amazon CLI 查看存储桶属性

以下命令展示如何使用 Amazon CLI 列出不同的通用存储桶属性。

以下命令返回与存储桶 *amzn-s3-demo-bucket1* 关联的标签集。有关存储桶标签的更多信息，请参阅使用成本分配 S3 存储桶标签。

```
aws s3api get-bucket-tagging --bucket amzn-s3-demo-bucket1
```

有关更多信息和示例，请参阅《Amazon CLI 命令参考》中的 get-bucket-tagging。

以下命令返回存储桶 *amzn-s3-demo-bucket1* 的版本控制状态。有关存储桶版本控制的信息，请参阅使用 S3 版本控制保留对象的多个版本。

```
aws s3api get-bucket-versioning --bucket amzn-s3-demo-bucket1
```

有关更多信息和示例，请参阅《Amazon CLI 命令参考》中的 get-bucket-versioning。

以下命令返回存储桶 *amzn-s3-demo-bucket1* 的默认加密配置。默认情况下，所有存储桶都有默认加密配置，该配置使用具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）。有关存储桶默认加密的信息，请参阅为 Amazon S3 存储桶设置默认服务器端加密行为。

```
aws s3api get-bucket-encryption --bucket amzn-s3-demo-bucket1
```

有关更多信息和示例，请参阅《Amazon CLI 命令参考》中的 get-bucket-encryption。

以下命令返回存储桶 *amzn-s3-demo-bucket1* 的通知配置。有关存储桶事件通知的信息，请参阅 Amazon S3 事件通知。

```
aws s3api get-bucket-notification-configuration --bucket amzn-s3-demo-bucket1
```

有关更多信息和示例，请参阅《Amazon CLI 命令参考》中的 get-bucket-notification-configuration。

以下命令返回存储桶 *amzn-s3-demo-bucket1* 的日志记录状态。有关存储桶日志记录的信息，请参阅使用服务器访问日志记录来记录请求。

```
aws s3api get-bucket-logging --bucket amzn-s3-demo-bucket1
```

有关更多信息和示例，请参阅 Amazon CLI 命令参考中的 get-bucket-logging。

### 使用 Amazon SDK

有关如何使用 Amazon SDK 返回通用存储桶属性（例如版本控制、标签等）的示例，请参阅《Amazon S3 API Reference》中的 Code examples。

有关使用不同 Amazon SDK 的一般信息，请参阅《Amazon S3 API 参考》中的 Developing with Amazon S3 using the Amazon SDKs。

## 列出 Amazon S3 通用存储桶

要返回您拥有的通用存储桶的列表，可以使用 ListBuckets。您可以使用 Amazon S3 控制台、Amazon Command Line Interface 或 Amazon SDK 来列出存储桶。对于使用 Amazon CLI、Amazon SDK 和 Amazon S3 REST API 发出的 `ListBuckets` 请求，如果 Amazon Web Services 账户 采用存储桶的默认服务配额（10000 个存储桶），则将同时支持分页和非分页请求。无论您的账户中有多少存储桶，您都可以创建介于 1 到 10000 个存储桶之间的页面大小来列出所有存储桶。对于分页请求，`ListBuckets` 请求会返回存储桶名称，以及每个存储桶的相应 Amazon Web Services 区域。以下 Amazon Command Line Interface 和 Amazon SDK 示例向您展示了如何在 `ListBuckets` 请求中使用分页。请注意，有些 Amazon SDK 可以协助进行分页。

权限

要列出所有通用存储桶，您必须拥有 `s3:ListAllMyBuckets` 权限。如果遇到 `HTTP Access Denied (403 Forbidden)` 错误，请参阅排查 Amazon S3 中的拒绝访问（403 Forbidden）错误。

> **Important**
>
> 我们强烈建议仅使用分页 `ListBuckets` 请求。只有设置为默认通用存储桶配额 10000 的 Amazon Web Services 账户，才支持未分页的 `ListBuckets` 请求。如果您批准的通用存储

桶配额超过 10000，则必须发送分页 `ListBuckets` 请求以列出您账户的存储桶。对于通用存储桶配额大于 10000 的 Amazon Web Services 账户，所有未分页的 `ListBuckets` 请求都将遭拒绝。

## 使用 S3 控制台

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在通用存储桶选项卡上，您可以看到通用存储桶的列表。
4. 要按名称查找存储桶，请在按名称查找存储桶字段中输入存储桶名称。

## 使用 Amazon CLI

要使用 Amazon CLI 生成通用存储桶的列表，可以使用 `ls` 或 `list-buckets` 命令。以下示例向您展示了如何创建分页 `list-buckets` 请求和未分页的 `ls` 请求。要使用这些示例，请替换*#######*。

Example – 使用 **`ls`**（未分页）列出您账户中的所有存储桶

以下示例命令将在单个非分页调用中列出您账户中的所有通用存储桶。此调用会返回您账户中所有存储桶的列表（最多 10000 个结果）：

```
$ aws s3 ls
```

有关更多信息和示例，请参阅列出存储桶和对象。

Example – 使用 **`ls`**（分页）列出您账户中的所有存储桶

以下示例命令会进行一次或多次分页调用，列出您账户中的所有通用存储桶，每页返回 100 个存储桶：

```
$ aws s3 ls --page-size 100
```

有关更多信息和示例，请参阅列出存储桶和对象。

Example – 列出您账户中的所有存储桶（分页）

以下示例提供了分页 `list-buckets` 命令，用于列出您账户中的所有通用存储桶。`--max-items` 和 `--page-size` 选项将列出的存储桶数量限制为每页 100 个。

```
$ aws s3api list-buckets /
    --max-items 100 /
    --page-size 100
```

如果项目输出的数量 (`--max-items`) 少于基础 API 调用所返回的项目总数，则输出将包含 `starting-token` 参数所指定的延续令牌，您可传递到后续命令以检索下一组项目。以下示例展示了如何使用上一示例返回的 `starting-token` 值。您可以指定 `starting-code` 检索接下来的 100 个存储桶。

```
$ aws s3api list-buckets /
    --max-items 100 /
    --page-size 100 /
    --starting-token eyJNYXJrZXIiOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAxfQ==
```

Example – 列出 Amazon Web Services 区域中的所有存储桶（分页）

以下示例命令使用 `--bucket-region` 参数来列出账户中位于 `us-east-2` 区域的最多 100 个存储桶。不支持向与 `--bucket-region` 参数中指定的值不同的区域端点发出请求。例如，如果您想将响应限制在 `us-east-2` 中的存储桶，则必须向 `us-east-2` 中的端点发出请求。

```
$ aws s3api list-buckets /
    --region us-east-2 /
    --max-items 100 /
    --page-size 100 /
    --bucket-region us-east-2
```

Example – 列出所有以特定存储桶名称前缀开头的存储桶（分页）

以下示例命令列出了最多 100 个名称以 *amzn-s3-demo-bucket* 前缀开头的存储桶。

```
$ aws s3api list-buckets /
    --max-items 100 /
    --page-size 100 /
```

```
    --prefix amzn-s3-demo-bucket
```

## 使用 Amazon SDK

以下示例向您展示如何使用 Amazon SDK 来列出通用存储桶。

### SDK for Python

#### Example – ListBuckets 请求（分页）

```
import boto3

s3 = boto3.client('s3')
response = s3.list_buckets(MaxBuckets=100)
```

#### Example – ListBuckets 响应（分页）

```
import boto3

s3 = boto3.client('s3')
response =
 s3.list_buckets(MaxBuckets=1,ContinuationToken="eyJNYXJrZXIiOiBudWxsLCAiYm90b190cnVuY2F0ZV9
```

### SDK for Java

```
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.Bucket;
import com.amazonaws.services.s3.model.ListBucketsPaginatedRequest;
import com.amazonaws.services.s3.model.ListBucketsPaginatedResult;

import java.util.List;

public class ListBuckets {
    public static void main(String[] args) {
        final AmazonS3 s3 =
 AmazonS3ClientBuilder.standard().withRegion(Regions.DEFAULT_REGION).build();
        ListBucketsPaginatedRequest listBucketsPaginatedRequest = new
 ListBucketsPaginatedRequest().withMaxBuckets(1);
        ListBucketsPaginatedResult listBucketsPaginatedResult =
 s3.listBuckets(listBucketsPaginatedRequest);
```

```
        List<Bucket> buckets = listBucketsPaginatedResult.getBuckets();
        System.out.println("Your Amazon S3 buckets are:");
        for (Bucket b : buckets) {
            System.out.println("* " + b.getName() + " region: " + b.getRegion());
        }
        System.out.println("continuation token: " +
 listBucketsPaginatedResult.getContinuationToken());
    }
}
```

SDK for Java 2.x

```
import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.Bucket;
import software.amazon.awssdk.services.s3.model.ListBucketsRequest;
import software.amazon.awssdk.services.s3.model.ListBucketsResponse;

import java.util.List;

public class ListBuckets {
    public static void main(String[] args) {
        // Create an S3 client
        S3Client s3 = S3Client.builder()
                .region(Region.US_EAST_1) // Replace with your preferred region
                .credentialsProvider(DefaultCredentialsProvider.create())
                .build();

        try {
            // List buckets
            ListBucketsRequest listBucketsRequest = ListBucketsRequest.builder()
                    .maxBuckets(10)
                    .build();
            ListBucketsResponse listBucketsResponse =
 s3.listBuckets(listBucketsRequest);
            List<Bucket> buckets = listBucketsResponse.buckets();

            // Print bucket names
            System.out.println("Your Amazon S3 buckets are:");
            for (Bucket bucket : buckets) {
                System.out.println(bucket.name());
                System.out.println(bucket.getBucketRegion());
```

```
            }

        } catch (Exception e) {
            System.err.println("Error listing buckets: " + e.getMessage());
            e.printStackTrace();
        } finally {
            // Close the S3 client to release resources
            s3.close();
        }
    }
}
```

## SDK for Go

```
package main
import (
 "context"
 "fmt"
 "log"
 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/config"
 "github.com/aws/aws-sdk-go-v2/service/s3"
)
func main() {
 cfg, err := config.LoadDefaultConfig(context.TODO(), config.WithRegion("us-
east-2"))
 if err != nil {
  log.Fatal(err)
 }
 client := s3.NewFromConfig(cfg)
 maxBuckets := 1000
 resp, err := client.ListBuckets(context.TODO(), management
 portals3.ListBucketsInput{MaxBuckets: aws.Int32(int32(maxBuckets))})
 if err != nil {
  log.Fatal(err)
 }
 fmt.Println("S3 Buckets:")
 for _, bucket := range resp.Buckets {
     fmt.Println("- Name:", *bucket.Name)
     fmt.Println("-BucketRegion", *bucket.BucketRegion)
 }
 fmt.Println(resp.ContinuationToken == nil)
 fmt.Println(resp.Prefix == nil)
```

```
}
```

# 清空通用存储桶

您可以使用 Amazon S3 控制台、Amazon SDK 或 Amazon Command Line Interface（Amazon CLI）清空通用存储桶的内容。清空通用存储桶时，您将删除所有对象，但会保留存储桶。清空存储桶的操作无法撤消。当正在执行清空存储桶操作时添加到存储桶的对象可能被删除。必须先删除存储桶中的所有对象（包括所有对象版本和删除标记），然后才能删除存储桶本身。

在清空已启用或暂停 S3 版本控制的通用存储桶时，存储桶中的所有对象的所有版本都将被删除。有关更多信息，请参阅 使用启用版本控制的存储桶中的对象。

清空存储桶时，我们建议您同时移除所有未完成的分段上传。您可以使用分段上传将非常大的对象（最大 5TB）分成多个分段上载，以提高吞吐量并更快地从网络问题中恢复。如果分段上传过程未完成，则未完成的分段将保留在桶中（处于不可用状态）。这些未完成的分段将产生存储成本，直到上载过程完成或删除未完成的分段。有关更多信息，请参阅 在 Amazon S3 中使用分段上传来上传和复制对象。

作为最佳实践，我们建议配置生命周期规则，使超过特定天数的对象和未完成分段上传过期。当您创建生命周期规则以使未完成分段上传过期时，我们建议以 7 天作为一个良好的起点。有关更多信息，请参阅 在存储桶上设置 S3 生命周期配置。

生命周期到期是一个异步过程，因此规则可能需要花数天时间运行，然后存储桶才能为空。在 Amazon S3 首次运行该规则后，所有符合过期条件的对象都将被标记为删除。您不再为那些标记为删除的对象付费。有关更多信息，请参阅如何使用生命周期配置规则清空 Amazon S3 存储桶？。

## 使用 S3 控制台

您可以使用 Amazon S3 控制台来清空通用存储桶，这将删除存储桶中的所有对象，而不删除存储桶。

清空 S3 存储桶

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在存储桶列表中，选择要清空的存储桶的名称旁边的选项，然后选择清空。
4. 在 Empty bucket（清空存储桶）页面上，通过在文本字段中输入存储桶名称来确认要清空存储桶，然后选择 Empty（清空）。
5. 在清空桶：状态页面上监控桶清空过程的进度。

## 使用 Amazon CLI

仅在存储桶未启用存储桶版本控制时，才可使用 Amazon CLI 清空通用存储桶。如果未启用版本控制，您可以将 `rm`（删除）Amazon CLI命令与 `--recursive` 参数结合使用来清空存储桶（或删除部分带特定键名前缀的对象）。

以下 `rm` 命令将删除拥有键名前缀 `doc` 的对象，例如，`doc/doc1` 和 `doc/doc2`。

```
$ aws s3 rm s3://bucket-name/doc --recursive
```

使用以下命令删除所有对象，而无需指定前缀。

```
$ aws s3 rm s3://bucket-name --recursive
```

有关更多信息，请参阅《Amazon Command Line Interface 用户指南》中的将高级别 S3 命令与 Amazon CLI 结合使用。

> **Note**
>
> 您无法从启用了版本控制的存储桶中删除对象。当您删除一个对象时（此命令将执行的操作），Amazon S3 将添加一个删除标记。有关 S3 存储桶版本控制的更多信息，请参阅使用 S3 版本控制保留对象的多个版本。

## 使用 Amazon 开发工具包

您可以使用 Amazon SDK 来清空通用存储桶或移除部分拥有特定键名称前缀的对象。

有关如何使用适用于 Java 的 Amazon SDK清空存储桶的示例，请参阅删除通用存储桶。该代码将删除所有对象（不论存储桶是否启用了版本控制），然后删除存储桶。要只清空存储桶，请确保删除用来删除存储桶的语句。

有关使用其他 Amazon SDK 的更多信息，请参阅用于 Amazon Web Services 的工具。

## 使用生命周期配置

要清空大型通用存储桶，我们建议您使用 S3 生命周期配置规则。生命周期到期是一个异步过程，因此规则可能需要花数天时间运行，然后才能清空存储桶。在 Amazon S3 首次运行该规则后，所有符合过期条件的对象都将被标记为删除。您不再为那些标记为删除的对象付费。有关更多信息，请参阅如何使用生命周期配置规则清空 Amazon S3 存储桶？。

如果使用生命周期配置清空存储桶，则配置应包括当前版本、非当前版本、删除标记和未完成的分段上传。

您可以添加生命周期配置规则，以使所有对象或部分拥有特定键名前缀的对象过期。例如，要删除存储桶中的所有对象，您可以将生命周期规则设置为使对象在创建一天后过期。

Amazon S3 支持一个存储桶生命周期规则，您可以使用该规则停止未在启动后的指定天数内完成的分段上传。我们建议您配置此生命周期规则以最大限度地降低存储成本。有关更多信息，请参阅 配置存储桶生命周期配置以删除未完成的分段上传。

有关使用生命周期配置清空存储桶的更多信息，请参阅在存储桶上设置 S3 生命周期配置和即将过期的对象。

## 清空配置了 Amazon CloudTrail 的通用存储桶

Amazon CloudTrail 跟踪 Amazon S3 通用存储桶中的对象级数据事件，例如删除对象。如果您使用通用存储桶作为记录 CloudTrail 事件的目标并从同一个存储桶中删除对象，则在清空存储桶的同时可能正在创建新对象。为了防止这种情况，请停止 Amazon CloudTrail 跟踪。有关让 CloudTrail 跟踪停止记录事件的更多信息，请参阅《Amazon CloudTrail 用户指南》中的关闭跟踪的日志记录。

停止将 CloudTrail 跟踪添加到存储桶中的另一种备选方法是：将 `s3:PutObject` 语句添加到存储桶策略中。如果您想稍后在存储桶中存储新对象，则需要删除此拒绝 `s3:PutObject` 语句。有关更多信息，请参阅《IAM 用户指南》中的 对象操作 和 IAM JSON 策略元素：效果。

# 删除通用存储桶

您可以删除空的 Amazon S3 通用存储桶。有关清空通用存储桶的信息，请参阅the section called “清空通用存储桶”。

可以使用 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 Amazon S3 REST API 删除存储桶。

> **Important**
>
> 在删除通用存储桶之前，请注意以下事项：
>
> - 通用存储桶名称在全局命名空间中是唯一的。如果删除存储桶，请注意，另一个 Amazon Web Services 账户可以使用相同的通用存储桶名称来表示新存储桶，因此可能会收到针对已删除存储桶的请求。如果需要防止出现这种情况，或者如果您希望继续使用相同的存储桶名称，请不要删除该存储桶。我们建议您清空并保留存储桶，同时根据需要阻止任何存储桶请

求。对于不再活跃使用的存储桶，我们建议清空存储桶中的所有对象，以最大限度地降低成本，同时保留存储桶本身。

- 删除通用存储桶时，可能不会立即移除存储桶。相反，Amazon S3 会将存储桶排队以等待删除。由于 Amazon S3 分布在各个 Amazon Web Services 区域中，因此删除过程需要一些时间，才能在整个系统中完全传播并实现一致性。
- 如果存储桶托管静态网站，并且您如 教程：使用注册到 Route 53 的自定义域配置静态网站 中所述创建并配置了 Amazon Route 53 托管区域，则必须清理与该存储桶相关的 Route 53 托管区域设置。有关更多信息，请参阅 步骤 2：删除 Route 53 托管区域。
- 如果存储桶收到来自弹性负载均衡（ELB）的日志数据，建议您先停止将 ELB 日志传输到该存储桶，然后再删除该存储桶。删除该存储桶后，如果其他用户创建使用相同名称的存储桶，则日志数据可能会传输到此同名存储桶。有关 ELB 访问日志的信息，请参阅《User Guide for Classic Load Balancers》中的 Access logs for your Classic Load Balancer 和《User Guide for Application Load Balancers》中的 Access logs for your Application Load Balancer。

故障排除

如果您无法删除 Amazon S3 通用存储桶，请考虑以下事项：

- 确保存储桶为空：仅当存储桶中没有任何对象时，才能删除存储桶。确保存储桶为空。有关清空存储桶的信息，请参阅the section called “清空通用存储桶”。
- 确保没有附加任何接入点：只有当存储桶在同一个账户中未附加任何 S3 接入点或多区域接入点时，您才能删除存储桶。在删除存储桶之前，请删除附加到该存储桶的任何同账户接入点。
- 确保您拥有 **`s3:DeleteBucket`** 权限：如果您无法删除存储桶，请与 IAM 管理员协作来确认您拥有 `s3:DeleteBucket` 权限。有关如何查看或更新 IAM 权限的信息，请参阅《IAM 用户指南》中的更改 IAM 用户的权限。有关问题排查信息，请参阅the section called “排查拒绝访问 (403 Forbidden) 错误”。
- 检查 Amazon Organizations 服务控制策略（SCP）和资源控制策略（RCP）中的 **`s3:DeleteBucket Deny`** 语句：SCP 和 RCP 可以拒绝对存储桶的删除权限。有关更多信息，请参阅《Amazon Organizations User Guide》中的 service control policies 和 resource control policies。
- 检查存储桶策略中的 **`s3:DeleteBucket Deny`** 语句：如果您在 IAM 用户或角色策略中拥有 `s3:DeleteBucket` 权限，但无法删除存储桶，则存储桶策略可能对于 `s3:DeleteBucket` 包含 Deny 语句。默认情况下，由 Amazon Elastic Beanstalk 创建的存储桶具有包含此语句的策略。您必须先删除此语句或存储桶策略，然后才能删除存储桶。

先决条件

您必须先清空通用存储桶，然后才能删除该存储桶。有关清空存储桶的信息，请参阅the section called “清空通用存储桶”。

## 使用 S3 控制台

删除 S3 存储桶

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在存储桶列表中，选择要删除的存储桶名称旁边的选项按钮，然后选择页面顶部的删除。
4. 在删除存储桶页面上，通过在文本字段中输入存储桶名称来确认要删除存储桶，然后选择删除存储桶。

   > **Note**
   >
   > 如果存储桶包含任何对象，请在删除存储桶之前清空存储桶，具体操作如下：在此存储桶不为空错误提醒中选择清空存储桶按钮，然后按照清空存储桶页面上的说明操作。然后，返回到 Delete bucket（删除存储桶）页面并删除存储桶。

5. 要验证您是否已删除存储桶，请打开通用存储桶列表，并输入您删除的存储桶的名称。如果无法找到此存储桶，则表示删除成功。

## 使用适用于 Java 的 Amazon SDK

以下示例展示了如何使用适用于 Java 的 Amazon SDK 清空和删除通用存储桶。该代码首先删除通用存储桶中的所有对象，然后删除该存储桶。

有关其它语言的示例，请参阅《Amazon Simple Storage Service API Reference》中的 Use DeleteBucket with an Amazon SDK or CLI。有关使用其它 Amazon SDK 的信息，请参阅用于 Amazon Web Services 的工具。

Java

以下 Java 示例删除包含对象的存储桶。该示例将删除所有对象，然后删除存储桶。该示例适用于已启用版本控制或未启用版本控制的存储桶。

> **Note**
>
> 对于未启用版本控制的存储桶，您可以直接删除所有对象，然后删除存储桶。对于启用了版本控制的存储桶，您必须先删除所有对象版本，然后再删除存储桶。

有关创建和测试有效示例的说明，请参阅 Amazon SDK for Java 2.x Developer Guide。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.util.Iterator;

public class DeleteBucket2 {

    public static void main(String[] args) {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Delete all objects from the bucket. This is sufficient
            // for unversioned buckets. For versioned buckets, when you attempt to
 delete
            // objects, Amazon S3 inserts
            // delete markers for all objects, but doesn't delete the object
 versions.
            // To delete objects from versioned buckets, delete all of the object
 versions
            // before deleting
            // the bucket (see below for an example).
            ObjectListing objectListing = s3Client.listObjects(bucketName);
            while (true) {
```

```
                Iterator<S3ObjectSummary> objIter =
objectListing.getObjectSummaries().iterator();
                while (objIter.hasNext()) {
                    s3Client.deleteObject(bucketName, objIter.next().getKey());
                }

                // If the bucket contains many objects, the listObjects() call
                // might not return all of the objects in the first listing. Check
to
                // see whether the listing was truncated. If so, retrieve the next
page of
                // objects
                // and delete them.
                if (objectListing.isTruncated()) {
                    objectListing = s3Client.listNextBatchOfObjects(objectListing);
                } else {
                    break;
                }
            }

            // Delete all object versions (required for versioned buckets).
            VersionListing versionList = s3Client.listVersions(new
ListVersionsRequest().withBucketName(bucketName));
            while (true) {
                Iterator<S3VersionSummary> versionIter =
versionList.getVersionSummaries().iterator();
                while (versionIter.hasNext()) {
                    S3VersionSummary vs = versionIter.next();
                    s3Client.deleteVersion(bucketName, vs.getKey(),
vs.getVersionId());
                }

                if (versionList.isTruncated()) {
                    versionList = s3Client.listNextBatchOfVersions(versionList);
                } else {
                    break;
                }
            }

            // After all objects and object versions are deleted, delete the bucket.
            s3Client.deleteBucket(bucketName);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
```

```
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
 couldn't
            // parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

### 使用 Amazon CLI

如果包含对象的通用存储桶没有启用版本控制，则可以使用 Amazon CLI 删除该存储桶。当您删除一个包含对象的存储桶时，该存储桶中的所有对象都将被永久删除，包括已转换为 S3 Glacier Flexible Retrieval 存储类的对象。

如果存储桶未启用版本控制，则可将 `rb`（移除存储桶）Amazon CLI 命令和 `--force` 参数结合使用，来删除存储桶及其中的所有对象。此命令先删除所有对象，然后再删除存储桶。

如果启用了版本控制，则将 `rb` 命令与 `--force` 参数结合使用不会删除受版本控制的对象，因此存储桶删除失败，因为存储桶不为空。有关删除受版本控制的对象的更多信息，请参阅删除对象版本。

要使用以下命令，请将 *amzn-s3-demo-bucket* 替换为您要删除的存储桶的名称：

```
$ aws s3 rb s3://amzn-s3-demo-bucket --force
```

有关更多信息，请参阅《Amazon Command Line Interface 用户指南》中的将高级别 S3 命令与 Amazon Command Line Interface结合使用。

## 使用适用于 Amazon S3 的 Mountpoint

适用于 Amazon S3 的 Mountpoint 是一款高吞吐量的开源文件客户端，用于将 Amazon S3 通用存储桶作为本地文件系统进行挂载。借助 Mountpoint，您的应用程序可以通过文件系统操作（例如打开和读取）访问存储在 Amazon S3 中的对象。Mountpoint 会自动将这些操作转换为 S3 对象 API 调用，让您的应用程序能够通过文件接口访问 Amazon S3 的弹性存储和吞吐量。

适用于 Amazon S3 的 Mountpoint 可用于大规模读取密集型应用程序上的生产用途：数据湖、机器学习训练、图像渲染、自动驾驶汽车模拟以及提取、转换、加载（ETL）等。

适用于 Amazon S3 的 Mountpoint 仅适用于 Linux 操作系统。您可以使用 Mountpoint 访问所有存储类中的 S3 对象，但 S3 Glacier Flexible Retrieval、S3 Glacier Deep Archive、S3 Intelligent-Tiering Archive Access Tier 和 S3 Intelligent-Tiering Deep Archive Access Tier 除外。

主题


- 安装 Mountpoint
- 配置和使用 Mountpoint
- Mountpoint 故障排除


# 安装 Mountpoint

您可以使用命令行下载和安装适用于 Amazon S3 的 Mountpoint 的预构建程序包。根据您正在使用哪个 Linux 操作系统，下载和安装 Mountpoint 的说明会有所不同。

主题


- 基于 RPM 的发行版（Amazon Linux、Fedora、CentOS、RHEL）
- 基于 DEB 的发行版（Debian、Ubuntu）
- 其他 Linux 发行版
- 验证适用于 Amazon S3 的 Mountpoint 程序包的签名


## 基于 RPM 的发行版（Amazon Linux、Fedora、CentOS、RHEL）

1. 下载适用于 Amazon S3 的 Mountpoint 程序包。将 *download-link* 替换为上一步中的相应下载 URL。

   ```
   wget download-link
   ```

2. 使用以下命令安装此程序包：

   ```
   sudo yum install ./mount-s3.rpm
   ```

3. 输入以下命令，验证 Mountpoint 是否已成功安装：

   ```
   mount-s3 --version
   ```

   您应该可以看到类似于如下所示的输出内容：

```
mount-s3 1.3.1
```

## 基于 DEB 的发行版（Debian、Ubuntu）

1. 下载适用于 Amazon S3 的 Mountpoint 程序包。将 *download-link* 替换为上一步中的相应下载 URL。

   ```
   wget download-link
   ```

2. 使用以下命令安装此程序包：

   ```
   sudo apt-get install ./mount-s3.deb
   ```

3. 运行以下命令，验证适用于 Amazon S3 的 Mountpoint 是否已成功安装：

   ```
   mount-s3 --version
   ```

   您应该可以看到类似于如下所示的输出内容：

   ```
   mount-s3 1.3.1
   ```

## 其他 Linux 发行版

1. 下载适用于 Amazon S3 的 Mountpoint 程序包。将 *download-link* 替换为上一步中的相应下载 URL。

   ```
   wget download-link
   ```

2. 使用以下命令安装此程序包：

   ```
   sudo mkdir -p /opt/aws/mountpoint-s3 && sudo tar -C /opt/aws/mountpoint-s3 -xzf ./
   mount-s3.tar.gz
   ```

3. 将 `mount-s3` 二进制文件添加到您的 `PATH` 环境变量。在您的 `$HOME/.profile` 文件中，附加下面一行：

```
export PATH=$PATH:/opt/aws/mountpoint-s3/bin
```

保存 .profile 文件，并运行以下命令：

```
source $HOME/.profile
```

4. 运行以下命令，验证适用于 Amazon S3 的 Mountpoint 是否已成功安装：

```
mount-s3 --version
```

您应该可以看到类似于如下所示的输出内容：

```
mount-s3 1.3.1
```

## 验证适用于 Amazon S3 的 Mountpoint 程序包的签名

1. 安装 GnuPG（gpg 命令）。需要验证所下载的适用于 Amazon S3 的 Mountpoint 程序包的真实性和完整性。默认情况下，GnuPG 安装在 Amazon Linux 亚马逊机器映像（AMI）上。安装 GnuPG 之后，继续执行步骤 2。
2. 通过运行以下命令下载 Mountpoint 公有密钥：
3. 通过运行以下命令将 Mountpoint 公有密钥导入到您的密钥环中：

```
gpg --import KEYS
```

4. 通过运行以下命令验证 Mountpoint 公有密钥的指纹：

```
gpg --fingerprint mountpoint-s3@amazon.com
```

确认显示的指纹字符串与以下内容相匹配：

```
673F E406 1506 BB46 9A0E  F857 BE39 7A52 B086 DA5A
```

如果指纹字符串不匹配，请不要完成安装 Mountpoint 并联系 Amazon Web Services 支持。

5. 通过运行以下命令验证下载的程序包的签名。将 *signature-filename* 替换为上一步中的文件名。

```
gpg --verify signature-filename
```

例如，在基于 RPM 的发行版（包括 Amazon Linux）上，运行以下命令：

```
gpg --verify mount-s3.rpm.asc
```

6. 输出应包含短语 `Good signature`。如果输出包含短语 `BAD signature`，请重新下载 Mountpoint 程序包文件并重复这些步骤。如果问题仍然存在，请不要完成 Mountpoint 的安装并联系 Amazon Web Services 支持。

   输出可能包括有关可信签名的警告。这并不表示存在问题。这仅表示您尚未独立验证 Mountpoint 公有密钥。

## 配置和使用 Mountpoint

要使用适用于 Amazon S3 的 Mountpoint，您的主机需要有效的 Amazon 凭证，有权访问您要挂载的一个或多个通用存储桶。有关不同的身份验证方式，请参阅 GitHub 上的 Mountpoint Amazon 凭证。

例如，您可以创建一个新的 Amazon Identity and Access Management（IAM）用户和角色用于此目的。请确保此角色有权访问您要挂载的一个或多个存储桶。您可以通过实例配置文件将 IAM 角色传递给您的 Amazon EC2 实例。

主题

- 使用适用于 Amazon S3 的 Mountpoint
- 在 Mountpoint 中配置缓存

### 使用适用于 Amazon S3 的 Mountpoint

使用适用于 Amazon S3 的 Mountpoint 执行以下操作：

1. 使用 `mount-s3` 命令挂载通用存储桶。

   在下面的示例中，将 *amzn-s3-demo-bucket* 替换为 S3 通用存储桶的名称，并将 *~/mnt* 替换为主机上您希望在其中挂载 S3 存储桶的目录。

```
mkdir ~/mnt
mount-s3 amzn-s3-demo-bucket ~/mnt
```

由于 Mountpoint 客户端在默认情况下在后台运行，因此 *~/mnt* 目录现在允许您访问 S3 存储桶中的对象。

2. 通过 Mountpoint 访问通用存储桶中的对象。

   在本地挂载存储桶后，您可以使用常用的 Linux 命令（例如 `cat` 或 `ls`）来处理您的 S3 对象。适用于 Amazon S3 的 Mountpoint 通过以正斜杠（`/`）字符为界拆分 S3 存储桶中的密钥，将这些密钥解释为文件系统路径。例如，如果您的存储桶中有对象密钥 `Data/2023-01-01.csv`，那么您的 Mountpoint 文件系统中将有一个名为 `Data` 的目录，其中有一个名称为 `2023-01-01.csv` 的文件。

3. 使用 `umount` 命令卸载您的存储桶。此命令卸载您的 S3 存储桶并退出 Mountpoint。

   要使用以下示例命令，请将 *~/mnt* 替换为主机上挂载 S3 存储桶的目录。

   ```
   umount ~/mnt
   ```

   > **Note**
   >
   > 要获取此命令的选项列表，请运行 `umount --help`。

有关 Mountpoint 配置的其他详细信息，请参阅 GitHub 上的 S3 存储桶配置和文件系统配置。

## 在 Mountpoint 中配置缓存

适用于 Amazon S3 的 Mountpoint 支持不同类型的数据缓存。要加快重复读取请求的速度，您可以选择以下选项：

- 本地缓存 – 您可以在 Amazon EC2 实例存储或 Amazon Elastic Block Store 卷中使用本地缓存。如果您重复从同一个计算实例读取相同的数据，并且本地实例存储中有未使用的空间用于存放重复读取的数据集，则应该选择使用本地缓存。
- 共享缓存 – 您可以在 S3 Express One Zone 上使用共享缓存。如果您重复读取多个计算实例中的小对象，或者您不知道重复读取的数据集的大小并希望从弹性缓存大小中受益，则应选择使用共享缓存。选择该选项后，Mountpoint 会在使用 S3 Express One Zone 的目录存储桶中，保留大小不超过一兆字节的对象。
- 合并本地缓存和共享缓存 – 如果您的本地缓存中有未使用的空间，但又想在多个实例之间共享缓存，则可以选择同时使用本地缓存和共享缓存。

在 Mountpoint 中缓存非常适合重复读取相同数据的使用场景，这些数据在多次读取期间不会发生更改。例如，可以将缓存用于需要多次读取训练数据集的机器学习训练作业，以提高模型精度。

有关如何在 Mountpoint 中配置缓存的更多信息，请参阅以下示例。

主题

- 本地缓存
- 共享缓存
- 合并本地缓存和共享缓存

### 本地缓存

您可以利用 `--cache` *`CACHE_PATH`* 标志选择使用本地缓存。在以下示例中，将 *`CACHE_PATH`* 替换为要在其中缓存数据的目录的文件路径。将 *`amzn-s3-demo-bucket`* 替换为 S3 存储桶的名称，并将 *`~/mnt`* 替换为主机上您希望在其中挂载 S3 存储桶的目录。

```
mkdir ~/mnt
mount-s3 --cache CACHE_PATH amzn-s3-demo-bucket ~/mnt
```

当您在挂载 S3 存储桶时选择使用本地缓存，Mountpoint 会在配置的缓存位置创建一个空的子目录（如果该子目录尚不存在）。首次挂载存储桶以及卸载存储桶时，Mountpoint 会删除本地缓存的内容。

> **Important**
>
> 如果启用本地缓存，Mountpoint 会将挂载的 S3 存储桶中的未加密对象内容，保存在挂载时提供的本地缓存位置。为了保护您的数据，您应使用文件系统访问控制机制，限制对数据缓存位置的访问。

### 共享缓存

如果您重复读取多个计算实例中的小对象（最大 1 MB），或者重复读取的数据集大小通常超过本地缓存的大小，则应在 S3 Express One Zone 中使用共享缓存。当您从多个实例重复读取相同的数据时，这样可以避免向挂载的 S3 存储桶发出冗余请求，从而缩短延迟。

选择使用共享缓存后，您需要为缓存在您的 S3 Express One Zone 目录存储桶中的数据付费。您还需要为针对您在 S3 Express One Zone 目录存储桶中存储的数据发出的请求付费。有关更多信息，请参阅 Amazon S3 定价。Mountpoint 从不删除目录存储桶中的缓存对象。要管理存储成本，您应

该在目录存储桶上设置生命周期策略，以便在您指定的时间段后，Amazon S3 可使 S3 Express One Zone 中的缓存数据过期。有关更多信息，请参阅 GitHub 上的 Mountpoint for Amazon S3 caching configuration。

要在将通用存储桶挂载到计算实例时选择在 S3 Express One Zone 中进行缓存，请使用 `--cache-xz` 标志并将目录存储桶指定为缓存位置。在以下示例中，替换*#######*。

```
mount-s3 amzn-s3-demo-bucket ~/mnt --cache-xz amzn-s3-demo-bucket--usw2-az1--x-s3
```

合并本地缓存和共享缓存

如果您的实例上有未使用的空间，但又想在多个实例之间使用共享缓存，则可以选择同时使用本地缓存和共享缓存。使用此缓存配置，当所需数据缓存在本地存储中时，您可以避免从同一实例向目录存储桶中的共享缓存发送冗余读取请求。这可以降低请求成本并提高性能。

要在挂载 S3 存储桶时同时选择使用本地缓存和共享缓存，请使用 `--cache` 和 `--cache-xz` 标志来指定这两个缓存位置。要利用以下示例来选择同时使用本地缓存和共享缓存，请替换*#######*。

```
mount -s3 amzn-s3-demo-bucket ~/mnt --cache /path/to/mountpoint/cache --cache -xz amzn-s3-demo-bucket--usw2-az1--x-s3
```

有关更多信息，请参阅 GitHub 上的 Mountpoint for Amazon S3 caching configuration。

> **Important**
>
> 如果您启用共享缓存，Mountpoint 会将对象内容从挂载的 S3 存储桶复制到您作为共享缓存位置提供的 S3 目录存储桶中，从而使任何有权访问 S3 目录存储桶的调用方都可以访问这些内容。要保护缓存的数据，您应遵循 Amazon S3 的安全最佳实践以确保存储桶使用了正确的策略，并且不是公开可访问的。您应该使用专用于 Mountpoint 共享缓存的目录存储桶，并仅向 Mountpoint 客户端授予访问权限。

## Mountpoint 故障排除

适用于 Amazon S3 的 Mountpoint 由 Amazon Web Services 支持 提供支持。如果您需要帮助，请联系 Amazon Web Services 支持 中心。

您也可以在 GitHub 上查看并提交 Mountpoint 问题。

如果您在该项目中发现潜在的安全问题，我们要求您通过我们的漏洞报告页面通知 Amazon 安全部门。不要创建公开的 GitHub 问题。

如果您的应用程序在使用 Mountpoint 时出现异常行为，则可以检查日志信息以诊断问题。

日志记录

默认情况下，Mountpoint 会将高严重性日志信息发送到 syslog。

要查看最新的 Linux 发行版（包括 Amazon Linux）上的日志，请运行以下 `journald` 命令：

```
journalctl -e SYSLOG_IDENTIFIER=mount-s3
```

在其他 Linux 系统上，`syslog` 条目很可能写入到文件（例如 `/var/log/syslog`）中。

您可以使用这些日志对应用程序进行故障排除。例如，如果您的应用程序尝试覆盖现有文件，操作将失败，并且您将在日志中看到类似于以下内容的行：

```
[WARN] open{req=12 ino=2}: mountpoint_s3::fuse: open failed: inode error: inode 2 (full
 key "README.md") is not writable
```

有关更多信息，请参阅 GitHub 上的适用于 Amazon S3 的 Mountpoint 的日志记录。

# 使用适用于 Amazon S3 的存储浏览器

适用于 S3 的存储浏览器是一个开源组件，您可以将其添加到 Web 应用程序中，为您的最终用户提供存储在 Amazon S3 中的数据的简单图形界面。借助适用于 S3 的存储浏览器，您可以为经授权的最终用户提供直接从您自己的应用程序浏览、下载、上传、复制和删除 S3 中数据的权限。

适用于 S3 的存储浏览器支持对文件执行以下操作：`LIST`、`GET`、`PUT`、`COPY`、`UPLOAD` 和 `DELETE`。为了提供高吞吐量数据传输，适用于 S3 的存储浏览器仅显示您的最终用户获得授权可访问的数据并优化上传请求。存储浏览器还可以优化性能来缩短加载时间，计算最终用户上传的数据的校验和，并在确认您的数据完整性已通过公共互联网维护（传输中）后接受对象。您可以使用 Amazon 安全和身份服务或您自己的托管式服务，根据最终用户的身份控制对数据的访问权限。还可以自定义存储浏览器，使其与现有应用程序的设计和品牌相匹配。

适用于 S3 的存储浏览器仅适用于 React 框架上的 Web 应用程序和内联网应用程序。可以使用存储浏览器访问所有存储类中的 Amazon S3 对象，但 S3 Glacier Flexible Retrieval、S3 Glacier Deep

Archive、S3 Intelligent-Tiering Archive Access 层和 S3 Intelligent-Tiering Deep Archive Access 层除外。

适用于 S3 的存储浏览器可与 Amazon Amplify React 库中的 Web 应用程序结合使用。有关存储浏览器的更多信息，请参阅适用于 S3 的存储浏览器。

主题


- 使用适用于 S3 的存储浏览器
- 安装适用于 S3 的存储浏览器
- 设置适用于 S3 的存储浏览器
- 配置适用于 S3 的存储浏览器
- 适用于 S3 的存储浏览器故障排除


## 使用适用于 S3 的存储浏览器

在适用于 S3 的存储浏览器中，位置是 S3 通用存储桶或前缀，您可以使用 S3 访问权限管控、IAM 策略或您自己的托管式授权服务向最终用户授予访问权限。在您授权最终用户访问特定位置后，他们可以处理该位置内的任何数据。

适用于 S3 的存储浏览器用户界面有四个主要视图：

- 主页：主页列出了您的用户可以访问的 S3 位置，以及您对每个位置的权限。这是用户的初始视图，它显示了最终用户有权访问的根级 S3 资源以及对每个 S3 位置的权限（READ/WRITE/READWRITE）。
- 位置详细信息：此视图可让用户浏览 S3 中的文件和文件夹，以及上传或下载文件。（请注意，在适用于 S3 的存储浏览器中，对象 称为文件，前缀 和存储桶 称为文件夹。）
- 位置操作：用户在存储浏览器中选择操作（例如上传）后，它会打开文件位置的另一个视图。
- 垂直省略号：垂直省略号图标可打开操作的下拉列表。

使用适用于 S3 的存储浏览器时，请注意以下限制：

- 不支持以句点（.）开头或结尾的文件夹。
- 不支持具有仅 WRITE 权限的 S3 访问权限管控。
- 适用于 S3 的存储浏览器对于大小不超过 160 GB 的文件支持 PUT 操作。
- 适用于 S3 的存储浏览器对于小于 5 GB 的文件仅支持 COPY 操作。如果文件大小超过 5 GB，存储浏览器将使请求失败。

# 安装适用于 S3 的存储浏览器

开始使用存储浏览器的最快方法是在 GitHub 上克隆示例项目之一。这些示例项目有助于您部署适用于存储浏览器的生产就绪型 Web 应用程序，其中包含适用于 Amazon Identity and Access Management 的 Amazon 服务的预设集成，因此您可以快速将获得授权的终端用户连接到 S3 中的数据。

有关更多信息，请参阅《Amplify Dev Center》中的 Quick start。

## 从 GitHub 安装适用于 S3 的存储浏览器

或者，您可以从 `aws-amplify` GitHub 存储库中最新版本的 `aws-amplify/ui-react-storage` 和 `aws-amplify` 软件包安装适用于 S3 的存储浏览器，以便开始将存储浏览器集成到现有应用程序中。安装适用于 S3 的存储浏览器时，请务必将以下依赖项添加到您的 `package.json` 文件中：

```
"dependencies": {
    "aws-amplify/ui-react-storage": "latest",
    "aws-amplify": "latest",
  }
```

或者，您可以使用 Node Package Manager（NPM）添加依赖项：

```
npm i --save @aws-amplify/ui-react-storage aws-amplify
```

# 设置适用于 S3 的存储浏览器

要将最终用户与 Amazon S3 位置 相连，您必须先设置身份验证和授权方法。使用存储浏览器设置身份验证和授权方法有三种方法：

- 方法 1：管理客户和第三方合作伙伴的数据访问权限
- 方法 2：管理您 Amazon 账户的 IAM 主体的数据访问权限
- 方法 3：大规模管理数据访问权限

## 方法 1：管理客户和第三方合作伙伴的数据访问权限

使用此方法，您可以使用 Amazon Amplify Auth 来管理文件的访问控制和安全性。当您想将客户或第三方合作伙伴与 S3 中的数据相连时，此方法非常适合。使用此选项，您的客户可以使用社交或企业身份提供者进行身份验证。

您可以将 Amazon Amplify Auth 与配置为使用 Amplify Storage 的 S3 存储桶结合使用，来向最终用户和第三方合作伙伴提供 IAM 凭证。Amazon AmplifyAuth 建立在 Amazon Cognito 的基础上，Amazon Cognito 是一项完全托管式客户身份和访问管理服务，其中，您可以通过内置的用户目录或企业目录或使用者身份提供者对用户进行身份验证和授权。Amplify 授权模型定义了当前经过身份验证的用户可以访问哪些前缀。有关如何为 Amazon Amplify 设置授权的更多信息，请参阅 Set up storage。

要使用 Amplify 身份验证和存储方法初始化组件，请将以下代码段添加到您的 Web 应用程序中：

```
import {
  createAmplifyAuthAdapter,
  createStorageBrowser,
} from '@aws-amplify/ui-react-storage/browser';
import "@aws-amplify/ui-react-storage/styles.css";

import config from './amplify_outputs.json';

Amplify.configure(config);

export const { StorageBrowser } = createStorageBrowser({
  config: createAmplifyAuthAdapter(),
});
```

### 方法 2：管理您 Amazon 账户的 IAM 主体的数据访问权限

如果您想直接管理 IAM 主体或您 Amazon Web Services 账户的访问权限，则可以创建一个有权调用 GetDataAccess S3 API 操作的 IAM 角色。要进行此设置，您必须创建一个 S3 访问权限管控实例，来将 S3 通用存储桶和前缀的权限映射到指定的 IAM 身份。然后，存储浏览器组件（必须在获取 IAM 凭证后在客户端上调用此组件）将调用 ListCallerAccessGrants S3 API 操作，来获取对身份请求者的可用授权，并在组件中填充位置。在您获得 `s3:GetDataAccess` 权限后，存储浏览器组件将使用这些凭证来请求对 S3 的数据访问权限。

```
import {
  createManagedAuthAdapter,
  createStorageBrowser,
} from '@aws-amplify/ui-react-storage/browser';
import "@aws-amplify/ui-react-storage/styles.css";

export const { StorageBrowser } = createStorageBrowser({
  config: createManagedAuthAdapter({
    credentialsProvider: async (options?: { forceRefresh?: boolean }) => {
      // return your credentials object
```

```
      return {
        credentials: {
          accessKeyId: 'my-access-key-id',
          secretAccessKey: 'my-secret-access-key',
          sessionToken: 'my-session-token',
          expiration: new Date()
        },
      }
    },
    // AWS `region` and `accountId`
    region: '',
    accountId: '',
    // call `onAuthStateChange` when end user auth state changes
    // to clear sensitive data from the `StorageBrowser` state
    registerAuthListener: (onAuthStateChange) => {},
  })
});
```

### 方法 3：大规模管理数据访问权限

如果您想将 S3 访问权限管控实例与 IAM Identity Center 关联，以获得更具可扩展性的解决方案（例如向整个公司提供数据访问权限），则可以代表当前经过身份验证的用户从 Amazon S3 请求数据。例如，您可以向公司目录中的用户组授予访问 S3 中数据的权限。这种方法可让您集中管理用户和组的 S3 访问权限管控权限，包括托管在外部提供商（例如 Microsoft Entra、Okta 等）上的用户和组的权限。

使用此方法时，integration with the IAM Identity Center 可让您使用现有的用户目录。IAM Identity Center 可信身份传播的另一个好处是：Amazon S3 的每个 Amazon CloudTrail 数据事件均包含对访问 S3 数据的最终用户身份的直接引用。

如果您的应用程序支持 OAuth 2.0，并且用户需要从这些应用程序访问 Amazon 服务，建议您使用可信身份传播。通过可信身份传播，用户可以登录应用程序，而该应用程序可以在任何旨在访问 Amazon 服务中数据的请求中传递用户的身份。此应用程序代表任何经过身份验证的用户与 IAM Identity Center 进行交互。有关更多信息，请参阅 Using trusted identity propagation with customer managed applications。

#### 设置

要在 Amazon Web Services Management Console中使用 S3 访问权限管控和 IAM Identity Center trusted identity propagation 设置存储浏览器身份验证，应用程序必须代表当前经过身份验证的用户从

Amazon S3 请求数据。通过这种方法，您可以为公司目录中的用户或用户组提供对 S3 存储桶、前缀或对象的直接访问权限。这意味着您的应用程序无需将任何用户映射到 IAM 主体。

以下工作流程概述了使用 IAM Identity Center 和 S3 访问权限管控来设置适用于 S3 的存储浏览器的步骤：

| 步骤 | 描述 |
| --- | --- |
| 1 | 为您的 Amazon Organizations 启用 IAM Identity Center |
| 2 | 配置 Amazon Identity and Access Management Identity Center 联合身份验证 |
| 3 | 在 Amazon Identity and Access Management Identity Center 控制台中添加可信令牌发布者<br><br>可信令牌发布者表示您在 IAM Identity Center 中的身份提供者（IdP），同时使其能够识别您的应用程序经过身份验证的用户的身份令牌。 |
| 4 | 为 `bootstrap  应用程序和 identity  bearer` 创建 IAM 角色 |
| 5 | 在 IAM Identity Center 中创建和配置应用程序<br><br>此应用程序代表经过身份验证的用户与 IAM Identity Center 进行交互。 |
| 6 | 将 S3 访问权限管控添加为身份传播的可信应用程序<br><br>此步骤将您的应用程序连接到 S3 访问权限管控，以便它可以代表经过身份验证的用户向 S3 访问权限管控提出请求。 |
| 7 | 创建对用户或组的授权<br><br>此步骤将 Amazon Identity and Access Management Identity Center 中的用户与跨域身份管理系统（SCIM）同步。SCIM 使您的 IAM Identity Center 身份与身份提供者（IdP）的身份保持同步。 |
| 8 | 创建适用于 S3 的存储浏览器组件 |

为您的 Amazon Organizations 启用 IAM Identity Center

要为您的 Amazon Organizations 启用 IAM Identity Center，请执行以下步骤：

1. 使用以下方法之一登录 Amazon Web Services Management Console：
   1. Amazon 新用户（根用户）：通过选择根用户并输入您的 Amazon Web Services 账户电子邮件地址，以账户所有者身份登录。在下一页，输入您的密码。
   2. 已经在使用 Amazon（IAM 凭证）：使用具有管理权限的 IAM 凭证登录。
2. 打开 IAM Identity Center 控制台。
3. 在启用 IAM Identity Center下，选择启用。

   > **Note**
   >
   > IAM Identity Center 要求设置 Amazon Organizations。如果您未设置组织，则可以选择让 Amazon 自动为您创建一个组织。选择创建 Amazon 组织完成此过程。

4. 然后选择使用 Amazon Organizations 启用。
5. 选择继续。
6. （可选）添加要与此组织实例关联的任何标签。
7. （可选）配置委托管理。

   > **Note**
   >
   > 如果您正在使用多账户环境，我们建议您配置委托管理。通过委托管理，您可以限制 Amazon Organizations 中需要访问管理帐户的人数。有关更多信息，请参阅 Delegated administration。

8. 选择保存。

Amazon Organizations 会自动向与管理帐户关联的地址发送验证电子邮件。在您接收到验证电子邮件之前可能会有一段延迟。请确保在验证电子邮件到期之前 24 小时内验证电子邮件地址。

配置 Amazon Identity and Access Management Identity Center 联合身份验证

要将适用于 S3 的存储浏览器用于公司目录用户，您必须将 IAM Identity Center 配置为使用外部身份提供者（IdP）。您可以使用您选择的首选身份提供者。但请注意，每个身份提供者使用不同的配置设置。有关使用不同外部身份提供者的教程，请参阅 IAM Identity Center source tutorials。

> **Note**
>
> 请务必记录您配置的身份提供者的发布者 URL 和受众属性，因为您需要在后续步骤中引用它。如果您没有配置 IdP 所需的访问权限，则可能需要联系外部 IdP 的管理员来获取访问权限。

在 Amazon Identity and Access Management Identity Center 控制台中添加可信令牌发布者

可信令牌发布者在 Amazon Identity and Access Management Identity Center 中表示外部身份提供者，并识别应用程序经过身份验证的用户的令牌。您的 Amazon Organizations 中 IAM Identity Center 实例的账户所有者必须执行这些步骤。这些步骤可以在 IAM Identity Center 控制台中完成，也可以通过编程方式完成。

要在 Amazon Identity and Access Management Identity Center 控制台中添加可信令牌发布者，请执行以下步骤：

1. 打开 IAM Identity Center 控制台。
2. 选择设置。
3. 选择身份验证选项卡。
4. 导航至可信令牌发布者部分，并填写以下详细信息：
    1. 在发布者 URL 下，输入作为可信令牌发布者的外部 IdP 的 URL。您可能需要联系外部 IdP 的管理员以获取此信息。有关更多信息，请参阅 Using applications with a trusted token issuer。
    2. 在可信令牌发布者名称下，输入可信令牌发布者的名称。当为身份传播配置应用程序资源时，该名称将出现在您可以在步骤 8 中选择的可信令牌发布者列表中。
5. 将映射属性更新为首选应用程序属性，其中每个身份提供者属性都映射到一个 IAM Identity Center 属性。例如，您可能希望 map the application attribute `email` 到 IAM Identity Center 用户属性 `email`。要查看 IAM Identity Center 中支持的用户属性列表，请参阅 Attribute mappings for Amazon Managed Microsoft AD directory 中的表。
6. （可选）如果要添加资源标签，请输入键和值对。要添加多个资源标签，请选择添加新标签以生成新条目并输入键和值对。
7. 选择创建可信令牌发布者。
8. 创建完可信令牌发布者后，请联系应用程序管理员，告知他们可信令牌发布者的名称，以便他们可以确认可信令牌发布者在适用的控制台中可见。

9. 确保应用程序管理员在适用的控制台中选择此可信令牌发布者，才能允许用户从为可信身份传播配置的应用程序中访问该应用程序。

### 为 **bootstrap** 应用程序和 **identity bearer** 创建 IAM 角色

为确保 bootstrap 应用程序和 identity bearer 用户可以正常相互协作，请务必 create two IAM roles。bootstrap 应用程序需要一个 IAM 角色，而另一个 IAM 角色必须用于身份持有者，或访问通过 S3 访问权限管控请求访问权限的 Web 应用程序的最终用户。bootstrap 应用程序接收身份提供者颁发的令牌并调用 CreateTokenWithIAM API，同时将此令牌与 Identity Center 发布的令牌交换。

创建具有如下权限的 IAM 角色，例如 bootstrap-role。以下示例 IAM 策略向 bootstrap-role 授予执行令牌交换的权限：

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": [
            "sso-oauth:CreateTokenWithIAM",
        ],
        "Resource": "arn:${Partition}:sso::${AccountId}:application/${InstanceId}/
${ApplicationId}",
        "Effect": "Allow"
    },
    {
        "Action": [
            "sts:AssumeRole",
            "sts:SetContext"
        ],
        "Resource": "arn:aws:iam::${AccountId}:role/identity-bearer-role",
        "Effect": "Allow"
    }]
}
```

然后，创建第二个 IAM 角色（例如 identity-bearer-role），身份凭证代理程序使用该角色生成 IAM 凭证。适用于 S3 的存储浏览器组件使用从身份凭证代理程序返回到 Web 应用程序的 IAM 凭证来支持访问 S3 数据：

```
{
    "Action": [
        "s3:GetDataAccess",
```

```
            "s3:ListCallerAccessGrants",
        ],
        "Resource": "arn:${Partition}:s3:${Region}:${Account}:access-grants/default",
        "Effect": "Allow"
}
```

此 IAM 角色 (`identity-bearer-role`) 必须使用带有以下语句的信任策略：

```
{
   "Effect": "Allow",
   "Principal": {
      "AWS": "arn:${Partition}:iam::${Account}:role/${RoleNameWithPath}"
   },
   "Action": [
       "sts:AssumeRole",
       "sts:SetContext"
   ]
}
```

在 IAM Identity Center 中创建和配置应用程序

> **Note**
>
> 开始之前，请确保您已在上一步中创建所需的 IAM 角色。您需要在此步骤中指定其中一个 IAM 角色。

要在 Amazon IAM Identity Center 中创建和配置客户托管式应用程序，请执行以下步骤：

1. 打开 IAM Identity Center 控制台。
2. 选择应用程序。
3. 选择客户托管选项卡。
4. 选择添加应用程序。
5. 在选择应用程序类型页面，选择设置首选项下的我有想设置的应用程序。
6. 在应用程序类型下，选择 OAuth 2.0。
7. 选择下一步。将显示指定应用程序页面。
8. 在应用程序名称和描述部分下，输入应用程序的显示名称，如 **`storage-browser-oauth`**。

9. 输入 Description（描述）。应用程序描述显示在 IAM Identity Center 控制台和 API 请求中，但不显示在 Amazon 访问门户中。
10. 在用户和组分配方法下，选择不需要分配。此选项可让所有经授权的 IAM Identity Center 用户和组访问此应用程序。
11. 在 Amazon 访问门户下，输入用户可以访问应用程序的应用程序 URL。
12. （可选）如果要添加资源标签，请输入键和值对。要添加多个资源标签，请选择添加新标签以生成新条目并输入键和值对。
13. 选择下一步。将显示指定身份验证页面。
14. 在使用可信令牌发布者进行身份验证下，使用复选框选择您之前创建的可信令牌发布者。
15. 在配置选定的可信令牌发布者下，输入 Aud 声明。Aud 声明标识 JSON Web 令牌（JWT）的受众，它是可信令牌发布者用来标识此应用程序的名称。

    > **Note**
    >
    > 您可能需要联系外部 IdP 的管理员以获取此信息。

16. 选择下一步。将显示指定身份验证凭证页面。
17. 在配置方法下，选择输入一个或多个 IAM 角色。
18. 在输入 IAM 角色下，为身份持有者令牌添加 IAM 角色或 Amazon 资源名称（ARN）。您必须输入您在上一步中为身份凭证代理程序应用程序创建的 IAM 角色（例如 **`bootstrap-role`**）。
19. 选择下一步。
20. 在查看和配置页面上，检查应用程序配置的详细信息。如果您需要修改任何设置，请对于要编辑和进行更改的部分选择编辑。
21. 选择提交。将显示您刚添加的应用程序的详细信息页面。

设置应用程序后，您的用户可以基于 permission sets that you've created 和 user access that you've assigned，从其 Amazon 访问门户中访问您的应用程序。

将 S3 访问权限管控添加为身份传播的可信应用程序

设置客户托管式应用程序后，您必须为身份传播指定 S3 访问权限管控。S3 访问权限管控提供凭证供用户访问 Amazon S3 数据。当您登录到客户托管式应用程序时，S3 访问权限管控会将您的用户身份传递给可信应用程序。

先决条件：在执行这些步骤之前，请确保您已设置 S3 访问权限管控（例如创建 S3 访问权限管控实例和注册位置）。有关更多信息，请参阅开始使用 S3 访问权限管控。

要向客户托管式应用程序中添加用于身份传播的 S3 访问权限管控，请执行以下步骤：

1. 打开 IAM Identity Center 控制台。
2. 选择应用程序。
3. 选择客户托管选项卡。
4. 在客户托管的应用程序列表中，选择要对其发起访问请求的 OAuth 2.0 应用程序。这是用户将登录的应用程序。
5. 在详细信息页面的用于身份传播的可信应用程序下，选择指定可信应用程序。
6. 在设置类型下，选择单个应用程序并指定访问权限，然后选择下一步。
7. 在选择服务页面上，选择 S3 访问权限管控。S3 访问权限管控具有的应用程序可供您定义您自己的 Web 应用程序以实现可信身份传播。
8. 选择下一步。您将在下一个步骤中选择应用程序。
9. 在选择应用程序页面，选择单个应用程序，对于每个可以接收访问请求的应用程序选中此复选框，然后选择下一步。
10. 在配置访问权限页面的配置方法下，选择以下任一项：
    - 选择每个应用程序的访问权限 - 选择此选项可为每个应用程序配置不同的访问权限级别。选择要为其配置访问权限级别的应用程序，然后选择编辑访问权限。在要应用的访问权限级别中，根据需要更改访问权限级别，然后选择保存更改。
    - 对所有应用程序应用相同的访问权限级别：如果不需要针对每个应用程序配置访问权限级别，请选择此选项。
11. 选择下一步。
12. 在审查配置页面中，审查您所做的选择。

> **Note**
>
> 您希望确保已向您的用户授予 `s3:access_grants:read_write` 权限。此权限使您的用户能够检索凭证以访问 Amazon S3。请务必使用您之前创建的 IAM 策略或 S3 访问权限管控，来限制对写入操作的访问权限。

13. 要进行更改，请为要更改的配置部分选择编辑。然后，进行所需的更改并选择保存更改。
14. 选择可信应用程序以添加用于身份传播的可信应用程序。

创建对用户或组的授权

在此步骤中，您将使用 IAM Identity Center 来预置您的用户。您可以使用 SCIM 来 automated or manual provisioning of users and groups。SCIM 使您的 IAM Identity Center 身份与身份提供者（IdP）的身份保持同步。这包括 IdP 和 IAM Identity Center 之间的任何用户预置、更新和取消预置。

> **Note**
>
> 此步骤是必需的，因为在将 S3 访问权限管控与 IAM Identity Center 结合使用时，不使用本地 IAM Identity Center 用户。相反，用户必须从身份提供者与 IAM Identity Center 同步。

要将来自身份提供者的用户与 IAM Identity Center 同步，请执行以下步骤：

1. Enable automatic provisioning。
2. Generate an access token。

有关如何针对您的特定应用场景使用 IAM Identity Center 设置身份提供者的示例，请参阅 IAM Identity Center Identity source tutorials。

创建适用于 S3 的存储浏览器组件

设置 IAM Identity Center 实例并在 S3 访问权限管控中创建授权后，打开您的 React 应用程序。在 React 应用程序中，使用 `createManagedAuthAdapter` 来设置授权规则。您必须提供凭证提供商，才能返回您从 IAM Identity Center 获得的凭证。然后，您可以调用 `createStorageBrowser` 来初始化适用于 S3 的存储浏览器组件：

```
import {
    createManagedAuthAdapter,
    createStorageBrowser,
} from '@aws-amplify/ui-react-storage/browser';
import '@aws-amplify/ui-react-storage/styles.css';

export const { StorageBrowser } = createStorageBrowser({
   config: createManagedAuthAdapter({
    credentialsProvider: async (options?: { forceRefresh?: boolean }) => {
      // return your credentials object
      return {
        credentials: {
          accessKeyId: 'my-access-key-id',
          secretAccessKey: 'my-secret-access-key',
```

```
          sessionToken: 'my-session-token',
          expiration: new Date(),
        },
      }
    },
    // AWS `region` and `accountId` of the S3 Access Grants Instance.
    region: '',
    accountId: '',
    // call `onAuthStateChange` when end user auth state changes
    // to clear sensitive data from the `StorageBrowser` state
    registerAuthListener: (onAuthStateChange) => {},
  })
});
```

接着，创建一种机制，将 Web 应用程序中的 JSON Web 令牌（JWT）与 IAM Identity Center 中的 IAM 凭证交换。有关如何交换 JWT 的更多信息，请参阅以下资源：

- Amazon 存储博客 中的 How to develop a user-facing data application with IAM Identity Center and S3 Access Grants 博文
- Amazon 存储博客 中的 Scaling data access with S3 Access Grants 博文
- Amazon 讲习会参与平台 上的 S3 Access Grants workshop
- GitHub 上的 S3 Access Grants workshop

然后，设置 API 端点来处理获取凭证的请求。要验证 JSON Web 令牌（JWT）交换，请执行以下步骤：

1. 从授权标头中检索传入请求的 JSON Web 令牌。
2. 使用指定的 JSON Web 密钥集（JWKS）URL 中的公有密钥验证令牌。
3. 验证令牌的到期时间、发布者、主体和受众声明。

要将身份提供者的 JSON Web 令牌与 Amazon IAM 凭证交换，请执行以下步骤：

> **Tip**
>
> 确保避免记录任何敏感信息。对于缺少授权、令牌过期和其它异常，我们建议您使用错误处理控件。有关更多信息，请参阅 Amazon 计算博客 中的 Implementing Amazon Lambda error handling patterns 博文。

1. 验证请求中是否提供了所需的权限和范围参数。
2. 使用 CreateTokenWithIAM API 将 JSON Web 令牌交换为 IAM Identity Center 令牌。

> **Note**
>
> 使用 IdP JSON Web 令牌后，无法再次使用该令牌。必须使用新令牌与 IAM Identity Center 进行交换。

3. 使用 AssumeRole API 操作通过 IAM Identity Center 令牌代入临时角色。请务必使用身份持有者角色，也称为携带身份上下文的角色（例如 **`identity-bearer-role`**），来请求凭证。
4. 将 IAM 凭证返回给 Web 应用程序。

> **Note**
>
> 确保您已设置了正确的日志记录机制。响应以带有相应 HTTP 状态代码的标准化 JSON 格式返回。

## 配置适用于 S3 的存储浏览器

为了支持适用于 S3 的存储浏览器访问 S3 存储桶，存储浏览器组件会对 Amazon S3 进行 REST API 调用。默认情况下，S3 存储桶上未启用跨源资源共享（CORS）。因此，您必须为存储浏览器从中访问数据的每个 S3 存储桶启用 CORS。

例如，要在 S3 存储桶上启用 CORS，可以按如下方式更新 CORS 策略：

```
[
    {
        "ID": "S3CORSRuleId1",
        "AllowedHeaders": [
            "*"
        ],
        "AllowedMethods": [
            "GET",
            "HEAD",
            "PUT",
            "POST",
            "DELETE"
        ],
        "AllowedOrigins": [
```

```
            "*"
        ],
        "ExposeHeaders": [
            "last-modified",
            "content-type",
            "content-length",
            "etag",
            "x-amz-version-id",
            "x-amz-request-id",
            "x-amz-id-2",
            "x-amz-cf-id",
            "x-amz-storage-class",
            "date",
            "access-control-expose-headers"
        ],
        "MaxAgeSeconds": 3000
    }
]
```

## 适用于 S3 的存储浏览器故障排除

如果您在使用适用于 S3 的存储浏览器时遇到问题，请务必查看以下故障排除提示：

- 避免尝试对多个请求使用相同的令牌（`idToken` 或 `accessToken`）。无法重用令牌。这将导致请求失败。
- 确保您提供给存储浏览器组件的 IAM 凭证包含调用 `s3:GetDataAccess` 操作的权限。否则，最终用户将无法访问您的数据。

或者，您可以检查以下资源：

- 适用于 S3 的存储浏览器由 Amazon Support 提供支持。如果您需要帮助，请联系 Amazon Support Center。
- 如果您在使用适用于 S3 的存储浏览器时遇到问题或想提交反馈，请访问 Amplify GitHub page。
- 如果您在该项目中发现潜在的安全问题，您可以通过 Amazon 漏洞报告页面通知 Amazon 安全部门。

# 使用 Amazon S3 Transfer Acceleration 配置快速、安全的文件传输

Amazon S3 Transfer Acceleration 是一项存储桶级别功能，可在您的客户端和 S3 通用存储桶之间实现快速、轻松、安全的远距离文件传输。Transfer Acceleration 旨在优化从世界各地传入 S3 通用存储桶的传输速度。Transfer Acceleration 利用 Amazon CloudFront 中的全球分布式边缘站点。当数据到达某个边缘站点时，数据会被经过优化的网络路径路由至 Amazon S3。

使用 Transfer Acceleration 时，可能会收取额外的数据传输费用。有关定价的更多信息，请参阅 Amazon S3 定价。

## 为什么要使用 Transfer Acceleration？

您可能出于各种原因需要对通用存储桶使用 Transfer Acceleration：

- 您位于全球各地的客户需要上传到集中式通用存储桶。
- 您定期跨大洲传输数 GB 至数 TB 数据。
- 您在上传到 Amazon S3 时无法充分利用 Internet 上的所有可用带宽。

有关何时使用 Transfer Acceleration 的更多信息，请参阅 Amazon S3 常见问题解答。

## 使用 Transfer Acceleration 的要求

在 S3 存储桶上使用 Transfer Acceleration 时，需要执行以下操作：

- 仅虚拟托管样式请求支持 Transfer Acceleration。有关虚拟托管样式请求的更多信息，请参阅《Amazon S3 API 参考》中的 Making requests using the REST API。
- 用于 Transfer Acceleration 的存储桶的名称必须符合 DNS 标准，且不得包含句点（“.”）。
- 必须在存储桶上启用 Transfer Acceleration。有关更多信息，请参阅 启用和使用 S3 Transfer Acceleration。

  在对存储桶启用 Transfer Acceleration 后，可能需要最多 20 分钟的时间才能加快向存储桶传输数据的速度。

> **Note**
>
> 位于以下区域的存储桶目前支持 Transfer Acceleration：
>
> - 亚太地区（东京）(ap-northeast-1)

  - 亚太地区（首尔）(ap-northeast-2)
  - 亚太地区（孟买）(ap-south-1)
  - 亚太地区（新加坡）(ap-southeast-1)
  - 亚太地区（悉尼）(ap-southeast-2)
  - 加拿大（中部）(ca-central-1)
  - 欧洲地区（法兰克福）(eu-central-1)
  - 欧洲地区（爱尔兰）(eu-west-1)
  - 欧洲（伦敦）(eu-west-2)
  - 欧洲地区（巴黎）（eu-west-3）
  - 南美洲（圣保罗）（sa-east-1）
  - 美国东部（弗吉尼亚州北部）(us-east-1)
  - 美国东部（俄亥俄州）(us-east-2)
  - 美国西部（加利福尼亚北部）(us-west-1)
  - 美国西部（俄勒冈州）(us-west-2)

- 要访问已启用 Transfer Acceleration 的存储桶，您必须使用端点 *bucket-name*.s3-accelerate.amazonaws.com。或者使用双堆栈端点 *bucket-name*.s3-accelerate.dualstack.amazonaws.com，以通过 IPv6 连接至启用的存储桶。您可以继续使用常规端点进行标准数据传输。
- 您必须是存储桶拥有者才能设置传输加速状态。存储桶拥有者可以向其他用户分配权限，使他们能够对存储桶设置加速状态。s3:PutAccelerateConfiguration 权限允许用户对存储桶启用或禁用 Transfer Acceleration。s3:GetAccelerateConfiguration 权限允许用户返回存储桶的 Transfer Acceleration 状态，即 Enabled 或 Suspended.。

以下各节介绍了如何开始使用 Amazon S3 Transfer Acceleration 传输数据。

主题

- 开始使用 Amazon S3 Transfer Acceleration
- 启用和使用 S3 Transfer Acceleration
- 使用 Amazon S3 Transfer Acceleration 速度比较工具

# 开始使用 Amazon S3 Transfer Acceleration

您可以使用 Amazon S3 Transfer Acceleration 在您的客户端和 S3 存储桶之间进行快速、轻松、安全的远距离文件传输。Transfer Acceleration 使用 Amazon CloudFront 中的全球分布式边缘站点。当数据到达某个边缘站点时，数据会被经过优化的网络路径路由至 Amazon S3。

要开始使用 Amazon S3 Transfer Acceleration，请执行以下步骤：

1. 在存储桶上启用 Transfer Acceleration

   您可以通过以下任一方式对存储桶启用 Transfer Acceleration：

   - 使用 Amazon S3 控制台。
   - 使用 REST API PutBucketAccelerateConfiguration 操作。
   - 使用 Amazon CLI 和 Amazon SDK。有关更多信息，请参阅《Amazon S3 API 参考》中的 Developing with Amazon S3 using the Amazon SDKs。

   有关更多信息，请参阅 启用和使用 S3 Transfer Acceleration。

   > **Note**
   >
   > 对于要使用传输加速的存储桶，存储桶名称必须符合 DNS 命名要求，且不得包含句点 (.)。

2. 在启用加速的存储桶之间传输数据

   使用以下 `s3-accelerate` 端点域名之一：

   - 要访问启用加速的存储桶，请使用 *`bucket-name`*`.s3-accelerate.amazonaws.com`。
   - 要通过 IPv6 访问启用了加速的存储桶，请使用*`bucket-name`*`.s3-accelerate.dualstack.amazonaws.com`。

     Amazon S3 双堆栈端点支持通过 IPv6 和 IPv4 向 S3 存储桶发出请求。Transfer Acceleration 双堆栈端点仅可使用端点名称的虚拟托管类型。有关更多信息，请参阅《Amazon S3 API 参考》中的 Making requests to Amazon S3 over IPv6 和《Amazon S3 API 参考》中的 Using Amazon S3 dual-stack endpoints。

   > **Note**
   >
   > 您的数据传输应用程序必须使用以下两种类型的端点之一来访问存储桶以加快数据传输：`.s3-accelerate.amazonaws.com`，或 `.s3-`

`accelerate.dualstack.amazonaws.com` 用于双栈端点。如果您想使用标准数据传输，则可以继续使用常规端点。

在启用 Transfer Acceleration 后，可以将 Amazon S3 PUT 对象和 GET 对象请求指向 `s3-accelerate` 端点域名。例如，假设您当前有一个使用 PutObject 的 REST API 应用程序，该应用程序在 PUT 请求中使用主机名 *amzn-s3-demo-bucket*`.s3.us-east-1.amazonaws.com`。要加速 PUT，请将请求中的主机名更改为 *amzn-s3-demo-bucket*`.s3-accelerate.amazonaws.com`。要重新使用标准上传速度，请将名称更改回 *amzn-s3-demo-bucket*`.s3.us-east-1.amazonaws.com`。

启用 Transfer Acceleration 后，最多 20 分钟后即可实现性能提升。但是，一旦启用 Transfer Acceleration，加速端点将随即可用。

您可以在 Amazon CLI、Amazon SDK 和其他向 Amazon S3 传入数据和从 Amazon S3 传出数据的工具中使用加速端点。如果您使用 Amazon SDK，则某些受支持的语言会使用加速端点客户端配置标记，这样一来，您便无需显式将 Transfer Acceleration 的端点设置为 *bucket-name*`.s3-accelerate.amazonaws.com`。有关如何使用加速端点客户端配置标记的示例，请参阅启用和使用 S3 Transfer Acceleration。

您可以通过传输加速端点使用所有的 Amazon S3 操作，除以下情况以外：

- ListBuckets
- CreateBucket
- DeleteBucket

此外，Amazon S3 Transfer Acceleration 不支持使用 CopyObject 进行跨区域复制。

## 启用和使用 S3 Transfer Acceleration

可以使用 Amazon S3 Transfer Acceleration 在客户端和 S3 通用存储桶之间进行快速、安全的远距离文件传输。您可以使用 S3 控制台、Amazon Command Line Interface（Amazon CLI）、API 或 Amazon SDK 启用 Transfer Acceleration。

本节提供了有关如何对存储桶启用 Amazon S3 Transfer Acceleration 和对启用的存储桶使用加速端点的示例。

有关 Transfer Acceleration 要求的更多信息，请参阅使用 Amazon S3 Transfer Acceleration 配置快速、安全的文件传输。

使用 S3 控制台

> **Note**
>
> 如果要比较加快的上传速度与未加快的上传速度，请打开 Amazon S3 Transfer Acceleration 速度比较工具。
> 此速度比较工具使用分段上传来将文件从浏览器传输到各种使用和未使用 Amazon S3 Transfer Acceleration 的 Amazon Web Services 区域。您可以比较直接上传和按区域传输加速上传的上传速度。

为 S3 通用存储桶启用传输加速

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在通用存储桶列表中，选择要为其启用加速传输的存储桶的名称。
4. 选择属性。
5. 在 Transfer acceleration (传输加速) 下，选择 Edit (编辑)。
6. 选择 Enable（启用），然后选择 Save changes（保存更改）。

要访问加速数据传输

1. 在 Amazon S3 为您的存储桶启用传输加速后，查看存储桶的 Properties（属性）选项卡。
2. 在 Transfer acceleration（传输加速）下，Accelerated endpoint（加速端点）显示存储桶的传输加速端点。使用此端点访问与存储桶之间的加速数据传输。

   如果您暂停传输加速，加速端点不再起作用。

使用 Amazon CLI

以下是用于 Transfer Acceleration 的 Amazon CLI 命令的示例。有关设置 Amazon CLI 的说明，请参阅《Amazon S3 API Reference》中的 Developing with Amazon S3 using the Amazon CLI。

在存储桶上启用 Transfer Acceleration

使用 Amazon CLI put-bucket-accelerate-configuration 命令对存储桶启用或暂停 Transfer Acceleration。

以下示例设置 Status=Enabled，以便对名为 *amzn-s3-demo-bucket* 的存储桶启用 Transfer Acceleration。要暂停 Transfer Acceleration，请使用 Status=Suspended。

Example

```
$ aws s3api put-bucket-accelerate-configuration --bucket amzn-s3-demo-bucket --
accelerate-configuration Status=Enabled
```

使用 Transfer Acceleration

您可以将 s3 和 s3api Amazon CLI 命令发出的所有 Amazon S3 请求定向到加速端点：s3-accelerate.amazonaws.com。为此，请在 Amazon Config 文件的配置文件中将配置值 use_accelerate_endpoint 设置为 true。必须对存储桶启用 Transfer Acceleration 才能使用加速端点。

所有请求都使用存储桶寻址的虚拟风格发送：*amzn-s3-demo-bucket*.s3-accelerate.amazonaws.com。不会将任何 ListBuckets、CreateBucket 和 DeleteBucket 请求发送到加速端点，因为该端点不支持这些操作。

有关 use_accelerate_endpoint 的更多信息，请参阅《Amazon CLI 命令参考》中的 Amazon CLI S3 配置。

以下示例在默认配置文件中将 use_accelerate_endpoint 设置为 true。

Example

```
$ aws configure set default.s3.use_accelerate_endpoint true
```

如果您需要对某些 Amazon CLI 命令使用加速端点，但不对其他此类命令使用加速端点，则可使用以下两种方法中的任一方法：

- 通过将 --endpoint-url 参数设置为 https://s3-accelerate.amazonaws.com，来对任何 s3 或 s3api 命令使用加速端点。
- 在 Amazon Config 文件中设置单独的配置文件。例如，创建一个将 use_accelerate_endpoint 设置为 true 的配置文件和一个不设置 use_accelerate_endpoint 的配置文件。在运行一条命令时，根据是否需要使用加速端点来指定要使用的配置文件。

将对象上传到已启用 Transfer Acceleration 的存储桶

以下示例通过使用已配置为使用加速端点的默认配置文件，来将文件上传到已启用 Transfer Acceleration 的名为 *amzn-s3-demo-bucket* 的存储桶。

Example

```
$ aws s3 cp file.txt s3://amzn-s3-demo-bucket/key-name --region region
```

以下示例通过使用 `--endpoint-url` 参数指定加速端点来将文件上传到已启用 Transfer Acceleration 的存储桶。

Example

```
$ aws configure set s3.addressing_style virtual
$ aws s3 cp file.txt s3://amzn-s3-demo-bucket/key-name --region region --endpoint-url
 https://s3-accelerate.amazonaws.com
```

使用 Amazon SDK

以下是使用 Transfer Acceleration 通过 Amazon SDK 将对象上传到 Amazon S3 的示例。Amazon SDK 支持的某些语言（例如 Java 和 .NET）使用加速端点客户端配置标志，这样一来，您便无需显式将 Transfer Acceleration 的端点设置为 *bucket-name*`.s3-accelerate.amazonaws.com`。

Java

Example

以下示例演示如何使用加速端点将对象上传到 Amazon S3。本示例执行以下操作：

- 创建配置为使用加速端点的 `AmazonS3Client`。客户端访问的所有存储桶都必须已启用 Transfer Acceleration。
- 对指定存储桶启用 Transfer Acceleration。仅当您指定的存储桶尚未启用 Transfer Acceleration 时，此步骤才是必需的。
- 验证是否为指定存储桶启用了传输加速。
- 使用存储桶的加速端点将新对象上传到指定存储桶。

有关使用 Transfer Acceleration 的更多信息，请参阅开始使用 Amazon S3 Transfer Acceleration。有关创建和测试有效示例的说明，请参阅《适用于 Java 的 Amazon SDK 开发人员指南》中的入门。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.BucketAccelerateConfiguration;
import com.amazonaws.services.s3.model.BucketAccelerateStatus;
import com.amazonaws.services.s3.model.GetBucketAccelerateConfigurationRequest;
import com.amazonaws.services.s3.model.SetBucketAccelerateConfigurationRequest;

public class TransferAcceleration {
    public static void main(String[] args) {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String keyName = "*** Key name ***";

        try {
            // Create an Amazon S3 client that is configured to use the accelerate
 endpoint.
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withRegion(clientRegion)
                    .withCredentials(new ProfileCredentialsProvider())
                    .enableAccelerateMode()
                    .build();

            // Enable Transfer Acceleration for the specified bucket.
            s3Client.setBucketAccelerateConfiguration(
                    new SetBucketAccelerateConfigurationRequest(bucketName,
                            new BucketAccelerateConfiguration(
                                    BucketAccelerateStatus.Enabled)));

            // Verify that transfer acceleration is enabled for the bucket.
            String accelerateStatus = s3Client.getBucketAccelerateConfiguration(
                    new GetBucketAccelerateConfigurationRequest(bucketName))
                    .getStatus();
            System.out.println("Bucket accelerate status: " + accelerateStatus);

            // Upload a new object using the accelerate endpoint.
            s3Client.putObject(bucketName, keyName, "Test object for transfer
 acceleration");
```

```
            System.out.println("Object \"" + keyName + "\" uploaded with transfer
 acceleration.");
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

以下示例说明如何使用 适用于 .NET 的 Amazon SDK 对存储桶启用 Transfer Acceleration。有关设置和运行代码示例的信息，请参阅《适用于 .NET 的 Amazon SDK 开发人员指南》中的 Getting Started with the 适用于 .NET 的 Amazon SDK。

Example

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class TransferAccelerationTest
    {
        private const string bucketName = "*** bucket name ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;
        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            EnableAccelerationAsync().Wait();
```

```
        }

        static async Task EnableAccelerationAsync()
        {
                try
                {
                    var putRequest = new PutBucketAccelerateConfigurationRequest
                    {
                        BucketName = bucketName,
                        AccelerateConfiguration = new AccelerateConfiguration
                        {
                            Status = BucketAccelerateStatus.Enabled
                        }
                    };
                    await
 s3Client.PutBucketAccelerateConfigurationAsync(putRequest);

                    var getRequest = new GetBucketAccelerateConfigurationRequest
                    {
                        BucketName = bucketName
                    };
                    var response = await
 s3Client.GetBucketAccelerateConfigurationAsync(getRequest);

                    Console.WriteLine("Acceleration state = '{0}' ",
 response.Status);
                }
                catch (AmazonS3Exception amazonS3Exception)
                {
                    Console.WriteLine(
                        "Error occurred. Message:'{0}' when setting transfer
 acceleration",
                        amazonS3Exception.Message);
                }
        }
    }
}
```

在将对象上传到启用了 Transfer Acceleration 的存储桶时，可指定在创建客户端时使用加速端点。

```
var client = new AmazonS3Client(new AmazonS3Config
            {
                RegionEndpoint = TestRegionEndpoint,
```

```
                UseAccelerateEndpoint = true
            }
```

JavaScript

有关使用适用于 JavaScript 的 Amazon SDK 启用 Transfer Acceleration 的示例，请参阅《适用于 JavaScript 的 Amazon SDK API Reference》中的 PutBucketAccelerateConfiguration command。

Python（Boto）

有关通过使用适用于 Python 的 SDK 启用 Transfer Acceleration 的示例，请参阅《Amazon SDK for Python (Boto3) API Reference》中的 put_bucket_accelerate_configuration。

Other

有关使用其他 Amazon SDK 的信息，请参阅示例代码和库。

使用 REST API

使用 REST API `PutBucketAccelerateConfiguration` 操作在现有存储桶上启用加速配置。

有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 PutBucketAccelerateConfiguration。

## 使用 Amazon S3 Transfer Acceleration 速度比较工具

可以使用 Amazon S3 Transfer Acceleration 速度比较工具来比较各个 Amazon S3 区域内加快的上传速度和未加快的上传速度。此速度比较工具使用分段上传来将文件从浏览器传输到各种使用和未使用 Transfer Acceleration 的 Amazon S3 区域。

可以使用以下任一方法访问此速度比较工具：

- 将以下 URL 复制到浏览器窗口中，同时将 *region* 替换为您正在使用的 Amazon Web Services 区域（例如 `us-west-2`），并将 *amzn-s3-demo-bucket* 替换为您要评估的存储桶的名称：

  `https://s3-accelerate-speedtest.s3-accelerate.amazonaws.com/en/accelerate-speed-comparsion.html?region=`*region*`&origBucketName=`*amzn-s3-demo-bucket*

  有关 Amazon S3 支持的区域列表，请参阅《Amazon Web Services 一般参考》中的 Amazon S3 端点和限额。

- 使用 Amazon S3 控制台。

# 使用申请方付款通用存储桶进行存储传输和使用

通常，存储桶拥有者将支付与他们的存储桶相关联的所有 Amazon S3 存储和数据传输费用。但是，您可以将通用存储桶配置为申请方付款存储桶。使用申请方付款存储桶时，申请方（而不是存储桶拥有者）将支付请求和从存储桶下载数据的费用。存储桶拥有者将始终支付存储数据的费用。

通常情况下，当您想共享数据，而又不希望产生与访问数据等其他操作相关联的费用时，您可以将存储桶配置为申请方付款存储桶。例如，当提供大型数据集（如邮政编码目录、参考数据、地理空间信息或网络爬取数据）时，您可能会使用申请方付款存储桶。

> **Important**
>
> 如果您在通用存储桶上启用了申请方付款，则不支持匿名访问该存储桶。

您必须对涉及申请方付款存储桶的所有请求进行身份验证。请求身份验证使 Amazon S3 能够识别申请方对申请方付款存储桶的使用并对其收费。

当请求者在做出其请求前担任 Amazon Identity and Access Management (IAM) 角色时，该角色所属的账户将负责处理此请求。有关 IAM 角色的更多信息，请参阅《IAM 用户指南》中的 IAM 角色。

在将桶配置为申请方付款桶后，申请方必须表明他们了解请求和数据下载将产生费用。为了表明他们接受这些费用，申请方必须在 DELETE、GET、HEAD、POST 和 PUT 请求的 API 请求中包含 `x-amz-request-payer` 作为标头，或者在其 REST 请求中添加 `RequestPayer` 参数。对于 CLI 请求，申请方可以使用 `--request-payer` 参数。

Example – 删除对象时使用申请方付款

要使用以下 DeleteObjectVersion API 示例，请将 *`user input placeholders`* 替换为您自己的信息。

```
DELETE /Key+?versionId=VersionId HTTP/1.1
Host: Bucket.s3.amazonaws.com
x-amz-mfa: MFA
x-amz-request-payer: RequestPayer
x-amz-bypass-governance-retention: BypassGovernanceRetention
```

```
x-amz-expected-bucket-owner: ExpectedBucketOwner
```

如果申请方使用 RestoreObject API 还原对象，则只要请求中包含 `x-amz-request-payer` 标头或 `RequestPayer` 参数，就会支持申请方付款；但是，申请方只需支付请求的费用。检索费用由桶拥有者支付。

申请方付款存储桶不支持以下内容：

- 匿名申请
- SOAP 请求
- 将申请方付款存储桶用作最终用户日志记录的目标存储桶，反之亦然。但是，当目标存储桶不是申请方付款存储桶时，您可以在申请方付款存储桶上开启最终用户日志记录。

## 申请方付款的费用支付方式

成功的申请方付款请求费用简单明了：申请方支付数据传输和请求方面的费用；存储桶拥有者支付数据存储方面的费用。但是，在以下条件下会对存储桶拥有者收取请求费用：

- 该请求返回 `AccessDenied`（HTTP `403 Forbidden`）错误，并且该请求是在存储桶拥有者的个人 Amazon 账户或 Amazon 组织内发起的。
- 请求是 SOAP 请求。

有关申请方付款的更多信息，请参阅以下主题。

主题

- 在存储桶上配置申请方付款
- 使用 REST API 检索 requestPayment 配置
- 从申请方付款桶中下载对象

## 在存储桶上配置申请方付款

您可以将 Amazon S3 存储桶配置为申请方付款存储桶，以便请求者而不是存储桶拥有者支付请求和数据下载费用。

本节提供了演示如何使用控制台和 REST API 在 Amazon S3 存储桶上配置申请方付款的示例。

使用 S3 控制台

为 S3 通用存储桶启用申请方付款

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在通用存储桶列表中，选择要为其启用申请方付款的存储桶的名称。
4. 选择属性。
5. 在 Requester pays (申请方付款) 下，选择 Edit (编辑)。
6. 选择 Enable (启用)，然后选择 Save changes (保存更改)。

   Amazon S3 为存储桶启用申请方付款，并显示 Bucket overview（存储桶概述）。在 Requester pays (申请方付款) 下，您将看到 Enabled (已启用)。

使用 REST API

只有存储桶拥有者才能将存储桶的 `RequestPaymentConfiguration.payer` 配置值设置为 `BucketOwner`（默认值）或 `Requester`。设置 `requestPayment` 资源是可选的。默认情况下，存储桶不是申请方付款存储桶。

要将申请方付款存储桶恢复为常规存储桶，请使用值 `BucketOwner`。通常情况下，在将数据上传到 Amazon S3 存储桶时，您将使用 `BucketOwner`，然后将值设置为 `Requester`，才能在该存储桶中发布对象。

设置 requestPayment 的步骤

- 使用 PUT 请求在指定存储桶上将 `Payer` 值设置为 `Requester`。

```
PUT ?requestPayment HTTP/1.1
Host: [BucketName].s3.amazonaws.com
Content-Length: 173
Date: Wed, 01 Mar 2009 12:00:00 GMT
Authorization: AWS [Signature]

<RequestPaymentConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
<Payer>Requester</Payer>
</RequestPaymentConfiguration>
```

如果请求成功，Amazon S3 将返回类似于以下内容的请求。

```
HTTP/1.1 200 OK
x-amz-id-2: [id]
x-amz-request-id: [request_id]
Date: Wed, 01 Mar 2009 12:00:00 GMT
Content-Length: 0
Connection: close
Server: AmazonS3
x-amz-request-charged:requester
```

您只能在存储桶级别设置申请方付款。您无法为存储桶中的特定对象设置申请方付款。

您可以随时将存储桶配置为 `BucketOwner` 或 `Requester`。但是，新配置值可能需要几分钟才能生效。

> **Note**
>
> 在将存储桶配置为申请方付款之前，分发预签名 URL 的存储桶拥有者应当再三考虑，尤其是在 URL 的生命周期非常长时更应如此。在每次申请方使用预签名 URL（使用存储桶拥有者的凭证）时，会向存储桶拥有者收取费用。

## 使用 REST API 检索 requestPayment 配置

您可以通过请求资源 `Payer` 来确定在存储桶上设置的 `requestPayment` 值。

返回 requestPayment 资源的步骤

- 使用 GET 请求来获取 `requestPayment` 资源，如以下请求所示。

  ```
  GET ?requestPayment HTTP/1.1
  Host: [BucketName].s3.amazonaws.com
  Date: Wed, 01 Mar 2009 12:00:00 GMT
  Authorization: AWS [Signature]
  ```

如果请求成功，Amazon S3 将返回类似于以下内容的请求。

```
HTTP/1.1 200 OK
x-amz-id-2: [id]
```

```
x-amz-request-id: [request_id]
Date: Wed, 01 Mar 2009 12:00:00 GMT
Content-Type: [type]
Content-Length: [length]
Connection: close
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<RequestPaymentConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
<Payer>Requester</Payer>
</RequestPaymentConfiguration>
```

此响应显示 payer 值已设置为 Requester。

## 从申请方付款桶中下载对象

因为会向申请方收取从申请方付款存储桶下载数据的费用，因此请求必须包含特殊参数 x-amz-request-payer，该参数确认申请方了解将向他们收取下载费用。要在申请方付款存储桶中访问对象，请求必须包含以下内容之一。

- 对于 DELETE、GET、HEAD、POST 和 PUT 请求，在标头中包含 x-amz-request-payer : requester
- 对于已签名的 URL，需在请求中包括 x-amz-request-payer=requester

如果请求成功且已向申请方收取费用，则响应将包括标头 x-amz-request-charged:requester。如果请求中没有 x-amz-request-payer，Amazon S3 将返回 403 错误并向存储桶拥有者收取请求的费用。

> **Note**
>
> 存储桶拥有者无需将 x-amz-request-payer 添加到他们的请求。
> 确保在您的签名计算中包含 x-amz-request-payer 及其值。有关更多信息，请参阅《Amazon S3 API 参考》中的 Using an Authorization Header。

使用 REST API

从申请方付款存储桶下载对象的步骤

- 使用 GET 请求从申请方付款存储桶下载对象，如以下请求所示。

```
GET / [destinationObject] HTTP/1.1
Host: [BucketName].s3.amazonaws.com
x-amz-request-payer : requester
Date: Wed, 01 Mar 2009 12:00:00 GMT
Authorization: AWS [Signature]
```

如果 GET 请求成功且已向申请方收取费用，则响应将包括 `x-amz-request-charged:requester`。

Amazon S3 可以为尝试从申请方付款存储桶获取对象的请求返回 `Access Denied` 错误。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的错误响应。

使用 Amazon CLI

要使用 Amazon CLI 从申请方付款存储桶下载对象，请指定 `--request-payer requester` 包含在您的 `get-object` 请求中。有关更多信息，请参阅《Amazon CLI 参考》中的 get-object。

# 使用 Amazon S3 中的对象

要将数据存储在 Amazon S3 中，您需要使用称为存储桶和对象的资源。存储桶是对象的容器。对象指的是一个文件和描述该文件的任何元数据。

要将对象存储在 Amazon S3 中，您需要创建存储桶，然后将该对象上传到存储桶。当对象位于存储桶时，您可以将其打开、下载并将其复制。当您不再需要对象或存储桶时，可以清理这些资源。

> **Note**
>
> 有关将 Amazon S3 Express One Zone 存储类与目录存储桶配合使用的更多信息，请参阅 S3 Express One Zone 和使用目录存储桶。

> **Important**
>
> 在 Amazon S3 控制台中，当您为对象选择 Open（打开）或 Download As（下载为）时，这些操作会创建预签名 URL。在五分钟的时间内，任何有权访问这些预签名 URL 的人都可以访问您的对象。有关使用预签名 URL 的更多信息，请参阅使用预签名 URL。

使用 Amazon S3，您只需按实际用量付费。有关 Amazon S3 特征和定价的更多信息，请参阅 Amazon S3。如果您是 Amazon S3 的新客户，则可以免费开始使用 Amazon S3。有关更多信息，请参阅 Amazon 免费套餐。

主题


- Amazon S3 对象概述
- 为 Amazon S3 对象命名
- 使用对象元数据
- 上传对象
- 使用有条件请求向 S3 操作添加前提条件
- 复制、移动和重命名对象
- 下载对象
- 在 Amazon S3 中检查对象完整性
- 删除 Amazon S3 对象

- 组织、列出和处理对象
- 使用预签名 URL 下载和上传对象
- 使用 S3 对象 Lambda 转换对象
- 使用批量操作批量执行对象操作
- 使用 Amazon S3 Select 就地查询数据

# Amazon S3 对象概述

Amazon S3 是一个对象存储，它使用唯一性键值来存储任意数量的对象。您将这些对象存储在一个或多个存储桶中，每个对象的大小最多可达 5 TB。对象由以下内容组成：

密钥

分配给对象的名称。您可以使用对象键检索该对象。有关更多信息，请参阅使用对象元数据。

版本 ID

在存储桶中，键和版本 ID 唯一地标识对象。版本 ID 是 Amazon S3 在对象添加到存储桶时生成的字符串。有关更多信息，请参阅 使用 S3 版本控制保留对象的多个版本。

值

您正在存储的内容。

对象值可以是任意序列的字节。对象的大小范围是 0 到 5 TB。有关更多信息，请参阅 上传对象。

Metadata

一组名称值对，可用于存储有关对象的信息。您可以将元数据（称为用户定义的元数据）分配给 Amazon S3 中的对象。Amazon S3 也可以将用于管理对象的系统元数据指定给这些对象。有关更多信息，请参阅使用对象元数据。

子资源

Amazon S3 使用子资源机制存储特定于对象的其他信息。因为子资源从属于对象，因此它们始终与某些其他实体（如对象或存储桶）相关联。有关更多信息，请参阅 对象子资源。

访问控制信息

您可以控制对您在 Amazon S3 中存储的对象的访问。Amazon S3 支持基于资源的访问控制（例如访问控制列表（ACL）和存储桶策略）和基于用户的访问控制。有关访问控制的更多信息，请参阅以下内容：

- Amazon S3 中的访问控制
- Amazon S3 的身份和访问管理
- 配置 ACL

您的 Amazon S3 资源（例如存储桶和对象）在默认情况下是私有的。您必须显式授予权限，才能允许其他人访问这些资源。有关共享对象的更多信息，请参阅使用预签名 URL 共享对象。

标签

您可以使用标签对存储的对象进行分类，进行访问控制或成本分配。有关更多信息，请参阅 使用标签对存储进行分类。

## 对象子资源

Amazon S3 将定义一组与存储桶和对象相关联的子资源。子资源是对象的从属项。这意味着子资源不独立存在。它们始终与某些其他实体（如对象或存储桶）相关联。

下表列出了与 Amazon S3 对象相关联的子资源。

| 子资源 | 描述 |
| --- | --- |
| acl | 包含可以识别被授权者和所授予的权限的授权列表。创建对象时，`acl` 将识别可以完全控制对象的对象所有者。您可以检索对象 ACL 或将其替换为更新的授权列表。对 ACL 的任何更新都需要您替换现有 ACL。有关 ACL 的更多信息，请参阅 访问控制列表 (ACL) 概述。 |

# 为 Amazon S3 对象命名

对象键（或键名称）唯一标识 Amazon S3 存储桶中的对象。创建对象时，需要指定键名称。例如，在 Amazon S3 控制台上，当您选择存储桶时，将显示存储桶中对象的列表。这些名称是对象键。

对象键名称是 Unicode 字符序列，采用 UTF-8 编码，长度最大为 1024 字节，或 1204 个拉丁字符。在某些区域设置中，单个字符可以等于 2 个字节。命名对象时，请注意以下几点：

- 对象键名称区分大小写。
- 对象键名称包括任何前缀（在控制台中称为文件夹）。例如，`Development/Projects.xls` 是位于 `Development` 前缀（或文件夹）内的 `Projects.xls` 对象的完整对象键名称。前缀、分隔符

（/）和对象名称包含在对象键名称的 1024 字节限制中。有关前缀和文件夹的更多信息，请参阅the section called “选择对象键名称”。

- 在对象键名称中使用某些字符时，可能需要特殊处理。有关更多信息，请参阅 the section called “对象键命名准则”。

> **Note**
>
> 对于虚拟托管类型请求，不支持值为 "soap" 的对象键名称。对于使用 "soap" 的对象键名称值，必须改用路径类型 URL。

## 选择对象键名称

Amazon S3 数据模型是一种扁平结构：您创建一个存储桶，存储桶存储对象。不存在子存储桶或子文件夹的层次结构。但您可以使用键名前缀和分隔符推断逻辑层次结构（如同 Amazon S3 控制台一样）。Amazon S3 控制台支持文件夹的概念。有关如何从 Amazon S3 控制台编辑元数据的更多信息，请参阅在 Amazon S3 控制台中编辑对象元数据。

假设您的存储桶（admin-created）包含具有以下对象键的四个对象：

```
Development/Projects.xls

Finance/statement1.pdf

Private/taxdocument.pdf

s3-dg.pdf
```

控制台使用键名称前缀（Development/、Finance/ 和 Private/）和分隔符 (/) 来呈现文件夹结构。s3-dg.pdf 键不包含斜线分隔的前缀，因此其对象直接在存储桶的根级别出现。如果您打开 Development/ 文件夹，可以看到 Projects.xlsx 对象。

- Amazon S3 支持存储桶和对象且没有层次结构。但是，通过在对象键名中使用前缀和分隔符，Amazon S3 控制台和 Amazon SDK 可以推断层次结构并引入文件夹的概念。
- Amazon S3 控制台通过创建以文件夹前缀和分隔符值作为键的零字节对象来实现文件夹对象创建。这些文件夹对象不会显示在控制台中。否则，它们的行为与任何其他对象一样，可以通过 REST API、Amazon CLI 和 Amazon SDK 进行查看和操作。

# 对象键命名准则

您可以在对象键名中使用任意 UTF-8 字符。但是，在键名中使用某些字符可能导致一些应用程序和协议出现问题。以下指导原则有助于最大程度符合 DNS、Web 安全字符、XML 分析器和其他 API 的要求。

## 安全字符

以下字符集通常可安全地用于键名称：

| | |
|---|---|
| Alphanumeric characters | • 0-9<br>• a-z<br>• A-Z |
| Special characters | • 感叹号 (!)<br>• 连字符 (-)<br>• 下划线 (_)<br>• 句点 (.)<br>• 星号 (*)<br>• 单引号 (')<br>• 左括号 (()<br>• 右括号 ()) |

以下是有效对象键名的示例：

- `4my-organization`
- `my.great_photos-2014/jan/myvacation.jpg`
- `videos/2014/birthday/video1.wmv`

> **Note**
>
> 如果使用 Amazon S3 控制台下载键名称以句点 (.) 结尾的对象，则会从下载对象的键名称末尾删除句点。要在下载的对象中保留键名称末尾的句点，必须使用 Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 Amazon S3 REST API。
> 此外，请注意以下前缀限制：

- 对于前缀为 `./` 的对象，必须使用 Amazon CLI、Amazon SDK 或 REST API 上传或下载。您无法使用 Amazon S3 控制台上传这些对象。
- 如果在从左到右解析时，相对路径段的累积计数从未超过遇到的非相对路径元素的数量，则包含相对路径元素（例如 `../`）的对象键是有效的。此规则适用于使用 Amazon S3 控制台、Amazon S3 REST API、Amazon CLI 和 Amazon SDK 发出的所有请求。

  例如：

  - `videos/2014/../../video1.wmv` 有效。
  - `videos/../../video1.wmv` 无效。
  - `videos/../../2014/video1.wmv` 无效。

## 可能需要特殊处理的字符

键名称中的以下字符可能需要另外进行代码处理，并且很可能需要以十六进制形式在 URL 中编码或引用。其中部分字符是不可打印的字符，浏览器可能无法处理它们，这也需要特殊处理：

- 与符号 (&)
- 美元符号 ($)
- ASCII 字符范围 00–1F 十六进制（0–31 十进制）和 7F（127 十进制）
- @ 符号 (@)
- 等号 (=)
- 分号 (;)
- 正斜杠 (/)
- 冒号 (:)
- 加号 (+)
- 空格：大量连续空格可能会在某些情况下丢失（特别是多个空格）
- 逗号 (,)
- 问号 (?)

## 要避免的字符

我们建议不要在键名称中使用以下字符，因为特殊字符的处理方式差异显著，且并非所有应用程序都保持一致：

- 反斜杠 (\)
- 左花括号 ({)
- 不可打印的 ASCII 字符（128–255 十进制字符）
- 脱字符或音调符号 (^)
- 右花括号 (})
- 百分比字符 (%)
- 重音符/反勾号 (`)
- 右方括号 (])
- 引号 (")
- 大于号 (>)
- 左方括号 ([)
- 波浪字符 (~)
- 小于号 (<)
- 英镑符号 (#)
- 竖线或管道符 (|)

## XML 相关的对象键约束

正如关于尾行处理的 XML 标准所指定的那样，所有 XML 文本都规范化，这样单个回车符（ASCII 代码 13）和回车符紧跟换行符（ASCII 代码 10，也称为换行字符）将替换为单个换行符。为了确保正确解析 XML 请求中的对象键，当将回车符和其它特殊字符插入 XML 标签时，回车符和其它特殊字符必须使用其等效的 XML 实体代码进行替换。

以下是此类特殊字符及其等效 XML 实体代码的列表：

- 撇号 (') 必须替换为 `'`
- 引号 (") 必须替换为 `"`
- 与符号 (&) 必须替换为 `&`
- 小于号 (<) 必须替换为 `<`
- 大于号（>>）必须替换为 `>`
- 回车符 (\r) 必须替换为 `` 或 ``
- 换行符 (\n) 必须替换为 `
` 或 `
`

Example

以下示例说明了使用 XML 实体代码替换回车的情况。此 DeleteObjects 请求将删除带有 key 参数 /some/prefix/objectwith\rcarriagereturn 的对象：（其中 \r 是回车符）。

```
<Delete xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Object>
    <Key>/some/prefix/objectwith&#13;carriagereturn</Key>
  </Object>
</Delete>
```

# 使用对象元数据

Amazon S3 中有两种对象元数据：系统定义的元数据 和用户定义的元数据。系统定义的元数据包括对象的创建日期、大小和存储类等元数据。用户定义的元数据是您可以在上传对象时选择设置的元数据。用户定义的元数据是一组名称/值对。有关更多信息，请参阅the section called “系统定义的对象元数据”和the section called “用户定义的对象元数据”。

创建对象时，请指定对象键（或键名称），它在 Amazon S3 存储桶中唯一地标识该对象。有关更多信息，请参阅 为 Amazon S3 对象命名。也可以在上传对象时在 Amazon S3 中设置用户定义的元数据。

上传对象后，您将无法修改此用户定义的元数据。修改此元数据的唯一方式是创建对象的副本并设置元数据。有关使用 Amazon S3 控制台编辑元数据的更多信息，请参阅在 Amazon S3 控制台中编辑对象元数据。

使用 S3 元数据查询元数据并加快数据发现速度

要轻松查找、存储和查询 S3 对象的元数据，可以使用 S3 元数据。借助 S3 元数据，可以快速准备数据，以用于业务分析、内容检索、人工智能和机器学习（AI/ML）模型训练等。

S3 元数据通过自动捕获通用存储桶中对象的元数据，并将其存储在您可以查询的只读、完全托管式 Apache Iceberg 表中，从而加快数据发现速度。这些只读表称为元数据表。在通用存储桶中添加、更新和移除对象时，S3 元数据会自动刷新相应的元数据表，以反映最新的更改。

默认情况下，S3 元数据提供系统定义的对象元数据，例如对象的创建时间和存储类，以及自定义元数据，例如对象上传期间包含的标签和用户定义的元数据。S3 元数据还提供事件元数据，例如何时更新或删除对象，以及发出请求的 Amazon Web Services 账户。

元数据表存储在 S3 表存储桶中，这些表存储桶可提供针对表数据进行优化的存储。要查询您的元数据，您可以将表存储桶与 Amazon 分析服务（例如 Amazon Athena、Amazon Redshift 和 Amazon QuickSight）集成。

有关 S3 元数据的更多信息，请参阅the section called “加快数据发现速度”。

## 系统定义的对象元数据

对存储桶中存储的每个对象，Amazon S3 将保留一组系统元数据。Amazon S3 将根据需要处理此系统元数据。例如，Amazon S3 将保留对象创建日期和大小元数据，并将此信息用作对象管理的一部分。

有两种类别的系统元数据：

- 受系统控制：元数据（例如对象创建日期）受系统控制，这意味着仅 Amazon S3 可以修改日期值。
- 受用户控制 – 其他系统元数据（例如，为对象配置的存储类以及对象是否已启用服务器端加密）是您可以控制其值的系统元数据的示例。如果存储桶配置为网站，有时您可能想要将页面请求重定向到其它页面或外部 URL。在这种情况下，网页就是您的存储桶中的对象。Amazon S3 将存储页面重定向值作为您可以控制的系统元数据。

  创建对象时，您可以配置这些系统元数据项目的值或在需要时更新这些值。有关存储类的更多信息，请参阅 了解和管理 Amazon S3 存储类。

  Amazon S3 使用 Amazon KMS 密钥加密您的 Amazon S3 对象。Amazon KMS 只加密对象数据。校验和与指定的算法存储为对象元数据的一部分。如果请求为对象进行服务器端加密，则校验和将以加密形式存储。有关服务器端加密的更多信息，请参阅 利用加密来保护数据。

> **Note**
>
> PUT 请求标头的大小限制为 8KB。在 PUT 请求标头中，系统定义的元数据的大小限制为 2KB。通过计算每个键和值的 US-ASCII 编码中的字节总数来测量系统定义的元数据的大小。

下表提供了系统定义的元数据列表以及您是否可以更新它。

| 名称 | 描述 | 用户是否可以修改该值？ |
| --- | --- | --- |
| `Date` | 当前日期和时间。 | 否 |
| `Cache-Control` | 用于指定缓存策略的常规标头字段。 | 是 |

| 名称 | 描述 | 用户是否可以修改该值？ |
| --- | --- | --- |
| Content-Disposition | 对象演示信息。 | 是 |
| Content-Length | 对象大小（以字节为单位）。 | 否 |
| Content-Type | 对象类型。 | 是 |
| Last-Modified | 对象创建日期或上次修改日期（以较晚者为准）。对于分段上传，对象的创建日期是开始分段上传的日期。 | 否 |
| ETag | 表示对象的特定版本的实体标签（ETag）。对于未作为分段上传上传、未加密或使用 Amazon S3 托管密钥 (SSE-S3) 的服务器端加密进行加密的对象，ETag 是数据的 MD5 摘要。 | 否 |
| x-amz-server-side-encryption | 一个标头，它指示是否为对象启用了服务器端加密，以及加密是使用 Amazon Key Management Service（Amazon KMS）密钥（SSE-KMS），还是使用 Amazon S3 托管式加密密钥（SSE-S3）。有关更多信息，请参阅 使用服务器端加密保护数据。 | 是 |
| x-amz-checksum-crc64nvme，x-amz-checksum-crc32，x-amz-checksum-crc32c，x-amz-checksum-sha1，x-amz-checksum-sha256 | 包含对象的校验和或摘要的标头。最多一次设置其中一个标头，具体取决于您指示 Amazon S3 使用的校验和算法。有关选择校验和算法的更多信息，请参阅在 Amazon S3 中检查对象完整性。 | 否 |
| x-amz-checksum-type | 校验和类型，它决定如何组合分段级校验和来为多分段对象创建对象级校验和。 | 是 |

| 名称 | 描述 | 用户是否可以修改该值？ |
| --- | --- | --- |
| x-amz-version-id | 对象版本。对存储桶启用版本控制时，Amazon S3 会为添加到存储桶的对象指定版本 ID。有关更多信息，请参阅 使用 S3 版本控制保留对象的多个版本。 | 否 |
| x-amz-delete-marker | 一个布尔值标记，指示对象是否为删除标记。此标记仅在启用了版本控制的存储桶中使用。 | 否 |
| x-amz-storage-class | 用于存储对象的存储类。有关更多信息，请参阅 了解和管理 Amazon S3 存储类。 | 是 |
| x-amz-website-redirect-location | 一个标头，用于将对于关联对象的请求重定向到同一个存储桶中的其他对象或外部 URL。有关更多信息，请参阅（可选）配置网页重定向。 | 是 |
| x-amz-server-side-encryption-aws-kms-key-id | 一个标头，表示用于加密对象的 Amazon KMS 对称加密 KMS 密钥的 ID。此标头仅在 x-amz-server-side-encryption 标头存在且值为 aws:kms 时使用。 | 是 |
| x-amz-server-side-encryption-customer-algorithm | 一个标头，指示是否启用了具有客户提供的加密密钥的服务器端加密（SSE-C）。有关更多信息，请参阅 使用具有客户提供的密钥的服务器端加密（SSE-C）。 | 是 |
| x-amz-tagging | 对象的标签集。标签集必须编码为 URL 查询参数。 | 是 |

## 用户定义的对象元数据

上传对象时，您也可以将元数据指定给该对象。发送 PUT 或 POST 请求以创建对象时，您将以名称-值（键-值）对的形式提供此可选信息。如果使用 REST API 上传对象，可选的用户定义的元数据名称必须以 x-amz-meta- 开头，以与其他 HTTP 标头区分开来。使用 REST API 检索对象时，将返回此前缀。如果使用 SOAP API 上传对象则无需前缀。使用 SOAP API 检索对象时，无论您使用哪种 API 上传对象，都将删除前缀。

> **Note**
>
> SOAP API 不适用于新客户，并将于 2025 年 8 月 31 日接近使用寿命终止（EOL）。我们建议您使用 REST API 或 Amazon 软件开发工具包。

通过 REST API 检索元数据时，Amazon S3 会将具有相同名称（不分大小写）的标头合并为逗号分隔的列表。如果某些元数据包含不可打印的字符，则不会返回它。但是，`x-amz-missing-meta` 标头将与不可打印的元数据条目的数量值一起返回。该 `HeadObject` 操作从对象检索元数据而不返回对象本身。如果您只对某个对象的元数据感兴趣，则此操作很有用。要使用 `HEAD`，您必须具有对象的 `READ` 访问权限。有关更多信息，请参阅 Amazon Simple Storage Service API 参考 中的 HeadObject。

用户定义的元数据是一组键值对。Amazon S3 以小写形式存储用户定义的元数据键。

Amazon S3 允许元数据值中有任意 Unicode 字符。

为避免与这些元数据值的显示有关的问题，如果使用 SOAP 或通过 `POST` 进行基于浏览器的上传，则当使用 REST 和 UTF-8 时，应遵守使用 US-ASCII 字符的规定。

在元数据值中使用非 US-ASCII 字符时，将检查提供的 Unicode 字符串中是否存在非 US-ASCII 字符。此类标头的值在存储前按照 RFC 2047 进行字符解码，并在返回前按照 RFC 2047 进行编码以确保邮件安全。如果字符串仅包含 US-ASCII 字符，则按原样显示。

示例如下：

```
PUT /Key HTTP/1.1
Host: amzn-s3-demo-bucket.s3.amazonaws.com
x-amz-meta-nonascii: ÄMÄZÕÑ S3

HEAD /Key HTTP/1.1
Host: amzn-s3-demo-bucket.s3.amazonaws.com
x-amz-meta-nonascii: =?UTF-8?B?w4PChE3Dg8KEWsODwpXDg8KRIFMz?=

PUT /Key HTTP/1.1
Host: amzn-s3-demo-bucket.s3.amazonaws.com
x-amz-meta-ascii: AMAZONS3

HEAD /Key HTTP/1.1
Host: amzn-s3-demo-bucket.s3.amazonaws.com
```

```
x-amz-meta-ascii: AMAZONS3
```

> **Note**
>
> PUT 请求标头的大小限制为 8KB。在 PUT 请求标头中，用户定义的元数据的大小限制为 2KB。通过计算每个键和值的 UTF-8 编码中的字节总数来测量用户定义的元数据的大小。

有关在上传对象后通过创建对象的副本、修改对象、替换旧对象或创建新版本来更改对象的元数据的信息，请参阅在 Amazon S3 控制台中编辑对象元数据。

## 在 Amazon S3 控制台中编辑对象元数据

可以使用 Amazon S3 控制台通过复制操作来编辑现有 S3 对象的元数据。要编辑元数据，请将对象复制到同一目标并指定要应用的新元数据，这将替换该对象的旧元数据。在您上传对象时，Amazon S3 会设置一些元数据。例如，`Content-Length` 和 `Last-Modified` 是系统定义的对象元数据字段，用户无法修改。

也可以在上传对象时设置用户定义的元数据，并在需求发生更改时替换此元数据。例如，您可能有一组初始存储在 `STANDARD` 存储类中的对象。随着时间推移，可能不再需要这些数据具有高可用性。因此，可以通过将 `x-amz-storage-class` 键的值从 `STANDARD` 替换为 `GLACIER` 来将存储类更改为 `GLACIER`。

> **Note**
>
> 当您在 Amazon S3 中替换对象元数据时，请考虑以下事项：
>
> - 必须指定要保留的现有元数据、要添加的元数据以及要编辑的元数据。
> - 如果对象小于 5 GB，可以使用 S3 控制台中的复制操作来替换对象元数据。如果对象大于 5 GB，可以在通过 Amazon CLI 或 Amazon SDK 使用分段上传来复制对象时，替换对象元数据。有关更多信息，请参阅 使用分段上传复制对象。
> - 有关替换元数据所需的其它权限的列表，请参阅 the section called “S3 API 操作所需的权限”。有关授予此权限的示例策略，请参阅the section called “基于身份的策略示例”。
> - 此操作将使用更新的设置和上次修改日期创建对象的副本。如果启用 S3 版本控制，则会创建对象的新版本，而现有对象将变为旧版本。如果未启用 S3 版本控制，则对象的新副本将替换原始对象。与更改属性的 IAM 角色关联的 Amazon Web Services 账户还会成为新对象或（对象版本）的拥有者。

- 编辑元数据会替换现有键名称的值。
- 无法使用控制台来复制使用客户提供的加密密钥（SSE-C）加密的对象。您必须使用 Amazon CLI、Amazon SDK 或 Amazon S3 REST API。
- 使用 Amazon S3 控制台复制对象时，您可能会收到错误消息 "Copied metadata can't be verified." 控制台使用标头来检索和设置对象的元数据。如果您的网络或浏览器配置修改了网络请求，则此行为可能会导致将意外的元数据（例如修改后的 `Cache-Control` 标头）写入复制的对象。Amazon S3 无法验证这种意外的元数据。

  要解决此问题，请检查您的网络和浏览器配置，以确保它不会修改标头，例如 `Cache-Control`。有关更多信息，请参阅 The Shared Responsibility Model。

> **Warning**
>
> 替换文件夹的元数据时，请等待复制操作完成，然后再将新对象添加到文件夹。否则，也可能会编辑新对象。

以下主题描述了如何使用 Amazon S3 控制台中的复制操作来替换对象的元数据。

替换系统定义的元数据

可以替换 S3 对象的一些系统定义的元数据。有关您可以修改的系统定义元数据和值的列表，请参阅系统定义的对象元数据。

替换对象的系统定义的元数据

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶或目录存储桶。
3. 在存储桶列表中，选择包含您想要更改的对象的存储桶的名称。
4. 选中要更改的对象所对应的复选框。
5. 在操作菜单上，从显示的选项列表中选择复制。
6. 要指定目标路径，请选择浏览 S3，导航到与源对象相同的目标，然后选中目标复选框。选择右下角的选择目标。

   或者，输入目标路径。

7. 如果您未 启用存储桶版本控制，则会看到一则警告，建议您启用存储桶版本控制，以防意外覆盖或删除对象。如果要在此存储桶中保留对象的所有版本，请选择 Enable Bucket Versioning（启用存储桶版本控制）。还可以在目标详细信息中查看默认加密和对象锁定属性。
8. 在其它复制设置下，选择指定设置来指定元数据的设置。
9. 滚动到元数据部分，然后选择替换所有元数据。
10. 选择添加元数据。
11. 对于元数据 Type (类型)，请选择 System-defined (系统定义)。
12. 指定唯一的 Key (键) 和元数据 Value (值)。
13. 要编辑其他元数据，请选择 Add metadata (添加元数据)。您还可以选择 Remove（删除）以删除一组类型-键-值。
14. 选择复制。Amazon S3 将保存元数据更改。

替换用户定义的元数据

可以通过组合元数据前缀 `x-amz-meta-` 和您选择用于创建自定义键的名称，来替换对象的用户定义元数据。例如，如果您添加自定义名称 `alt-name`，则元数据键为 `x-amz-meta-alt-name`。

用户定义元数据最大总计可为 2 KB。要计算用户定义元数据的总大小，请将 UTF-8 编码中每个键和值的字节数求和。键及其值均必须符合 US-ASCII 标准。有关更多信息，请参阅 用户定义的对象元数据。

替换对象的用户定义的元数据

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在导航窗格中，选择存储桶，然后选择通用存储桶或目录存储桶选项卡。导航到包含要更改的对象的 Amazon S3 存储桶或文件夹。
3. 选中要更改的对象所对应的复选框。
4. 在操作菜单上，从显示的选项列表中选择复制。
5. 要指定目标路径，请选择浏览 S3，导航到与源对象相同的目标，然后选中目标复选框。选择选择目标。

   或者，输入目标路径。
6. 如果您未 启用存储桶版本控制，则会看到一则警告，建议您启用存储桶版本控制，以防意外覆盖或删除对象。如果要在此存储桶中保留对象的所有版本，请选择 Enable Bucket Versioning（启用存储桶版本控制）。还可以在目标详细信息中查看默认加密和对象锁定属性。

7. 在其它复制设置下，选择指定设置来指定元数据的设置。
8. 滚动到元数据部分，然后选择替换所有元数据。
9. 选择添加元数据。
10. 对于元数据类型，请选择 User-defined（用户定义）。
11. 在 `x-amz-meta-` 后面输入唯一的自定义 Key（键）。还输入元数据 Value (值)。
12. 要添加其他元数据，请选择 Add metadata (添加元数据)。您还可以选择 Remove（删除）以删除一组类型-键-值。
13. 选择复制。Amazon S3 将保存元数据更改。

## 使用 S3 元数据加快数据发现速度

Amazon S3 元数据通过自动捕获通用存储桶中对象的元数据，并将其存储在您可以查询的只读、完全托管式 Apache Iceberg 表中，从而加快数据发现速度。这些只读表称为元数据表。在通用存储桶中添加、更新和移除对象时，S3 元数据会自动刷新相应的元数据表，以反映最新的更改。

默认情况下，S3 元数据提供三种类型的元数据：

- 系统定义的元数据，例如对象的创建时间和存储类
- 自定义元数据，例如标签和对象上传期间包含的用户定义的元数据
- 事件元数据，例如何时更新或删除对象，以及发出请求的 Amazon Web Services 账户

有关在元数据表中存储哪些数据的详细信息，请参阅 the section called “元数据表架构”。

借助 S3 元数据，您可以轻松查找、存储和查询 S3 对象的元数据，这样您就可以快速准备数据，以用于业务分析、内容检索、人工智能和机器学习（AI/ML）模型训练等。

元数据表存储在 S3 表存储桶中，这些表存储桶可提供针对表数据进行优化的存储。要轻松查询元数据，您可以将表存储桶与 Amazon Glue Data Catalog 集成。将表存储桶与 Amazon Glue Data Catalog 集成后，您可以直接使用查询引擎查询元数据表，例如 Amazon Athena、Amazon EMR、Amazon Redshift、Apache Spark 和 Trino。也可以使用任何其它支持 Apache Iceberg 格式的应用程序查询元数据表。要从元数据表创建控制面板，请使用 Amazon QuickSight。

有关 S3 元数据定价，请参阅 Amazon S3 定价。

## 元数据表的工作原理

元数据表由 Amazon S3 管理，而不能由 Amazon S3 本身以外的任何 IAM 主体进行修改。（但是，您可以删除元数据表。）因此，元数据表是只读的，这有助于确保它们正确地反映存储桶的内容。

为了使 Apache Iceberg 元数据表保持最佳性能，Amazon S3 会定期对表执行维护活动，例如压缩和未引用文件移除。这些维护活动既有助于最大限度地降低存储元数据表的成本，又有助于优化查询性能。这种表维护是自动进行的，无需您选择加入或持续管理。但是，如果需要，您可以配置这些表维护活动。有关更多信息，请参阅表存储桶维护。

> **Note**
>
> S3 元数据旨在当您对通用存储桶进行更改时持续追加到元数据表中。每次更新都会创建一个快照，即元数据表的新版本。由于元数据表的只读性质，因此您无法删除元数据表中的记录。您也无法使用 S3 表类数据存储服务的快照到期功能使元数据表的旧快照到期。
> 为了最大限度地降低成本，您可以定期删除元数据表配置和元数据表，然后重新创建它们。
> 有关更多信息，请参阅the section called “删除元数据表配置”和the section called “删除元数据表”。

要生成对象元数据并将其存储在 S3 托管式元数据表中，您需要为通用存储桶创建元数据表配置。只要存储桶上的配置处于活动状态，Amazon S3 就会持续更新元数据表以反映对数据的最新更改。

要创建元数据表配置，必须确保您拥有创建和管理元数据表所必需的 Amazon Identity and Access Management（IAM）权限。有关更多信息，请参阅 the section called “元数据表的权限”。您还必须创建或指定用于存储元数据表的 S3 表存储桶。此表存储桶必须与通用存储桶位于相同的 Amazon Web Services 区域和账户中。有关创建表存储桶的更多信息，请参阅创建表存储桶。

> **Note**
>
> S3 元数据不适用于在您创建元数据表配置之前已存在于通用存储桶中的任何对象。换句话说，S3 元数据仅捕获在您创建元数据表配置后发生的更改事件（例如上传、更新和删除）的元数据。

要监控对元数据表配置的更新，可以使用 Amazon CloudTrail。有关更多信息，请参阅 the section called “CloudTrail 日志记录跟踪的 Amazon S3 存储桶级操作”。

主题

- 元数据表限制和局限性
- S3 元数据表架构
- 配置元数据表
- 查询元数据表


## 元数据表限制和局限性

在创建元数据表配置之前，请注意以下限制和局限性：

- S3 元数据目前仅在美国东部（弗吉尼亚州北部）、美国东部（俄亥俄州）和美国西部（俄勒冈州）区域中提供。
- S3 元数据支持除以下存储类外的所有存储类：
  - S3 Express One Zone 存储类
  - Local Zones 的目录存储桶中的 S3 One Zone-Infrequent Access（S3 One Zone-IA）存储类

  > **Note**
  >
  > 对于 S3 Intelligent-Tiering 存储类，元数据表中未显示特定层。

- 要创建元数据表配置，必须创建或指定用于存储元数据表的 S3 表存储桶。此表存储桶必须与通用存储桶位于相同的 Amazon Web Services 区域和 Amazon Web Services 账户中。
- 目录存储桶或表存储桶不支持 S3 元数据。您只能为通用存储桶创建元数据表配置。
- S3 元数据不适用于在您创建元数据表配置之前已存在于通用存储桶中的任何对象。换句话说，S3 元数据仅捕获在您创建元数据表配置后发生的更改事件（例如上传、更新和删除）的元数据。
- S3 元数据旨在当您对通用存储桶进行更改时持续追加到元数据表中。每次更新都会创建一个快照，即元数据表的新版本。由于元数据表的只读性质，因此您无法删除元数据表中的记录。您也无法使用 S3 表类数据存储服务的快照到期功能使元数据表的旧快照到期。

  为了最大限度地降低成本，您可以定期删除元数据表配置和元数据表，然后重新创建它们。有关更多信息，请参阅the section called “删除元数据表配置”和the section called “删除元数据表”。
- 创建或更新表存储桶或表策略时，请确保不限制 Amazon S3 写入您的表存储桶或元数据表。如果 Amazon S3 无法写入您的表存储桶或元数据表，则必须通过删除元数据表配置和元数据表，然后创建新配置来创建新的元数据表。
- 在删除元数据表之前，必须先删除通用存储桶中的关联元数据表配置。
- 您只能为整个通用存储桶创建元数据表配置。您不能在前缀级应用元数据表配置。

- 您无法暂停和恢复对元数据表的更新。相反，您可以通过删除与元数据表关联的元数据表配置来阻止元数据表进行更新。要重新开始接收更新，必须创建新的元数据表配置，这会创建新的元数据表。
- 元数据表所包含的元数据与通过 S3 清单或 Amazon S3 REST API 提供的元数据不完全相同。例如，元数据表中未提供以下信息：
  - S3 生命周期到期或转换状态
  - 对象锁定保留期或治理模式
  - 对象访问控制列表（ACL）信息
  - 复制状态
- 您无法调整元数据表的分区或排序。因此，某些查询可能需要表扫描，因此效率可能较低。

## S3 元数据表架构

Amazon S3 元数据表包含行和列。每行代表一个突变事件，该事件在您的通用存储桶中创建、更新或删除了一个对象。这些事件中大多数是各种用户操作的结果，但其中一些事件是由 Amazon S3 代表您执行的操作的结果，例如 S3 生命周期到期或存储类转换。

S3 元数据是一个事件处理管道，旨在使元数据表与通用存储桶中发生的更改保持最终一致。请注意，当 S3 元数据收到创建或更新对象的通知时，该对象可能已经在存储桶中被覆盖或删除。默认情况下，会为每个 S3 bucket operation 创建一个表行。但是，如果任何对象元数据被删除或覆盖，或者无法再检索对象，则某些列可能会显示一个 NULL 值来指示任何缺失的元数据架构。

下面是名为 amzn-s3-demo-bucket: 的通用存储桶的元数据表示例：

```
bucket               key                          sequence_number
                                                                  record_type
 record_timestamp          version_id   is_delete_marker   size   last_modified_date
   e_tag                           storage_class  is_multipart   encryption_status
 is_bucket_key_enabled   kms_key_arn
               checksum_algorithm   object_tags   user_metadata

    requester      source_ip_address   request_id
amzn-s3-demo-bucket   Finance/statement1.pdf
 80e737d8b4d82f776affffffffffffff006737d8b4d82f776a00000000000000000000000000000000000000000000000
   CREATE        2024-11-15 23:26:44.899                 FALSE
 6223   11/15/2024 23:26     e131b86632dda753aac4018f72192b83    STANDARD
 FALSE          SSE-KMS             FALSE                   arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890df   SSECRC32            {}
            {count -> Asia, customs -> false, family -> true, location -> Mary, name ->
```

```
 football, user -> United States}                        111122223333   192.0.2.1
    CVK8FWYRW0M9JW65
amzn-s3-demo-bucket   s3-dg.pdf
 80e737d8b4e39f1dbdfffffffffffffff006737d8b4e39f1dbd000000000000000000000000000000000000000000000000
   CREATE        2024-11-15 23:26:44.942                 FALSE
 3554   11/15/2024 23:26     9bb49efc2d92c05558ddffbbde8636d5    STANDARD
 FALSE          DSSE-KMS            FALSE                    arn:aws:kms:us-
east-1:936810216292:key/0dcebce6-49fd-4cae-b2e2-5512ad281afd   SSESHA1              {}
           {}
                                                          111122223333   192.0.2.1
   CVKAQDRAZEG7KXAY
amzn-s3-demo-bucket   Development/Projects.xls
 80e737d8b4ed9ac5c6ffffffffffffffff006737d8b4ed9ac5c600000000000000000000000000000000000000000000000
   CREATE        2024-11-15 23:26:44.966                 FALSE               7746
 11/15/2024 23:26     729a6863e47fb9955b31bfabce984908    STANDARD   FALSE
 SSE-S3              FALSE                   NULL
                                    SSECRC32             {}            {count -> Asia,
 customs -> Canada, family -> Billiards, filter -> true, location -> Europe, name ->
 Asia, user -> United States}   111122223333   192.0.2.1           CVK7Z6XQTQ90BSRV
```

元数据表具有以下架构：

| 列名称 | 必填？ | 数据类型 | |
|---|---|---|---|
| bucket | 是 | 字符串 | 通用存储桶名称。有关更多信息，请参阅 the section called “命名规则”。 |
| key | 是 | 字符串 | 在存储桶中唯一地标识对象的对象键名称（或键）。有关更多信息，请参阅 the section called “为对象命名”。 |
| sequence_number | 是 | 字符串 | 序列号，它是一个序数，包含在给定对象的记录中。要对相同存储桶和键的记录进 |

| 列名称 | 必填？ | 数据类型 | |
|---|---|---|---|
| | | | 行排序，您可以按 sequence_number 进行排序。对于给定的存储桶和键，按字典顺序排列的较大 sequence_number 值意味着该记录是更近被引入存储桶的。 |

| 列名称 | 必填？ | 数据类型 | |
|---|---|---|---|
| record_type | 是 | 字符串 | 此记录的类型，为以下值之一：CREATE、UPDATE_METADATA 或 DELETE。<br><br>CREATE 记录表明已将新对象（或对象的新版本）写入存储桶。<br><br>UPDATE_METADATA 记录捕获对现有对象的可变元数据（例如存储类或标签）的更改。<br><br>DELETE 记录表明此对象（或该对象的此版本）已被删除。启用版本控制后，DELETE 记录代表删除标记或永久删除。删除标记的 record_type 值为 DELETE，is_delete_marker 值为 True。永久删除记录在除 bucket、key、sequence_number 、record_type 、record_timestamp 和 version_id 之外的所有其它列中都有 null 值。有关更多信息， |

| 列名称 | 必填？ | 数据类型 | |
|---|---|---|---|
| | | | 请参阅 the section called “删除对象版本”。 |
| record_timestamp | 是 | 时间戳 NTZ（无时区） | 与此记录关联的时间戳。 |
| version_id | 否 | 字符串 | 对象的版本 ID。在存储桶上启用版本控制后，Amazon S3 会为添加到存储桶的对象指定版本号。有关更多信息，请参阅 the section called “保留对象的多个版本”。<br><br>在您设置版本控制状态之前存储在存储桶中的对象的版本 ID 为 null。 |

| 列名称 | 必填？ | 数据类型 | |
|---|---|---|---|
| is_delete_marker | 否 | 布尔值 | 对象的删除标记状态。如果对象是删除标记，则此值为 True。否则为 False。有关更多信息，请参阅 the section called “使用删除标记”。<br><br>**Note**<br>为删除标记添加的行的 record_type 值为 DELETE，而不是 UPDATE_METADATA。如果删除标记是因为 S3 生命周期到期而创建的，则 requester 值为 s3.amazonaws.com。 |

| 列名称 | 必填？ | 数据类型 | |
|---|---|---|---|
| size | 否 | 长整型 | 以字节为单位的对象大小，不包括未完成的分段上传或对象元数据的大小。如果 is_delete_marker 为 True，则大小为 0。有关更多信息，请参阅 the section called “系统定义的对象元数据”。 |
| last_modified_date | 否 | 时间戳 NTZ（无时区） | 对象创建日期或上次修改日期（以较晚者为准）。对于分段上传，对象创建日期是开始分段上传的日期。有关更多信息，请参阅 the section called “系统定义的对象元数据”。 |
| e_tag | 否 | 字符串 | 实体标签（ETag），这是对象的哈希。ETag 仅反映对于对象的内容的更改，而不反映对于对象的元数据的更改。ETag 可能是对象数据的 MD5 摘要。ETag 是否为 MD5 摘要取决于对象的创建方式及其加密方式。有关更多信息，请参阅《Amazon S3 API 参考》中的 Object。 |

| 列名称 | 必填？ | 数据类型 | |
|---|---|---|---|
| storage_class | 否 | 字符串 | 用于存储对象的存储类。以下值之一：STANDARD、REDUCED_REDUNDANCY 、STANDARD_IA 、ONEZONE_IA 、INTELLIGENT_TIERING 、GLACIER、DEEP_ARCHIVE 或 GLACIER_IR 。有关更多信息，请参阅 the section called “了解和管理存储类”。 |
| is_multipart | 否 | 布尔值 | 对象的上传类型。如果对象以分段上传形式上传，则此值为 True。否则为 False。有关更多信息，请参阅 the section called “使用分段上传”。 |

| 列名称 | 必填？ | 数据类型 | |
|---|---|---|---|
| encryption_status | 否 | 字符串 | 对象的服务器端加密状态，具体取决于使用哪种加密密钥：具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）、具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）、具有 Amazon KMS keys 的双层服务器端加密（DSSE-C）或具有客户提供的密钥的服务器端加密（SSE-C）。如果对象未加密，则此值为 null。可能的值为 SSE-S3、SSE-KMS、DSSE-KMS、SSE-C 或 null。有关更多信息，请参阅 the section called “数据加密”。 |

| 列名称 | 必填？ | 数据类型 | |
|---|---|---|---|
| is_bucket_key_enabled | 否 | 布尔值 | 对象的 S3 存储桶密钥启用状态。如果对象将 S3 存储桶密钥用于 SSE-KMS，则此值为 True。否则为 False。有关更多信息，请参阅 the section called “为对象配置 S3 存储桶密钥”。 |

| 列名称 | 必填？ | 数据类型 | |
|---|---|---|---|
| kms_key_arn | 否 | 字符串 | 用于加密对象的 KMS 密钥的 Amazon 资源名称（ARN），适用于 encryption_status 为 SSE-KMS 或 DSSE-KMS 的行。如果对象未使用 SSE-KMS 或 DSSE-KMS 进行加密，则值为 null。有关更多信息，请参阅the section called “KMS 密钥存储在 Amazon KMS (SSE-KMS) 中”和the section called “双层服务器端加密（DSSE-KMS）”。<br><br>**Note**<br>如果某行代表的对象版本在处理删除或覆盖事件时不再存在，则即使 encryption_status 列的值为 SSE-KMS 或 DSSE-KMS，kms_key_arn 也将包含 null 值。 |

| 列名称 | 必填？ | 数据类型 | |
|---|---|---|---|
| checksum_algorithm | 否 | 字符串 | 用于为对象创建校验和的算法，为以下值之一：CRC64-NVME 、CRC32、CRC32C、SHA1 或 SHA256。如果不存在校验和，则此值为 null。有关更多信息，请参阅 the section called “使用支持的校验和算法”。 |

| 列名称 | 必填？ | 数据类型 | |
|---|---|---|---|
| object_tags | 否 | Map <String, String> | 与对象关联的对象标签。对象标签存储为键值对的映射。如果对象没有对象标签，则会存储空映射 ({})。有关更多信息，请参阅 the section called “使用标签对于对象进行分类”。<br><br>**Note**<br>如果 record_type 值为 DELETE，则 object_tags 列包含 null 值。如果 record_type 值为 CREATE 或 UPDATE_METADATA ，则表示在处理删除或覆盖事件时已不再存在的对象版本的行在 object_tags 列中将包含 null 值。 |

| 列名称 | 必填？ | 数据类型 | |
|---|---|---|---|
| user_metadata | 否 | Map <String, String> | 与对象关联的用户元数据。用户元数据存储为键值对的映射。如果对象没有用户元数据，则会存储空映射 ({})。有关更多信息，请参阅 the section called “用户定义的对象元数据”。<br><br>**Note**<br>如果 record_type 值为 DELETE，则 user_metadata 列包含 null 值。如果 record_type 值为 CREATE 或 UPDATE_METADATA，则表示在处理删除或覆盖事件时已不再存在的对象版本的行在 user_metadata 列中将包含 null 值。 |

| 列名称 | 必填？ | 数据类型 | |
|---|---|---|---|
| requester | 否 | 字符串 | 提出请求的请求者或 Amazon Web Services 服务 主体的 Amazon Web Services 账户 ID。 |
| source_ip_address | 否 | 字符串 | 请求的源 IP 地址。对于由用户请求生成的记录，此列包含请求的源 IP 地址。对于 Amazon S3 或其它 Amazon Web Services 服务 代表用户采取的操作，此列包含 null 值。 |
| request_id | 否 | 字符串 | 与请求关联的请求 ID。 |

## 配置元数据表

Amazon S3 元数据通过自动捕获通用存储桶中对象的元数据，并将其存储在您可以查询的只读、完全托管式 Apache Iceberg 表中，从而加快数据发现速度。这些只读表称为元数据表。在通用存储桶中添加、更新和移除对象时，S3 元数据会自动刷新相应的元数据表，以反映最新的更改。

借助 S3 元数据，您可以轻松查找、存储和查询 S3 对象的元数据，这样您就可以快速准备数据，以用于业务分析、人工智能和机器学习（AI/ML）模型训练等。

要生成对象元数据并将其存储在 S3 托管式元数据表中，您需要为通用存储桶创建元数据表配置。只要存储桶上的配置处于活动状态，Amazon S3 就会持续更新元数据表以反映对数据的最新更改。此外，Amazon S3 会持续优化您的元数据表，以有助于降低存储成本并提高分析查询性能。

要创建元数据表配置，确保您拥有创建和管理元数据表所必需的 Amazon Identity and Access Management（IAM）权限。您还必须创建或指定用于存储元数据表的 S3 表存储桶。此表存储桶必须与通用存储桶位于相同的 Amazon Web Services 区域和 Amazon Web Services 账户中。

要监控对元数据表配置的更新，可以使用 Amazon CloudTrail。有关更多信息，请参阅 the section called “CloudTrail 日志记录跟踪的 Amazon S3 存储桶级操作”。

主题

- 为配置元数据表设置权限
- 创建元数据表配置
- 控制对元数据表的访问
- 删除元数据表配置
- 删除元数据表

为配置元数据表设置权限

要创建元数据表配置，您必须拥有必要的 Amazon Identity and Access Management（IAM）权限，才能创建和管理元数据表配置，以及创建和管理元数据表及存储元数据表的表存储桶。

要创建和管理您的元数据表配置，您必须具有以下权限：

- `s3:CreateBucketMetadataTableConfiguration`：此权限可让您为通用存储桶创建元数据表配置。
- `s3:GetBucketMetadataTableConfiguration`：此权限可让您检索有关元数据表配置的信息。
- `s3:DeleteBucketMetadataTableConfiguration`：此权限可让您删除元数据表配置。

要创建和使用表和表存储桶，您必须具有某些 `s3tables` 权限。要创建元数据表配置，您至少必须具有以下 `s3tables` 权限：

- `s3tables:CreateNamespace`：此权限可让您在表存储桶中创建命名空间。元数据表使用默认 `aws_s3_metadata` 命名空间。
- `s3tables:GetTable`：此权限可让您检索有关元数据表的信息。
- `s3tables:CreateTable`：此权限可让您创建元数据表。
- `s3tables:PutTablePolicy`：此权限可让您添加或更新元数据表策略。

有关所有表和表存储桶权限的详细信息，请参阅 S3 表类数据存储服务的访问管理。

**Important**

- 如果您还想将表存储桶与 Amazon 分析服务集成，以便您能够查询元数据表，则需要额外的权限。有关更多信息，请参阅集成 Amazon S3 表类数据存储服务与 Amazon 分析服务。
- 如果表存储桶使用具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS），则您还需要 `kms:GenerateDataKey` 和 `kms:Decrypt` 权限。此外，您需要向 `metadata.s3.amazonaws.com` 和 `maintenance.s3tables.amazonaws.com` 服务主体授予访问 KMS 密钥的权限。有关更多信息，请参阅 向 S3 元数据服务主体授予使用您的 KMS 密钥的权限 。

要创建和使用元数据表和表存储桶，可以使用以下示例策略。在本策略中，您要对其应用元数据表配置的通用存储桶称为 *amzn-s3-demo-source-bucket*。您要在其中存储元数据表的表存储桶称为 *amzn-s3-demo-bucket*。要使用此策略，请将这些存储桶名称和 *user input placeholders* 替换为您自己的信息：

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"PermissionsToWorkWithMetadataTables",
         "Effect":"Allow",
         "Action":[
            "s3:CreateBucketMetadataTableConfiguration",
            "s3:GetBucketMetadataTableConfiguration",
            "s3:DeleteBucketMetadataTableConfiguration",
            "s3tables:*"
         ],
         "Resource":[
            "arn:aws:s3:::bucket/amzn-s3-demo-source-bucket",
            "arn:aws:s3tables:region:account_id:bucket/amzn-s3-demo-bucket",
            "arn:aws:s3tables:region:account_id:bucket/amzn-s3-demo-bucket/table/*"
         ]
       }
    ]
}
```

创建元数据表配置

要生成 Amazon S3 元数据并将其存储在完全托管式 Apache Iceberg 元数据表中，您需要为通用存储桶创建元数据表配置。只要存储桶上的配置处于活动状态，Amazon S3 就会持续更新元数据表以反映对数据的最新更改。此外，Amazon S3 会持续优化您的元数据表，以有助于降低存储成本并提高分析查询性能。

元数据表具有以下 Amazon 资源名称（ARN）格式：

`arn:aws:s3tables:region-code:account-id:bucket/table-bucket-name/table/metadata_table_name`

Amazon S3 完全托管式元数据表存储在表存储桶的 `aws_s3_metadata` 命名空间中。有关表存储桶中命名空间的更多信息，请参阅表命名空间。

您可以使用 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 Amazon S3 REST API 创建元数据表配置。

先决条件

要创建元数据表配置，您必须先执行以下操作：

- 确保您拥有创建和管理元数据表所必需的 Amazon Identity and Access Management（IAM）权限。有关更多信息，请参阅 the section called “元数据表的权限”。
- 创建一个 S3 表存储桶来存储元数据表。此表存储桶必须与通用存储桶位于相同的 Amazon Web Services 区域和 Amazon Web Services 账户中。有关创建表存储桶的更多信息，请参阅创建表存储桶。如果您使用 Amazon S3 控制台来创建配置，则可以在此过程中执行此步骤。
- 将您的表存储桶与 Amazon Glue Data Catalog 集成，这样您就可以使用 Amazon Athena、Amazon EMR、Amazon Redshift、Apache Spark 和 Apache Trino 等查询引擎以及任何其它支持 Apache Iceberg 格式的应用程序直接查询元数据表。有关更多信息，请参阅 the section called “使用 Amazon 分析服务查询元数据表”。

创建元数据表配置

使用 S3 控制台

创建元数据表配置

在创建元数据表配置之前，请确保您已查看并满足先决条件，并且已经查看了the section called “限制和局限性”。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 选择要为其创建元数据表配置的通用存储桶。

   > **Note**
   >
   > 请确保此通用存储桶位于表存储桶可用的 Amazon Web Services 区域。表存储桶仅在美国东部（弗吉尼亚州北部）、美国东部（俄亥俄州）和美国西部（俄勒冈州）区域中提供。

4. 在存储桶详细信息页面上，选择元数据选项卡。
5. 在元数据选项卡上，选择创建元数据配置。
6. 在创建元数据配置页面的目标表存储桶下，指定用于存储元数据表的表存储桶。表存储桶必须与通用存储桶位于相同的 Amazon Web Services 账户和 Amazon Web Services 区域中。

   如果您还没有表存储桶，选择创建表存储桶。表存储桶名称必须为 3 到 63 个字符，并且在您选择的 Amazon Web Services 区域的 Amazon Web Services 账户中是唯一的。有效字符：a-z、0-9 和连字符（-）。有关创建表存储桶的更多信息，请参阅创建表存储桶。

   在创建表存储桶时，请确保将其与 Amazon Glue Data Catalog 集成。有关更多信息，请参阅 the section called “使用 Amazon 分析服务查询元数据表”。
7. 对于元数据表名称，指定您希望表具有的名称。元数据表名称必须介于 1 到 255 个字符之间，并且在表存储桶的 `aws_s3_metadata` 命名空间中是唯一的。有效的字符为小写字母、数字和下划线 (_)。
8. 选择创建元数据表配置。

如果元数据表配置取得成功，则元数据表的 ARN 以及指定的表存储桶和元数据表名称将显示在元数据选项卡上。

要监控对元数据表配置的更新，可以使用 Amazon CloudTrail。有关更多信息，请参阅 the section called “CloudTrail 日志记录跟踪的 Amazon S3 存储桶级操作”。

使用 Amazon CLI

要运行以下命令，您必须安装并配置 Amazon CLI。如果未安装 Amazon CLI，请参阅《Amazon Command Line Interface 用户指南》中的安装或更新最新版本的 Amazon CLI。

或者，可以从控制台中使用 Amazon CloudShell 运行 Amazon CLI 命令。Amazon CloudShell 是一个基于浏览器、预先经过身份验证的 Shell，您可以直接从 Amazon Web Services Management Console 中启动它。有关更多信息，请参阅《Amazon CloudShell 用户指南》中的 What is CloudShell? 和 Getting started with Amazon CloudShell。

使用 Amazon CLI 创建元数据表配置

在创建元数据表配置之前，请确保您已查看并满足先决条件，并且已经查看了the section called “限制和局限性”。

要使用以下示例命令，请将 *user input placeholders* 替换为您自己的信息。

1. 如果您还没有表存储桶，请使用以下命令创建一个用于存储元数据表的表存储桶。确保表存储桶与您要为其创建元数据表配置的通用存储桶位于同一 Amazon Web Services 区域中。

```
aws s3tables create-table-bucket --name amzn-s3-demo-bucket --region us-east-2
```

2. 要验证表存储桶是否已创建，请使用以下命令：

```
aws s3tables list-table-buckets --region us-east-2
```

3. 创建包含元数据表配置的 JSON 文件并将其保存（例如 `metadata-config.json`）。以下是一个示例配置：

   表存储桶名称必须为 3 到 63 个字符，并且在您选择的 Amazon Web Services 区域的 Amazon Web Services 账户中是唯一的。有效字符：a-z、0-9 和连字符（-）。有关创建表存储桶的更多信息，请参阅创建表存储桶。

   元数据表名称必须介于 1 到 255 个字符之间，并且在表存储桶的 `aws_s3_metadata` 命名空间中是唯一的。有效的字符为小写字母、数字和下划线 (_)。

```
{
  "S3TablesDestination": {
    "TableBucketArn": "arn:aws:s3tables:us-east-2:111122223333:bucket/amzn-s3-demo-bucket",
    "TableName": "test_metadata_table"
  }
}
```

4. 使用以下命令将元数据表配置应用于通用存储桶（例如 *amzn-s3-demo-source-bucket*）：

```
aws s3api create-bucket-metadata-table-configuration \
--bucket amzn-s3-demo-source-bucket \
--metadata-table-configuration  file://./metadata-config.json \
--region us-east-2
```

5. 要验证配置是否已创建，请使用以下命令：

```
aws s3api get-bucket-metadata-table-configuration \
--bucket amzn-s3-demo-source-bucket \
--region us-east-2
```

要监控对元数据表配置的更新，可以使用 Amazon CloudTrail。有关更多信息，请参阅 the section called “CloudTrail 日志记录跟踪的 Amazon S3 存储桶级操作”。

使用 REST API

可以发送 REST 请求来创建元数据表配置。有关更多信息，请参阅《Amazon S3 API 参考》中的 CreateBucketMetadataTableConfiguration。

使用 Amazon SDK

可以使用 Amazon SDK 在 Amazon S3 中创建元数据表配置。有关信息，请参阅《Amazon S3 API Reference》中的 list of supported SDKs。

控制对元数据表的访问

要控制对 Amazon S3 元数据表的访问权限，可以使用附加到表存储桶和元数据表的基于 Amazon Identity and Access Management（IAM）资源的策略。换句话说，您可以在表存储桶级和表级控制对元数据表的访问权限。

有关控制对表存储桶和表的访问权限的更多信息，请参阅 S3 表类数据存储服务的访问管理。

> **Important**
>
> 确保您不限制 Amazon S3 写入表存储桶或元数据表。如果 Amazon S3 无法写入您的表存储桶或元数据表，则必须通过删除元数据表配置，然后创建新配置来创建新的元数据表。

还可以通过 Amazon Lake Formation 控制对元数据表中行和列的访问权限。有关更多信息，请参阅《Amazon Lake Formation Developer Guide》中的 Managing Lake Formation permissions 和 Data filtering and cell-level security in Lake Formation。

删除元数据表配置

如果您想停止更新 Amazon S3 通用存储桶的元数据表配置，可以删除附加到存储桶的元数据表配置。删除元数据表配置仅删除配置。即使您删除元数据表配置，表存储桶和您的元数据表仍然存在。但是，将不再更新元数据表。

要删除元数据表，请参阅the section called “删除元数据表”。要删除表存储桶，请参阅删除表存储桶和《Amazon S3 API Reference》中的 DeleteTableBucket。

您可以使用 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 Amazon S3 REST API 删除元数据表配置。

删除元数据表配置

使用 S3 控制台

删除元数据表配置

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 选择要从中移除元数据表配置的通用存储桶。
4. 在存储桶详细信息页面上，选择元数据选项卡。
5. 在元数据选项卡上，选择删除。
6. 在删除元数据配置对话框中，输入 **`confirm`** 以确认要删除该配置。然后选择删除。

使用 Amazon CLI

要运行以下命令，您必须安装并配置 Amazon CLI。如果未安装 Amazon CLI，请参阅《Amazon Command Line Interface 用户指南》中的安装或更新最新版本的 Amazon CLI。

或者，可以从控制台中使用 Amazon CloudShell 运行 Amazon CLI 命令。Amazon CloudShell 是一个基于浏览器、预先经过身份验证的 Shell，您可以直接从 Amazon Web Services Management Console 中启动它。有关更多信息，请参阅《Amazon CloudShell 用户指南》中的 What is CloudShell? 和 Getting started with Amazon CloudShell。

使用 Amazon CLI 删除元数据表配置

要使用以下示例命令，请将 *user input placeholders* 替换为您自己的信息。

1. 使用以下命令从通用存储桶中删除元数据表配置（例如 *amzn-s3-demo-source-bucket*）：

```
aws s3api delete-bucket-metadata-table-configuration \
--bucket amzn-s3-demo-source-bucket \
--region us-east-2
```

2. 要验证配置是否已删除，请使用以下命令：

```
aws s3api get-bucket-metadata-table-configuration \
--bucket amzn-s3-demo-source-bucket \
--region us-east-2
```

使用 REST API

可以发送 REST 请求来删除元数据表配置。有关更多信息，请参阅 DeleteBucketMetadataTableConfiguration。

使用 Amazon SDK

可以使用 Amazon SDK 在 Amazon S3 中删除元数据表配置。有关信息，请参阅 list of supported SDKs。

删除元数据表

如果您想删除为 Amazon S3 通用存储桶创建的元数据表，可以从表存储桶中删除该元数据表。

> **Note**
>
> 在删除元数据表之前，建议您先删除通用存储桶中的关联元数据表配置。有关更多信息，请参阅 the section called “删除元数据表配置”。

要删除表存储桶，请参阅删除表存储桶和《Amazon S3 API Reference》中的 DeleteTableBucket。

可以使用 Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 Amazon S3 REST API 删除元数据表。

删除元数据表

使用 Amazon CLI

要运行以下命令，您必须安装并配置 Amazon CLI。如果未安装 Amazon CLI，请参阅《Amazon Command Line Interface 用户指南》中的安装或更新最新版本的 Amazon CLI。

或者，可以从控制台中使用 Amazon CloudShell 运行 Amazon CLI 命令。Amazon CloudShell 是一个基于浏览器、预先经过身份验证的 Shell，您可以直接从 Amazon Web Services Management Console 中启动它。有关更多信息，请参阅《Amazon CloudShell 用户指南》中的 What is CloudShell? 和 Getting started with Amazon CloudShell。

使用 Amazon CLI 删除元数据表配置

要使用以下示例命令，请将 *user input placeholders* 替换为您自己的信息。

1. 使用以下命令从表存储桶（例如 *amzn-s3-demo-bucket*）中删除元数据表：

```
aws s3tables delete-table \
--table-bucket-arn arn:aws:s3tables:us-east-2:111122223333:bucket/amzn-s3-demo-bucket \
--namespace aws_s3_metadata \
--name test_metadata_table \
--region us-east-2
```

2. 要验证表是否已删除，请使用以下命令：

```
aws s3tables get-table \
--table-bucket-arn arn:aws:s3tables:us-east-2:111122223333:bucket/amzn-s3-demo-bucket \
--namespace aws_s3_metadata \
--name test_metadata_table \
--region us-east-2
```

使用 REST API

可以发送 REST 请求来删除元数据表配置。有关更多信息，请参阅《Amazon S3 API 参考》中的 DeleteTable。

使用 Amazon SDK

可以使用 Amazon SDK 在 Amazon S3 中删除元数据表配置。有关信息，请参阅《Amazon S3 API Reference》中的 list of supported SDKs。

## 查询元数据表

Amazon S3 元数据可让您使用任何支持 Apache Iceberg 格式的查询引擎来分析 S3 托管式元数据表。将 S3 表存储桶与 Amazon 分析服务集成时，可以使用诸如 Amazon Athena、Amazon Redshift 等服务来协助您对元数据表执行以下操作：

- 发现存储使用规律和趋势
- 审计对象间的 Amazon Key Management Service（Amazon KMS）加密密钥使用情况
- 通过用户定义的元数据和对象标签搜索对象
- 了解对象元数据随时间的变化
- 了解何时更新或删除对象，包括发出请求的 Amazon Web Services 账户 ID 或 IP 地址

在表存储桶与 Amazon 分析服务集成后，您可以查询元数据表。这包括联接 S3 托管式元数据表和自定义元数据表，只要元数据表存储在同一个表存储桶中，您就可以跨多个数据集进行查询。

然后，可以使用 Amazon QuickSight 创建包含查询数据的交互式控制面板。

查询定价注意事项

在元数据表上运行查询需支付额外费用。有关更多信息，请参阅您使用的查询引擎的定价信息。

有关提高查询的成本效益的信息，请参阅优化元数据表查询性能。

主题

- 使用 Amazon 分析服务查询元数据表
- 使用开源查询引擎查询元数据表
- 优化元数据表查询性能
- 元数据表查询示例
- 将自定义元数据与 S3 元数据表相联接
- 使用 Amazon QuickSight 实现元数据表数据可视化

使用 Amazon 分析服务查询元数据表

可以使用诸如 Amazon Athena、Amazon Redshift 和 Amazon EMR 等 Amazon 分析服务查询 S3 托管式元数据表。

在可以运行查询之前，必须先将您的 Amazon Web Services 账户和区域中的 S3 表存储桶与 Amazon 分析服务集成。

使用 Amazon Athena 查询元数据表

集成 S3 表存储桶与 Amazon 分析服务后，即可开始在 Athena 中查询元数据表。在查询中，将目录指定为 `s3tablescatalog`，并将数据库指定为 `aws_s3_metadata`（这是元数据表的命名空间）。有关更多信息，请参阅使用 Athena 查询 Amazon S3 表类数据存储服务。

使用 Amazon Redshift 查询元数据表

集成 S3 表存储桶与 Amazon 分析服务后，您可以创建资源链接来指向元数据表命名空间 (`aws_s3_metadata`)。完成后，您就可以开始在 Amazon Redshift 控制台中查询元数据表了。有关更多信息，请参阅使用 Amazon Redshift 访问 Amazon S3 表类数据存储服务。

使用 Amazon EMR 查询元数据表

要使用 Amazon EMR 查询元数据表，您需要创建为 Apache Iceberg 配置的 Amazon EMR 集群，然后使用 Apache Spark 连接到元数据表。您可以通过将 S3 表存储桶与 Amazon 分析服务集成，或者使用适用于 Iceberg 的开源 Amazon S3 表类数据存储服务目录客户端目录，来对此进行设置。

有关更多信息，请参阅使用 Amazon EMR 访问 Amazon S3 表类数据存储服务。

使用开源查询引擎查询元数据表

可以使用开源查询引擎（例如 Apache Spark）查询 S3 托管式元数据表。要查询元数据表，您需要适用于 Apache Iceberg 的 Amazon S3 表类数据存储服务目录客户端目录（由 Amazon 实验室托管的开源库）。

有关更多信息，请参阅使用 Apache Spark 查询 Amazon S3 表类数据存储服务。

优化元数据表查询性能

由于 S3 元数据基于 Apache Iceberg 表格式，因此您可以使用特定的时间范围来优化元数据表查询的性能和成本。

例如，以下 SQL 查询提供了 S3 通用存储桶中新对象的敏感级别：

```
SELECT key, object_tags['SensitivityLevel']
FROM aws_s3_metadata.my_metadata_table
WHERE record_type = 'CREATE'
GROUP BY object_tags['SensitivityLevel']
```

此查询将扫描整个元数据表，运行可能需要很长时间。要提高性能，您可以包括 `record_timestamp` 列以专注于特定的时间范围。以下是上一个查询的更新版本，它查看了过去一个月的新对象：

```
SELECT key, object_tags['SensitivityLevel']
FROM aws_s3_metadata.my_metadata_table
WHERE record_type = 'CREATE'
AND record_timestamp > (CURRENT_TIMESTAMP - interval '1' month)
GROUP BY object_tags['SensitivityLevel']
```

元数据表查询示例

以下示例说明如何使用标准 SQL 查询从 S3 元数据表中获取不同类型的信息。

使用这些示例时请记住：

- 这些示例是为与 Amazon Athena 结合使用而编写的。您可能需要修改示例才能使用其它查询引擎。
- 确保您了解如何优化查询。
- 将 *amzn-s3-demo-bucket* 替换为存储元数据表的 S3 表存储桶的名称。
- 将 *my_metadata_table* 替换为您正在查询的元数据表的名称。
- 有关支持的列的完整列表，请参阅 S3 元数据表架构。

按文件扩展名查找对象

以下查询返回具有特定文件扩展名（在本例中为 `.jpg`）的对象。

```
SELECT key FROM "s3tablescatalog/amzn-s3-demo-
bucket"."aws_s3_metadata"."my_metadata_table"
WHERE key LIKE '%.jpg'
AND record_type = 'CREATE'
```

列出对象删除操作

以下查询返回对象删除事件，包括发出请求的 Amazon Web Services 账户 ID 或 Amazon 服务主体。

```
SELECT DISTINCT bucket, key, sequence_number, record_type, record_timestamp, requester,
 source_ip_address, version_id
FROM "s3tablescatalog/amzn-s3-demo-bucket"."aws_s3_metadata"."my_metadata_table"
WHERE record_type = 'DELETE';
```

列出您的对象使用的 Amazon KMS 加密密钥

以下查询返回加密对象的 Amazon Key Management Service（Amazon KMS）密钥的 ARN。

```
SELECT DISTINCT kms_key_arn
FROM "s3tablescatalog/amzn-s3-demo-bucket"."aws_s3_metadata"."my_metadata_table";
```

列出不使用 KMS 密钥的对象

以下查询返回未使用 Amazon KMS 密钥加密的对象。

```
SELECT DISTINCT kms_key_arn
FROM "s3tablescatalog/amzn-s3-demo-bucket"."aws_s3_metadata"."my_metadata_table"
WHERE encryption_status NOT IN ('SSE-KMS', 'DSSE-KMS')
AND record_type = 'CREATE';
```

查看 Amazon Bedrock 提供的元数据

某些 Amazon 服务（例如 Amazon Bedrock）将对象上传到 Amazon S3。您可以查询这些服务提供的对象元数据。例如，以下查询包含用于确定 Amazon Bedrock 是否有对象上传到通用存储桶的 `user_metadata` 列。

```
SELECT DISTINCT bucket, key, sequence_number, record_type, record_timestamp,
 user_metadata
FROM "s3tablescatalog/amzn-s3-demo-bucket"."aws_s3_metadata"."my_metadata_table"
WHERE record_type = 'CREATE'
AND user_metadata['content-source'] = 'AmazonBedrock';
```

如果 Amazon Bedrock 将对象上传到存储桶，则 `user_metadata` 列将在查询结果中显示与该对象关联的以下元数据：

```
user_metadata
{content-additional-params -> requestid="CVK8FWYRW0M9JW65",
 signedContentSHA384="38b060a751ac96384cd9327eb1b1e36a21fdb71114be07434c0cc7bf63f6e1da274edebfe
 content-model-id -> bedrock-model-arn, content-source -> AmazonBedrock}
```

了解对象的当前状态

以下查询有助于您确定对象的当前状态。该查询可识别每个对象的最新版本，筛选掉已删除的对象，并根据序列号标记每个对象的最新版本。结果按 bucket、key 和 sequence_number 列排序。

```
WITH records_of_interest as (
   -- Start with a query that can narrow down the records of interest.
    SELECT * from "s3tablescatalog/amzn-s3-demo-
bucket"."aws_s3_metadata"."my_metadata_table"
),

version_stacks as (
   SELECT *,
          -- Introduce a column called 'next_sequence_number', which is the next larger
          -- sequence_number for the same key version_id in sorted order.
          LEAD(sequence_number, 1) over (partition by (bucket, key,
 coalesce(version_id, '')) order by sequence_number ASC) as next_sequence_number
   from records_of_interest
),

-- Pick the 'tip' of each version stack triple: (bucket, key, version_id).
-- The tip of the version stack is the row of that triple with the largest sequencer.
-- Selecting only the tip filters out any row duplicates.
-- This isn't typical, but some events can be delivered more than once to the table
-- and include rows that might no longer exist in the bucket (since the
-- table contains rows for both extant and extinct objects).
-- In the next subquery, eliminate the rows that contain deleted objects.
current_versions as (
    SELECT * from version_stacks where next_sequence_number is NULL
),

-- Eliminate the rows that are extinct from the bucket by filtering with
-- record_type. An object version has been deleted from the bucket if its tip is
-- record_type==DELETE.
existing_current_versions as (
    SELECT * from current_versions where not (record_type = 'DELETE' and
 is_delete_marker = FALSE)
),

-- Optionally, to determine which of several object versions is the 'latest',
-- you can compare their sequence numbers. A version_id is the latest if its
-- tip's sequencer is the largest among all other tips in the same key.
with_is_latest as (
    SELECT *,
```

```
            -- Determine if the sequence_number of this row is the same as the largest
 sequencer for the key that still exists.
            sequence_number = (MAX(sequence_number) over (partition by (bucket, key)))
 as is_latest_version
    FROM existing_current_versions
)

SELECT * from with_is_latest
ORDER BY bucket, key, sequence_number;
```

将自定义元数据与 S3 元数据表相联接

您可以分析 S3 托管式元数据表和客户（自行管理的）元数据表中的数据。通过使用标准 SQL JOIN 运算符，您可以查询来自这些多个来源的数据。

以下示例 SQL 查询在 S3 托管式元数据表 (*my_s3_metadata_table*) 和自行管理的元数据表 (*my_self_managed_metadata_table*) 之间查找匹配的记录。该查询还会根据 CREATE 事件筛选信息，这些事件表明已将新对象（或对象的新版本）写入存储桶。(有关更多信息，请参阅 S3 元数据表架构。)

```
SELECT *
FROM aws_s3_metadata.my_s3_metadata_table a
JOIN my_namespace.my_self_managed_metadata_table b
ON a.bucket = b.bucket AND a.key = b.key AND a.version_id = b.version_id
WHERE a.record_type = 'CREATE';
```

使用 Amazon QuickSight 实现元数据表数据可视化

借助 Amazon QuickSight，可以创建交互式控制面板，以分析和可视化有关 S3 托管式元数据表的 SQL 查询结果。QuickSight 控制面板有助于您监控统计数据、跟踪更改并获得有关元数据表的操作见解。

有关元数据表的控制面板可能会向您显示：

- 有多少个对象属于不同的存储类？
- 与大型对象相比，小型对象占存储数据的百分比是多少？
- 我的存储桶中有哪些类型的对象？
- 与删除对象相比，对象上传的百分比是多少？

集成 S3 表存储桶与 Amazon 分析服务后，您可以从元数据表中创建数据集，然后通过从查询引擎中使用 SPICE 或直接 SQL 查询，来在 Amazon QuickSight 中使用这些数据集。QuickSight 支持将 Amazon Athena 和 Amazon Redshift 作为数据来源。

有关更多信息，请参阅 Visualizing table data with Amazon QuickSight。

# 上传对象

在您将文件上传至 Amazon S3 时，文件会存储为 S3 对象。对象由文件数据和描述对象的元数据组成。一个存储桶中可以有无限量的对象。您需要拥有存储桶写入权限，才能将文件上传至 Amazon S3 存储桶。有关访问权限的更多信息，请参阅Amazon S3 的身份和访问管理。

您可以将任何类型的文件上传至 S3 存储桶，包括图像、备份、数据、电影等。可使用 Amazon S3 控制台上传的文件的最大大小为 160 GB。要上传大于 160GB 的文件，请使用 Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 Amazon S3 REST API。

如果启用了版本控制的存储桶中已存在所上传对象的键名，则 Amazon S3 会创建该对象的另一个版本，而不是替换现有对象。有关启用版本控制的更多信息，请参阅在存储桶上启用版本控制。

根据您要上传的数据大小，Amazon S3 提供以下选项：

- 使用 Amazon SDK、REST API 或 Amazon CLI 在单个操作中上传对象 – 您可以在单个 PUT 操作中上传最大为 5GB 的单个对象。
- 使用 Amazon S3 控制台上传单个对象 – 通过 Amazon S3 控制台，您可以上传最大 160GB 的单个对象。
- 使用 Amazon SDK、REST API 或 Amazon CLI 分段上传对象 – 您可以使用分段上传 API 操作来上传单个大型对象（最大大小为 5TB）。

  分段上传 API 操作旨在改进大型对象的上传体验。您可以分段上传对象。这些对象分段可以按任何顺序并行独立上传。您可以对大小在 5 MB 到 5 TB 范围内的对象使用分段上传。有关更多信息，请参阅 在 Amazon S3 中使用分段上传来上传和复制对象。

当您上传对象时，默认情况下，将使用具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）自动加密对象。当您下载对象时，该对象将被解密。有关更多信息，请参阅为 Amazon S3 存储桶设置默认服务器端加密行为和利用加密来保护数据。

上传对象时，如果您想使用不同类型的默认加密，也可以在 S3 PUT 请求中指定具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS），或者将目标存储桶中的

默认加密配置设置为使用 SSE-KMS 来加密数据。有关 SSE-KMS 的更多信息，请参阅 使用 Amazon KMS (SSE-KMS) 指定服务器端加密。如果您希望使用其他账户拥有的 KMS 密钥，则您必须有权使用该密钥。有关 KMS 密钥的跨账户权限的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的创建其他账户可以使用的 KMS 密钥。

如果您在 Amazon S3 中遇到拒绝访问（403 禁止访问）错误，请参阅排查 Amazon S3 中的拒绝访问（403 Forbidden）错误详细了解其常见原因。

## 上传对象

使用 S3 控制台

此过程介绍如何使用控制台将对象和文件夹上传到 Amazon S3 存储桶。

上传对象时，对象键名称是文件名和任何可选前缀。在 Amazon S3 控制台中，您可以创建文件夹来组织对象。在 Amazon S3 中，文件夹表示为出现在对象键名称中的前缀。如果您将单个对象上传到 Amazon S3 控制台中的文件夹，则文件夹名称将包含在对象键名称中。

例如，如果您将名为的对象上传 `sample1.jpg` 到名为 `backup` 的文件夹，则密钥名称为 `backup/sample1.jpg`。但是，对象会像 `sample1.jpg` 在 `backup` 文件夹中一样在控制台中显示。有关键名称的更多信息，请参阅 使用对象元数据。

> **Note**
>
> 如果在 Amazon S3 控制台中重命名对象或更改诸如存储类、加密或元数据等任何属性，将创建一个新对象来替换旧对象。如果启用 S3 版本控制，则会创建对象的新版本，而现有对象将变为旧版本。更改属性的角色也会成为新对象（或对象版本）的拥有者。

上传文件夹时，Amazon S3 会将所有文件和子文件夹从指定文件夹中上传至存储桶。然后，它会分配由上传文件名和文件夹名组成的对象键名。例如，如果您上传包含 `/images` 和 `sample1.jpg` 这两个文件的名为 `sample2.jpg` 的文件夹，则 Amazon S3 会上传这两个文件，然后分配相应的键名 `images/sample1.jpg` 和 `images/sample2.jpg`。键名包括作为前缀的文件夹名。Amazon S3 控制台仅显示最后一个“/”后面的键名部分。例如，在 `images` 文件夹中，`images/sample1.jpg` 和 `images/sample2.jpg` 对象显示为 `sample1.jpg` 和 `sample2.jpg`。

将文件夹和文件上传到 S3 存储桶

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。

2. 在左侧导航窗格中，选择存储桶。
3. 在 Buckets（存储桶）列表中，请选择要将文件夹和文件上传到的存储桶的名称。
4. 请选择 Upload（上传）。
5. 在上传窗口中，执行下列操作之一：
   - 将文件和文件夹拖放到上传窗口。
   - 选择添加文件或添加文件夹，选择要上传的文件或文件夹，然后选择打开。
6. 要启用版本控制，请在目标下选择启用存储桶版本控制。
7. 要上传列出的文件和文件夹而不配置其他上传选项，请选择页面底部的上传。

   Amazon S3 会上传您的对象和文件夹。上传完成后，您可以在上传：状态页面上看到成功消息。

### 配置其他对象属性

1. 要更改访问控制列表权限，请选择 Permissions（权限）。
2. 在 Access control list (ACL) [访问控制列表 (ACL)]下，编辑权限。

   有关对象访问权限的信息，请参阅 使用 S3 控制台为对象设置 ACL 权限。您可以向公众（世界上的每一个人）授予对您的对象的读取访问权限，使其能够获取您正在上传的所有文件。但是，我们建议您不要更改公共读取访问的默认设置。授予公有读取访问权限适用于一小部分的使用案例（如存储桶用于网站时）。您始终可以在上传对象后更改对象权限。
3. 要配置其他附加属性，请选择 Properties（属性）。
4. 在存储类下，为正在上传的文件选择存储类。

   有关存储类的更多信息，请参阅 了解和管理 Amazon S3 存储类。
5. 要更新对象的加密设置，请在服务器端加密设置下执行以下操作：
   a. 选择 Specify an encryption key（指定加密密钥）。
   b. 在加密设置下，选择使用默认加密的存储桶设置或覆盖默认加密的存储桶设置。
   c. 如果您选择覆盖默认加密的存储桶设置，则必须配置以下加密设置。
      - 要使用由 Amazon S3 托管的密钥加密上传的文件，请选择 Amazon S3 托管式密钥（SSE-S3）。

        有关更多信息，请参阅 使用具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）。

- 要使用存储在 Amazon Key Management Service（Amazon KMS）中的密钥加密上传的文件，请选择 Amazon Key Management Service 密钥（SSE-KMS）。然后，为 Amazon KMS 密钥选择以下选项之一：
  - 要从可用的 KMS 密钥列表中进行选择，请选择从您的 Amazon KMS keys 中进行选择，然后从可用密钥的列表中选择您的 KMS 密钥。

    Amazon 托管式密钥（aws/s3）和您的客户自主管理型密钥都显示在此列表中。有关客户自主管理型密钥的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的客户密钥和 Amazon 密钥。
  - 要输入 KMS 密钥 ARN，请选择输入 Amazon KMS key ARN，然后在显示的字段中输入您的 KMS 密钥 ARN。
  - 要在 Amazon KMS 控制台中创建新的客户自主管理型密钥，请选择创建 KMS 密钥。

    有关创建 Amazon KMS key 的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的创建密钥。

    > **Important**
    >
    > 您只能使用与存储桶所在相同的 Amazon Web Services 区域中可用的 KMS 密钥。Amazon S3 控制台仅列出与存储桶位于同一区域中的前 100 个 KMS 密钥。要使用未列出的 KMS 密钥，您必须输入 KMS 密钥 ARN。如果您希望使用其他账户拥有的 KMS 密钥，则必须首先有权使用该密钥，然后必须输入相应的 KMS 密钥 ARN。
    >
    > Amazon S3 仅支持对称加密 KMS 密钥，不支持非对称 KMS 密钥。有关更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的确定对称和非对称 KMS 密钥。

6. 要使用其他校验和，请选择 On（打开）。然后对于 Checksum function（校验和函数），选择要使用的函数。Amazon S3 在收到整个对象后计算并存储校验和值。您可以使用 Precalculated value（预计算值）框来提供预先计算的值。这样，Amazon S3 会将您提供的值与其计算的值进行比较。如果两个值不匹配，Amazon S3 将生成错误。

   其他校验和使您能够指定要用于验证数据的校验和算法。有关其他校验和的更多信息，请参阅在 Amazon S3 中检查对象完整性。
7. 要向上传的所有对象添加标签，请选择 Add tag (添加标签)。在键字段中输入标签名称。输入标签的值。

对象标签为您提供了对存储进行分类的方法。每个标签都是一个键-值对。键和标签值区分大小写。对于每个对象，您最多可以有 10 个标签。标签键的长度最大可以为 128 个 Unicode 字符，标签值的长度最大可以为 255 个 Unicode 字符。有关对象标签的更多信息，请参阅 使用标签对存储进行分类。

8. 要添加元数据，请选择添加元数据。

   a. 在类型下，请选择系统定义或用户定义。

      对于系统定义元数据，您可以选择通用的 HTTP 标头，如 Content-Type 和 Content-Disposition。有关系统定义元数据的列表以及您能否添加值的信息，请参阅系统定义的对象元数据。以前缀 `x-amz-meta-` 开头的任何元数据都被视为用户定义的元数据。用户定义元数据会与对象存储在一起，并会在您下载该对象时返回。密钥及其值均必须符合 US-ASCII 标准。用户定义元数据最大可为 2 KB。如需详细了解系统定义和用户定义的元数据，请参阅使用对象元数据。

   b. 对于键，请选择一个键。

   c. 键入该键的值。

9. 要上传对象，请选择上传。

   Amazon S3 将上传您的对象。上传完成后，您可以在上传：状态页面上看到成功消息。

10. 请选择 Exit（退出）。

使用 Amazon CLI

您可以发送 PUT 请求，在单个操作中上传最大 5 GB 的对象。有关更多信息，请参阅 Amazon CLI 命令参考中的 `PutObject` 示例。

使用 REST API

您可以发送 REST 请求以上传对象。您可以发送 PUT 请求以在单个操作中上传数据。有关更多信息，请参阅 PUT Object。

使用 Amazon SDK

您可以使用 Amazon SDK 在 Amazon S3 中上传对象。SDK 向您提供了包装程序库，使您可以更轻松地上传数据。有关信息，请参阅支持的 SDK 列表。

以下是几个特色级 SDK 的示例：

.NET

以下 C# 代码示例将使用两个 PutObjectRequest 请求创建两个对象：

- 第一个 PutObjectRequest 请求将文本字符串保存为示例对象数据。它还指定存储桶和对象键名。
- 第二个 PutObjectRequest 请求通过指定文件名上传文件。此请求还指定 ContentType 标头和可选对象元数据（标题）。

有关设置和运行代码示例的信息，请参阅《适用于 .NET 的 Amazon SDK 开发人员指南》中的适用于 .NET 的 Amazon SDK 入门。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class UploadObjectTest
    {
        private const string bucketName = "*** bucket name ***";
        // For simplicity the example creates two objects from the same file.
        // You specify key names for these objects.
        private const string keyName1 = "*** key name for first object created ***";
        private const string keyName2 = "*** key name for second object created
 ***";
        private const string filePath = @"*** file path ***";
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.EUWest1;

        private static IAmazonS3 client;

        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            WritingAnObjectAsync().Wait();
        }

        static async Task WritingAnObjectAsync()
        {
```

```
            try
            {
                // 1. Put object-specify only key name for the new object.
                var putRequest1 = new PutObjectRequest
                {
                    BucketName = bucketName,
                    Key = keyName1,
                    ContentBody = "sample text"
                };

                PutObjectResponse response1 = await
 client.PutObjectAsync(putRequest1);

                // 2. Put the object-set ContentType and add metadata.
                var putRequest2 = new PutObjectRequest
                {
                    BucketName = bucketName,
                    Key = keyName2,
                    FilePath = filePath,
                    ContentType = "text/plain"
                };

                putRequest2.Metadata.Add("x-amz-meta-title", "someTitle");
                PutObjectResponse response2 = await
 client.PutObjectAsync(putRequest2);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine(
                        "Error encountered ***. Message:'{0}' when writing an
 object"
                        , e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine(
                    "Unknown encountered on server. Message:'{0}' when writing an
 object"
                    , e.Message);
            }
        }
    }
}
```

Java

以下示例将创建两个对象。第一个对象将一个文本字符串作为数据，第二对象是一个文件。该示例通过在对 AmazonS3Client.putObject() 的调用中直接指定存储桶名称、对象键和文本数据来创建第一个对象。该示例通过使用指定存储桶、对象键和文件路径的 PutObjectRequest 来创建第二个对象。PutObjectRequest 还指定 ContentType 标头和标题元数据。

有关创建和测试有效示例的说明，请参阅《适用于 Java 的 Amazon SDK 开发人员指南》中的入门。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.ObjectMetadata;
import com.amazonaws.services.s3.model.PutObjectRequest;

import java.io.File;
import java.io.IOException;

public class UploadObject {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String stringObjKeyName = "*** String object key name ***";
        String fileObjKeyName = "*** File object key name ***";
        String fileName = "*** Path to file to upload ***";

        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withRegion(clientRegion)
                    .build();

            // Upload a text string as a new object.
            s3Client.putObject(bucketName, stringObjKeyName, "Uploaded String
 Object");
```

```
            // Upload a file as a new object with ContentType and title specified.
            PutObjectRequest request = new PutObjectRequest(bucketName,
 fileObjKeyName, new File(fileName));
            ObjectMetadata metadata = new ObjectMetadata();
            metadata.setContentType("plain/text");
            metadata.addUserMetadata("title", "someTitle");
            request.setMetadata(metadata);
            s3Client.putObject(request);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

### JavaScript

以下示例将现有文件上传到特定区域中的 Amazon S3 存储桶。

```
import { readFile } from "node:fs/promises";

import {
  PutObjectCommand,
  S3Client,
  S3ServiceException,
} from "@aws-sdk/client-s3";

/**
 * Upload a file to an S3 bucket.
 * @param {{ bucketName: string, key: string, filePath: string }}
 */
export const main = async ({ bucketName, key, filePath }) => {
  const client = new S3Client({});
  const command = new PutObjectCommand({
    Bucket: bucketName,
    Key: key,
    Body: await readFile(filePath),
  });
```

```
  try {
    const response = await client.send(command);
    console.log(response);
  } catch (caught) {
    if (
      caught instanceof S3ServiceException &&
      caught.name === "EntityTooLarge"
    ) {
      console.error(
        `Error from S3 while uploading object to ${bucketName}. \
The object was too large. To upload objects larger than 5GB, use the S3 console
 (160GB max) \
or the multipart upload API (5TB max).`,
      );
    } else if (caught instanceof S3ServiceException) {
      console.error(
        `Error from S3 while uploading object to ${bucketName}.  ${caught.name}:
 ${caught.message}`,
      );
    } else {
      throw caught;
    }
  }
};
```

PHP

此示例将指导您使用 适用于 PHP 的 Amazon SDK 中的类上传大小最大为 5GB 的对象。对于更大的文件，您必须使用分段上传 API 操作。有关更多信息，请参阅 在 Amazon S3 中使用分段上传来上传和复制对象。

有关适用于 Ruby 的 Amazon 开发工具包 API 的更多信息，请转到适用于 Ruby 的 Amazon 开发工具包 – 版本 2。

Example — 通过上传数据在 Amazon S3 存储桶中创建对象

通过使用 `putObject()` 方法来上传数据，以下 PHP 示例在指定存储桶中创建对象。

```
 require 'vendor/autoload.php';

use Aws\S3\Exception\S3Exception;
use Aws\S3\S3Client;
```

```
$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

try {
    // Upload data.
    $result = $s3->putObject([
        'Bucket' => $bucket,
        'Key'    => $keyname,
        'Body'   => 'Hello, world!',
        'ACL'    => 'public-read'
    ]);

    // Print the URL to the object.
    echo $result['ObjectURL'] . PHP_EOL;
} catch (S3Exception $e) {
    echo $e->getMessage() . PHP_EOL;
}
```

### Ruby

适用于 Ruby 的 Amazon SDK – 版本 3 通过两种方式将对象上传到 Amazon S3。第一种方式使用托管式文件上传程序，从而能更轻松地从磁盘上传任何大小的文件。使用托管文件上传程序方法：

1. 创建 `Aws::S3::Resource` 类的实例。
2. 按存储桶名称和键引用目标对象。位于存储桶中的对象具有可识别每个对象的唯一密钥。
3. 在对象上调用 `#upload_file`。

#### Example

```
require 'aws-sdk-s3'

# Wraps Amazon S3 object actions.
class ObjectUploadFileWrapper
  attr_reader :object
```

```
  # @param object [Aws::S3::Object] An existing Amazon S3 object.
  def initialize(object)
    @object = object
  end

  # Uploads a file to an Amazon S3 object by using a managed uploader.
  #
  # @param file_path [String] The path to the file to upload.
  # @return [Boolean] True when the file is uploaded; otherwise false.
  def upload_file(file_path)
    @object.upload_file(file_path)
    true
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't upload file #{file_path} to #{@object.key}. Here's why:
 #{e.message}"
    false
  end
end

# Example usage:
def run_demo
  bucket_name = "amzn-s3-demo-bucket"
  object_key = "my-uploaded-file"
  file_path = "object_upload_file.rb"

  wrapper = ObjectUploadFileWrapper.new(Aws::S3::Object.new(bucket_name,
 object_key))
  return unless wrapper.upload_file(file_path)

  puts "File #{file_path} successfully uploaded to #{bucket_name}:#{object_key}."
end

run_demo if $PROGRAM_NAME == __FILE__
```

适用于 Ruby 的 Amazon SDK - 版本 3 上传对象的第二种方式是使用 `Aws::S3::Object` 的 `#put` 方法。如果对象为字符串或者为不是磁盘上的文件的 I/O 对象，此方式很有用。要使用此方法，请执行以下操作：

1. 创建 `Aws::S3::Resource` 类的实例。
2. 按存储桶名称和键引用目标对象。
3. 调用 `#put`，从而传入字符串或 I/O 对象。

### Example

```
require 'aws-sdk-s3'

# Wraps Amazon S3 object actions.
class ObjectPutWrapper
  attr_reader :object

  # @param object [Aws::S3::Object] An existing Amazon S3 object.
  def initialize(object)
    @object = object
  end

  def put_object(source_file_path)
    File.open(source_file_path, 'rb') do |file|
      @object.put(body: file)
    end
    true
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't put #{source_file_path} to #{object.key}. Here's why:
 #{e.message}"
    false
  end
end

# Example usage:
def run_demo
  bucket_name = "amzn-s3-demo-bucket"
  object_key = "my-object-key"
  file_path = "my-local-file.txt"

  wrapper = ObjectPutWrapper.new(Aws::S3::Object.new(bucket_name, object_key))
  success = wrapper.put_object(file_path)
  return unless success

  puts "Put file #{file_path} into #{object_key} in #{bucket_name}."
end

run_demo if $PROGRAM_NAME == __FILE__
```

## 防止上传具有相同键名称的对象

在对上传操作使用有条件写入来创建对象之前，您可以检查存储桶中是否存在该对象。这样可以防止覆盖现有数据。当上传时，有条件写入将验证存储桶中尚不存在具有相同键名称的现有对象。

可以将有条件写入用于 PutObject 或 CompleteMultipartUpload 请求。

有关有条件请求的更多信息，请参阅使用有条件请求向 S3 操作添加前提条件。

## 在 Amazon S3 中使用分段上传来上传和复制对象

分段上传支持您将单个对象作为一组分段上传到 Amazon S3。每个分段都是对象数据的连续部分。您可以独立上传以及按任意顺序上传这些对象分段。对于上传，更新后的 Amazon 客户端会自动计算对象的校验和，并将其连同对象的大小一起作为请求的一部分发送到 Amazon S3。如果任意分段传输失败，可以重新传输该分段且不会影响其它分段。上传完对象的所有分段后，Amazon S3 将汇集这些分段并创建对象。最佳做法是对 100 MB 或更大的对象使用分段上传，而不是在单个操作中上传它们。

使用分段上传可提供以下优势：

- 提高吞吐量 – 您可以并行上传分段以提高吞吐量。
- 从任何网络问题中快速恢复 – 较小的分段大小可以将由于网络错误而需重启失败的上传所产生的影响降至最低。
- 暂停和恢复对象上传 – 您可以在一段时间内逐步上传对象分段。启动分段上传后，不存在过期期限；您必须显式地完成或停止分段上传。
- 在您知道对象的最终大小前开始上传：您可以在创建对象时将其上传。

我们建议您按以下方式使用分段上传：

- 如果您在稳定的高带宽网络上传大型对象，请通过并行上传对象分段来实现多线程性能，从而使用分段上传以最大限度地利用您的可用带宽。
- 如果您通过断点网络进行上传，请使用分段上传，通过避免重新开始上传来提高应对网络错误的复原能力。在使用分段上传时，只需重试上传在上传期间中断的分段即可。而无需从头重新开始上传对象。

> **Note**
>
> 有关将 Amazon S3 Express One Zone 存储类与目录存储桶配合使用的更多信息，请参阅 S3 Express One Zone 和使用目录存储桶。有关将分段上传用于 S3 Express One Zone 和目录存储桶的更多信息，请参阅对目录桶使用分段上传。

## 分段上传流程

分段上传分为三个步骤：开始上传、上传对象分段，以及在上传所有分段后完成分段上传。在收到完成分段上传请求后，Amazon S3 会利用上传的分段构造对象，而您可以像访问您存储桶中的任何其它对象一样访问该对象。

您可以列出所有正在执行的分段上传，或者获取为特定分段上传操作上传的分段列表。以上每个操作都在本节中进行了说明。

### 分段上传开始

当您发送请求以开始分段上传时，请确保指定校验和类型。然后，Amazon S3 将返回具有上传 ID 的响应，此 ID 是分段上传的唯一标识符。当您上传分段、列出分段、完成上传或停止上传时，需要此上传 ID。如果您想要提供描述正上传的对象的元数据，必须在请求中提供它以便开始分段上传。匿名用户无法发起分段上传。

### 分段上传

上传分段时，除了上传 ID 之外，还必须指定分段编号。您可以选择 1 和 10000 之间的任意分段编号。分段编号在您正在上传的对象中唯一地识别分段及其位置。您选择的分段编号不必是连续序列（例如，它可以是 1、5 和 14）。请注意，如果您使用之前上传的分段的同一分段编号上传新分段，则之前上传的分段会被覆盖。

当您上传分段时，Amazon S3 将在响应中返回校验和算法类型，其中每个分段的校验和值作为标头。对于每个分段上传，您必须记录分段编号和 ETag 值。您必须在随后的请求中包括这些值以完成分段上传。每个分段在上传时都有自己的 ETag。但是，一旦分段上传完成并且合并了所有分段，所有分段都会属于一个 ETag，作为多个校验和的校验和。

> **Important**
>
> 启动分段上传并上传一个或多个分段之后，您必须完成或停止分段上传，才能停止因存储已上传的分段而产生费用。只有在完成或停止分段上传之后，Amazon S3 才会释放分段存储并停止向您收取分段存储费用。

停止分段上传后，无法再次使用该上传 ID 上传任何分段。如果分段上传正在进行中，则即使在您停止上传后，它们仍然可能会成功或失败。为了确保释放所有分段使用的所有存储，必须仅在完成所有分段的上传后才停止分段上传。

### 分段上传完成

完成分段上传时，Amazon S3 通过按升序的分段编号规范化分段来创建对象。如果在开始分段上传请求中提供了任何对象元数据，则 Amazon S3 会将该元数据与对象相关联。成功完成请求后，分段将不再存在。

完成分段上传 请求必须包括上传 ID、分段编号及其相应的 ETag 值的列表。Amazon S3 响应包括可唯一地识别组合对象数据的 ETag。此 ETag 无需成为对象数据的 MD5 哈希。

当您在分段上传期间提供完整的对象校验和时，Amazon SDK 会将校验和传递给 Amazon S3，而 S3 会在服务器端验证对象完整性，将其与接收到的值进行比较。然后，如果值匹配，S3 将存储对象。如果这两个值不匹配，Amazon S3 将使请求失败并出现 `BadDigest` 错误。对象的校验和还存储在对象元数据中，您稍后将使用这些元数据来验证对象的数据完整性。

### 分段上传调用示例

对于此示例，假设您正在为一个 100 GB 的文件生成分段上传。在这种情况下，您应在整个过程中进行以下 API 调用。总共将有 1002 个 API 调用。

- 一个用于启动该过程的 `CreateMultipartUpload` 调用。
- 1000 个单独的 `UploadPart` 调用，每次上传一个 100 MB 的分段，总大小为 100 GB。
- 用于完成该过程的 `CompleteMultipartUpload` 调用。

### 分段上传列表

您可以列出特定分段上传或所有正在进行的分段上传的分段。列出分段操作将返回您已为特定分段上传而上传的分段信息。对于每个列出分段请求，Amazon S3 将返回有关特定分段上传的分段信息，最多为 1000 个分段。如果分段上传中的分段数量超过 1000 个，您必须发送一系列列出分段请求以检索所有分段。请注意，返回的分段列表不包括未完成上传的分段。使用列出分段上传 操作，您可以获得正在进行的分段上传的列表。

正在进行的分段上传是已开始但还未完成或停止的上传。每个请求将返回最多 1000 个分段上传。如果正在进行的分段上传超过 1000 个，您必须发送其他请求才能检索剩余的分段上传。仅使用返回的列表进行验证。

> **Important**
>
> 发送完成分段上传 请求时，请勿使用此列表的结果。相反，当上传分段和 Amazon S3 返回的相应 ETag 值时，请保留您自己的指定分段编号的列表。

## 使用分段上传操作的校验和

在将对象上传到 Amazon S3 时，可指定校验和算法以供 Amazon S3 使用。默认情况下，Amazon SDK 和 S3 控制台对所有对象上传使用一种算法，您可以覆盖该算法。如果您使用的是较旧的 SDK，并且您上传的对象没有指定的校验和，则 Amazon S3 会自动使用 CRC-64/NVME (CRC64NVME) 校验和算法。（这也是高效数据完整性验证的推荐选项。）当使用 CRC-64/NVME 时，Amazon S3 会在多分段或单分段上传完成后计算完整对象的校验和。CRC-64/NVME 校验和算法用于计算整个对象的直接校验和，或每个单独分段的多个校验和的校验和。

在使用分段上传将对象上传到 S3 后，Amazon S3 将计算每个分段或完整对象的校验和值并存储这些值。可以通过以下方式使用 S3 API 或 Amazon SDK 来检索校验和值：

- 对于单个分段，可以使用 `GetObject` 或 `HeadObject`。如果您想在分段上传仍在进行时检索各个分段的校验和值，可以使用 `ListParts`。
- 对于整个对象，可以使用 `PutObject`。如果要使用完整对象校验和执行分段上传，请通过指定完整对象校验和类型来使用 `CreateMultipartUpload` 和 `CompleteMultipartUpload`。要验证整个对象的校验和值或要确认分段上传中使用的是哪种校验和类型，请使用 `ListParts`。

> **Important**
>
> 如果您将分段上传与校验和结合使用，则上传每个分段（在分段上传中）时的分段编号必须使用连续的分段编号并从 1 开始。使用校验和时，如果您尝试使用非连续分段编号完成分段上传请求，Amazon S3 将生成 `HTTP 500 Internal Server` 错误。

有关校验和如何处理分段上传对象的更多信息，请参阅在 Amazon S3 中检查对象完整性。

有关用于演示如何使用分段上传以及额外的校验和来上传对象的端到端过程，请参阅教程：通过分段上传来上传对象并验证其数据完整性。

## 并发分段上传操作

在分布式开发环境中，您的应用程序可以同时在同一对象上开始多个更新。您的应用程序可能会使用同一对象键开始多个分段上传。然后，对于其中每个上传，您的应用程序可以上传分段并将完成上传请求发送到 Amazon S3，以创建对象。当存储桶启用了 S3 版本控制时，完成分段上传将始终创建一个新版本。当您在启用版本控制的存储桶中启动使用相同对象键的多个分段上传时，对象的当前版本将由最新（`createdDate`）开始的上传决定。

例如，您在上午 10:00 启动对某个对象的 `CreateMultipartUpload` 请求。然后，您在上午 11:00 提交对同一对象的第二个 `CreateMultipartUpload` 请求。因为第二个请求是最新提交的，所以上午 11:00 的请求所上传的对象将成为当前版本，即使第一个上传是在第二个上传之后完成的，也是如此。对于未启用版本控制的存储桶，在启动分段上传与完成分段上传期间接收的任何其它请求都可能会优先。

另一个可以优先处理并发分段上传请求的例子是，在使用某个键开始分段上传之后，其它操作删除了该键。在完成此操作之前，完成分段上传的响应可能表示在未看到对象的情况下成功创建了对象。

## 防止在分段上传期间上传具有相同键名称的对象

在对上传操作使用有条件写入来创建对象之前，您可以检查存储桶中是否存在该对象。这样可以防止覆盖现有数据。当上传时，有条件写入将验证存储桶中尚不存在具有相同键名称的现有对象。

可以将有条件写入用于 PutObject 或 CompleteMultipartUpload 请求。

有关有条件请求的更多信息，请参阅使用有条件请求向 S3 操作添加前提条件。

## 分段上传和定价

开始分段上传后，Amazon S3 将保留所有分段，直到您完成或停止上传。在整个其生命周期内，您将支付有关此分段上传及其关联分段的所有存储、带宽和请求的费用。

将根据在上传各个分段时指定的存储类对这些分段收费。但是，如果将这些分段上传到 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive，则无需为这些分段付费。在上传完成之前，针对 S3 Glacier Flexible Retrieval 存储类的 PUT 请求的正在上传的分段采用 S3 Standard 存储费率按 S3 Glacier Flexible Retrieval 暂存存储计费。此外，`CreateMultipartUpload` 和 `UploadPart` 均按 S3 Standard 费率计费。只有 `CompleteMultipartUpload` 请求按 S3 Glacier Flexible Retrieval 费率计费。同样，在上传完成之前，针对 S3 Glacier Deep Archive 存储类的 PUT 请求的正在上传的分段采用 S3 Standard 存储费率按 S3 Glacier Flexible Retrieval 暂存存储计费，而只有 `CompleteMultipartUpload` 请求按 S3 Glacier Deep Archive 费率计费。

如果您停止分段上传，Amazon S3 将删除上传构件和已上传的任何分段。您无需为这些构件付费。无论指定的存储类如何，删除未完成的分段上传均不收取提前删除费用。有关定价的更多信息，请参阅 Amazon S3 定价。

> **Note**
>
> 为了最大程度地降低存储成本，我们建议您配置生命周期规则，以便使用 `AbortIncompleteMultipartUpload` 操作在指定的天数后删除未完成的分段上传。有关创建生命周期规则以删除未完成的分段上传的更多信息，请参阅配置存储桶生命周期配置以删除未完成的分段上传。

## 分段上传的 API 支持

Amazon Simple Storage Service API 参考的下面几节描述了适用于分段上传的 REST API。

有关使用 Amazon Lambda 函数的分段上传演练，请参阅 Uploading large objects to Amazon S3 using multipart upload and transfer acceleration。

- 创建分段上传
- 上传分段
- 上传分段（复制）
- 完成分段上传
- 中止分段上传
- 列出分段
- 列出分段上传

## Amazon Command Line Interface 对于分段上传的支持

Amazon Command Line Interface 中的以下主题介绍了适用于分段上传的操作。

- 开始分段上传
- 上传分段
- 上传分段（复制）
- 完成分段上传
- 中止分段上传

- 列出分段
- 列出分段上传

## Amazon SDK 对于分段上传的支持

您可以使用 Amazon SDK 分段上传对象。有关 API 操作支持的 Amazon SDK 的列表，请参阅：

- 创建分段上传
- 上传分段
- 上传分段（复制）
- 完成分段上传
- 中止分段上传
- 列出分段
- 列出分段上传

## 分段上传 API 和权限

您必须具有使用分段上传操作的所需权限。您可以使用访问控制列表（ACL）、存储桶策略或用户策略来授予个人执行这些操作的权限。下表列出了使用 ACL、存储桶策略或用户策略时，各种分段上传操作的所需权限。

| 操作 | 所需权限 |
| --- | --- |
| 创建分段上传 | 必须支持您对于对象执行 `s3:PutObject` 操作，才能创建分段上传请求。<br><br>存储桶拥有者可以允许其他主体执行 `s3:PutObject` 操作。 |
| 开始分段上传 | 必须支持您对于对象执行 `s3:PutObject` 操作，才能发起分段上传。<br><br>存储桶拥有者可以允许其他主体执行 `s3:PutObject` 操作。 |
| 发起者 | 标识分段上传发起者的容器元素。如果发起者是 Amazon Web Services 账户，此元素将提供与 Owner 元素相同的信息。如果发起者是 IAM 用户，此元素将提供用户 ARN 和显示名称。 |
| 上传分段 | 必须允许您对对象执行 `s3:PutObject` 操作，才能上传分段。 |

| 操作 | 所需权限 |
| --- | --- |
| | 存储桶拥有者必须允许发起者对对象执行 s3:PutObject 操作，以便发起者可以上传该对象的分段。 |
| 上传分段（复制） | 必须允许您对对象执行 s3:PutObject 操作，才能上传分段。因为您正在上传现有对象的分段，因此必须允许您对源对象执行 s3:GetObject 。<br><br>存储桶拥有者必须允许发起者对对象执行 s3:PutObject 操作，发起者才能上传该对象的分段。 |
| 完成分段上传 | 必须允许您对对象执行 s3:PutObject 操作，才能完成分段上传。<br><br>存储桶拥有者必须允许发起者对对象执行 s3:PutObject 操作，以便发起者可以完成该对象的分段上传。 |
| 停止分段上传 | 必须允许您执行 s3:AbortMultipartUpload 操作，才能停止分段上传。<br><br>默认情况下，支持存储桶拥有者和分段上传的发起者执行此操作，作为 IAM 和 S3 存储桶策略的一部分。如果发起者是 IAM 用户，也允许该用户的 Amazon Web Services 账户停止此分段上传。使用 VPC 端点策略，分段上传的发起者不会自动获得执行 s3:AbortMultipartUpload 操作的权限。<br><br>除了这些默认情况之外，存储桶拥有者可以允许其他主体对对象执行 s3:AbortMultipartUpload 操作。存储桶拥有者可以拒绝任何主体，使其无法执行 s3:AbortMultipartUpload 操作。 |
| 列出分段 | 您必须得到可以执行 s3:ListMultipartUploadParts 操作的允许，才能在分段上传中列出分段。<br><br>在默认情况下，存储桶拥有者有权为任何针对存储桶的分段上传列出分段。分段上传的发起者有权为特定分段上传列出分段。如果分段上传的发起者是 IAM 用户，则控制该 IAM 用户的 Amazon Web Services 账户 同样有权列出此次上传的分段。<br><br>除了这些默认情况之外，存储桶拥有者可以允许其他主体对对象执行 s3:ListMultipartUploadParts 操作。存储桶拥有者也可以拒绝任何主体，使其无法执行 s3:ListMultipartUploadParts 操作。 |

| 操作 | 所需权限 |
| --- | --- |
| 列出分段上传 | 您必须得到可以对存储桶执行 `s3:ListBucketMultipartUploads` 操作的允许，才能列出正在上传到该存储桶的分段上传。<br><br>除了默认情况之外，存储桶拥有者可以允许其他主体对存储桶执行 `s3:ListBucketMultipartUploads` 操作。 |
| Amazon KMS 加密和解密相关权限 | 要通过采用 Amazon Key Management Service（Amazon KMS）KMS 密钥的加密执行分段上传，请求者必须具有以下权限：<br><br>• 对密钥执行 `kms:Decrypt` 和 `kms:GenerateDataKey` 操作。<br>• CreateMultipartUpload API 的 `kms:GenerateDataKey` 操作。<br>• UploadPart 和 UploadPartCopy API 的 `kms:Decrypt` 操作。<br><br>这些权限是必需的，因为 Amazon S3 必须在完成分段上传之前解密并读取加密的文件段中的数据。要获得对象的校验和值，还需要 `kms:Decrypt` 权限以及具有客户提供的加密密钥的服务器端加密。如果您在使用 CompleteMultipartUpload API 时没有这些必需的权限，则将在没有校验和的情况下创建对象。<br><br>如果 IAM 用户或角色与 KMS 密钥位于相同的 Amazon Web Services 账户中，则验证您对密钥和 IAM 策略都拥有权限。如果您的 IAM 用户或角色属于与 KMS 密钥不同的账户，您必须在密钥策略和 IAM 用户或角色中具有这些权限。 |
| SSE-C（具有客户提供的加密密钥的服务器端加密） | 使用 CompleteMultipartUpload API 时，必须提供 SSE-C（具有客户提供的加密密钥的服务器端加密），否则将在没有校验和的情况下创建对象，并且不会返回校验和值。 |

有关 ACL 权限与访问策略中的权限之间关系的信息，请参阅 ACL 权限和访问策略权限的映射。有关 IAM 用户、角色和最佳实践的信息，请参阅《IAM 用户指南》中的 IAM 身份（用户、用户组和角色）。

## 使用分段上传操作的校验和

有三个 Amazon S3 API 用于执行实际的分段上传：`CreateMultipartUpload`、`UploadPart` 和 `CompleteMultipartUpload`。下表指出了必须为其中每个 API 提供哪些校验和标头和值：

| 校验和算法 | 校验和类型 | **CreateMultipartUpload** | **UploadPart** | **CompleteMultipartUpoad** |
|---|---|---|---|---|
| CRC-64/NVME (CRC64NVME ) | 完整对象 | 必需的标头：<br>x-amz-checksum-algorithm | 可选标头：<br>x-amz-checksum-crc64nvme | 可选标头：<br>x-amz-checksum-algorithm<br>x-amz-crc64 |
| CRC-32 (CRC32)<br>CRC 32-C (CRC32C) | 完整对象 | 必需的标头：<br>x-amz-checksum-algorithm<br>x-amz-checksum-type | 可选标头：<br>x-amz-checksum-crc64nvme | 可选标头：<br>x-amz-checksum-algorithm<br>x-amz-crc32<br>x-amz-crc32c |
| CRC-32 (CRC32)<br>CRC-32C (CRC32C)<br>SHA-1 (SHA1)<br>SHA-256 (SHA256) | 复合键 | 必需的标头：<br>x-amz-checksum-algorithm | 必需的标头：<br>x-amz-checksum-crc32<br>x-amz-checksum-crc32c<br>x-amz-checksum-sha1<br>x-amz-checksum-sha256 | 必需的标头：<br>所有分段级的校验和都需要包含在 CompleteMultiPartUpload 请求中。<br>可选标头：<br>x-amz-crc32<br>x-amz-crc32c<br>x-amz-sha1 |

| 校验和算法 | 校验和类型 | CreateMultipartUpload | UploadPart | CompleteMultipartUpload |
|---|---|---|---|---|
| | | | | x-amz-sha256 |

主题

- 配置存储桶生命周期配置以删除未完成的分段上传
- 使用分段上传操作上传对象
- 使用高级别 .NET TransferUtility 类上传目录。
- 列出分段上传
- 使用 Amazon SDK 跟踪分段上传
- 中止分段上传
- 使用分段上传复制对象
- 教程：通过分段上传来上传对象并验证其数据完整性
- Amazon S3 分段上传限制

## 配置存储桶生命周期配置以删除未完成的分段上传

作为最佳实践，我们建议您使用 AbortIncompleteMultipartUpload 操作配置生命周期规则，以最大程度地降低存储成本。有关中止分段上传的更多信息，请参阅 中止分段上传。

Amazon S3 支持存储桶生命周期规则，您可以使用该规则指示 Amazon S3 停止未在启动后的指定天数内完成的分段上传。如果分段上传未在指定的时间范围内完成，则符合中止操作的条件。然后，Amazon S3 停止分段上传，并删除与分段上传关联的分段。此规则既适用于现有的分段上传，也适用于您后续创建的分段上传。

下面是使用 AbortIncompleteMultipartUpload 操作指定规则的示例生命周期配置。

```
<LifecycleConfiguration>
    <Rule>
        <ID>sample-rule</ID>
        <Prefix></Prefix>
        <Status>Enabled</Status>
        <AbortIncompleteMultipartUpload>
```

```
            <DaysAfterInitiation>7</DaysAfterInitiation>
        </AbortIncompleteMultipartUpload>
    </Rule>
</LifecycleConfiguration>
```

在本示例中，该规则不为 Prefix 元素（对象键名称前缀）指定值。因此，该规则适用于您启动了分段上传的存储桶中的所有对象。任何已启动但未在七天内完成的分段上传都符合执行中止操作的条件。中止操作对已完成的分段上传没有任何效果。

有关存储桶生命周期配置的更多信息，请参阅 管理对象的生命周期。

> **Note**
>
> 如果分段上传在规则中指定的天数内完成，则 AbortIncompleteMultipartUpload 生命周期操作不适用（即，Amazon S3 不会执行任何操作）。此外，此操作不适用于对象。此生命周期操作不会删除任何对象。此外，当您删除任何未完成的分段上传分段时，不会收取 S3 生命周期的提前删除费用。

使用 S3 控制台

要自动管理未完成的分段上传，您可以使用 S3 控制台创建生命周期规则，以使存储桶中的未完成分段上传字节在指定天数后过期。以下过程介绍如何添加生命周期规则，以在 7 天后删除未完成的分段上传。有关添加生命周期规则的更多信息，请参阅在存储桶上设置 S3 生命周期配置。

添加生命周期规则以中止超过 7 天的未完成的分段上传

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets（存储桶）列表中，请选择要为其创建生命周期规则的存储桶的名称。
3. 请选择 Management（管理）选项卡，然后选择 Create lifecycle rule（创建生命周期规则）。
4. 在 Lifecycle rule name (生命周期规则名称) 中，输入规则的名称。

   在该存储桶内，此名称必须是唯一的。
5. 请选择生命周期规则的范围：

   - 要为具有特定前缀的所有对象创建生命周期规则，请选择 Limit the scope of this rule using one or more filters（使用一个或多个筛选条件限制此规则的范围），然后在 Prefix（前缀）字段中输入前缀。

- 要为存储桶中的所有对象创建生命周期规则，请选择 This rule applies to all objects in the bucket（此规则适用于存储桶中的所有对象），然后选择 I acknowledge that this rule applies to all objects in the bucket（我确认此规则适用于存储桶中的所有对象）。

6. 在 Lifecycle rule actions（生命周期规则操作）下，选择 Delete expired object delete markers or incomplete multipart uploads（删除过期的对象删除标记或未完成的分段上传）。
7. 在 Delete expired object delete markers or incomplete multipart uploads（删除过期的对象删除标记或未完成的分段上传）下，选择 Delete incomplete multipart uploads（删除未完成的分段上传）。
8. 在 Number of days（天数）字段中，输入天数，在此天数之后将删除未完成的分段上传（在本例中为 7 天）。
9. 选择创建规则。

使用 Amazon CLI

以下 `put-bucket-lifecycle-configuration` Amazon Command Line Interface（Amazon CLI）命令为指定的存储桶添加生命周期配置。要使用此命令，请将 *`user input placeholders`* 替换为您的信息。

```
aws s3api put-bucket-lifecycle-configuration  \
        --bucket amzn-s3-demo-bucket  \
        --lifecycle-configuration filename-containing-lifecycle-configuration
```

以下示例显示如何使用 Amazon CLI 添加生命周期规则以中止未完成的分段上传。它包括一个示例 JSON 生命周期配置，以中止超过 7 天的未完成的分段上传。

要使用本示例中的 CLI 命令，请将 *`user input placeholders`* 替换为您的信息。

添加生命周期规则以中止未完成的分段上传

1. 设置 Amazon CLI。有关说明，请参阅《Amazon S3 API 参考》中的 Developing with Amazon S3 using the Amazon CLI。
2. 将以下示例生命周期配置保存在一个文件（例如 *`lifecycle.json`*）中。该示例配置指定了空前缀，因此它适用于存储桶中的所有对象。为将配置限制为某个对象子集，您可以指定前缀。

```
{
    "Rules": [
        {
```

```
            "ID": "Test Rule",
            "Status": "Enabled",
            "Filter": {
                "Prefix": ""
            },
            "AbortIncompleteMultipartUpload": {
                "DaysAfterInitiation": 7
            }
        }
    ]
}
```

3. 运行以下 CLI 命令以在存储桶上设置此生命周期配置。

```
aws s3api put-bucket-lifecycle-configuration   \
--bucket amzn-s3-demo-bucket  \
--lifecycle-configuration file://lifecycle.json
```

4. 要验证是否已在您的存储桶上设置了生命周期配置，请使用以下 get-bucket-lifecycle 命令检索生命周期配置。

```
aws s3api get-bucket-lifecycle  \
--bucket amzn-s3-demo-bucket
```

5. 要删除生命周期配置，请使用以下 delete-bucket-lifecycle 命令。

```
aws s3api delete-bucket-lifecycle \
--bucket amzn-s3-demo-bucket
```

## 使用分段上传操作上传对象

您可以使用分段上传以编程方式将单个对象上传到 Amazon S3。每个对象作为一组分段进行上传。每个分段都是对象数据的连续部分。您可以独立上传以及按任意顺序上传这些对象分段。如果任意分段传输失败，可以重新传输该分段且不会影响其他分段。上传完所有的对象分段后，Amazon S3 将汇集这些分段并创建对象。匿名用户无法发起分段上传。

有关使用分段上传以及额外的校验和来上传对象的端到端过程，请参阅教程：通过分段上传来上传对象并验证其数据完整性。

下一节介绍如何通过 Amazon Command Line Interface和 Amazon SDK 使用分段上传。

使用 S3 控制台

您可以将任何类型的文件上传至 S3 存储桶，包括图像、备份、数据、电影等。可使用 Amazon S3 控制台上传的文件的最大大小为 160 GB。要上传大于 160GB 的文件，请使用 Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 Amazon S3 REST API。

有关通过 Amazon Web Services Management Console上传对象的说明，请参阅上传对象。

使用 Amazon CLI

以下内容介绍使用 Amazon CLI 进行分段上传的 Amazon S3 操作。

- 开始分段上传
- 上传分段
- 上传分段（复制）
- 完成分段上传
- 中止分段上传
- 列出分段
- 列出分段上传

使用 REST API

Amazon Simple Storage Service API 参考的下面几节描述了适用于分段上传的 REST API。

- 开始分段上传
- 上传分段
- 完成分段上传
- 停止分段上传
- 列出分段
- 列出分段上传

使用 Amazon SDK（高级别 API）

一些 Amazon SDK 公开了一个高级别 API，该 API 通过将完成分段上传所需的不同 API 操作组合成单个操作，来简化分段上传。有关更多信息，请参阅 在 Amazon S3 中使用分段上传来上传和复制对象。

如果您需要暂停并恢复分段上传、在上传期间改变分段大小，或者事先不知道数据大小，请使用低级别 API 方法。用于分段上传的低级别 API 方法提供了额外功能，有关更多信息，请参阅使用 Amazon SDK（低级别 API）。

.NET

要将文件上传到 S3 存储桶，请使用 `TransferUtility` 类。在从文件上传数据时，您必须提供对象的键名。如果未提供，该 API 将使用文件名作为键名。在从流上传数据时，您必须提供对象的键名。

要设置高级上传选项（如段大小、并发上传段时的线程数、元数据、存储类或 ACL），请使用 `TransferUtilityUploadRequest` 类。

> **Note**
>
> 如果您将流用作数据源，`TransferUtility` 类不会执行并发上传。

以下 C# 示例将文件分段上传到 Amazon S3 存储桶。它说明如何使用各种 `TransferUtility.Upload` 重载来上传文件。每个对上传的后续调用都将替换先前的上传。有关设置和运行代码示例的信息，请参阅《适用于 .NET 的 Amazon SDK 开发人员指南》中的适用于 .NET 的 Amazon SDK 入门。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Transfer;
using System;
using System.IO;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class UploadFileMPUHighLevelAPITest
    {
        private const string bucketName = "*** provide bucket name ***";
        private const string keyName = "*** provide a name for the uploaded object
 ***";
        private const string filePath = "*** provide the full path name of the file
 to upload ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
```

```
        private static IAmazonS3 s3Client;

        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            UploadFileAsync().Wait();
        }

        private static async Task UploadFileAsync()
        {
            try
            {
                var fileTransferUtility =
                    new TransferUtility(s3Client);

                // Option 1. Upload a file. The file name is used as the object key
name.
                await fileTransferUtility.UploadAsync(filePath, bucketName);
                Console.WriteLine("Upload 1 completed");

                // Option 2. Specify object key name explicitly.
                await fileTransferUtility.UploadAsync(filePath, bucketName,
keyName);
                Console.WriteLine("Upload 2 completed");

                // Option 3. Upload data from a type of System.IO.Stream.
                using (var fileToUpload =
                    new FileStream(filePath, FileMode.Open, FileAccess.Read))
                {
                    await fileTransferUtility.UploadAsync(fileToUpload,
                                                bucketName, keyName);
                }
                Console.WriteLine("Upload 3 completed");

                // Option 4. Specify advanced settings.
                var fileTransferUtilityRequest = new TransferUtilityUploadRequest
                {
                    BucketName = bucketName,
                    FilePath = filePath,
                    StorageClass = S3StorageClass.StandardInfrequentAccess,
                    PartSize = 6291456, // 6 MB.
                    Key = keyName,
                    CannedACL = S3CannedACL.PublicRead
                };
```

```
                fileTransferUtilityRequest.Metadata.Add("param1", "Value1");
                fileTransferUtilityRequest.Metadata.Add("param2", "Value2");

                await fileTransferUtility.UploadAsync(fileTransferUtilityRequest);
                Console.WriteLine("Upload 4 completed");
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }

        }
    }
}
```

JavaScript

Example

上传大文件。

```
import { S3Client } from "@aws-sdk/client-s3";
import { Upload } from "@aws-sdk/lib-storage";

import {
  ProgressBar,
  logger,
} from "@aws-doc-sdk-examples/lib/utils/util-log.js";

const twentyFiveMB = 25 * 1024 * 1024;

export const createString = (size = twentyFiveMB) => {
  return "x".repeat(size);
};

/**
 * Create a 25MB file and upload it in parts to the specified
 * Amazon S3 bucket.
```

```
 * @param {{ bucketName: string, key: string }}
 */
export const main = async ({ bucketName, key }) => {
  const str = createString();
  const buffer = Buffer.from(str, "utf8");
  const progressBar = new ProgressBar({
    description: `Uploading "${key}" to "${bucketName}"`,
    barLength: 30,
  });

  try {
    const upload = new Upload({
      client: new S3Client({}),
      params: {
        Bucket: bucketName,
        Key: key,
        Body: buffer,
      },
    });

    upload.on("httpUploadProgress", ({ loaded, total }) => {
      progressBar.update({ current: loaded, total });
    });

    await upload.done();
  } catch (caught) {
    if (caught instanceof Error && caught.name === "AbortError") {
      logger.error(`Multipart upload was aborted. ${caught.message}`);
    } else {
      throw caught;
    }
  }
};
```

### Example

下载大文件。

```
import { fileURLToPath } from "node:url";
import { GetObjectCommand, NoSuchKey, S3Client } from "@aws-sdk/client-s3";
import { createWriteStream, rmSync } from "node:fs";

const s3Client = new S3Client({});
```

```
const oneMB = 1024 * 1024;

export const getObjectRange = ({ bucket, key, start, end }) => {
  const command = new GetObjectCommand({
    Bucket: bucket,
    Key: key,
    Range: `bytes=${start}-${end}`,
  });

  return s3Client.send(command);
};

/**
 * @param {string | undefined} contentRange
 */
export const getRangeAndLength = (contentRange) => {
  const [range, length] = contentRange.split("/");
  const [start, end] = range.split("-");
  return {
    start: Number.parseInt(start),
    end: Number.parseInt(end),
    length: Number.parseInt(length),
  };
};

export const isComplete = ({ end, length }) => end === length - 1;

const downloadInChunks = async ({ bucket, key }) => {
  const writeStream = createWriteStream(
    fileURLToPath(new URL(`./${key}`, import.meta.url)),
  ).on("error", (err) => console.error(err));

  let rangeAndLength = { start: -1, end: -1, length: -1 };

  while (!isComplete(rangeAndLength)) {
    const { end } = rangeAndLength;
    const nextRange = { start: end + 1, end: end + oneMB };

    const { ContentRange, Body } = await getObjectRange({
      bucket,
      key,
      ...nextRange,
    });
    console.log(`Downloaded bytes ${nextRange.start} to ${nextRange.end}`);
```

```
    writeStream.write(await Body.transformToByteArray());
    rangeAndLength = getRangeAndLength(ContentRange);
  }
};

/**
 * Download a large object from and Amazon S3 bucket.
 *
 * When downloading a large file, you might want to break it down into
 * smaller pieces. Amazon S3 accepts a Range header to specify the start
 * and end of the byte range to be downloaded.
 *
 * @param {{ bucketName: string, key: string }}
 */
export const main = async ({ bucketName, key }) => {
  try {
    await downloadInChunks({
      bucket: bucketName,
      key: key,
    });
  } catch (caught) {
    if (caught instanceof NoSuchKey) {
      console.error(`Failed to download object. No such key "${key}".`);
      rmSync(key);
    }
  }
};
```

Go

有关分段上传的 Go 代码示例的更多信息，请参阅 Upload or download large files to and from Amazon S3 using an Amazon SDK。

Example

使用上传管理器上传大型对象，以将数据分成多个分段，然后同时上传。

```
import (
 "bytes"
 "context"
 "errors"
```

```
 "fmt"
 "io"
 "log"
 "os"
 "time"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/feature/s3/manager"
 "github.com/aws/aws-sdk-go-v2/service/s3"
 "github.com/aws/aws-sdk-go-v2/service/s3/types"
 "github.com/aws/smithy-go"
)

// BucketBasics encapsulates the Amazon Simple Storage Service (Amazon S3) actions
// used in the examples.
// It contains S3Client, an Amazon S3 service client that is used to perform bucket
// and object actions.
type BucketBasics struct {
 S3Client *s3.Client
}
```

```
// UploadLargeObject uses an upload manager to upload data to an object in a bucket.
// The upload manager breaks large data into parts and uploads the parts
 concurrently.
func (basics BucketBasics) UploadLargeObject(ctx context.Context, bucketName string,
 objectKey string, largeObject []byte) error {
 largeBuffer := bytes.NewReader(largeObject)
 var partMiBs int64 = 10
 uploader := manager.NewUploader(basics.S3Client, func(u *manager.Uploader) {
  u.PartSize = partMiBs * 1024 * 1024
 })
 _, err := uploader.Upload(ctx, &s3.PutObjectInput{
  Bucket: aws.String(bucketName),
  Key:    aws.String(objectKey),
  Body:   largeBuffer,
 })
 if err != nil {
  var apiErr smithy.APIError
  if errors.As(err, &apiErr) && apiErr.ErrorCode() == "EntityTooLarge" {
   log.Printf("Error while uploading object to %s. The object is too large.\n"+
    "The maximum size for a multipart upload is 5TB.", bucketName)
```

```
  } else {
   log.Printf("Couldn't upload large object to %v:%v. Here's why: %v\n",
    bucketName, objectKey, err)
  }
 } else {
  err = s3.NewObjectExistsWaiter(basics.S3Client).Wait(
   ctx, &s3.HeadObjectInput{Bucket: aws.String(bucketName), Key:
 aws.String(objectKey)}, time.Minute)
  if err != nil {
   log.Printf("Failed attempt to wait for object %s to exist.\n", objectKey)
  }
 }

 return err
}
```

### Example

使用下载管理器下载大型对象，以分段获取数据并同时下载它们。

```
// DownloadLargeObject uses a download manager to download an object from a bucket.
// The download manager gets the data in parts and writes them to a buffer until all
 of
// the data has been downloaded.
func (basics BucketBasics) DownloadLargeObject(ctx context.Context, bucketName
 string, objectKey string) ([]byte, error) {
 var partMiBs int64 = 10
 downloader := manager.NewDownloader(basics.S3Client, func(d *manager.Downloader) {
  d.PartSize = partMiBs * 1024 * 1024
 })
 buffer := manager.NewWriteAtBuffer([]byte{})
 _, err := downloader.Download(ctx, buffer, &s3.GetObjectInput{
  Bucket: aws.String(bucketName),
  Key:    aws.String(objectKey),
 })
 if err != nil {
  log.Printf("Couldn't download large object from %v:%v. Here's why: %v\n",
   bucketName, objectKey, err)
 }
 return buffer.Bytes(), err
}
```

PHP

本主题介绍如何使用 `Aws\S3\Model\MultipartUpload\UploadBuilder` 中的高级别 适用于 PHP 的 Amazon SDK 类执行文件分段上传。有关适用于 Ruby 的 Amazon 开发工具包 API 的更多信息，请转到适用于 Ruby 的 Amazon 开发工具包 – 版本 2。

以下 PHP 代码示例将文件上传到 Amazon S3 存储桶。该示例演示如何设置 `MultipartUploader` 对象的参数。

```
 require 'vendor/autoload.php';

use Aws\Exception\MultipartUploadException;
use Aws\S3\MultipartUploader;
use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// Prepare the upload parameters.
$uploader = new MultipartUploader($s3, '/path/to/large/file.zip', [
    'bucket' => $bucket,
    'key'    => $keyname
]);

// Perform the upload.
try {
    $result = $uploader->upload();
    echo "Upload complete: {$result['ObjectURL']}" . PHP_EOL;
} catch (MultipartUploadException $e) {
    echo $e->getMessage() . PHP_EOL;
}
```

Python

以下示例使用高级别分段上传 Python API（`TransferManager` 类）上传对象。

```
import sys
import threading

import boto3
from boto3.s3.transfer import TransferConfig


MB = 1024 * 1024
s3 = boto3.resource("s3")


class TransferCallback:
    """
    Handle callbacks from the transfer manager.

    The transfer manager periodically calls the __call__ method throughout
    the upload and download process so that it can take action, such as
    displaying progress to the user and collecting data about the transfer.
    """

    def __init__(self, target_size):
        self._target_size = target_size
        self._total_transferred = 0
        self._lock = threading.Lock()
        self.thread_info = {}

    def __call__(self, bytes_transferred):
        """
        The callback method that is called by the transfer manager.

        Display progress during file transfer and collect per-thread transfer
        data. This method can be called by multiple threads, so shared instance
        data is protected by a thread lock.
        """
        thread = threading.current_thread()
        with self._lock:
            self._total_transferred += bytes_transferred
            if thread.ident not in self.thread_info.keys():
                self.thread_info[thread.ident] = bytes_transferred
            else:
                self.thread_info[thread.ident] += bytes_transferred

            target = self._target_size * MB
```

```
            sys.stdout.write(
                f"\r{self._total_transferred} of {target} transferred "
                f"({(self._total_transferred / target) * 100:.2f}%)."
            )
            sys.stdout.flush()


def upload_with_default_configuration(
    local_file_path, bucket_name, object_key, file_size_mb
):
    """
    Upload a file from a local folder to an Amazon S3 bucket, using the default
    configuration.
    """
    transfer_callback = TransferCallback(file_size_mb)
    s3.Bucket(bucket_name).upload_file(
        local_file_path, object_key, Callback=transfer_callback
    )
    return transfer_callback.thread_info


def upload_with_chunksize_and_meta(
    local_file_path, bucket_name, object_key, file_size_mb, metadata=None
):
    """
    Upload a file from a local folder to an Amazon S3 bucket, setting a
    multipart chunk size and adding metadata to the Amazon S3 object.

    The multipart chunk size controls the size of the chunks of data that are
    sent in the request. A smaller chunk size typically results in the transfer
    manager using more threads for the upload.

    The metadata is a set of key-value pairs that are stored with the object
    in Amazon S3.
    """
    transfer_callback = TransferCallback(file_size_mb)

    config = TransferConfig(multipart_chunksize=1 * MB)
    extra_args = {"Metadata": metadata} if metadata else None
    s3.Bucket(bucket_name).upload_file(
        local_file_path,
        object_key,
        Config=config,
        ExtraArgs=extra_args,
```

```
        Callback=transfer_callback,
    )
    return transfer_callback.thread_info


def upload_with_high_threshold(local_file_path, bucket_name, object_key,
 file_size_mb):
    """
    Upload a file from a local folder to an Amazon S3 bucket, setting a
    multipart threshold larger than the size of the file.

    Setting a multipart threshold larger than the size of the file results
    in the transfer manager sending the file as a standard upload instead of
    a multipart upload.
    """
    transfer_callback = TransferCallback(file_size_mb)
    config = TransferConfig(multipart_threshold=file_size_mb * 2 * MB)
    s3.Bucket(bucket_name).upload_file(
        local_file_path, object_key, Config=config, Callback=transfer_callback
    )
    return transfer_callback.thread_info


def upload_with_sse(
    local_file_path, bucket_name, object_key, file_size_mb, sse_key=None
):
    """
    Upload a file from a local folder to an Amazon S3 bucket, adding server-side
    encryption with customer-provided encryption keys to the object.

    When this kind of encryption is specified, Amazon S3 encrypts the object
    at rest and allows downloads only when the expected encryption key is
    provided in the download request.
    """
    transfer_callback = TransferCallback(file_size_mb)
    if sse_key:
        extra_args = {"SSECustomerAlgorithm": "AES256", "SSECustomerKey": sse_key}
    else:
        extra_args = None
    s3.Bucket(bucket_name).upload_file(
        local_file_path, object_key, ExtraArgs=extra_args,
 Callback=transfer_callback
    )
    return transfer_callback.thread_info
```

```
def download_with_default_configuration(
    bucket_name, object_key, download_file_path, file_size_mb
):
    """
    Download a file from an Amazon S3 bucket to a local folder, using the
    default configuration.
    """
    transfer_callback = TransferCallback(file_size_mb)
    s3.Bucket(bucket_name).Object(object_key).download_file(
        download_file_path, Callback=transfer_callback
    )
    return transfer_callback.thread_info


def download_with_single_thread(
    bucket_name, object_key, download_file_path, file_size_mb
):
    """
    Download a file from an Amazon S3 bucket to a local folder, using a
    single thread.
    """
    transfer_callback = TransferCallback(file_size_mb)
    config = TransferConfig(use_threads=False)
    s3.Bucket(bucket_name).Object(object_key).download_file(
        download_file_path, Config=config, Callback=transfer_callback
    )
    return transfer_callback.thread_info


def download_with_high_threshold(
    bucket_name, object_key, download_file_path, file_size_mb
):
    """
    Download a file from an Amazon S3 bucket to a local folder, setting a
    multipart threshold larger than the size of the file.

    Setting a multipart threshold larger than the size of the file results
    in the transfer manager sending the file as a standard download instead
    of a multipart download.
    """
    transfer_callback = TransferCallback(file_size_mb)
    config = TransferConfig(multipart_threshold=file_size_mb * 2 * MB)
```

```
    s3.Bucket(bucket_name).Object(object_key).download_file(
        download_file_path, Config=config, Callback=transfer_callback
    )
    return transfer_callback.thread_info


def download_with_sse(
    bucket_name, object_key, download_file_path, file_size_mb, sse_key
):
    """
    Download a file from an Amazon S3 bucket to a local folder, adding a
    customer-provided encryption key to the request.

    When this kind of encryption is specified, Amazon S3 encrypts the object
    at rest and allows downloads only when the expected encryption key is
    provided in the download request.
    """
    transfer_callback = TransferCallback(file_size_mb)

    if sse_key:
        extra_args = {"SSECustomerAlgorithm": "AES256", "SSECustomerKey": sse_key}
    else:
        extra_args = None
    s3.Bucket(bucket_name).Object(object_key).download_file(
        download_file_path, ExtraArgs=extra_args, Callback=transfer_callback
    )
    return transfer_callback.thread_info
```

使用 Amazon SDK（低级别 API）

Amazon SDK 公开了一个与 Amazon S3 REST API 非常相似的用于分段上传的低级别 API（请参阅在 Amazon S3 中使用分段上传来上传和复制对象）。当您需要暂停和恢复分段上传、在上传过程中更改部分大小或事先不知道上传数据的大小时，请使用低级别 API。当您没有这些需求时，请使用高级别 API（请参阅使用 Amazon SDK（高级别 API））。

Java

以下示例演示如何使用低级别 Java 类上传文件。它将执行以下步骤：

- 使用 AmazonS3Client.initiateMultipartUpload() 方法初始化分段上传，并传入 InitiateMultipartUploadRequest 对象。
- 保存 AmazonS3Client.initiateMultipartUpload() 方法返回的上传 ID。您为随后的每个分段上传操作提供此上传 ID。
- 上传对象的分段。对于每个分段，您将调用 AmazonS3Client.uploadPart() 方法。您使用 UploadPartRequest 对象提供分段上传信息。
- 对于每个分段，在列表中保存来自 AmazonS3Client.uploadPart() 方法的响应的 ETag。您使用 ETag 值完成分段上传。
- 调用 AmazonS3Client.completeMultipartUpload() 方法来完成分段上传。

### Example

有关创建和测试有效示例的说明，请参阅《适用于 Java 的 Amazon SDK 开发人员指南》中的入门。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.io.File;
import java.io.IOException;
import java.util.ArrayList;
import java.util.List;

public class LowLevelMultipartUpload {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String keyName = "*** Key name ***";
        String filePath = "*** Path to file to upload ***";

        File file = new File(filePath);
        long contentLength = file.length();
        long partSize = 5 * 1024 * 1024; // Set part size to 5 MB.
```

```
        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withRegion(clientRegion)
                    .withCredentials(new ProfileCredentialsProvider())
                    .build();

            // Create a list of ETag objects. You retrieve ETags for each object
part
            // uploaded,
            // then, after each individual part has been uploaded, pass the list of
ETags to
            // the request to complete the upload.
            List<PartETag> partETags = new ArrayList<PartETag>();

            // Initiate the multipart upload.
            InitiateMultipartUploadRequest initRequest = new
InitiateMultipartUploadRequest(bucketName, keyName);
            InitiateMultipartUploadResult initResponse =
s3Client.initiateMultipartUpload(initRequest);

            // Upload the file parts.
            long filePosition = 0;
            for (int i = 1; filePosition < contentLength; i++) {
                // Because the last part could be less than 5 MB, adjust the part
size as
                // needed.
                partSize = Math.min(partSize, (contentLength - filePosition));

                // Create the request to upload a part.
                UploadPartRequest uploadRequest = new UploadPartRequest()
                        .withBucketName(bucketName)
                        .withKey(keyName)
                        .withUploadId(initResponse.getUploadId())
                        .withPartNumber(i)
                        .withFileOffset(filePosition)
                        .withFile(file)
                        .withPartSize(partSize);

                // Upload the part and add the response's ETag to our list.
                UploadPartResult uploadResult = s3Client.uploadPart(uploadRequest);
                partETags.add(uploadResult.getPartETag());

                filePosition += partSize;
```

```
            }

            // Complete the multipart upload.
            CompleteMultipartUploadRequest compRequest = new
 CompleteMultipartUploadRequest(bucketName, keyName,
                    initResponse.getUploadId(), partETags);
            s3Client.completeMultipartUpload(compRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

以下 C# 示例演示如何使用低级别 适用于 .NET 的 Amazon SDK 分段上传 API 将文件上传到 S3 存储桶。有关 Amazon S3 分段上传的信息，请参阅 在 Amazon S3 中使用分段上传来上传和复制对象。

> **Note**
>
> 如果使用 适用于 .NET 的 Amazon SDK API 上传大型对象，数据写入到请求流时可能出现超时。您可以使用 `UploadPartRequest` 设置显式超时。

以下 C# 示例使用低级别分段上传 API 将文件上传到 S3 存储桶。有关设置和运行代码示例的信息，请参阅《适用于 .NET 的 Amazon SDK 开发人员指南》中的适用于 .NET 的 Amazon SDK 入门。

```
using Amazon;
using Amazon.Runtime;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
```

```
using System.IO;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class UploadFileMPULowLevelAPITest
    {
        private const string bucketName = "*** provide bucket name ***";
        private const string keyName = "*** provide a name for the uploaded object
 ***";
        private const string filePath = "*** provide the full path name of the file
 to upload ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            Console.WriteLine("Uploading an object");
            UploadObjectAsync().Wait();
        }

        private static async Task UploadObjectAsync()
        {
            // Create list to store upload part responses.
            List<UploadPartResponse> uploadResponses = new
 List<UploadPartResponse>();

            // Setup information required to initiate the multipart upload.
            InitiateMultipartUploadRequest initiateRequest = new
 InitiateMultipartUploadRequest
            {
                BucketName = bucketName,
                Key = keyName
            };

            // Initiate the upload.
            InitiateMultipartUploadResponse initResponse =
                await s3Client.InitiateMultipartUploadAsync(initiateRequest);

            // Upload parts.
            long contentLength = new FileInfo(filePath).Length;
```

```
            long partSize = 5 * (long)Math.Pow(2, 20); // 5 MB

            try
            {
                Console.WriteLine("Uploading parts");

                long filePosition = 0;
                for (int i = 1; filePosition < contentLength; i++)
                {
                    UploadPartRequest uploadRequest = new UploadPartRequest
                        {
                            BucketName = bucketName,
                            Key = keyName,
                            UploadId = initResponse.UploadId,
                            PartNumber = i,
                            PartSize = partSize,
                            FilePosition = filePosition,
                            FilePath = filePath
                        };

                    // Track upload progress.
                    uploadRequest.StreamTransferProgress +=
                        new
EventHandler<StreamTransferProgressArgs>(UploadPartProgressEventCallback);

                    // Upload a part and add the response to our list.
                    uploadResponses.Add(await
s3Client.UploadPartAsync(uploadRequest));

                    filePosition += partSize;
                }

                // Setup to complete the upload.
                CompleteMultipartUploadRequest completeRequest = new
CompleteMultipartUploadRequest
                    {
                        BucketName = bucketName,
                        Key = keyName,
                        UploadId = initResponse.UploadId
                     };
                completeRequest.AddPartETags(uploadResponses);

                // Complete the upload.
                CompleteMultipartUploadResponse completeUploadResponse =
```

```
                    await s3Client.CompleteMultipartUploadAsync(completeRequest);
            }
            catch (Exception exception)
            {
                Console.WriteLine("An AmazonS3Exception was thrown: { 0}",
 exception.Message);

                // Abort the upload.
                AbortMultipartUploadRequest abortMPURequest = new
 AbortMultipartUploadRequest
                {
                    BucketName = bucketName,
                    Key = keyName,
                    UploadId = initResponse.UploadId
                };
               await s3Client.AbortMultipartUploadAsync(abortMPURequest);
            }
        }
        public static void UploadPartProgressEventCallback(object sender,
 StreamTransferProgressArgs e)
        {
            // Process event.
            Console.WriteLine("{0}/{1}", e.TransferredBytes, e.TotalBytes);
        }
    }
}
```

PHP

本主题说明如何使用 适用于 PHP 的 Amazon SDK 版本 3 中的低级别 uploadPart 方法来以分段形式上传文件。有关适用于 Ruby 的 Amazon 开发工具包 API 的更多信息，请转到适用于 Ruby 的 Amazon 开发工具包 – 版本 2。

以下 PHP 示例使用低级别 PHP API 分段上传将文件上传到 Amazon S3 存储桶。

```
 require 'vendor/autoload.php';

use Aws\S3\Exception\S3Exception;
use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';
$filename = '*** Path to and Name of the File to Upload ***';
```

```
$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

$result = $s3->createMultipartUpload([
    'Bucket'       => $bucket,
    'Key'          => $keyname,
    'StorageClass' => 'REDUCED_REDUNDANCY',
    'Metadata'     => [
        'param1' => 'value 1',
        'param2' => 'value 2',
        'param3' => 'value 3'
    ]
]);
$uploadId = $result['UploadId'];

// Upload the file in parts.
try {
    $file = fopen($filename, 'r');
    $partNumber = 1;
    while (!feof($file)) {
        $result = $s3->uploadPart([
            'Bucket'     => $bucket,
            'Key'        => $keyname,
            'UploadId'   => $uploadId,
            'PartNumber' => $partNumber,
            'Body'       => fread($file, 5 * 1024 * 1024),
        ]);
        $parts['Parts'][$partNumber] = [
            'PartNumber' => $partNumber,
            'ETag' => $result['ETag'],
        ];
        $partNumber++;

        echo "Uploading part $partNumber of $filename." . PHP_EOL;
    }
    fclose($file);
} catch (S3Exception $e) {
    $result = $s3->abortMultipartUpload([
        'Bucket'   => $bucket,
        'Key'      => $keyname,
        'UploadId' => $uploadId
```

```
    ]);

    echo "Upload of $filename failed." . PHP_EOL;
}

// Complete the multipart upload.
$result = $s3->completeMultipartUpload([
    'Bucket'   => $bucket,
    'Key'      => $keyname,
    'UploadId' => $uploadId,
    'MultipartUpload'    => $parts,
]);
$url = $result['Location'];

echo "Uploaded $filename to $url." . PHP_EOL;
```

使用 适用于 Ruby 的 Amazon SDK

适用于 Ruby 的 Amazon SDK 版本 3 支持两种 Amazon S3 分段上传方式。对于第一个选项，您可以使用托管文件上传。有关更多信息，请参阅 Amazon 开发人员博客中的将文件上传至 Amazon S3。托管文件上传是建议用于将文件上传到存储桶的方法。它们提供以下优势：

- 管理大于 15MB 的对象的分段上传。
- 正确打开二进制模式的文件，规避编码问题。
- 在并行上传较大对象的多个部分时，使用多个线程。

此外，您还可以直接使用以下分段上传客户端操作：

- create_multipart_upload – 启动分段上传，并返回上传 ID。
- upload_part – 上传分段上传中的一部分。
- upload_part_copy – 将现有对象作为数据源，并复制其中的数据，上传一部分。
- complete_multipart_upload – 整合先前上传的部分，完成分段上传。
- abort_multipart_upload – 停止分段上传。

## 使用高级别 .NET TransferUtility 类上传目录。

您可以使用 `TransferUtility` 类上传整个目录。默认情况下，该 API 仅上传位于指定目录的根目录中的文件。但是，您可以指定以递归方式上传所有子目录中的文件。

要根据筛选条件选择指定目录中的文件，请指定筛选表达式。例如，要从目录中仅上传 PDF 文件，请指定 "*.pdf" 筛选表达式。

在从目录中上传文件时，您不必为生成的对象指定键名。Amazon S3 会使用原始文件路径构造键名。例如，假设您有一个名为 c:\myfolder 的目录，并且此目录具有以下结构：

Example

```
C:\myfolder
      \a.txt
      \b.pdf
      \media\
             An.mp3
```

上传此目录时，Amazon S3 将使用以下密钥名称：

Example

```
a.txt
b.pdf
media/An.mp3
```

Example

以下 C# 代码示例将一个目录上传到 Amazon S3 存储桶。它说明如何使用各种 TransferUtility.UploadDirectory 重载来上传目录。每个对上传的后续调用都将替换先前的上传。有关设置和运行代码示例的信息，请参阅《适用于 .NET 的 Amazon SDK 开发人员指南》中的适用于 .NET 的 Amazon SDK 入门。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Transfer;
using System;
using System.IO;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class UploadDirMPUHighLevelAPITest
    {
        private const string existingBucketName = "*** bucket name ***";
        private const string directoryPath = @"*** directory path ***";
```

```
        // The example uploads only .txt files.
        private const string wildCard = "*.txt";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion = RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;
        static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            UploadDirAsync().Wait();
        }

        private static async Task UploadDirAsync()
        {
            try
            {
                var directoryTransferUtility =
                    new TransferUtility(s3Client);

                // 1. Upload a directory.
                await directoryTransferUtility.UploadDirectoryAsync(directoryPath,
                    existingBucketName);
                Console.WriteLine("Upload statement 1 completed");

                // 2. Upload only the .txt files from a directory
                //    and search recursively.
                await directoryTransferUtility.UploadDirectoryAsync(
                                                directoryPath,
                                                existingBucketName,
                                                wildCard,
                                                SearchOption.AllDirectories);
                Console.WriteLine("Upload statement 2 completed");

                // 3. The same as Step 2 and some optional configuration.
                //    Search recursively for .txt files to upload.
                var request = new TransferUtilityUploadDirectoryRequest
                {
                    BucketName = existingBucketName,
                    Directory = directoryPath,
                    SearchOption = SearchOption.AllDirectories,
                    SearchPattern = wildCard
                };

                await directoryTransferUtility.UploadDirectoryAsync(request);
                Console.WriteLine("Upload statement 3 completed");
```

```
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine(
                        "Error encountered ***. Message:'{0}' when writing an object",
 e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine(
                    "Unknown encountered on server. Message:'{0}' when writing an
 object", e.Message);
            }
        }
    }
}
```

## 列出分段上传

可以使用 Amazon CLI、REST API 或 Amazon SDK 检索 Amazon S3 中正在进行的分段上传的列表。您可以使用分段上传以编程方式将单个对象上传到 Amazon S3。分段上传通过一次移动对象数据的一部分，将对象移动到 Amazon S3 中。有关分段上传的更多一般信息，请参阅在 Amazon S3 中使用分段上传来上传和复制对象。

有关使用分段上传以及额外的校验和来上传对象的端到端过程，请参阅教程：通过分段上传来上传对象并验证其数据完整性。

下一节介绍如何使用 Amazon Command Line Interface、Amazon S3 REST API 和 Amazon SDK 列出正在进行的分段上传。

### 使用 Amazon CLI 列出分段上传

Amazon Command Line Interface 中的以下各部分介绍了适用于列出分段上传的操作。

- list-parts- 列出特定分段上传的已上传部分。
- list-multipart-uploads- 列出正在进行的分段上传。

### 使用 REST API 列出分段上传

Amazon Simple Storage Service API 参考的下面几节描述了列出分段上传的 REST API：

- ListParts- 列出特定分段上传的已上传部分。

- ListMultipartUploads- 列出正在进行的分段上传。

使用 Amazon SDK（低级别 API）列出分段上传

Java

以下任务将引导您使用低级别 Java 类来列出存储桶上所有正在进行的分段上传。

低级别 API 分段上传列表过程

| | |
|---|---|
| 1 | 创建 `ListMultipartUploadsRequest` 类的实例并提供存储桶名称。 |
| 2 | 运行 `AmazonS3Client.listMultipartUploads` 方法。该方法将返回 `MultipartUploadListing` 类的实例，以向您提供有关正在进行的分段上传的信息。 |

以下 Java 代码示例演示了上述任务。

Example

```
ListMultipartUploadsRequest allMultpartUploadsRequest =
     new ListMultipartUploadsRequest(existingBucketName);
MultipartUploadListing multipartUploadListing =
     s3Client.listMultipartUploads(allMultpartUploadsRequest);
```

.NET

要列出特定存储桶上所有正在进行的分段上传，请使用 适用于 .NET 的 Amazon SDK 低级别分段上传 API 的 `ListMultipartUploadsRequest` 类。`AmazonS3Client.ListMultipartUploads` 方法将返回 `ListMultipartUploadsResponse` 类（提供有关正在进行的分段上传的信息）的实例。

正在进行的分段上传是使用启动分段上传请求启动但尚未完成或停止的分段上传。有关 Amazon S3 分段上传的更多信息，请参阅 在 Amazon S3 中使用分段上传来上传和复制对象。

以下 C# 示例演示如何使用 适用于 .NET 的 Amazon SDK 列出存储桶上所有正在进行的分段上传。有关设置和运行代码示例的信息，请参阅《适用于 .NET 的 Amazon SDK 开发人员指南》中的适用于 .NET 的 Amazon SDK 入门。

```
ListMultipartUploadsRequest request = new ListMultipartUploadsRequest
{
```

```
  BucketName = bucketName // Bucket receiving the uploads.
};

ListMultipartUploadsResponse response = await
 AmazonS3Client.ListMultipartUploadsAsync(request);
```

PHP

本主题说明如何使用版本 3 的 适用于 PHP 的 Amazon SDK 中的低级别 API 类列出存储桶上所有正在进行的分段上传。有关适用于 Ruby 的 Amazon 开发工具包 API 的更多信息，请转到适用于 Ruby 的 Amazon 开发工具包 – 版本 2。

以下 PHP 示例演示如何列出存储桶上所有正在进行的分段上传。

```
 require 'vendor/autoload.php';

use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// Retrieve a list of the current multipart uploads.
$result = $s3->listMultipartUploads([
    'Bucket' => $bucket
]);

// Write the list of uploads to the page.
print_r($result->toArray());
```

## 使用 Amazon SDK 跟踪分段上传

可以使用侦听接口跟踪对象上传到 Amazon S3 的进度。高级别分段上传 API 提供了这样的侦听接口，名为 `ProgressListener`。进度事件将定期发生，并且会通知侦听者已传输的字节。有关分段上传的更多一般信息，请参阅在 Amazon S3 中使用分段上传来上传和复制对象。

有关使用分段上传以及额外的校验和来上传对象的端到端过程，请参阅教程：通过分段上传来上传对象并验证其数据完整性。

下一节介绍如何通过 Amazon SDK 跟踪分段上传。

### Java

#### Example

```
TransferManager tm = new TransferManager(new ProfileCredentialsProvider());

PutObjectRequest request = new PutObjectRequest(
    existingBucketName, keyName, new File(filePath));

// Subscribe to the event and provide event handler.
request.setProgressListener(new ProgressListener() {
   public void progressChanged(ProgressEvent event) {
    System.out.println("Transferred bytes: " +
      event.getBytesTransfered());
            }
});
```

#### Example

以下 Java 代码将上传文件并使用 `ProgressListener` 来跟踪上传进度。有关如何创建和测试有效示例的说明，请参阅《适用于 Java 的 Amazon SDK 开发人员指南》中的入门。

```
import java.io.File;

import com.amazonaws.AmazonClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.event.ProgressEvent;
import com.amazonaws.event.ProgressListener;
import com.amazonaws.services.s3.model.PutObjectRequest;
import com.amazonaws.services.s3.transfer.TransferManager;
import com.amazonaws.services.s3.transfer.Upload;

public class TrackMPUProgressUsingHighLevelAPI {

    public static void main(String[] args) throws Exception {
        String existingBucketName = "*** Provide bucket name ***";
        String keyName            = "*** Provide object key ***";
        String filePath           = "*** file to upload ***";

        TransferManager tm = new TransferManager(new ProfileCredentialsProvider());
```

```
        // For more advanced uploads, you can create a request object
        // and supply additional request parameters (ex: progress listeners,
        // canned ACLs, etc.)
        PutObjectRequest request = new PutObjectRequest(
          existingBucketName, keyName, new File(filePath));

        // You can ask the upload for its progress, or you can
        // add a ProgressListener to your request to receive notifications
        // when bytes are transferred.
        request.setGeneralProgressListener(new ProgressListener() {
   @Override
   public void progressChanged(ProgressEvent progressEvent) {
    System.out.println("Transferred bytes: " +
      progressEvent.getBytesTransferred());
   }
  });

        // TransferManager processes all transfers asynchronously,
        // so this call will return immediately.
        Upload upload = tm.upload(request);

        try {
         // You can block and wait for the upload to finish
         upload.waitForCompletion();
        } catch (AmazonClientException amazonClientException) {
         System.out.println("Unable to upload file, upload aborted.");
         amazonClientException.printStackTrace();
        }
    }
}
```

.NET

以下 C# 示例使用 TransferUtility 类将文件上传到 S3 存储桶并跟踪上传的进度。有关设置和运行代码示例的信息，请参阅《适用于 .NET 的 Amazon SDK 开发人员指南》中的适用于 .NET 的 Amazon SDK 入门。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Transfer;
using System;
using System.Threading.Tasks;
```

```
namespace Amazon.DocSamples.S3
{
    class TrackMPUUsingHighLevelAPITest
    {
        private const string bucketName = "*** provide the bucket name ***";
        private const string keyName = "*** provide the name for the uploaded object
 ***";
        private const string filePath = " *** provide the full path name of the file
 to upload **";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;


        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            TrackMPUAsync().Wait();
        }

        private static async Task TrackMPUAsync()
        {
            try
            {
                var fileTransferUtility = new TransferUtility(s3Client);

                // Use TransferUtilityUploadRequest to configure options.
                // In this example we subscribe to an event.
                var uploadRequest =
                    new TransferUtilityUploadRequest
                    {
                        BucketName = bucketName,
                        FilePath = filePath,
                        Key = keyName
                    };

                uploadRequest.UploadProgressEvent +=
                    new EventHandler<UploadProgressArgs>
                        (uploadRequest_UploadPartProgressEvent);

                await fileTransferUtility.UploadAsync(uploadRequest);
                Console.WriteLine("Upload completed");
```

```
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
        }

        static void uploadRequest_UploadPartProgressEvent(object sender,
 UploadProgressArgs e)
        {
            // Process event.
            Console.WriteLine("{0}/{1}", e.TransferredBytes, e.TotalBytes);
        }
    }
}
```

## 中止分段上传

启动分段上传后，您便开始上传段。Amazon S3 存储这些分段，并且仅当您上传了所有分段并发送请求来完成分段上传后，才创建对象。在收到完成分段上传请求后，Amazon S3 会将这些段汇集在一起并创建一个对象。如果您未成功发送完成分段上传请求，S3 不会汇集这些分段，并且不会创建任何对象。如果您不希望在上传各分段后完成分段上传，则应中止分段上传。

您需要为与上传的分段关联的所有存储付费。建议务必完成分段上传，或者停止分段上传来移除任何已上传的分段。有关定价的更多信息，请参阅分段上传和定价。

您还可以使用存储桶生命周期配置停止未完成的分段上传。有关更多信息，请参阅 配置存储桶生命周期配置以删除未完成的分段上传。

下一节介绍如何使用 Amazon Command Line Interface、REST API 或 Amazon SDK 来停止 Amazon S3 中正在进行的分段上传。

### 使用 Amazon CLI

有关使用 Amazon CLI 停止分段上传的更多信息，请参阅《Amazon CLI 命令参考》中的 abort-multipart-upload。

使用 REST API

有关使用 REST API 停止分段上传的更多信息，请参阅 Amazon Simple Storage Service API 参考中的 AbortMultipartUpload。

使用 Amazon 软件开发工具包（高级别 API）

Java

TransferManager 类提供了停止正在进行的分段上传的 abortMultipartUploads 方法。启动上传后，上传将被视为正在进行，直到您完成或停止该操作。您可以提供 Date 值和此 API 来停止该存储桶上所有在指定 Date 前启动的并且仍在进行的上传。

以下任务将引导您使用高级别 Java 类来停止分段上传。

高级别 API 分段上传停止过程

| | |
|---|---|
| 1 | 创建 TransferManager 类的实例。 |
| 2 | 通过传递存储桶名称和 Date 值执行 TransferManager.abortMultipartUploads 方法。 |

以下 Java 代码将停止特定存储桶上所有在一周前启动的并且仍在进行的分段上传。有关如何创建和测试有效示例的说明，请参阅《适用于 Java 的 Amazon SDK 开发人员指南》中的入门。

```
import java.util.Date;

import com.amazonaws.AmazonClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3.transfer.TransferManager;

public class AbortMPUUsingHighLevelAPI {

    public static void main(String[] args) throws Exception {
        String existingBucketName = "*** Provide existing bucket name ***";

        TransferManager tm = new TransferManager(new ProfileCredentialsProvider());


        int sevenDays = 1000 * 60 * 60 * 24 * 7;
  Date oneWeekAgo = new Date(System.currentTimeMillis() - sevenDays);
```

```
        try {
         tm.abortMultipartUploads(existingBucketName, oneWeekAgo);
        } catch (AmazonClientException amazonClientException) {
         System.out.println("Unable to upload file, upload was aborted.");
         amazonClientException.printStackTrace();
        }
    }
}
```

> **Note**
>
> 您也可以停止特定的分段上传。有关更多信息，请参阅 使用 Amazon SDK（低级别 API）。

.NET

以下 C# 示例将停止一周前在特定存储桶上启动的正在进行的所有分段上传。有关设置和运行代码示例的信息，请参阅《适用于 .NET 的 Amazon SDK 开发人员指南》中的适用于 .NET 的 Amazon SDK 入门。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Transfer;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class AbortMPUUsingHighLevelAPITest
    {
        private const string bucketName = "*** provide bucket name ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            AbortMPUAsync().Wait();
```

```
        }

        private static async Task AbortMPUAsync()
        {
            try
            {
                var transferUtility = new TransferUtility(s3Client);

                // Abort all in-progress uploads initiated before the specified
 date.
                await transferUtility.AbortMultipartUploadsAsync(
                    bucketName, DateTime.Now.AddDays(-7));
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
        }
    }
}
```

> **Note**
>
> 您也可以停止特定的分段上传。有关更多信息，请参阅 使用 Amazon SDK（低级别 API）。

使用 Amazon SDK（低级别 API）

您可以通过调用 `AmazonS3.abortMultipartUpload` 方法停止正在进行的分段上传。此方法将删除任何已上传到 Amazon S3 的分段并释放资源。您必须提供上传 ID、存储桶名称和键名称。以下 Java 代码示例演示如何停止正在进行的分段上传。

要停止分段上传，请提供上传时使用的上传 ID、存储桶名称和键名。停止一个分段上传之后，您便无法使用相应的上传 ID 上传其他分段。有关 Amazon S3 分段上传的更多信息，请参阅 在 Amazon S3 中使用分段上传来上传和复制对象。

Java

以下 Java 代码示例停止正在进行的分段上传。

Example

```
InitiateMultipartUploadRequest initRequest =
    new InitiateMultipartUploadRequest(existingBucketName, keyName);
InitiateMultipartUploadResult initResponse =
               s3Client.initiateMultipartUpload(initRequest);

AmazonS3 s3Client = new AmazonS3Client(new ProfileCredentialsProvider());
s3Client.abortMultipartUpload(new AbortMultipartUploadRequest(
            existingBucketName, keyName, initResponse.getUploadId()));
```

> **Note**
>
> 您可以在特定时间之前停止所有仍在进行的分段上传，而不是停止某个特定的分段上传。此清理操作对于停止您已启动但未完成或停止的旧分段上传非常有用。有关更多信息，请参阅使用 Amazon 软件开发工具包（高级别 API）。

.NET

以下 C# 示例演示如何停止分段上传。有关包含以下代码的完整 C# 示例，请参阅 使用 Amazon SDK（低级别 API）。

```
AbortMultipartUploadRequest abortMPURequest = new AbortMultipartUploadRequest
{
    BucketName = existingBucketName,
    Key = keyName,
    UploadId = initResponse.UploadId
};
await AmazonS3Client.AbortMultipartUploadAsync(abortMPURequest);
```

还可以中止在特定时间之前启动的所有正在进行的分段上传。对于中止未完成或已中止的分段上传，此清理操作很有用。有关更多信息，请参阅 使用 Amazon 软件开发工具包（高级别 API）。

PHP

本示例介绍如何使用 适用于 PHP 的 Amazon SDK 的版本 3 中的类中止正在进行的分段上传。有关适用于 Ruby 的 Amazon 开发工具包 API 的更多信息，请转到适用于 Ruby 的 Amazon 开发工具包 – 版本 2。例如，`abortMultipartUpload()` 方法。

有关适用于 Ruby 的 Amazon 开发工具包 API 的更多信息，请转到适用于 Ruby 的 Amazon 开发工具包 – 版本 2。

```
 require 'vendor/autoload.php';

use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';
$uploadId = '*** Upload ID of upload to Abort ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// Abort the multipart upload.
$s3->abortMultipartUpload([
    'Bucket'   => $bucket,
    'Key'      => $keyname,
    'UploadId' => $uploadId,
]);
```

## 使用分段上传复制对象

分段上传支持您将对象作为一组分段进行上传。本节中的示例将向您展示如何使用分段上传 API 复制大于 5 GB 的对象。有关分段上传的信息，请参阅在 Amazon S3 中使用分段上传来上传和复制对象。

可以在单个操作中复制小于 5 GB 的对象，而无需使用分段上传 API。可以使用 Amazon Web Services Management Console、Amazon CLI、REST API 或 Amazon SDK 复制小于 5 GB 的对象。有关更多信息，请参阅 复制、移动和重命名对象。

有关使用分段上传以及额外的校验和来上传对象的端到端过程，请参阅教程：通过分段上传来上传对象并验证其数据完整性。

下一节介绍如何使用 REST API 或 Amazon SDK 通过分段上传来复制对象。

使用 REST API

Amazon Simple Storage Service API 参考的下面几节描述了适用于分段上传的 REST API。使用上传分段（复制）API 复制现有的对象，并通过在请求中添加 `x-amz-copy-source` 请求标头指定源对象。

- 开始分段上传
- 上传分段
- 上传分段（复制）
- 完成分段上传
- 中止分段上传
- 列出分段
- 列出分段上传

您可以使用这些 API 生成您自己的 REST 请求，也可以使用我们提供的 SDK 之一。有关通过 Amazon CLI 执行分段上传的更多信息，请参阅 使用 Amazon CLI。有关 SDK 的更多信息，请参阅 Amazon SDK 对于分段上传的支持。

使用 Amazon SDK

要使用低级别 API 复制对象，请执行以下操作：

- 通过调用 `AmazonS3Client.initiateMultipartUpload()` 方法启动分段上传。
- 从 `AmazonS3Client.initiateMultipartUpload()` 方法返回的响应对象保存上传 ID。您为每个分段上传操作提供此上传 ID。
- 复制所有段。对于需要复制的每个段，创建一个 `CopyPartRequest` 类的新实例。提供段信息，包括源和目标存储桶名称、源和目标对象键、上传 ID、段的第一个字节和最后一个字节的位置以及段编号。
- 保存 `AmazonS3Client.copyPart()` 方法调用的响应。每个响应均包括 `ETag` 值和已上传分段的段编号。您需要此信息才能完成分段上传。
- 调用 `AmazonS3Client.completeMultipartUpload()` 方法以完成复制操作。

Java

Example

以下示例说明如何使用 Amazon S3 低级别 Java API 执行分段复制。有关创建和测试有效示例的说明，请参阅《适用于 Java 的 Amazon SDK 开发人员指南》中的入门。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.io.IOException;
import java.util.ArrayList;
import java.util.List;

public class LowLevelMultipartCopy {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String sourceBucketName = "*** Source bucket name ***";
        String sourceObjectKey = "*** Source object key ***";
        String destBucketName = "*** Target bucket name ***";
        String destObjectKey = "*** Target object key ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Initiate the multipart upload.
            InitiateMultipartUploadRequest initRequest = new
 InitiateMultipartUploadRequest(destBucketName,
                    destObjectKey);
            InitiateMultipartUploadResult initResult =
 s3Client.initiateMultipartUpload(initRequest);

            // Get the object size to track the end of the copy operation.
```

```
            GetObjectMetadataRequest metadataRequest = new
GetObjectMetadataRequest(sourceBucketName, sourceObjectKey);
            ObjectMetadata metadataResult =
s3Client.getObjectMetadata(metadataRequest);
            long objectSize = metadataResult.getContentLength();

            // Copy the object using 5 MB parts.
            long partSize = 5 * 1024 * 1024;
            long bytePosition = 0;
            int partNum = 1;
            List<CopyPartResult> copyResponses = new ArrayList<CopyPartResult>();
            while (bytePosition < objectSize) {
                // The last part might be smaller than partSize, so check to make
sure
                // that lastByte isn't beyond the end of the object.
                long lastByte = Math.min(bytePosition + partSize - 1, objectSize -
1);

                // Copy this part.
                CopyPartRequest copyRequest = new CopyPartRequest()
                        .withSourceBucketName(sourceBucketName)
                        .withSourceKey(sourceObjectKey)
                        .withDestinationBucketName(destBucketName)
                        .withDestinationKey(destObjectKey)
                        .withUploadId(initResult.getUploadId())
                        .withFirstByte(bytePosition)
                        .withLastByte(lastByte)
                        .withPartNumber(partNum++);
                copyResponses.add(s3Client.copyPart(copyRequest));
                bytePosition += partSize;
            }

            // Complete the upload request to concatenate all uploaded parts and
make the
            // copied object available.
            CompleteMultipartUploadRequest completeRequest = new
CompleteMultipartUploadRequest(
                    destBucketName,
                    destObjectKey,
                    initResult.getUploadId(),
                    getETags(copyResponses));
            s3Client.completeMultipartUpload(completeRequest);
            System.out.println("Multipart copy complete.");
        } catch (AmazonServiceException e) {
```

```
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }

    // This is a helper function to construct a list of ETags.
    private static List<PartETag> getETags(List<CopyPartResult> responses) {
        List<PartETag> etags = new ArrayList<PartETag>();
        for (CopyPartResult response : responses) {
            etags.add(new PartETag(response.getPartNumber(), response.getETag()));
        }
        return etags;
    }
}
```

.NET

以下 C# 示例说明如何使用 适用于 .NET 的 Amazon SDK 将大于 5 GB 的 Amazon S3 对象从一个源位置复制到另一个源位置，例如从一个存储桶复制到另一个存储桶。要复制小于 5 GB 的对象，请使用 使用 Amazon SDK 中所述的单个操作复制过程。有关 Amazon S3 分段上传的更多信息，请参阅 在 Amazon S3 中使用分段上传来上传和复制对象。

此示例说明如何使用 适用于 .NET 的 Amazon SDK 分段上传 API 将大于 5 GB 的 Amazon S3 对象从一个 S3 存储桶复制到另一个存储桶。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class CopyObjectUsingMPUapiTest
    {
```

```
        private const string sourceBucket = "*** provide the name of the bucket with
source object ***";
        private const string targetBucket = "*** provide the name of the bucket to
copy the object to ***";
        private const string sourceObjectKey = "*** provide the name of object to
copy ***";
        private const string targetObjectKey = "*** provide the name of the object
copy ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            Console.WriteLine("Copying an object");
            MPUCopyObjectAsync().Wait();
        }
        private static async Task MPUCopyObjectAsync()
        {
            // Create a list to store the upload part responses.
            List<UploadPartResponse> uploadResponses = new
List<UploadPartResponse>();
            List<CopyPartResponse> copyResponses = new List<CopyPartResponse>();

            // Setup information required to initiate the multipart upload.
            InitiateMultipartUploadRequest initiateRequest =
                new InitiateMultipartUploadRequest
                {
                    BucketName = targetBucket,
                    Key = targetObjectKey
                };

            // Initiate the upload.
            InitiateMultipartUploadResponse initResponse =
                await s3Client.InitiateMultipartUploadAsync(initiateRequest);

            // Save the upload ID.
            String uploadId = initResponse.UploadId;

            try
            {
                // Get the size of the object.
```

```
                GetObjectMetadataRequest metadataRequest = new
GetObjectMetadataRequest
                {
                    BucketName = sourceBucket,
                    Key = sourceObjectKey
                };

                GetObjectMetadataResponse metadataResponse =
                    await s3Client.GetObjectMetadataAsync(metadataRequest);
                long objectSize = metadataResponse.ContentLength; // Length in
bytes.

                // Copy the parts.
                long partSize = 5 * (long)Math.Pow(2, 20); // Part size is 5 MB.

                long bytePosition = 0;
                for (int i = 1; bytePosition < objectSize; i++)
                {
                    CopyPartRequest copyRequest = new CopyPartRequest
                    {
                        DestinationBucket = targetBucket,
                        DestinationKey = targetObjectKey,
                        SourceBucket = sourceBucket,
                        SourceKey = sourceObjectKey,
                        UploadId = uploadId,
                        FirstByte = bytePosition,
                        LastByte = bytePosition + partSize - 1 >= objectSize ?
objectSize - 1 : bytePosition + partSize - 1,
                        PartNumber = i
                    };

                    copyResponses.Add(await s3Client.CopyPartAsync(copyRequest));

                    bytePosition += partSize;
                }

                // Set up to complete the copy.
                CompleteMultipartUploadRequest completeRequest =
                new CompleteMultipartUploadRequest
                {
                    BucketName = targetBucket,
                    Key = targetObjectKey,
                    UploadId = initResponse.UploadId
                };
```

```
                completeRequest.AddPartETags(copyResponses);

                // Complete the copy.
                CompleteMultipartUploadResponse completeUploadResponse =
                    await s3Client.CompleteMultipartUploadAsync(completeRequest);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
        }
    }
}
```

## 教程：通过分段上传来上传对象并验证其数据完整性

分段上传允许将单个对象作为一组分段上传。每个分段都是对象数据的连续部分。您可以独立上传以及按任意顺序上传这些对象分段。如果任意分段传输失败，可以重新传输该分段且不会影响其他分段。上传完所有的对象分段后，Amazon S3 将汇集这些分段并创建对象。一般而言，如果您的对象大小达到了 100 MB，您应该考虑使用分段上传，而不是在单个操作中上传对象。有关分段上传的更多信息，请参阅 在 Amazon S3 中使用分段上传来上传和复制对象。有关分段上传的相关限制，请参阅 Amazon S3 分段上传限制。

可以使用校验和来验证资产在复制时是否未被更改。执行校验和包括使用算法按顺序迭代文件中的每个字节。Amazon S3 提供了多个校验和选项，用于检查数据的完整性。我们建议您将这些完整性检查作为持久性最佳实践加以执行，并确认每个字节在传输过程中都未经更改。Amazon S3 还支持以下算法：SHA-1、SHA-256、CRC32 和 CRC32C。Amazon S3 使用其中一个或多个算法来计算额外的校验和值，并将其存储为对象元数据的一部分。有关校验和的更多信息，请参阅在 Amazon S3 中检查对象完整性。

目标

在本教程中，您将学习如何在 Amazon 命令行界面（Amazon CLI）中使用分段上传和额外的 SHA-256 校验和将对象上传到 Amazon S3。您还将学习如何通过计算已上传对象的 MD5 哈希值和 SHA-256 校验和，来检查对象的数据完整性。

主题


- 先决条件
- 步骤 1：创建大文件
- 步骤 2：将文件拆分为多个文件
- 步骤 3：创建分段上传并指定额外的校验和
- 步骤 4：上传分段上传的分段
- 步骤 5：列出分段上传的所有分段
- 步骤 6：完成分段上传
- 步骤 7：确认对象上传到存储桶
- 步骤 8：使用 MD5 校验和验证对象完整性
- 步骤 9：使用额外的校验和验证对象完整性
- 步骤 10：清除资源


## 先决条件

- 在开始本教程之前，请确保您有权访问要上传到的 Amazon S3 存储桶。有关更多信息，请参阅 创建通用存储桶。
- 您必须安装并配置了 Amazon CLI。如果未安装 Amazon CLI，请参阅《Amazon Command Line Interface用户指南》中的 Install or update to the latest version of the Amazon CLI。
- 或者，您可以从控制台中使用 Amazon CloudShell 运行 Amazon CLI 命令。Amazon CloudShell 是一个基于浏览器、预先经过身份验证的 Shell，您可以直接从 Amazon Web Services Management Console中启动它。有关更多信息，请参阅《Amazon CloudShell 用户指南》中的 What is CloudShell? 和 Getting started with Amazon CloudShell。

## 步骤 1：创建大文件

如果您已经准备好要上传的文件，则可以在本教程中使用该文件。否则，请使用以下步骤创建一个 15 MB 的文件。有关分段上传的相关限制，请参阅 Amazon S3 分段上传限制。

### 创建大文件

根据您使用的操作系统，使用以下命令之一来创建文件。

#### Linux 或 macOS

要创建 15 MB 的文件，请打开本地终端并运行以下命令：

```
dd if=/dev/urandom of=census-data.bin bs=1M count=15
```

此命令创建一个名为 census-data.bin 的文件，其中填充了随机字节，大小为 15 MB。

Windows

要创建 15 MB 的文件，请打开本地终端并运行以下命令：

```
fsutil file createnew census-data.bin 15728640
```

此命令创建一个名为 census-data.bin 的文件，其中包含任意数据，大小为 15 MB（15728640 字节）。

步骤 2：将文件拆分为多个文件

要执行分段上传，必须将大文件拆分为若干较小的分段。然后，可以使用分段上传过程来上传较小的分段。此步骤演示如何将步骤 1 中创建的大文件拆分为较小的分段。以下示例使用名为 census-data.bin 的 15 MB 文件。

将大文件拆分为多个分段

Linux 或 macOS

要将大文件分成 5 MB 的分段，请使用 split 命令。打开终端并运行以下命令：

```
split -b 5M -d census-data.bin census-part
```

此命令将 census-data.bin 拆分成名为 census-part** 的 5 MB 分段，其中 ** 是从 00 开始的数字后缀。

Windows

要拆分大文件，请使用 PowerShell。打开 Powershell 并运行以下命令：

```
$inputFile = "census-data.bin"
$outputFilePrefix = "census-part"
$chunkSize = 5MB

$fs = [System.IO.File]::OpenRead($inputFile)
$buffer = New-Object byte[] $chunkSize
$fileNumber = 0
```

```
while ($fs.Position -lt $fs.Length) {
$bytesRead = $fs.Read($buffer, 0, $chunkSize)
$outputFile = "{0}{1:D2}" -f $outputFilePrefix, $fileNumber
$fileStream = [System.IO.File]::Create($outputFile)
$fileStream.Write($buffer, 0, $bytesRead)
$fileStream.Close()
$fileNumber++
}

$fs.Close()
```

此 PowerShell 脚本以 5 MB 大小的分块读取大文件，并将每个分块写入一个带有数字后缀的新文件。

运行相应的命令后，您应该会在执行该命令的目录中看到各个分段。每个分段都有一个与其分段编号对应的后缀，例如：

```
census-part00 census-part01 census-part02
```

步骤 3：创建分段上传并指定额外的校验和

要开始分段上传过程，您需要创建分段上传请求。此步骤包括启动分段上传以及为数据完整性指定额外的校验和。以下示例使用 SHA-256 校验和。如果您想要提供描述正上传的对象的任何元数据，必须在请求中提供它以便开始分段上传。

> **Note**
>
> 在本步骤和后续步骤中，本教程使用 SHA-256 额外算法。您可以选择为这些步骤使用其他的额外校验和，例如 CRC32、CRC32C 或 SHA-1。如果使用不同的算法，则必须在整个教程步骤中都使用该算法。

开始分段上传

在终端中，使用以下 `create-multipart-upload` 命令开始存储桶的分段上传。将 *amzn-s3-demo-bucket1* 替换为实际存储桶名称。另外，请用您选择的文件名替换 `census_data_file`。上传完成后，此文件名将成为对象键。

```
aws s3api create-multipart-upload --bucket amzn-s3-demo-bucket1 --key
 'census_data_file' --checksum-algorithm sha256
```

如果您的请求执行成功，您将看到如下 JSON 输出：

```
{
    "ServerSideEncryption": "AES256",
    "ChecksumAlgorithm": "SHA256",
    "Bucket": "amzn-s3-demo-bucket1",
    "Key": "census_data_file",
    "UploadId":
 "cNV6KCSNANFZapz1LUGPC5XwUVi1n6yUoIeSP138sNOKPeMhpKQRrbT9k0ePmgoOTCj9K83T4e2Gb5hQvNoNpCKqyb8m3
}
```

> **Note**
>
> 当您发送请求以开始分段上传时，Amazon S3 将返回具有上传 ID 的响应，此 ID 是分段上传的唯一标识符。无论您何时上传分段、列出分段、完成上传或停止上传，您都必须包括此上传 ID。后续步骤需要用到 UploadId、Key 和 Bucket 值，因此请务必保存这些值。
> 此外，如果您将分段上传与额外的校验和结合使用，则分段编号必须是连续的。如果您使用不连续的分段编号，则 complete-multipart-upload 请求可能会导致 HTTP 500 Internal Server Error。

步骤 4：上传分段上传的分段

在此步骤中，您将分段上传的各个分段上传到 S3 存储桶。使用 upload-part 命令单独上传每个分段。此过程要求为每个分段指定上传 ID、分段编号和要上传的文件。

上传分段

1. 上传分段时，除了上传 ID，还必须使用 --part-number 参数来指定分段编号。您可以选择 1 和 10000 之间的任意分段编号。分段编号在您正在上传的对象中唯一地识别分段及其位置。您选择的分段编号必须为连续序列（例如，它可以是 1、2 或 3）。如果您使用之前上传的分段的同一分段编号上传新分段，则之前上传的分段将被覆盖。
2. 使用 upload-part 命令来上传分段上传的每个分段。--upload-id 与步骤 3 中 create-multipart-upload 命令创建的输出内容相同。要上传数据的第一个分段，请使用以下命令：

```
aws s3api upload-part --bucket amzn-s3-demo-bucket1 --key
 'census_data_file' --part-number 1 --body census-part00 --upload-id
```

```
 "cNV6KCSNANFZapz1LUGPC5XwUVi1n6yUoIeSP138sNOKPeMhpKQRrbT9k0ePmgoOTCj9K83T4e2Gb5hQvNoNpCKqy
 --checksum-algorithm SHA256
```

完成每个 upload-part 命令后，您应该会看到类似以下示例的输出：

```
{
    "ServerSideEncryption": "AES256",
    "ETag": "\"e611693805e812ef37f96c9937605e69\"",
    "ChecksumSHA256": "QLl8R4i4+SaJlrl8ZIcutc5TbZtwt2NwB8lTXkd3GH0="
}
```

3. 对于后续分段，相应地递增分段编号：

```
aws s3api upload-part --bucket amzn-s3-demo-bucket1 --key 'census_data_file' --
part-number <part-number> --body <file-path> --upload-id "<your-upload-id>" --
checksum-algorithm SHA256
```

例如，使用以下命令来上传第二个分段：

```
aws s3api upload-part --bucket amzn-s3-demo-bucket1 --key
 'census_data_file' --part-number 2 --body census-part01 --upload-id
 "cNV6KCSNANFZapz1LUGPC5XwUVi1n6yUoIeSP138sNOKPeMhpKQRrbT9k0ePmgoOTCj9K83T4e2Gb5hQvNoNpCKqy
 --checksum-algorithm SHA256
```

Amazon S3 将在响应的标头中返回每个已上传分段的实体标签（ETag）和额外的校验和。

4. 继续使用 upload-part 命令，直到上传了对象的所有分段。

步骤 5：列出分段上传的所有分段

要完成分段上传，您需要列出在这个特定分段上传任务中已经上传的所有分段。list-parts 命令的输出提供了诸如存储桶名称、键、上传 ID、分段编号、ETag、额外的校验和等信息。将此输出保存在文件中会很有帮助，这样您就可以在完成分段上传过程的下一步中使用它。可以使用以下方法创建名为 parts.json 的 JSON 输出文件。

创建列出所有分段的文件

1. 要生成包含所有已上传分段详细信息的 JSON 文件，请使用以下 list-parts 命令。将 ***amzn-s3-demo-bucket1*** 替换为实际的存储桶名称，并将 **<your-upload-id>** 替换为您在步骤 3 中

收到的上传 ID。有关 `list-parts` 命令的更多信息，请参阅《Amazon Command Line Interface 用户指南》中的 list-parts。

```
aws s3api list-parts --bucket amzn-s3-demo-bucket1 --key 'census_data_file' --
upload-id <your-upload-id> --query '{Parts: Parts[*].{PartNumber: PartNumber, ETag:
 ETag, ChecksumSHA256: ChecksumSHA256}}' --output json > parts.json
```

这样会生成一个名为 `parts.json` 的新文件。该文件采用 JSON 格式，包含所有已上传分段的信息。`parts.json` 文件包含分段上传的每个分段的基本信息，例如分段编号及其相应的 ETag 值，这些是完成分段上传过程所必需的。

2. 使用任何文本编辑器或通过终端打开 `parts.json`。以下是示例输出：

```
{
    "Parts": [
        {
            "PartNumber": 1,
            "ETag": "\"3c3097f89e2a2fece47ac54b243c9d97\"",
            "ChecksumSHA256": "fTPVHfyNHdv5VkR4S3EewdyioXECv7JBxN+d4FXYYTw="
        },
        {
            "PartNumber": 2,
            "ETag": "\"03c71cc160261b20ab74f6d2c476b450\"",
            "ChecksumSHA256": "VDWTa8enjOvULBAO3W2a6C+5/7ZnNjrnLApa1QVc3FE="
        },
        {
            "PartNumber": 3,
            "ETag": "\"81ae0937404429a97967dffa7eb4affb\"",
            "ChecksumSHA256": "cVVkXehUlzcwrBrXgPIM+EKQXPUvWist8mlUTCs4bg8="
        }
    ]
}
```

步骤 6：完成分段上传

在分段上传的所有分段都上传完毕并且列出分段信息后，最后一步是完成分段上传。此步骤会在 S3 存储桶中将所有上传的分段合并成单个对象。

> **Note**
>
> 您可以在调用 complete-multipart-upload 之前，通过在请求中包含 --checksum-sha256 来计算对象的校验和。如果校验和不匹配，Amazon S3 就会让请求失败。有关更多信息，请参阅《Amazon Command Line Interface 用户指南》中的 complete-multipart-upload。

完成分段上传

要最终完成分段上传，请使用 complete-multipart-upload 命令。此命令需要用到步骤 5 中创建的 parts.json 文件、存储桶名称以及上传 ID。将 **<*amzn-s3-demo-bucket1*>** 替换为存储桶名称，并将 **<your-upload-id>** 替换为 parts.json 的上传 ID。

```
aws s3api complete-multipart-upload --multipart-upload file://parts.json --bucket amzn-s3-demo-bucket1 --key 'census_data_file' --upload-id <your-upload-id>
```

以下是示例输出：

```
{
    "ServerSideEncryption": "AES256",
    "Location": "https://amzn-s3-demo-bucket1.s3.us-east-2.amazonaws.com/census_data_file",
    "Bucket": "amzn-s3-demo-bucket1",
    "Key": "census_data_file",
    "ETag": "\"f453c6dccca969c457efdf9b1361e291-3\"",
    "ChecksumSHA256": "aI8EoktCdotjU8Bq46DrPCxQCGuGcPIhJ51noWs6hvk=-3"
}
```

> **Note**
>
> 此时请勿删除各个分段文件。您还需要使用各个分段来对它们执行校验和，从而验证合并在一起的对象的完整性。

步骤 7：确认对象上传到存储桶

完成分段上传后，您可以验证对象已成功地上传到 S3 存储桶。要列出存储桶中的对象并确认新上传的文件已经存在，请使用 list-objects-v2 命令。

列出上传的对象

要列出存储桶中的对象，请使用 `list-objects-v2` 命令。将 ***amzn-s3-demo-bucket1*** 替换为实际存储桶名称：

```
aws s3api list-objects-v2 --bucket amzn-s3-demo-bucket1
```

此命令将返回存储桶中对象的列表。在对象列表中查找您上传的文件（例如 `census_data_file`）。

有关更多信息，请参阅《Amazon Command Line Interface用户指南》中 `list-objects-v2` 命令的 Examples 部分。

步骤 8：使用 MD5 校验和验证对象完整性

在上传对象时，可以指定校验和算法以供 Amazon S3 使用。默认情况下，Amazon S3 将 MD5 字节摘要存储为对象的 ETag。对于分段上传，ETag 不是完整对象的校验和，而是每个单独分段的校验和组合。

使用 MD5 校验和验证对象完整性

1. 要检索已上传对象的 ETag，请执行 `head-object` 请求：

   ```
   aws s3api head-object --bucket amzn-s3-demo-bucket1 --key census_data_file
   ```

   以下是示例输出：

   ```
   {
       "AcceptRanges": "bytes",
       "LastModified": "2024-07-26T19:04:13+00:00",
       "ContentLength": 16106127360,
       "ETag": "\"f453c6dccca969c457efdf9b1361e291-3\"",
       "ContentType": "binary/octet-stream",
       "ServerSideEncryption": "AES256",
       "Metadata": {}
   }
   ```

   此 ETag 的末尾附有“-3”。这表示对象是使用分段上传分为三个分段进行上传的。

2. 接下来，使用 `md5sum` 命令计算每个分段的 MD5 校验和。请确保提供指向分段文件的正确路径：

```
md5sum census-part*
```

以下是示例输出：

```
e611693805e812ef37f96c9937605e69 census-part00
63d2d5da159178785bfd6b6a5c635854 census-part01
95b87c7db852451bb38b3b44a4e6d310 census-part02
```

3. 对于此步骤，手动将 MD5 哈希值合并为一个字符串。然后，运行以下命令，将字符串转换为二进制并计算二进制值的 MD5 校验和：

```
echo
 "e611693805e812ef37f96c9937605e6963d2d5da159178785bfd6b6a5c63585495b87c7db852451bb38b3b44a
 | xxd -r -p | md5sum
```

以下是示例输出：

```
f453c6dccca969c457efdf9b1361e291 -
```

此哈希值应与步骤 1 中原始 ETag 值的哈希值相匹配，这可验证 `census_data_file` 对象的完整性。

当您指示 Amazon S3 使用其他校验和时，Amazon S3 会计算每个分段的校验和值并存储这些值。如果您想检索仍在进行的分段上传的各个分段的校验和值，可以使用 `list-parts`。

有关校验和如何处理分段上传对象的更多信息，请参阅在 Amazon S3 中检查对象完整性。

步骤 9：使用额外的校验和验证对象完整性

在本步骤中，教程使用 SHA-256 作为额外的校验和来验证对象完整性。如果您使用了不同的额外校验和，请改用该校验和值。

使用 SHA256 验证对象完整性

1. 在终端中运行以下命令（包括 `--checksum-mode enabled` 参数），以显示对象的 `ChecksumSHA256` 值：

```
aws s3api head-object --bucket amzn-s3-demo-bucket1 --key census_data_file --
checksum-mode enabled
```

以下是示例输出：

```
{
    "AcceptRanges": "bytes",
    "LastModified": "2024-07-26T19:04:13+00:00",
    "ContentLength": 16106127360,
    "ChecksumSHA256": "aI8EoktCdotjU8Bq46DrPCxQCGuGcPIhJ51noWs6hvk=-3",
    "ETag": "\"f453c6dccca969c457efdf9b1361e291-3\"",
    "ContentType": "binary/octet-stream",
    "ServerSideEncryption": "AES256",
    "Metadata": {}
}
```

2. 使用以下命令将各个分段的 ChecksumSHA256 值解码为 base64，然后将其保存到名为 outfile 的二进制文件中。这些值可以在 parts.json 文件中找到。将示例 base64 字符串替换为实际的 ChecksumSHA256 值。

```
echo "QLl8R4i4+SaJlrl8ZIcutc5TbZtwt2NwB8lTXkd3GH0=" | base64 --decode >> outfile
echo "xCdgs1K5Bm4jWETYw/CmGYr+m6O2DcGfpckx5NVokvE=" | base64 --decode >> outfile
echo "f5wsfsa5bB+yXuwzqG1Bst91uYneqGD3CCidpb54mAo=" | base64 --decode >> outfile
```

3. 运行以下命令计算 outfile 的 SHA256 校验和：

```
sha256sum outfile
```

以下是示例输出：

```
688f04a24b42768b6353c06ae3a0eb3c2c50086b8670f221279d67a16b3a86f9 outfile
```

在下一步中，获取哈希值并将其转换为二进制值。此二进制值应与步骤 1 中的 ChecksumSHA256 值相匹配。

4. 将步骤 3 中的 SHA256 校验和转换为二进制，然后将其编码为 base64，来验证它与步骤 1 中的 ChecksumSHA256 值相匹配：

```
echo "688f04a24b42768b6353c06ae3a0eb3c2c50086b8670f221279d67a16b3a86f9" | xxd -r -p
 | base64
```

以下是示例输出：

```
aI8EoktCdotjU8Bq46DrPCxQCGuGcPIhJ51noWs6hvk=
```

此输出应确认 base64 输出与 head-object 命令输出中的 ChecksumSHA256 值相匹配。如果输出与校验和值匹配，则该对象有效。

**Important**

- 当您指示 Amazon S3 使用额外的校验和时，Amazon S3 会计算每个分段的校验和值并存储这些值。
- 如果您想检索仍在进行的分段上传的各个分段的校验和值，可以使用 list-parts 命令。

步骤 10：清除资源

如果要清理在本教程中创建的文件，请使用以下方法。有关删除上传到 S3 存储桶的文件的说明，请参阅删除 Amazon S3 对象。

删除步骤 1 中创建的本地文件：

要删除您为分段上传创建的文件，请从工作目录中运行以下命令：

```
rm census-data.bin census-part* outfile parts.json
```

## Amazon S3 分段上传限制

分段上传允许将单个对象作为一组分段上传。每个分段都是对象数据的连续部分。上传完所有的对象分段后，Amazon S3 将汇集这些分段并创建对象。一般而言，如果您的对象大小达到了 100 MB，您应该考虑使用分段上传，而不是在单个操作中上传对象。有关分段上传的更多信息，请参阅 在 Amazon S3 中使用分段上传来上传和复制对象。

下表提供了分段上传的核心规范。其中包括最大对象大小、最大分段数、最大分段大小等等。未对分段上传的最后一段施加最小大小限制。

| Item | 规范 |
| --- | --- |
| 最大对象大小 | 5 TiB |
| 每次上传的分段的最大数量 | 10000 |
| 分段编号 | 1 到 10,000（含） |
| 分段大小 | 5MiB 到 5GiB。未对分段上传的最后一段施加最小大小限制。 |
| 列出分段请求返回的分段的最大数量 | 1000 |
| 在列出分段上传请求中返回的分段的最大数量 | 1000 |

# 使用有条件请求向 S3 操作添加前提条件

可以使用有条件请求向 S3 操作添加前提条件。要使用有条件请求，需要向 Amazon S3 API 操作添加一个额外的标头。此标头指定了一个条件，如果不满足该条件，将导致 S3 操作失败。

GET、HEAD 和 COPY 请求支持有条件读取。可以添加前提条件，来根据对象的实体标签（ETag）或上次修改日期返回或复制该对象。这可以将 S3 操作限制为自指定日期以来更新的对象。也可以将 S3 操作限制为特定的 ETag。这可以确保您只返回或复制特定的对象版本。有关对象元数据的详细信息，请参阅 使用对象元数据。

有条件写入可以确保在 PUT 操作期间，存储桶中不存在具有相同键名称的现有对象。这可以防止覆盖具有相同键名称的现有对象。同样，在更新对象之前，可以使用有条件写入来检查对象的 ETag 是否未更改。这样可以防止在不知道对象内容状态的情况下意外覆盖该对象。可以将有条件写入用于 PutObject 或 CompleteMultipartUpload 请求。有关键名称的更多信息，请参阅 为 Amazon S3 对象命名。

有条件读取或有条件写入无需额外付费。对于适用的请求，包括失败的请求，您只需按现有费率付费。有关 Amazon S3 特征和定价的信息，请参阅 Amazon S3 定价。

主题

- 如何使用有条件读取根据元数据检索或复制对象
- 如何使用有条件写入来防止对象覆盖

## 如何使用有条件读取根据元数据检索或复制对象

通过有条件读取，可以向读取请求中添加一个额外的标头，以便向 S3 操作添加前提条件。如果未满足这些前提条件，读取请求将失败。

可以对 GET、HEAD 或 COPY 请求使用有条件读取，以便仅根据对象的元数据返回该对象。

当您上传对象时，Amazon S3 将创建只能由 S3 修改的系统控制的元数据。实体标签（ETag）和 Last-Modified 是系统控制的元数据的示例。对象的 ETag 是一个字符串，表示对象的特定版本。Last-Modified 日期是元数据，表示对象的创建日期或上次修改日期（以较晚者为准）。

通过有条件读取，可以根据对象的 ETag 或 Last-Modified 日期返回该对象。可以在请求中指定 ETag 值，并且仅在 ETag 值匹配时才返回对象。这可以确保您只返回或复制对象的特定版本。可以在读取请求中指定 Last-Modified 值，并且仅当对象自您提供的日期以来已被修改时，才返回该对象。

### 支持的 API

以下 S3 API 支持使用有条件读取：

- GetObject
- HeadObject
- CopyObject

可以使用以下标头来返回依赖于实体标签（ETag）或上次修改日期的对象。有关对象元数据（例如 ETag 和 Last-Modified）的更多信息，请参阅the section called “系统定义的对象元数据”。

GetObject

- `If-Match` — 仅当对象的 ETag 与提供的 ETag 匹配时，才返回该对象。
- `If-Modified-Since` — 仅当对象自指定时间以来已被修改时，才返回该对象。
- `If-None-Match` — 仅当对象的 ETag 与提供的 ETag 不匹配时，才返回该对象。
- `If-Unmodified-Since` — 仅当对象自指定时间以来未被修改时，才返回该对象。

有关这些标头、返回的错误以及 S3 在单个请求中处理多个条件标头的顺序的更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 GetObject。

HeadObject

- `If-Match` — 仅当对象的 ETag 与提供的 ETag 匹配时，才返回该对象。
- `If-Modified-Since` — 仅当对象自指定时间以来已被修改时，才返回该对象。
- `If-None-Match` — 仅当对象的 ETag 与提供的 ETag 不匹配时，才返回该对象。
- `If-Unmodified-Since` — 仅当对象自指定时间以来未被修改时，才返回该对象。

有关这些标头、返回的错误以及 S3 在单个请求中处理多个条件标头的顺序的更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 HeadObject。

CopyObject

- `x-amz-copy-source-if-match` — 仅当对象的 ETag 与提供的 ETag 匹配时，才复制源对象。
- `x-amz-copy-source-if-modified-since` — 仅当对象自指定时间以来已被修改时，才复制源对象。
- `x-amz-copy-source-if-none-match` — 仅当对象的 ETag 与提供的 ETag 不匹配时，才复制源对象。
- `x-amz-copy-source-if-unmodified-since` — 仅当对象自指定时间以来未被修改时，才复制源对象。

有关这些标头、返回的错误以及 S3 在单个请求中处理多个条件标头的顺序的更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 CopyObject。

## 如何使用有条件写入来防止对象覆盖

通过使用有条件写入，可以向 `WRITE` 请求中添加一个额外的标头，以便为 Amazon S3 操作指定前提条件。要有条件地写入对象，请添加 HTTP `If-None-Match` 或 `If-Match` 标头。

`If-None-Match` 标头通过验证存储桶中尚不存在具有相同键名称的对象，来防止覆盖现有数据。

或者，您可以在写入对象之前添加 `If-Match` 标头来检查对象的实体标签（ETag）。通过此标头，Amazon S3 将提供的 ETag 值与 S3 中对象的 ETag 值进行比较。如果 ETag 值不匹配，则操作会失败。

存储桶拥有者可以使用存储桶策略对上传的对象强制实施有条件写入。有关更多信息，请参阅 the section called “强制实施有条件写入”。

> **Note**
>
> 要使用有条件写入，必须通过 HTTPS（TLS）发出请求，或使用 Amazon 签名版本 4 对请求进行签名。

主题

- 如何防止基于键名称的对象覆盖
- 如果对象已更改，如何防止被覆盖
- 有条件写入行为
- 有条件写入场景
- 强制对 Amazon S3 存储桶实施有条件写入

## 如何防止基于键名称的对象覆盖

在创建对象之前，可以使用 HTTP `If-None-Match` 有条件标头，根据其键名称检查指定存储桶中是否已存在该对象。在将对象上传到 Amazon S3 时，请指定键名称：存储桶中对象的唯一且区分大小写的标识符。在不使用 `If-None-Match` 标头时，如果您在未受版本控制或已暂停版本控制的存储桶中上传具有相同键名称的对象，则该对象将被覆盖。在受版本控制的存储桶中，最近上传的对象成为对象的当前版本。具有 HTTP `If-None-Match` 标头的有条件写入将在 `WRITE` 操作期间检查对象是否存在。如果在存储桶中找到相同的键名称，则操作失败。有关使用键名称的更多信息，请参阅the section called “为对象命名”。

要执行具有 HTTP `If-None-Match` 标头的有条件写入，您必须拥有 `s3:PutObject` 权限。这使调用方能够检查存储桶中是否存在对象。`If-None-Match` 标头需要 `*`（星号）值。

您可以将 `If-None-Match` 标头与以下 API 结合使用：

- PutObject
- CompleteMultipartUpload

### 使用 Amazon CLI

以下 `put-object` 示例命令尝试对键名称为 `dir-1/my_images.tar.bz2` 的对象执行有条件写入。

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key dir-1/my_images.tar.bz2 --body
 my_images.tar.bz2 --if-none-match "*"
```

有关更多信息，请参阅 Amazon CLI 命令参考 中的 put-object。

有关 Amazon CLI 的更多信息，请参阅《Amazon Command Line Interface 用户指南》中的什么是 Amazon Command Line Interface？。

### 如果对象已更改，如何防止被覆盖

对象的 ETag 是该对象所特有的字符串，它反映了对象内容的变化。可以使用 `If-Match` 标头将 Amazon S3 存储桶中对象的 ETag 值与您在 `WRITE` 操作期间提供的值进行比较。如果 ETag 值不匹配，则操作会失败。有关 ETag 的更多信息，请参阅the section called “使用 Content-MD5 和 ETag 验证上传的对象”。

要执行具有 HTTP `If-Match` 标头的有条件写入，您必须拥有 `s3:PutObject` 和 `s3:GetObject` 权限。这使调用方能够检查 ETag 并验证存储桶中对象的状态。`If-Match` 标头要求将 ETag 值作为字符串。

您可以将 `If-Match` 标头与以下 API 结合使用：

- PutObject
- CompleteMultipartUpload

使用 Amazon CLI

以下 `put-object` 示例命令尝试使用提供的 ETag 值 `6805f2cfc46c0f04559748bb039d69ae` 执行有条件写入。

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key dir-1/my_images.tar.bz2 --body
 my_images.tar.bz2 --if-match "6805f2cfc46c0f04559748bb039d69ae"
```

有关更多信息，请参阅 Amazon CLI 命令参考 中的 put-object。

有关 Amazon CLI 的更多信息，请参阅《Amazon Command Line Interface 用户指南》中的什么是 Amazon Command Line Interface？。

## 有条件写入行为

### 具有 **If-None-Match** 标头的有条件写入

具有 If-None-Match 标头的有条件写入会针对存储桶中的现有对象进行评估。如果存储桶中不存在具有相同键名称的现有对象，则写入操作将成功并导致 200 OK 响应。如果存在现有对象，则写入操作将失败，并导致 412 Precondition Failed 响应。

对于启用了版本控制的存储桶，如果没有同名的当前对象版本，或者当前对象版本是删除标记，则写入操作将成功。否则，它会导致写入操作失败和 412 Precondition Failed 响应。

如果对同一个对象名称进行多个有条件写入，则第一个要完成的写入操作将成功。然后，Amazon S3 使后续写入失败并生成 412 Precondition Failed 响应。

如果在针对某个对象的有条件写入操作完成之前，对于该对象的删除请求获得成功，则在并发请求的情况下也可能收到 409 Conflict 响应。将有条件写入与 PutObject 结合使用时，可能会在收到 409 Conflict 错误后重试上传。使用 CompleteMultipartUpload 时，必须使用 CreateMultipartUpload 重新启动分段上传，以便在收到 409 Conflict 错误后再次上传对象。

### 具有 **If-Match** 标头的有条件写入

If-Match 标头会针对存储桶中的现有对象进行评估。如果存在具有相同键名称和匹配 ETag 的现有对象，则写入操作将成功并导致 200 OK 响应。如果 ETag 不匹配，则写入操作将失败并导致 412 Precondition Failed 响应。

如果是并发请求，您也可能收到 409 Conflict 响应。

如果在针对对象的有条件写入操作完成之前，对于对象的并发删除请求获得成功，您将收到 404 Not Found 响应，因为对象键不再存在。收到 404 Not Found 响应后，您应该重新上传对象。

如果没有同名的当前对象版本，或者当前对象版本是删除标记，则该操作失败并出现 404 Not Found 错误。

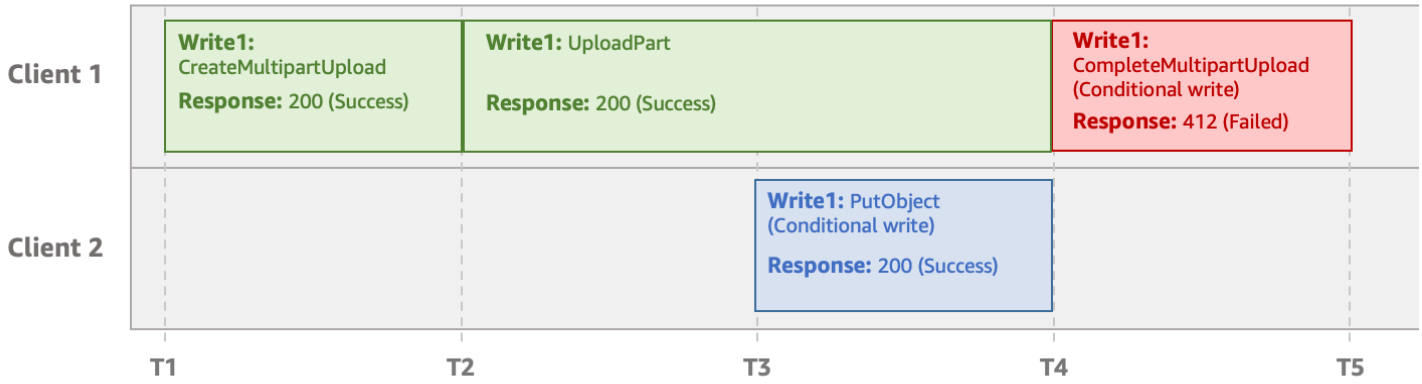
## 有条件写入场景

考虑以下场景，即两个客户端对同一个存储桶运行操作。

### 分段上传期间的有条件写入

有条件写入不考虑任何正在进行的分段上传请求，因为这些对象还不是完全写入的对象。请考虑以下示例，其中客户端 1 正在使用分段上传来上传对象。在分段上传期间，客户端 2 能够通过有条件写入操作成功写入相同的对象。随后，当客户端 1 尝试使用有条件写入完成分段上传时，上传将失败。

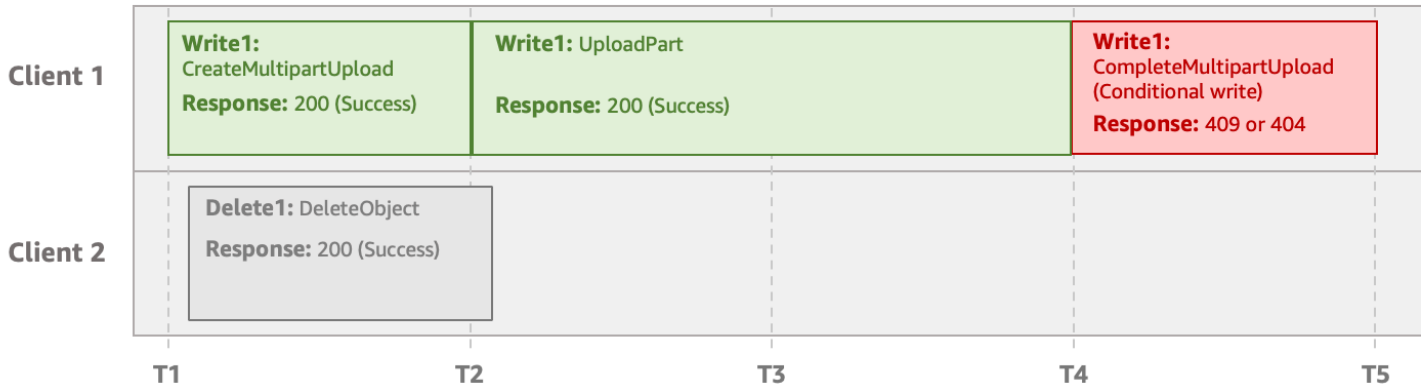
> **Note**
>
> 这种情况将导致 `If-None-Match` 和 `If-Match` 标头都得到 `412 Precondition Failed` 响应。




分段上传期间的并发删除

如果在有条件写入请求可以完成之前，删除请求获得成功，则 Amazon S3 为写入操作返回 `409 Conflict` 或 `404 Not Found` 响应。这是因为更早启动的删除请求优先于有条件写入操作。在这种情况下，您必须启动新的分段上传。

> **Note**
>
> 这种情况将对 `If-None-Match` 标头导致 `409 Conflict` 响应和对 `If-Match` 标头导致 `404 Not Found` 响应。




> **Note**
>
> 为了最大程度地降低存储成本，我们建议您配置生命周期规则，以便使用 `AbortIncompleteMultipartUpload` 操作在指定的天数后删除未完成的分段上传。有关创建生命周期规则以删除未完成的分段上传的更多信息，请参阅配置存储桶生命周期配置以删除未完成的分段上传。

## 强制对 Amazon S3 存储桶实施有条件写入

通过使用 Amazon S3 存储桶策略，可以对通用存储桶中的对象上传强制实施有条件写入。

存储桶策略是基于资源的策略，您可以使用该策略向 Amazon S3 存储桶及其中的对象授予访问权限。只有存储桶拥有者才能将策略与存储桶关联。有关存储桶策略的更多信息，请参阅 the section called “存储桶策略”。

您可以使用条件键 `s3:if-match` 或 `s3:if-none-match` 作为可选的 `Condition` 元素或 `Condition` 块来指定策略何时生效。对于分段上传，您必须指定 `s3:ObjectCreationOperation` 条件键以豁免 `CreateMultipartUpload`、`UploadPart` 和 `UploadPartCopy` 操作，因为这些 API 不接受有条件标头。有关在存储桶策略中使用条件的更多信息，请参阅the section called “条件键示例”。

> **Note**
>
> 如果您使用存储桶策略来强制实施有条件写入，则无法对在存储桶策略中指定的存储桶或前缀执行复制操作。不带 `If-None-Match` 或 `If-Match` HTTP 标头的 `CopyObject` 请求失败并

出现 403 Access Denied 错误。使用这些 HTTP 标头发出的 CopyObject 请求失败并导致 501 Not Implemented 响应。

以下示例说明如何使用存储桶策略中的条件来强制客户端使用 If-None-Match 或 If-Match HTTP 标头。

主题


- 示例 1：仅支持使用包含 if-none-match 标头的 PutObject 和 CompleteMultipartUpload 请求上传对象
- 示例 2：仅支持使用包含 if-match 标头的 PutObject 和 CompleteMultipartUpload 请求上传对象
- 示例 3：仅支持包含 if-none-match 或 if-match 标头的对象上传请求


### 示例 1：仅支持使用包含 **if-none-match** 标头的 **PutObject** 和 **CompleteMultipartUpload** 请求上传对象

如果请求包含 if-none-match 标头，则此策略支持账户 111122223333（用户 Alice）写入 *amzn-s3-demo-bucket1* 存储桶，从而确保存储桶中不存在对象键。针对指定存储桶的所有 PutObject 和 CompleteMultipartUpload 请求都必须包含 if-none-match 标头才能获得成功。使用此标头，仅当存储桶中不存在对象键时，客户才能写入该存储桶。

> **Note**
>
> 该策略还设置了 s3:ObjectCreationOperation 条件键，以支持使用 CreateMultipartUpload、UploadPart 和 UploadPartCopy API 进行分段上传。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowConditionalPut",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
```

```
            "Condition": {
                "Null": {
                    "s3:if-none-match": "false"
                }
            }
        },
        {
            "Sid": "AllowConditionalPutwithMPUs",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition": {
                "Bool": {
                    "s3:ObjectCreationOperation": "false"
                }
            }
        }
    ]
}
```

示例 2：仅支持使用包含 **if-match** 标头的 **PutObject** 和 **CompleteMultipartUpload** 请求上传对象

只有在请求包含 if-match 标头的情况下，此策略才支持账户 111122223333（用户 Alice）写入 *amzn-s3-demo-bucket1*。此标头将 S3 中对象的 ETag 值与您在 WRITE 操作期间提供的值进行比较。如果 ETag 值不匹配，则操作将失败。针对指定存储桶的所有 PutObject 和 CompleteMultipartUpload 请求都必须包含 if-match 标头才能获得成功。

> **Note**
>
> 该策略还设置了 s3:ObjectCreationOperation 条件键，以支持使用 CreateMultipartUpload、UploadPart 和 UploadPartCopy API 进行分段上传。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "AllowPutObject",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
        },
        {
            "Sid": "BlockNonConditionalObjectCreation",
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition": {
                "Null": {
                    "s3:if-match": "true"
                },
                "Bool": {
                    "s3:ObjectCreationOperation": "true"
                }
            }
        },
        {
            "Sid": "AllowGetObjectBecauseConditionalPutIfMatchETag",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*"
        }
    ]
}
```

示例 3：仅支持包含 **if-none-match** 或 **if-match** 标头的对象上传请求

如果请求包含 `if-none-match` 或 `if-match` 标头，则此策略支持账户 111122223333（用户 Alice）写入 *amzn-s3-demo-bucket1*。这可让 Alice 在存储桶中不存在键名称的情况下上传对象，或者，如果键名称确实存在，当对象 ETag 与 PUT 请求中提供的 ETag 匹配时，Alice 可以覆盖该对象。

> **Note**
>
> 该策略还设置了 s3:ObjectCreationOperation 条件键，以支持使用 CreateMultipartUpload、UploadPart 和 UploadPartCopy API 进行分段上传。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": " AllowConditionalPutifAbsent",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition": {
                "Null": {
                    "s3:if-none-match": "false"
                }
            }
        },
        {
            "Sid": "AllowConditionalPutIfMatchEtag",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition": {
                "Null": {
                    "s3:if-match": "false"
                }
            }
        },
        {
            "Sid": "AllowConditionalObjectCreation",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
```

```
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition": {
                "Bool": {
                    "s3:ObjectCreationOperation": "false"
                }
            }
        },
        {
            "Sid": " AllowGetObjectBecauseConditionalPutIfMatchETag",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*"
        }
    ]
}
```

# 复制、移动和重命名对象

`CopyObject` 操作将创建已存储在 Amazon S3 中的对象的副本。

在单个原子操作中，您可以创建最大 5GB 的对象副本。但是，要复制大于 5 GB 的对象，必须通过 Amazon CLI 或 Amazon SDK 使用分段上传。有关更多信息，请参阅 使用分段上传复制对象。

> **Note**
>
> 要保持使用分段上传所上传的对象的性能优势，必须使用 Amazon CLI 或 Amazon SDK 而不是 S3 控制台，通过分段上传来复制对象。有关更多信息，请参阅 使用分段上传复制对象。

通过使用 `CopyObject` 操作，您可以：

- 创建对象的其它副本。
- 通过复制对象并删除原始对象来重命名它们。

- 将对象从一个存储桶复制或移动到另一个存储桶，包括跨 Amazon Web Services 区域（例如，从 `us-west-1` 到 `eu-west-2`）。移动对象时，Amazon S3 将对象复制到指定目标，然后删除源对象。

  > **Note**
  >
  > 跨 Amazon Web Services 区域复制或移动对象会产生带宽费用。有关更多信息，请参阅 Amazon S3 定价。

- 更改对象元数据。每个 Amazon S3 对象都有元数据。此元数据是一组名称/值对。您可以在上传对象时设置对象元数据。上传对象后，您将无法修改对象元数据。修改对象元数据的唯一方式是创建对象的副本并设置元数据。为此，在复制操作中，将相同的对象设置为源和目标。

  有些对象元数据是系统元数据，而另外一些则是用户定义的元数据。您可以控制某些系统元数据。例如，您可以控制要用于对象的存储类和服务器端加密的类型。复制对象时，还会复制用户控制的系统元数据和用户定义的元数据。Amazon S3 将重置系统控制的元数据。例如，在复制对象时，Amazon S3 将重置已复制对象的创建日期。您不需要在复制请求中设置任何这些系统控制的元数据值。

  复制对象时，您可能会决定更新某些元数据值。例如，如果您的源对象被配置为使用 S3 Standard 存储，您可以选择对对象复制使用 S3 Intelligent-Tiering。您可能还会决定更改源对象上某些用户定义的元数据值。请注意，如果您选择在复制期间更新任意对象的用户可配置元数据（系统或用户定义的元数据），则必须显式指定请求中源对象上存在的所有用户可配置的元数据，即使您只更改其中一个元数据值也是如此。

  > **Note**
  >
  > 使用 Amazon S3 控制台复制对象时，您可能会收到错误消息 "Copied metadata can't be verified." 控制台使用标头来检索和设置对象的元数据。如果您的网络或浏览器配置修改了网络请求，则此行为可能会导致将意外的元数据（例如修改后的 `Cache-Control` 标头）写入复制的对象。Amazon S3 无法验证这种意外的元数据。
  > 要解决此问题，请检查您的网络和浏览器配置，以确保它不会修改标头，例如 `Cache-Control`。有关更多信息，请参阅 The Shared Responsibility Model。

  有关对象元数据的更多信息，请参阅 使用对象元数据。

复制已存档和已还原的对象

如果源对象归档在 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 中，您必须先还原临时副本，然后才能将对象复制到另一个存储桶中。有关对象归档的更多信息，请参阅 使用归档的对象。

在 Amazon S3 控制台中，不支持对 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储类中的已还原对象执行复制操作。要复制这些已还原对象，请使用 Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 Amazon S3 REST API。

复制加密对象

Amazon S3 会自动加密所有复制到 S3 存储桶的新对象。如果您未在复制请求中指定加密信息，则目标对象的加密设置将设为目标存储桶的默认加密配置。默认情况下，所有存储桶都有基本级别的加密配置，该配置使用具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）。如果目标存储桶的默认加密配置使用具有 Amazon Key Management Service（Amazon KMS）密钥（SSE-KMS）或客户提供加密密钥（SSE-C）的服务器端加密，则 Amazon S3 使用相应的 KMS 密钥或客户提供的密钥来加密目标对象副本。

在复制对象时，如果您希望对目标对象使用其他类型的加密设置，您可以请求 Amazon S3 使用 KMS 密钥、Amazon S3 托管式密钥或客户提供的密钥对目标对象加密。如果您的请求中的加密设置与目标存储桶的默认加密配置不同，则您的请求中的加密设置优先。如果副本的源对象是用 SSE-C 加密的，您必须在请求中提供必需的加密信息，以便 Amazon S3 可以解密对象以进行复制。有关更多信息，请参阅 利用加密来保护数据。

复制对象时使用校验和

复制对象时，可以选择对对象使用不同的校验和算法。无论您选择使用相同的算法还是新算法，Amazon S3 都会在复制对象后计算一个新的校验和值。Amazon S3 不直接复制校验和的值。所有不带校验和及指定的目标校验和算法的复制对象都会自动获得 CRC-64NVME 校验和算法。有关如何计算此校验和的更多信息，请参阅在 Amazon S3 中使用分段上传来上传和复制对象。

在单个请求中复制多个对象

要使用单个请求复制多个 Amazon S3 对象，您还可以使用 S3 批量操作。您为 S3 批量操作提供要操作的对象列表。S3 批量操作调用相应的 API 操作来执行指定的操作。单个批量操作任务可对包含 EB 级数据的数十亿个对象执行指定操作。

S3 批量操作特征包括跟踪进度、发送通知并存储所有操作的详细完成报告，从而提供完全托管、可审核的无服务器体验。您可以通过 Amazon S3 控制台、Amazon CLI、Amazon SDK 或 REST API 使用 S3 批量操作。有关更多信息，请参阅 the section called “批量操作基础知识”。

将对象复制到目录存储桶

有关将对象复制到目录存储桶的信息，请参阅从目录存储桶复制对象或向目录存储桶复制对象。有关将 Amazon S3 Express One Zone 存储类与目录存储桶结合使用的信息，请参阅S3 Express One Zone和使用目录存储桶。

## 复制对象

要复制对象，请使用以下方法。

使用 S3 控制台

> **Note**
>
> 使用控制台复制对象时的限制和局限性如下所示：
>
> - 如果对象小于 5 GB，则可以复制对象。如果对象大于 5GB，则必须使用 Amazon CLI 或 Amazon SDK 来复制对象。
> - 有关复制对象所需的其它权限的列表，请参阅 the section called “S3 API 操作所需的权限”。有关授予此权限的示例策略，请参阅the section called “基于身份的策略示例”。
> - Copy 操作适用于指定文件夹（前缀）中的所有对象。当正在执行操作时添加到这些文件夹的对象可能受到影响。
> - Amazon S3 控制台不支持跨区域复制使用 SSE-KMS 加密的对象。要跨区域复制使用 SSE-KMS 加密的对象，请使用 Amazon CLI、Amazon SDK 或 Amazon S3 REST API。
> - 无法使用 S3 控制台复制使用客户提供的加密密钥（SSE-C）加密的对象。要复制使用 SSE-C 加密的对象，请使用 Amazon CLI、Amazon SDK 或 Amazon S3 REST API。
> - 复制的对象将不会保留原始对象的对象锁定设置。
> - 如果要从中复制对象的存储桶对于 S3 对象所有权使用“强制存储桶拥有者”设置，则对象 ACL 将不会复制到指定的目标。
> - 如果要将对象复制到对于 S3 对象所有权使用“强制存储桶拥有者”设置的存储桶，请确保源存储桶也使用“强制存储桶拥有者”设置，或移除对其它 Amazon 账户和组的任何对象 ACL 授权。

复制对象

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶或目录存储桶。

3. 在存储桶列表中，选择包含您想要复制的对象的存储桶的名称。
4. 选中要复制的对象名称左侧的复选框。
5. 在操作菜单上，从显示的选项列表中选择复制。
6. 选择目标类型和目标账户。要指定目标路径，请选择 Browse S3（浏览 S3），导航到目标，然后选中目标左侧的复选框。选择右下角的选择目标。

   或者，输入目标路径。
7. 如果您未 启用存储桶版本控制，则会看到一则警告，建议您启用存储桶版本控制，以防意外覆盖或删除对象。如果要在此存储桶中保留对象的所有版本，请选择 Enable Bucket Versioning（启用存储桶版本控制）。还可以在目标详细信息中查看默认加密和 S3 对象锁定属性。
8. 在其它复制设置下，选择是要复制源设置、请勿指定设置还是指定设置。复制源设置是默认选项。如果您只想复制不带源设置属性的对象，请选择请勿指定设置。选择指定设置，来指定存储类、ACL、对象标签、元数据、服务器端加密和其它校验和的设置。
9. 选择右下角的复制。Amazon S3 会将对象复制到目标。

### 使用 Amazon SDK

本节中的示例向您展示了如何复制单个操作中大于 5 GB 的对象。要复制大于 5GB 的对象，您必须使用分段上传。有关更多信息，请参阅 使用分段上传复制对象。

#### Java

##### Example

以下示例使用 适用于 Java 的 Amazon SDK 复制 Amazon S3 中的对象。有关创建和测试有效示例的说明，请参阅《适用于 Java 的 Amazon SDK 开发人员指南》中的入门。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.CopyObjectRequest;

import java.io.IOException;

public class CopyObjectSingleOperation {
```

```
    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String sourceKey = "*** Source object key *** ";
        String destinationKey = "*** Destination object key ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Copy the object into a new object in the same bucket.
            CopyObjectRequest copyObjRequest = new CopyObjectRequest(bucketName,
 sourceKey, bucketName, destinationKey);
            s3Client.copyObject(copyObjRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

以下 C# 示例使用高级别 适用于 .NET 的 Amazon SDK 在单次操作中复制最大为 5 GB 的对象。对于大于 5 GB 的对象，请使用 使用分段上传复制对象 中所述的分段上传复制示例。

此示例将创建最大为 5 GB 的对象的副本。有关设置和运行代码示例的信息，请参阅《适用于 .NET 的 Amazon SDK 开发人员指南》中的适用于 .NET 的 Amazon SDK 入门。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;
```

```
namespace Amazon.DocSamples.S3
{
    class CopyObjectTest
    {
        private const string sourceBucket = "*** provide the name of the bucket with
 source object ***";
        private const string destinationBucket = "*** provide the name of the bucket
 to copy the object to ***";
        private const string objectKey = "*** provide the name of object to copy
 ***";
        private const string destObjectKey = "*** provide the destination object key
 name ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            Console.WriteLine("Copying an object");
            CopyingObjectAsync().Wait();
        }

        private static async Task CopyingObjectAsync()
        {
            try
            {
                CopyObjectRequest request = new CopyObjectRequest
                {
                    SourceBucket = sourceBucket,
                    SourceKey = objectKey,
                    DestinationBucket = destinationBucket,
                    DestinationKey = destObjectKey
                };
                CopyObjectResponse response = await
 s3Client.CopyObjectAsync(request);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
            catch (Exception e)
```

```
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
        }
    }
}
```

PHP

此主题将指导您使用第 3 版 适用于 PHP 的 Amazon SDK，将 Amazon S3 中的单个对象和多个对象从一个存储桶复制到另一个存储桶或者在同一存储桶中进行复制。

有关适用于 Ruby 的 Amazon 开发工具包 API 的更多信息，请转到适用于 Ruby 的 Amazon 开发工具包 – 版本 2。

以下 PHP 示例演示使用 `copyObject()` 方法复制 Amazon S3 中的单个对象。它还演示如何通过使用 `getcommand()` 方法对 `CopyObject` 进行批量调用来制作对象的多个副本。

复制对象

| | |
|---|---|
| 1 | 使用 `Aws\S3\S3Client` 类构造函数创建 Amazon S3 客户端的实例。 |
| 2 | 要制作对象的多个副本，请运行对 Amazon S3 客户端 getCommand() 方法的批量调用，该方法是从 Aws\CommandInterface 类继承的。您提供 `CopyObject` 命令作为第一个参数，提供包含源存储桶、源键名、目标存储桶和目标键名的数组作为第二个参数。 |

```
 require 'vendor/autoload.php';

use Aws\CommandPool;
use Aws\Exception\AwsException;
use Aws\ResultInterface;
use Aws\S3\S3Client;

$sourceBucket = '*** Your Source Bucket Name ***';
$sourceKeyname = '*** Your Source Object Key ***';
$targetBucket = '*** Your Target Bucket Name ***';

$s3 = new S3Client([
    'version' => 'latest',
```

```
    'region' => 'us-east-1'
]);

// Copy an object.
$s3->copyObject([
    'Bucket' => $targetBucket,
    'Key' => "$sourceKeyname-copy",
    'CopySource' => "$sourceBucket/$sourceKeyname",
]);

// Perform a batch of CopyObject operations.
$batch = array();
for ($i = 1; $i <= 3; $i++) {
    $batch[] = $s3->getCommand('CopyObject', [
        'Bucket' => $targetBucket,
        'Key' => "{targetKeyname}-$i",
        'CopySource' => "$sourceBucket/$sourceKeyname",
    ]);
}
try {
    $results = CommandPool::batch($s3, $batch);
    foreach ($results as $result) {
        if ($result instanceof ResultInterface) {
            // Result handling here
        }
        if ($result instanceof AwsException) {
            // AwsException handling here
        }
    }
} catch (Exception $e) {
    // General error handling here
}
```

Python

```
class ObjectWrapper:
    """Encapsulates S3 object actions."""

    def __init__(self, s3_object):
        """
        :param s3_object: A Boto3 Object resource. This is a high-level resource in
 Boto3
```

```
                        that wraps object actions in a class-like structure.
        """
        self.object = s3_object
        self.key = self.object.key
```

```
    def copy(self, dest_object):
        """
        Copies the object to another bucket.

        :param dest_object: The destination object initialized with a bucket and
key.
                            This is a Boto3 Object resource.
        """
        try:
            dest_object.copy_from(
                CopySource={"Bucket": self.object.bucket_name, "Key":
self.object.key}
            )
            dest_object.wait_until_exists()
            logger.info(
                "Copied object from %s:%s to %s:%s.",
                self.object.bucket_name,
                self.object.key,
                dest_object.bucket_name,
                dest_object.key,
            )
        except ClientError:
            logger.exception(
                "Couldn't copy object from %s/%s to %s/%s.",
                self.object.bucket_name,
                self.object.key,
                dest_object.bucket_name,
                dest_object.key,
            )
            raise
```

### Ruby

以下任务将引导您使用 Ruby 类将 Amazon S3 中的对象从一个存储桶复制到另一个存储桶，或者在同一个存储桶内复制。

复制对象

| | |
|---|---|
| 1 | 对 适用于 Ruby 的 Amazon SDK 的版本 3 使用 Amazon S3 模块化 Gem 时，需要 `aws-sdk-s3` 并提供您的 Amazon 凭证。有关如何提供凭证的更多信息，请参阅《Amazon S3 API 参考》中的 Making requests using Amazon account or IAM user credentials。 |
| 2 | 提供源存储桶名称、源键名、目标存储桶名称和目标键等请求信息。 |

下面的 Ruby 代码示例通过使用 `#copy_object` 方法将对象从一个存储桶复制到另一个存储桶，演示了上述任务。

```
require 'aws-sdk-s3'

# Wraps Amazon S3 object actions.
class ObjectCopyWrapper
  attr_reader :source_object

  # @param source_object [Aws::S3::Object] An existing Amazon S3 object. This is
 used as the source object for
  #                                        copy actions.
  def initialize(source_object)
    @source_object = source_object
  end

  # Copy the source object to the specified target bucket and rename it with the
 target key.
  #
  # @param target_bucket [Aws::S3::Bucket] An existing Amazon S3 bucket where the
 object is copied.
  # @param target_object_key [String] The key to give the copy of the object.
  # @return [Aws::S3::Object, nil] The copied object when successful; otherwise,
 nil.
  def copy_object(target_bucket, target_object_key)
    @source_object.copy_to(bucket: target_bucket.name, key: target_object_key)
    target_bucket.object(target_object_key)
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't copy #{@source_object.key} to #{target_object_key}. Here's why:
 #{e.message}"
  end
end
```

```
# Example usage:
def run_demo
  source_bucket_name = "amzn-s3-demo-bucket1"
  source_key = "my-source-file.txt"
  target_bucket_name = "amzn-s3-demo-bucket2"
  target_key = "my-target-file.txt"

  source_bucket = Aws::S3::Bucket.new(source_bucket_name)
  wrapper = ObjectCopyWrapper.new(source_bucket.object(source_key))
  target_bucket = Aws::S3::Bucket.new(target_bucket_name)
  target_object = wrapper.copy_object(target_bucket, target_key)
  return unless target_object

  puts "Copied #{source_key} from #{source_bucket_name} to
 #{target_object.bucket_name}:#{target_object.key}."
end

run_demo if $PROGRAM_NAME == __FILE__
```

使用 REST API

本示例描述了如何使用 Amazon S3 REST API 复制对象。有关 REST API 的更多信息，请参阅CopyObject。

本示例将 flotsam 存储桶中的 *amzn-s3-demo-bucket1* 对象复制到 jetsam 存储桶的 *amzn-s3-demo-bucket2* 对象，同时保留其元数据。

```
PUT /jetsam HTTP/1.1
Host: amzn-s3-demo-bucket2.s3.amazonaws.com
x-amz-copy-source: /amzn-s3-demo-bucket1/flotsam
Authorization: AWS AKIAIOSFODNN7EXAMPLE:ENoSbxYByFA0UGLZUqJN5EUnLDg=
Date: Wed, 20 Feb 2008 22:12:21 +0000
```

将从以下信息生成签名。

```
PUT\r\n
\r\n
\r\n
Wed, 20 Feb 2008 22:12:21 +0000\r\n

x-amz-copy-source:/amzn-s3-demo-bucket1/flotsam\r\n
```

```
/amzn-s3-demo-bucket2/jetsam
```

Amazon S3 将返回以下响应来指定对象的 ETag 及其上次修改的时间。

```
HTTP/1.1 200 OK
x-amz-id-2: Vyaxt7qEbzv34BnSu5hctyyNSlHTYZFMWK4FtzO+iX8JQNyaLdTshL0KxatbaOZt
x-amz-request-id: 6B13C3C5B34AF333
Date: Wed, 20 Feb 2008 22:13:01 +0000

Content-Type: application/xml
Transfer-Encoding: chunked
Connection: close
Server: AmazonS3
<?xml version="1.0" encoding="UTF-8"?>

<CopyObjectResult>
   <LastModified>2008-02-20T22:13:01</LastModified>
   <ETag>"7e9c608af58950deeb370c98608ed097"</ETag>
</CopyObjectResult>
```

使用 Amazon CLI

也可以使用 Amazon Command Line Interface（Amazon CLI）复制 S3 对象。有关更多信息，请参阅 Amazon CLI 命令参考 中的 copy-object。

有关 Amazon CLI 的更多信息，请参阅《Amazon Command Line Interface 用户指南》中的什么是 Amazon Command Line Interface？。

## 移动对象

要移动对象，请使用以下方法。

使用 S3 控制台

> **Note**
>
> - 如果对象小于 5 GB，则可以移动对象。如果对象大于 5GB，必须使用 Amazon CLI 或 Amazon SDK 来移动对象。
> - 有关移动对象所需的其它权限的列表，请参阅 the section called “S3 API 操作所需的权限”。有关授予此权限的示例策略，请参阅the section called “基于身份的策略示例”。

- 无法使用 Amazon S3 控制台移动使用客户提供的加密密钥（SSE-C）加密的对象。要移动使用 SSE-C 加密的对象，请使用 Amazon CLI、Amazon SDK 或 Amazon S3 REST API。
- 移动文件夹时，请等待移动操作完成，然后再对文件夹进行其它更改。
- 您不能使用 S3 接入点别名作为 Amazon S3 控制台中移动操作的源或目标。

移动对象

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。导航到包含待移动对象的 Amazon S3 存储桶或文件夹。
3. 选中要移动的对象所对应的复选框。
4. 在操作菜单上，选择移动。
5. 要指定目标路径，请选择浏览 S3，导航到目标，然后选中目标复选框。选择选择目标。

   或者，输入目标路径。
6. 如果您未 启用存储桶版本控制，则会看到一则警告，建议您启用存储桶版本控制，以防意外覆盖或删除对象。如果要在此存储桶中保留对象的所有版本，请选择 Enable Bucket Versioning（启用存储桶版本控制）。还可以在目标详细信息中查看默认加密和对象锁定属性。
7. 在其它复制设置下，选择是要复制源设置、请勿指定设置还是指定设置。复制源设置是默认选项。如果您只想复制不带源设置属性的对象，请选择请勿指定设置。选择指定设置，来指定存储类、ACL、对象标签、元数据、服务器端加密和其它校验和的设置。
8. 选择右下角的移动。Amazon S3 将您的对象移动到目标位置。

使用 Amazon CLI

您也可以使用 Amazon Command Line Interface（Amazon CLI）移动 S3 对象。有关更多信息，请参阅 Amazon CLI 命令参考 中的 mv。

有关 Amazon CLI 的更多信息，请参阅《Amazon Command Line Interface 用户指南》中的什么是 Amazon Command Line Interface？。

## 重命名对象

要重命名对象，请使用以下过程。

Note

- 如果对象小于 5 GB，则可以重命名对象。要重命名大于 5 GB 的对象，必须使用 Amazon CLI 或 Amazon SDK 来复制具有新名称的对象，然后删除原始对象。
- 有关复制对象所需的其它权限的列表，请参阅 the section called “S3 API 操作所需的权限”。有关授予此权限的示例策略，请参阅the section called “基于身份的策略示例”。
- 重命名对象将创建具有新的上次修改日期的对象副本，然后在原始对象上添加删除标记。
- 默认加密的存储桶设置会自动应用于任何未加密的指定对象。
- 您无法使用 Amazon S3 控制台来重命名采用客户提供的加密密钥（SSE-C）的对象。要重命名使用 SSE-C 加密的对象，请使用 Amazon CLI、Amazon SDK 或 Amazon S3 REST API 以新名称复制这些对象。
- 如果此存储桶的 S3 对象所有权使用强制存储桶拥有者设置，则不会复制对象访问控制列表（ACL）。

重命名对象

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在导航窗格中，选择存储桶，然后选择通用存储桶选项卡。导航到包含待重命名的对象的 Amazon S3 存储桶或文件夹。
3. 选择要重命名的对象所对应的复选框。
4. 在操作菜单中，选择重命名对象。
5. 在新对象名称框中，输入对象的新名称。
6. 在其它复制设置下，选择是要复制源设置、请勿指定设置还是指定设置。复制源设置是默认选项。如果您只想复制不带源设置属性的对象，请选择请勿指定设置。选择指定设置，来指定存储类、ACL、对象标签、元数据、服务器端加密和其它校验和的设置。
7. 选择保存更改。Amazon S3 随即重命名您的对象。

# 下载对象

本部分介绍如何从 Amazon S3 存储桶下载对象。使用 Amazon S3，您将这些对象存储在一个或多个存储桶中，每个对象的大小最多为 5 TB。任何未归档的 Amazon S3 对象都可以实时访问。但对于

已归档的对象，必须先进行还原，然后才能下载。有关下载归档对象的更多信息，请参阅the section called “下载归档对象”。

您可以使用 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 Amazon S3 REST API 下载单个对象。要从 S3 下载对象而无需编写任何代码或运行任何命令，请使用 S3 控制台。有关更多信息，请参阅 the section called “下载对象”。

要下载多个对象，请使用 Amazon CloudShell、Amazon CLI 或 Amazon SDK。有关更多信息，请参阅 the section called “下载多个对象”。

如果您需要下载对象的一部分，则需要将 Amazon CLI 与额外的参数结合使用，或者使用 REST API 来仅指定要下载的字节。有关更多信息，请参阅 the section called “下载对象的一部分”。

如果您需要下载不属于您的对象，请让对象所有者生成一个允许您下载该对象的预签名 URL。有关更多信息，请参阅 the section called “从另一个 Amazon Web Services 账户下载对象”。

当您在 Amazon 网络之外下载对象时，将收取数据传输费用。在同一个 Amazon Web Services 区域中，Amazon 网络内部的数据传输免费，但任何 GET 请求都将收取费用。有关数据传输成本和数据检索费用的更多信息，请参阅 Amazon S3 定价。

主题


- 下载对象
- 下载多个对象
- 下载对象的一部分
- 从另一个 Amazon Web Services 账户下载对象
- 下载归档对象
- 根据元数据下载对象
- 下载对象故障排查


## 下载对象

您可以使用 Amazon S3 控制台、Amazon CLI、Amazon SDK 或 REST API 下载单个对象。

使用 S3 控制台

本部分介绍如何使用 Amazon S3 控制台从 S3 存储桶下载对象。

> **Note**
>
> - 一次只能下载一个对象。
> - 如果您使用 Amazon S3 控制台下载对象的键名以句点 (.) 结尾，则该句点将从下载对象的键名中删除。要保留所下载对象名称末尾的句点，您必须使用 Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 Amazon S3 REST API。

从 S3 存储桶下载对象

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶或目录存储桶。
3. 在存储桶列表中，选择要从中下载对象的存储桶的名称。
4. 您可以使用以下任一方式从 S3 存储桶下载对象：
   - 选中对象旁边的复选框，然后选择下载。如果您要将对象下载到特定文件夹，请在操作菜单中，选择下载为。
   - 如果要下载对象的特定版本，请打开显示版本（位于搜索框旁边）。选中所需对象版本旁边的复选框，然后选择下载。如果您要将对象下载到特定文件夹，请在操作菜单中，选择下载为。

使用 Amazon CLI

以下 `get-object` 示例将向您展示如何使用 Amazon CLI 从 Amazon S3 下载对象。此命令从存储桶 *amzn-s3-demo-bucket1* 获取对象 *folder/my_image*。您必须包含 `outfile`，这是已下载对象的文件名，例如 *my_downloaded_image.jpg*。

```
aws s3api get-object --bucket amzn-s3-demo-bucket1 --key folder/
my_image my_downloaded_image.jpg
```

有关更多信息和示例，请参阅 Amazon CLI 命令参考中的 get-object。

使用 Amazon SDK

有关如何使用 Amazon SDK 下载对象的示例，请参阅《Amazon S3 API 参考》中的 Code examples。

有关使用不同 Amazon SDK 的一般信息，请参阅《Amazon S3 API 参考》中的 Developing with Amazon S3 using the Amazon SDKs。

使用 REST API

您可以使用 REST API 从 Amazon S3 中检索对象。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 GetObject。

## 下载多个对象

您可以使用 Amazon CloudShell、Amazon CLI 或 Amazon SDK 下载多个对象。

在 Amazon Web Services Management Console中使用Amazon CloudShell

Amazon CloudShell 是一个已经事先完成身份验证的浏览器式 Shell，您可以直接从 Amazon Web Services Management Console启动它。

有关 Amazon CloudShell 的更多信息，请参阅《Amazon CloudShell User Guide》中的What is CloudShell?。

> **Important**
>
> 使用 Amazon CloudShell，您的主目录的存储空间最高为每个 Amazon Web Services 区域 1 GB。因此，您无法将存储桶与总大小超过此数量的对象同步。有关更多限制，请参阅《Amazon CloudShell User Guide》中的 eService quotas and restrictions。

使用 Amazon CloudShell 下载对象

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 CloudShell 控制台：https://console.aws.amazon.com/cloudshell/.
2. 运行以下命令，将存储桶中的对象同步到 CloudShell。以下命令同步名为 *amzn-s3-demo-bucket1* 的存储桶中的对象，并在 CloudShell 中创建一个名为 *temp* 的文件夹。CloudShell 会将您的对象同步到这个文件夹。要使用此命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3 sync s3://amzn-s3-demo-bucket1 ./temp
```

> **Note**
>
> sync 命令与目录存储桶不兼容。
> 要执行模式匹配以排除或包含特定对象，您可以在 sync 命令中使用 --exclude "*value*" 和 --include "*value*" 参数。

3. 运行以下命令，将名为 *temp* 的文件夹中的对象压缩到名为 *temp.zip* 的文件中。

```
zip temp.zip -r temp/
```

4. 选择操作，然后选择下载文件。
5. 输入文件名 **temp.zip**，然后选择下载。
6. （可选）删除同步到 CloudShell 中 *temp* 文件夹的 *temp.zip* 文件和对象。使用 Amazon CloudShell，您可在每个 Amazon Web Services 区域中拥有最高 1 GB 的持久性存储。

   您可以使用此示例命令来删除您的 .zip 文件和文件夹。要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
rm temp.zip && rm -rf temp/
```

使用 Amazon CLI

此示例说明如何使用 Amazon CLI 下载指定目录或前缀下的所有文件或对象。此命令将存储桶 *amzn-s3-demo-bucket1* 中的所有对象复制到您的当前目录。要使用此示例命令，请使用您的存储桶名称代替 *amzn-s3-demo-bucket1*。

```
aws s3 cp s3://amzn-s3-demo-bucket1 . --recursive
```

以下命令将存储桶 *amzn-s3-demo-bucket1* 中前缀 *logs* 下的所有对象下载到您的当前目录。它还使用 --exclude 和 --include 参数仅复制带有后缀 *.log* 的对象。要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3 cp s3://amzn-s3-demo-bucket1/logs/ . --recursive --exclude "*" --include "*.log"
```

有关更多信息和示例，请参阅 Amazon CLI 命令参考中的 cp。

使用 Amazon SDK

有关如何使用 Amazon SDK 下载 Amazon S3 存储桶中所有对象的示例，请参阅《Amazon S3 API 参考》中的 Code examples。

有关使用不同 Amazon SDK 的一般信息，请参阅《Amazon S3 API 参考》中的 Developing with Amazon S3 using the Amazon SDKs。

## 下载对象的一部分

您可以使用 Amazon CLI 或 REST API 下载对象的一部分。为此，您需要使用额外的参数来指定要下载对象的哪一部分。

使用 Amazon CLI

以下示例命令在名为 *amzn-s3-demo-bucket1* 的存储桶中，对名为 *folder/my_data* 的对象中的字节范围执行 GET 请求。在请求中，字节范围必须以 bytes= 为前缀。部分对象将下载到名为 *my_data_range* 的输出文件中。要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3api get-object --bucket amzn-s3-demo-bucket1 --key folder/my_data --range
 bytes=0-500 my_data_range
```

有关更多信息和示例，请参阅 Amazon CLI 命令参考中的 get-object。

有关 HTTP Range 标头的更多信息，请参阅 RFC 编辑器网站上的 RFC 9110。

> **Note**
>
> Amazon S3 不支持在单个 GET 请求中检索多个数据范围。

使用 REST API

您可以在 REST API 中使用 partNumber 和 Range 参数，从 Amazon S3 检索对象部分。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 GetObject。

## 从另一个 Amazon Web Services 账户下载对象

您可以使用预签名 URL 授予对对象的限时访问权限，而不更新存储桶策略。

预签名 URL 可以在浏览器中输入，或者由程序用来下载对象。URL 使用的凭证是生成该 URL 的 Amazon 用户的凭证。创建 URL 后，在该 URL 过期之前，任何拥有预签名 URL 的人都可以下载相应的对象。

在 S3 控制台中使用预签名 URL

您可以使用 Amazon S3 控制台，按照以下步骤生成预签名 URL 来共享通用存储桶中的对象。使用控制台时，预签名 URL 的最长过期时间为自创建时起 12 小时。

使用 Amazon S3 控制台生成预签名 URL

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在存储桶列表中，选择包含要为其生成预签名 URL 的对象的存储桶的名称。
4. 在 Objects（对象）列表中，选择要为其生成预签名 URL 的对象。
5. 在对象操作菜单上，请选择使用预签名 URL 共享。
6. 指定您希望的预签名 URL 有效时间长度。
7. 请选择 Create presigned URL（创建预签名 URL）。
8. 出现确认消息时，URL 将自动复制到剪贴板。如果您需要再次复制预签名 URL，您将看到一个按钮，用于复制该 URL。
9. 要下载对象，请将 URL 粘贴到任何浏览器中，此时机会尝试下载该对象。

有关预签名 URL 和其他创建预签名 URL 方法的更多信息，请参阅使用预签名 URL 下载和上传对象。

## 下载归档对象

要降低不经常访问的对象的存储成本，您可以对此类对象进行归档。当您归档对象时，它会被移动到低成本存储中，这意味着您无法实时访问它。要下载归档对象，您必须先还原该对象。

根据存储类的不同，您可以在几分钟或几小时内还原归档对象。您可以使用 Amazon S3 控制台、S3 批量操作、Amazon S3 REST API、Amazon SDK 和 Amazon Command Line Interface（Amazon CLI）还原归档的对象。

有关说明，请参阅恢复已归档的对象。您可在还原归档对象后下载它。

## 根据元数据下载对象

可以使用有条件读取请求添加前提条件，来根据对象的元数据下载该对象。可以根据对象的实体标签（ETag）或上次修改日期返回该对象。这可以将 S3 操作限制为自指定日期以来更新的对象，或者仅返回特定的对象版本。

可以将有条件写入用于 GetObject 或 HeadObject 请求。

有关有条件请求的更多信息，请参阅使用有条件请求向 S3 操作添加前提条件。

## 下载对象故障排查

当您尝试从 Amazon S3 下载对象时，权限不足、错误的存储桶或错误的 Amazon Identity and Access Management（IAM）用户策略会导致出错。这些问题通常会导致访问被拒绝（403 禁止）错误，此时 Amazon S3 会禁止访问资源。

有关拒绝访问（403 禁止）错误的常见原因，请参阅排查 Amazon S3 中的拒绝访问（403 Forbidden）错误。

# 在 Amazon S3 中检查对象完整性

Amazon S3 使用校验和值来验证您上传或下载的数据的完整性。此外，您可以请求为存储在 Amazon S3 中的任何对象计算另一个校验和值。您可以选择在上传、复制或批量复制数据时要使用的校验和算法。

当您上传数据时，Amazon S3 使用您选择的算法在服务器端计算校验和，并使用提供的值对其进行验证，然后再存储对象并将校验和作为对象元数据的一部分存储。对于单分段上传和多分段上传，这种验证在加密模式、对象大小和存储类方面是一致的。但是，当您复制或批量复制数据时，Amazon S3 会计算源对象的校验和并将其移动到目标对象。

> **Note**
>
> 当您执行单分段上传或多分段上传时，您可以选择将预先计算的校验和作为请求的一部分包含在内，并使用完整对象校验和类型。要将预先计算的值用于多个对象，请使用 Amazon CLI 或 Amazon SDK。

# 使用支持的校验和算法

使用 Amazon S3，您可以选择要在上传期间验证数据的校验和算法。然后，指定的校验和算法将与对象一起存储，并可用于在下载期间验证数据完整性。您可以选择以下安全哈希算法（SHA）或循环冗余校验（CRC）校验和算法之一来计算校验和值：

- CRC-64/NVME (CRC64NVME)
- CRC-32 (CRC32)
- CRC-32C (CRC32C)
- SHA-1 (SHA1)
- SHA-256 (SHA256)

此外，您可以使用 Content-MD5 标头为每个请求提供校验和。

在上传对象时，请指定要使用的算法：

- 使用 Amazon Web Services Management Console时，请选择要使用的校验和算法。您可以选择指定对象的校验和值。当 Amazon S3 收到对象时，它使用您指定的算法计算校验和。如果这两个校验和值不匹配，Amazon S3 会生成错误。
- 使用 SDK 时，请注意以下事项：
  - 将 ChecksumAlgorithm 参数设置为您希望 Amazon S3 使用的算法。如果您已经有了预先计算的校验和，则可以将校验和值传递给 Amazon SDK，然后此 SDK 会在请求中包含该值。如果您未传递校验和值或未指定校验和算法，SDK 会自动为您计算校验和值，并将其包含在请求中以提供完整性保护。如果单个校验和值与校验和算法的设置值不匹配，Amazon S3 会使请求失败并出现 BadDigest 错误。
  - 如果您使用的是升级的 Amazon SDK，此 SDK 会为您选择校验和算法。但是，您可以覆盖此校验和算法。
  - 如果您未指定校验和算法，且 SDK 也没有为您计算校验和，则 S3 会自动选择 CRC-64/NVME (CRC64NVME) 校验和算法。
- 使用 REST API 时，不使用 x-amz-sdk-checksum-algorithm 参数。而是使用特定于算法的标头之一（例如 x-amz-checksum-crc32）。

要将这些校验和值中的任何一个应用于已上传到 Amazon S3 的对象，您可以复制该对象，并指定是要使用现有的校验和算法，还是使用新的算法。如果您未指定算法，S3 将使用现有算法。如果源对象没

有指定的校验和算法或校验和值，Amazon S3 会使用 CRC-64/NVME 算法来计算目标对象的校验和值。还可以在使用 S3 批量操作复制对象时指定校验和算法。

> **Important**
>
> 如果您将分段上传与校验和结合使用来获得复合（或分段级）校验和，则分段上传的分段编号必须是连续的并从 1 开始。如果您尝试使用非连续分段编号来完成分段上传请求，Amazon S3 会生成 `HTTP 500 Internal Server` 错误。

## 完整对象和复合校验和类型

在 Amazon S3 中，支持两种类型的校验和：

- 完整对象校验和：完整对象校验和是根据分段上传的所有内容计算的，涵盖从第一分段的第一个字节到最后分段的最后一个字节的所有数据。

  > **Note**
  >
  > 所有 PUT 请求都需要完整对象校验和类型。

- 复合校验和：复合校验和是根据分段上传中每个分段的各个校验和计算得出的。这种方法不是根据所有数据内容计算校验和，而是聚合分段级的校验和（从第一个分段到最后一个分段），以便为完整对象生成单个组合校验和。

  > **Note**
  >
  > 当对象作为分段上传进行上传时，该对象的实体标签（ETag）不是整个对象的 MD5 摘要。相反，Amazon S3 会在上传时计算每个分段的 MD5 摘要。MD5 摘要用于确定最终对象的 ETag。Amazon S3 将 MD5 摘要的字节串联在一起，然后计算这些串联值的 MD5 摘要。在最终创建 ETag 的步骤中，Amazon S3 将在末尾添加一个短横线以及分段总数。

Amazon S3 支持以下完整对象和复合校验和算法类型：

- CRC-64/NVME (`CRC64NVME`)：仅支持完整对象算法类型。
- CRC-32 (`CRC32`)：支持完整对象和复合算法类型。
- CRC-32C (`CRC32C`)：支持完整对象和复合算法类型。

- SHA-1 (SHA1)：支持完整对象和复合算法类型。
- SHA-256 (SHA256)：支持完整对象和复合算法类型。

> **Note**
>
> 如果您使用 SHA-1 或 SHA-256 校验和算法进行分段上传，则必须使用复合算法类型。如果您使用 SHA-1 或 SHA-256 校验和算法进行单分段上传，则仅支持完整对象算法类型。

### 单分段上传

以单分段（使用 PutObject）上传的对象的校验和被视为完整对象校验和。在 Amazon S3 控制台中上传对象时，您可以选择希望 S3 使用的校验和算法，并且还（可选）提供预先计算的值。然后，Amazon S3 会在存储对象及其校验和值之前验证此校验和。在对象下载期间请求校验和值时，可以验证对象的数据完整性。

### 分段上传

使用 MultipartUpload API 将对象分成多个分段进行上传时，您可以指定希望 Amazon S3 使用的校验和算法以及校验和类型（完整对象或复合）。

下表显示了分段上传中每种校验和算法支持哪种校验和算法类型：

| 校验和算法 | 完整对象 | 复合键 |
| --- | --- | --- |
| CRC-64/NVME (CRC64NVME) | 是 | 否 |
| CRC-32 (CRC32) | 支持 | 是 |
| CRC-32C (CRC32C) | 支持 | 是 |
| SHA-1 (SHA1) | 否 | 是 |
| SHA-256 (SHA256) | 否 | 是 |

## 使用完整对象校验和进行分段上传

创建或执行分段上传时，可以在上传时使用完整对象校验和来进行验证。这意味着您可以为 `MultipartUpload` API 提供校验和算法，从而简化完整性验证工具，因为您不再需要跟踪已上传对象的分段边界。您可以在 `CompleteMultipartUpload` 请求中提供整个对象的校验和以及对象大小。

当您在分段上传期间提供完整的对象校验和时，Amazon SDK 会将校验和传递给 Amazon S3，而 S3 会在服务器端验证对象完整性，将其与接收到的值进行比较。然后，如果值匹配，Amazon S3 会存储对象。如果这两个值不匹配，S3 将使请求失败并出现 `BadDigest` 错误。对象的校验和还存储在对象元数据中，您稍后将使用这些元数据来验证对象的数据完整性。

要获得完整对象校验和，可以在 S3 中使用 CRC-64/NVME (`CRC64NVME`)、CRC-32 (`CRC32`) 或 CRC-32C (`CRC32C`) 校验和算法。分段上传中的完整对象校验和仅适用于基于 CRC 的校验和，因为它们可以线性化为完整对象校验和。这种线性化可让 Amazon S3 并行处理您的请求，以提高性能。尤其是，S3 可以根据分段级校验和计算整个对象的校验和。这种类型的验证不适用于其它算法，例如 SHA 和 MD5。由于 S3 具有默认的完整性保护，因此，如果在没有校验和的情况下上传对象，S3 会自动将推荐的完整对象 CRC-64/NVME (`CRC64NVME`) 校验和算法附加到该对象。

> **Note**
>
> 要启动分段上传，您可以指定校验和算法和完整对象校验和类型。指定校验和算法和完整对象校验和类型后，您可以为分段上传提供完整对象校验和值。

## 使用分段级校验和进行分段上传

将对象上传到 Amazon S3 时，它们可以作为单个对象上传，也可以通过分段上传过程以多个分段进行上传。您可以为分段上传选择校验和类型。对于分段上传分段级校验和（或复合校验和），Amazon S3 使用指定的校验和算法来计算每个分段的校验和。您可以使用 `UploadPart` 提供每个分段的校验和值。如果您尝试在 Amazon S3 控制台中上传的对象设置为使用 CRC-64/NVME (`CRC64NVME`) 校验和算法且超过 16 MB，则会自动将其指定为完整对象校验和。

然后，Amazon S3 使用存储的分段级校验和值来确认每个分段是否正确上传。当提供每个分段的校验和（针对整个对象）时，S3 使用每个分段的已存储校验和值来在内部计算完整对象校验和，并将其与提供的校验和值进行比较。这可最大限度地降低计算成本，因为 S3 可以使用各分段的校验和计算整个对象的校验和。有关分段上传的更多信息，请参阅在 Amazon S3 中使用分段上传来上传和复制对象和使用完整对象校验和进行分段上传。

完全上传对象后，可以使用最终计算出的校验和来验证对象的数据完整性。

上传分段上传的某个分段时，请注意以下几点：

- 要检索有关对象的信息，包括组成整个对象的分段数，可以使用 GetObjectAttributes 操作。借助其它校验和，还可以恢复每个单独分段的信息，包括该分段的校验和值。
- 对于已完成的分段上传，您可以使用 GetObject 或 HeadObject 操作，并指定与单个分段相符的分段编号或字节范围，来获取单个分段的校验和。如果您想检索仍在进行的分段上传的各个分段的校验和值，可以使用 ListParts。
- 由于 Amazon S3 计算分段对象的校验和的方式，复制对象时，对象的校验和值可能会发生变化。如果您使用的是 SDK 或 REST API，并且调用 CopyObject，Amazon S3 将复制不超过 CopyObject API 操作的大小限制的任何对象。无论对象是在单个请求中上传还是作为分段上传的一部分上传，Amazon S3 都可以作为单个操作执行此复制。使用 copy 命令，对象的校验和是完整对象的直接校验和。如果对象最初是使用分段上传进行上传的，即使数据没有变化，校验和值也会发生变化。
- 大于 CopyObject API 操作的大小限制的对象必须使用分段上传复制命令。
- 当您使用 Amazon Web Services Management Console执行某些操作时，如果对象大于 16 MB，则 Amazon S3 将使用分段上传。

## 校验和操作

上传对象后，您可以获取校验和值，并将其与预先计算的或之前存储的相同算法类型的校验和值进行比较。以下示例说明可以使用哪些校验和操作或方法来验证数据完整性。

使用 S3 控制台

要了解有关使用控制台和指定在上传对象时要使用的校验和算法的更多信息，请参阅上传对象和教程：使用其他校验和检查 Amazon S3 中数据的完整性。

使用 Amazon SDK

以下示例显示了如何使用 Amazon SDK 通过分段上传来上传大文件、下载大文件和验证分段上传文件，所有这些都使用 SHA-256 进行文件验证。

Java

Example 示例：使用 SHA-256 上传、下载和验证大文件

有关创建和测试有效示例的说明，请参阅《适用于 Java 的 Amazon SDK 开发人员指南》中的入门。

```
import software.amazon.awssdk.auth.credentials.AwsCredentials;
import software.amazon.awssdk.auth.credentials.AwsCredentialsProvider;
import software.amazon.awssdk.core.ResponseInputStream;
import software.amazon.awssdk.core.sync.RequestBody;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.AbortMultipartUploadRequest;
import software.amazon.awssdk.services.s3.model.ChecksumAlgorithm;
import software.amazon.awssdk.services.s3.model.ChecksumMode;
import software.amazon.awssdk.services.s3.model.CompleteMultipartUploadRequest;
import software.amazon.awssdk.services.s3.model.CompleteMultipartUploadResponse;
import software.amazon.awssdk.services.s3.model.CompletedMultipartUpload;
import software.amazon.awssdk.services.s3.model.CompletedPart;
import software.amazon.awssdk.services.s3.model.CreateMultipartUploadRequest;
import software.amazon.awssdk.services.s3.model.CreateMultipartUploadResponse;
import software.amazon.awssdk.services.s3.model.GetObjectAttributesRequest;
import software.amazon.awssdk.services.s3.model.GetObjectAttributesResponse;
import software.amazon.awssdk.services.s3.model.GetObjectRequest;
import software.amazon.awssdk.services.s3.model.GetObjectResponse;
import software.amazon.awssdk.services.s3.model.GetObjectTaggingRequest;
import software.amazon.awssdk.services.s3.model.ObjectAttributes;
import software.amazon.awssdk.services.s3.model.PutObjectTaggingRequest;
import software.amazon.awssdk.services.s3.model.Tag;
import software.amazon.awssdk.services.s3.model.Tagging;
import software.amazon.awssdk.services.s3.model.UploadPartRequest;
import software.amazon.awssdk.services.s3.model.UploadPartResponse;

import java.io.File;
import java.io.FileInputStream;
import java.io.FileOutputStream;
import java.io.IOException;
import java.io.InputStream;
import java.io.OutputStream;
import java.nio.ByteBuffer;
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;
import java.util.ArrayList;
```

```
    import java.util.Base64;
    import java.util.List;

    public class LargeObjectValidation {
        private static String FILE_NAME = "sample.file";
        private static String BUCKET = "sample-bucket";
        //Optional, if you want a method of storing the full multipart object
 checksum in S3.
        private static String CHECKSUM_TAG_KEYNAME = "fullObjectChecksum";
        //If you have existing full-object checksums that you need to validate
 against, you can do the full object validation on a sequential upload.
        private static String SHA256_FILE_BYTES = "htCM5g7ZNdoSw8bN/
mkgiAhXt5MFoVowVg+LE9aIQmI=";
        //Example Chunk Size - this must be greater than or equal to 5MB.
        private static int CHUNK_SIZE = 5 * 1024 * 1024;

        public static void main(String[] args) {
            S3Client s3Client = S3Client.builder()
                    .region(Region.US_EAST_1)
                    .credentialsProvider(new AwsCredentialsProvider() {
                        @Override
                        public AwsCredentials resolveCredentials() {
                            return new AwsCredentials() {
                                @Override
                                public String accessKeyId() {
                                    return Constants.ACCESS_KEY;
                                }

                                @Override
                                public String secretAccessKey() {
                                    return Constants.SECRET;
                                }
                            };
                        }
                    })
                    .build();
            uploadLargeFileBracketedByChecksum(s3Client);
            downloadLargeFileBracketedByChecksum(s3Client);
            validateExistingFileAgainstS3Checksum(s3Client);
        }

        public static void uploadLargeFileBracketedByChecksum(S3Client s3Client) {
            System.out.println("Starting uploading file validation");
            File file = new File(FILE_NAME);
```

```
            try (InputStream in = new FileInputStream(file)) {
                MessageDigest sha256 = MessageDigest.getInstance("SHA-256");
                CreateMultipartUploadRequest createMultipartUploadRequest =
CreateMultipartUploadRequest.builder()
                        .bucket(BUCKET)
                        .key(FILE_NAME)
                        .checksumAlgorithm(ChecksumAlgorithm.SHA256)
                        .build();
                CreateMultipartUploadResponse createdUpload =
s3Client.createMultipartUpload(createMultipartUploadRequest);
                List<CompletedPart> completedParts = new ArrayList<CompletedPart>();
                int partNumber = 1;
                byte[] buffer = new byte[CHUNK_SIZE];
                int read = in.read(buffer);
                while (read != -1) {
                    UploadPartRequest uploadPartRequest =
UploadPartRequest.builder()

.partNumber(partNumber).uploadId(createdUpload.uploadId()).key(FILE_NAME).bucket(BUCKET).ch
                    UploadPartResponse uploadedPart =
s3Client.uploadPart(uploadPartRequest,
RequestBody.fromByteBuffer(ByteBuffer.wrap(buffer, 0, read)));
                    CompletedPart part =
CompletedPart.builder().partNumber(partNumber).checksumSHA256(uploadedPart.checksumSHA256()
                    completedParts.add(part);
                    sha256.update(buffer, 0, read);
                    read = in.read(buffer);
                    partNumber++;
                }
                String fullObjectChecksum =
Base64.getEncoder().encodeToString(sha256.digest());
                if (!fullObjectChecksum.equals(SHA256_FILE_BYTES)) {
                    //Because the SHA256 is uploaded after the part is uploaded; the
upload is bracketed and the full object can be fully validated.

s3Client.abortMultipartUpload(AbortMultipartUploadRequest.builder().bucket(BUCKET).key(FILE
                    throw new IOException("Byte mismatch between stored checksum and
upload, do not proceed with upload and cleanup");
                }
                CompletedMultipartUpload completedMultipartUpload =
CompletedMultipartUpload.builder().parts(completedParts).build();
                CompleteMultipartUploadResponse completedUploadResponse =
s3Client.completeMultipartUpload(
```

```
CompleteMultipartUploadRequest.builder().bucket(BUCKET).key(FILE_NAME).uploadId(createdUplo
                Tag checksumTag =
Tag.builder().key(CHECKSUM_TAG_KEYNAME).value(fullObjectChecksum).build();
                //Optionally, if you need the full object checksum stored with the
file; you could add it as a tag after completion.

s3Client.putObjectTagging(PutObjectTaggingRequest.builder().bucket(BUCKET).key(FILE_NAME).t
            } catch (IOException | NoSuchAlgorithmException e) {
                e.printStackTrace();
            }
            GetObjectAttributesResponse
                    objectAttributes =
s3Client.getObjectAttributes(GetObjectAttributesRequest.builder().bucket(BUCKET).key(FILE_N
                    .objectAttributes(ObjectAttributes.OBJECT_PARTS,
ObjectAttributes.CHECKSUM).build());
            System.out.println(objectAttributes.objectParts().parts());
            System.out.println(objectAttributes.checksum().checksumSHA256());
        }

        public static void downloadLargeFileBracketedByChecksum(S3Client s3Client) {
            System.out.println("Starting downloading file validation");
            File file = new File("DOWNLOADED_" + FILE_NAME);
            try (OutputStream out = new FileOutputStream(file)) {
                GetObjectAttributesResponse
                        objectAttributes =
s3Client.getObjectAttributes(GetObjectAttributesRequest.builder().bucket(BUCKET).key(FILE_N
                        .objectAttributes(ObjectAttributes.OBJECT_PARTS,
ObjectAttributes.CHECKSUM).build());
                //Optionally if you need the full object checksum, you can grab a
tag you added on the upload
                List<Tag> objectTags =
s3Client.getObjectTagging(GetObjectTaggingRequest.builder().bucket(BUCKET).key(FILE_NAME).b
                String fullObjectChecksum = null;
                for (Tag objectTag : objectTags) {
                    if (objectTag.key().equals(CHECKSUM_TAG_KEYNAME)) {
                        fullObjectChecksum = objectTag.value();
                        break;
                    }
                }
                MessageDigest sha256FullObject =
MessageDigest.getInstance("SHA-256");
                MessageDigest sha256ChecksumOfChecksums =
MessageDigest.getInstance("SHA-256");
```

```
                //If you retrieve the object in parts, and set the ChecksumMode to
 enabled, the SDK will automatically validate the part checksum
                for (int partNumber = 1; partNumber <=
 objectAttributes.objectParts().totalPartsCount(); partNumber++) {
                    MessageDigest sha256Part = MessageDigest.getInstance("SHA-256");
                    ResponseInputStream<GetObjectResponse> response =
 s3Client.getObject(GetObjectRequest.builder().bucket(BUCKET).key(FILE_NAME).partNumber(part
                    GetObjectResponse getObjectResponse = response.response();
                    byte[] buffer = new byte[CHUNK_SIZE];
                    int read = response.read(buffer);
                    while (read != -1) {
                        out.write(buffer, 0, read);
                        sha256FullObject.update(buffer, 0, read);
                        sha256Part.update(buffer, 0, read);
                        read = response.read(buffer);
                    }
                    byte[] sha256PartBytes = sha256Part.digest();
                    sha256ChecksumOfChecksums.update(sha256PartBytes);
                    //Optionally, you can do an additional manual validation again
 the part checksum if needed in addition to the SDK check
                    String base64PartChecksum =
 Base64.getEncoder().encodeToString(sha256PartBytes);
                    String base64PartChecksumFromObjectAttributes =
 objectAttributes.objectParts().parts().get(partNumber - 1).checksumSHA256();
                    if (!
base64PartChecksum.equals(getObjectResponse.checksumSHA256()) || !
base64PartChecksum.equals(base64PartChecksumFromObjectAttributes)) {
                        throw new IOException("Part checksum didn't match for the
 part");
                    }
                    System.out.println(partNumber + " " + base64PartChecksum);
                }
                //Before finalizing, do the final checksum validation.
                String base64FullObject =
 Base64.getEncoder().encodeToString(sha256FullObject.digest());
                String base64ChecksumOfChecksums =
 Base64.getEncoder().encodeToString(sha256ChecksumOfChecksums.digest());
                if (fullObjectChecksum != null && !
fullObjectChecksum.equals(base64FullObject)) {
                    throw new IOException("Failed checksum validation for full
 object");
                }
                System.out.println(fullObjectChecksum);
```

```
                String base64ChecksumOfChecksumFromAttributes =
 objectAttributes.checksum().checksumSHA256();
                if (base64ChecksumOfChecksumFromAttributes != null && !
base64ChecksumOfChecksums.equals(base64ChecksumOfChecksumFromAttributes)) {
                    throw new IOException("Failed checksum validation for full
 object checksum of checksums");
                }
                System.out.println(base64ChecksumOfChecksumFromAttributes);
                out.flush();
            } catch (IOException | NoSuchAlgorithmException e) {
                //Cleanup bad file
                file.delete();
                e.printStackTrace();
            }
        }

        public static void validateExistingFileAgainstS3Checksum(S3Client s3Client)
 {
            System.out.println("Starting existing file validation");
            File file = new File("DOWNLOADED_" + FILE_NAME);
            GetObjectAttributesResponse
                    objectAttributes =
 s3Client.getObjectAttributes(GetObjectAttributesRequest.builder().bucket(BUCKET).key(FILE_N
                    .objectAttributes(ObjectAttributes.OBJECT_PARTS,
 ObjectAttributes.CHECKSUM).build());
            try (InputStream in = new FileInputStream(file)) {
                MessageDigest sha256ChecksumOfChecksums =
 MessageDigest.getInstance("SHA-256");
                MessageDigest sha256Part = MessageDigest.getInstance("SHA-256");
                byte[] buffer = new byte[CHUNK_SIZE];
                int currentPart = 0;
                int partBreak =
 objectAttributes.objectParts().parts().get(currentPart).size();
                int totalRead = 0;
                int read = in.read(buffer);
                while (read != -1) {
                    totalRead += read;
                    if (totalRead >= partBreak) {
                        int difference = totalRead - partBreak;
                        byte[] partChecksum;
                        if (totalRead != partBreak) {
                            sha256Part.update(buffer, 0, read - difference);
                            partChecksum = sha256Part.digest();
                            sha256ChecksumOfChecksums.update(partChecksum);
```

```
                            sha256Part.reset();
                            sha256Part.update(buffer, read - difference,
 difference);
                        } else {
                            sha256Part.update(buffer, 0, read);
                            partChecksum = sha256Part.digest();
                            sha256ChecksumOfChecksums.update(partChecksum);
                            sha256Part.reset();
                        }
                        String base64PartChecksum =
 Base64.getEncoder().encodeToString(partChecksum);
                        if (!
base64PartChecksum.equals(objectAttributes.objectParts().parts().get(currentPart).checksumSH
 {
                            throw new IOException("Part checksum didn't match S3");
                        }
                        currentPart++;
                        System.out.println(currentPart + " " + base64PartChecksum);
                        if (currentPart <
 objectAttributes.objectParts().totalPartsCount()) {
                            partBreak +=
 objectAttributes.objectParts().parts().get(currentPart - 1).size();
                        }
                    } else {
                        sha256Part.update(buffer, 0, read);
                    }
                    read = in.read(buffer);
                }
                if (currentPart != objectAttributes.objectParts().totalPartsCount())
 {
                    currentPart++;
                    byte[] partChecksum = sha256Part.digest();
                    sha256ChecksumOfChecksums.update(partChecksum);
                    String base64PartChecksum =
 Base64.getEncoder().encodeToString(partChecksum);
                    System.out.println(currentPart + " " + base64PartChecksum);
                }

                String base64CalculatedChecksumOfChecksums =
 Base64.getEncoder().encodeToString(sha256ChecksumOfChecksums.digest());
                System.out.println(base64CalculatedChecksumOfChecksums);
                System.out.println(objectAttributes.checksum().checksumSHA256());
```

```
                if (!
base64CalculatedChecksumOfChecksums.equals(objectAttributes.checksum().checksumSHA256()))
 {
                    throw new IOException("Full object checksum of checksums don't
 match S3");
                }

            } catch (IOException | NoSuchAlgorithmException e) {
                e.printStackTrace();
            }
        }
    }
```

使用 REST API

您可以发送 REST 请求以上传具有校验和值的对象，通过 PutObject 验证数据的完整性。您还可以使用 GetObject 或 HeadObject 检索对象的校验和值。

使用 Amazon CLI

您可以发送 PUT 请求，在单个操作中上传最大 5 GB 的对象。有关更多信息，请参阅《Amazon CLI 命令参考》中的 `PutObject`。您还可以使用 `get-object` 和 `head-object` 检索已上传对象的校验和以验证数据的完整性。

有关信息，请参阅《Amazon Command Line Interface 用户指南》中的 Amazon S3 CLI FAQ。

## 在上传对象时使用 Content-M5

上传后验证对象完整性的另一种方法是在上传对象时提供其 MD5 摘要。如果您计算对象的 MD5 摘要，则可以使用 `Content-MD5` 标头向 PUT 命令提供摘要。

上传对象后，Amazon S3 会计算对象的 MD5 摘要，并将其与您提供的值进行比较。只有在两个摘要匹配的情况下，请求才会成功。

不要求提供 MD5 摘要，但您可以在上传过程中使用它来验证对象的完整性。

## 使用 Content-MD5 和 ETag 验证上传的对象

对象的实体标签 (ETag) 表示该对象的特定版本。请注意，ETag 仅反映对于对象内容的更改，而不反映对其对象元数据的更改。如果只有对象的元数据发生变化，eTag 将保持不变。

根据对象的不同，对象的 ETag 可能是对象数据的 MD5 摘要：

- 如果对象是由 PutObject、PostObject 或 CopyObject 操作创建或通过 Amazon Web Services Management Console创建，并且该对象还是纯文本或使用具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）进行加密的，则该对象的 ETag 将是其对象数据的 MD5 摘要。
- 如果对象是由 PutObject、PostObject 或 CopyObject 操作创建或通过 Amazon Web Services Management Console创建，并且该对象使用客户提供的密钥 (SSE-C) 或 Amazon Key Management Service (Amazon KMS) 密钥 (SSE-KMS) 通过服务器端加密进行加密，则该对象的 ETag 将不是其对象数据的 MD5 摘要。
- 如果对象由分段上传过程或 UploadPartCopy 操作创建，则无论使用哪种加密方法，对象的 ETag 都不是 MD5 摘要。如果对象大于 16 MB，则 Amazon Web Services Management Console会作为分段上传来上传或复制该对象，因此 ETag 不是 MD5 摘要。

对于 ETag 是对象的 Content-MD5 摘要的对象，您可以将对象的 ETag 值与计算出的或之前存储的 Content-MD5 摘要进行比较。

## 使用尾随校验和

将对象上传到 Amazon S3 时，您可以为对象提供预先计算的校验和，也可以使用 Amazon SDK 代表您自动为分块上传创建尾随校验和。如果您使用尾随校验和，当您上传对象时，Amazon S3 会使用您指定的算法自动生成校验和，以便在分块上传期间验证对象的完整性。

要使用 Amazon SDK 时创建尾随校验和，请使用您首选的算法填充 ChecksumAlgorithm 参数。SDK 使用该算法计算对象（或对象分段）的校验和，并自动将其附加到分块上传请求的末尾。这种行为可以节省您的时间，因为 Amazon S3 一次性执行数据的验证和上传。

> **Important**
>
> 如果您使用的是 S3 对象 Lambda，则对 S3 对象 Lambda 的所有请求都使用 s3-object-lambda 而不是 s3。此行为会影响尾随校验和值的签名。有关 S3 对象 Lambda 的更多信息，请参阅 使用 S3 对象 Lambda 转换对象。

### 尾随校验和标头

要发出分块内容编码请求，Amazon S3 要求客户端包含多个标头，以正确地解析请求。客户端必须包括以下标头：

- **x-amz-decoded-content-length**：此标头表示随请求一起上传到 Amazon S3 的实际数据的纯文本大小。

- **x-amz-content-sha256**：此标头表示请求中包含的分块上传的类型。对于带有尾随校验和的分块上传，针对不使用有效载荷签名的请求，标头值为 STREAMING-UNSIGNED-PAYLOAD-TRAILER，而针对使用 SigV4 有效载荷签名的请求，标头值为 STREAMING-AWS4-HMAC-SHA256-PAYLOAD-TRAILER。（有关实现签名有效载荷的更多信息，请参阅 Signature calculations for the authorization header: Transferring a payload in multiple chunks。）
- **x-amz-trailer**：此标头表示请求中尾随标头的名称。如果尾随校验和存在（其中 Amazon SDK 将校验和附加到已编码的请求正文），则 x-amz-trailer 标头值包含 x-amz-checksum- 前缀并以算法名称结尾。目前支持以下 x-amz-trailer 值：
  - x-amz-checksum-crc32
  - x-amz-checksum-crc32c
  - x-amz-checksum-crc64nvme
  - x-amz-checksum-sha1
  - x-amz-checksum-sha256

> **Note**
>
> 还可以在请求中包含 Content-Encoding 标头以及分块值。虽然此标头不是必需的，但包含此标头可以最大限度地减少传输编码数据时的 HTTP 代理问题。如果请求中存在其它 Content-Encoding 标头（例如 gzip），则 Content-Encoding 标头会将分块值包含在以逗号分隔的编码列表中。例如 Content-Encoding: aws-chunked, gzip。

## 分块分段

当您使用分块编码将对象上传到 Amazon S3 时，上传请求包括以下类型的分块（按列出的顺序进行格式化）：

- 对象主体分块：可以有一个、多个或零个主体分块与分块上传请求相关联。
- 完成分块：可以有一个、多个或零个主体分块与分块上传请求相关联。
- 尾随分块：尾随校验和列在完成分块之后。只支持一个尾随分块。

> **Note**
>
> 每个分块上传都必须以最终的 CRLF（例如 \r\n）结尾，以表示请求的结尾。

有关分块格式化的示例，请参阅示例：带有尾随校验和的分块上传。

对象主体分块

对象主体分块是包含要上传到 S3 的实际对象数据的分块。这些分块具有一致的大小和格式约束。

对象主体分块大小

这些分块必须包含至少 8192 字节（或 8 KiB）的对象数据，但最后一个主体分块除外，它可以更小。没有明确的最大分块大小，但您可以预期所有分块都将小于 5 GB 的最大上传大小。根据您的客户端服务器实现，每个分块的大小可能会有所不同。

对象主体分块格式

对象主体分块以对象主体分块中字节数的十六进制编码开头，然后是 CRLF（回车换行符）、该分块的对象字节和另一个 CRLF。

例如：

```
hex-encoding-of-object-bytes-in-chunk\r\n
chunk-object-bytes\r\n
```

但是，在对分块进行签名时，对象主体分块遵循不同的格式，其中签名通过分号分隔符附加到分块大小后面。例如：

```
hex-encoding-of-object-bytes-in-chunk;chunk-signature\r\n
 chunk-object-bytes\r\n
```

有关分块签名的更多信息，请参阅 Signature calculations for the Authorization Header: Transferring a payload in multiple chunks (Amazon Signature Version 4)。有关分块格式的更多信息，请参阅 RFC 编辑器 网站上的 Chunked transfer encoding。

完成分块

完成分块必须是每个分块上传的最后一个对象主体分块。完成分块的格式与主体分块类似，但始终包含零字节的对象数据。（零字节的对象数据表示所有数据都已上传。）分块上传必须包含一个完成分块作为其最终对象主体分块，格式如下：

```
0\r\n
```

但是，如果内容编码请求使用有效载荷签名，则它将改用以下格式：

```
0;chunk-signature\r\n
```

尾随分块

尾随分块保存所有 S3 上传请求的计算校验和。尾随分块包括两个字段：一个标头名称字段和一个标头值字段。上传请求的标头名称字段必须与传递到 x-amz-trailer 请求标头的值相匹配。例如，如果请求包含 x-amz-trailer: x-amz-checksum-crc32 并且尾随分块具有标头名称 x-amz-checksum-sha1，则请求将失败。尾随分块中的值字段包括该对象的大端校验和值的 base64 编码。（大端序将数据的最高有效字节存储在最低的内存地址，将最低有效字节存储在最大的内存地址）。用于计算此校验和的算法与标头名称的后缀相同（例如 crc32）。

尾随分块格式

对于未签名的有效载荷请求，尾随分块使用以下格式：

```
x-amz-checksum-lowercase-checksum-algorithm-name:base64-checksum-value\n\r\n\r\n
```

对于具有 SigV4 signed payloads 的请求，尾随分块在尾随分块后面包含一个尾随签名。

```
trailer-checksum\n\r\n
trailer-signature\r\n
```

也可以将 CRLF 直接添加到 base64 校验和值的末尾。例如：

```
x-amz-checksum-lowercase-checksum-algorithm-name:base64-checksum-value\r\n\r\n
```

示例：带有尾随校验和的分块上传

对于带有尾随校验和的 PutObject 和 UploadPart 请求，Amazon S3 支持使用 aws-chunked 内容编码的分块上传。

Example 1：带有尾随 CRC-32 校验和的未签名分块 **PutObject** 请求

以下是具有尾随 CRC-32 校验和的分块 PutObject 请求的示例。在此示例中，客户端将一个 17 KB 的对象分成三个未签名的分块进行上传，并使用 x-amz-checksum-crc32 标头附加一个尾随 CRC-32 校验和分块。

```
PUT /Key+ HTTP/1.1
Host: amzn-s3-demo-bucket
Content-Encoding: aws-chunked
```

```
x-amz-decoded-content-length: 17408
x-amz-content-sha256: STREAMING-UNSIGNED-PAYLOAD-TRAILER
x-amz-trailer: x-amz-checksum-crc32

2000\r\n                                    // Object body chunk 1 (8192 bytes)
object-bytes\r\n
2000\r\n                                    // Object body chunk 2 (8192 bytes)
object-bytes\r\n
400\r\n                                     // Object body chunk 3 (1024 bytes)
object-bytes\r\n
0\r\n                                       // Completion chunk
x-amz-checksum-crc32:YABb/g==\n\r\n\r\n     // Trailer chunk (note optional \n
 character)
\r\n                                          // CRLF
```

以下是示例响应：

```
HTTP/1.1 200
ETag: ETag
x-amz-checksum-crc32: YABb/g==
```

> **Note**
>
> 校验和值末尾的换行符 \n 的使用可能因客户端而异。

Example 2：带有尾随 CRC-32 (**CRC32**) 校验和的 SigV4 签名的分块 **PutObject** 请求

以下是具有尾随 CRC-32 校验和的分块 PutObject 请求的示例。此请求使用 SigV4 有效载荷签名。在此示例中，客户端将一个 17 KB 的对象分成三个签名的分块进行上传。除了 object body 分块之外，completion chunk 和 trailer chunk 也已签名。

```
PUT /Key+ HTTP/1.1
Host: amzn-s3-demo-bucket.s3.amazonaws.com
Content-Encoding: aws-chunked
x-amz-decoded-content-length: 17408
x-amz-content-sha256: STREAMING-AWS4-HMAC-SHA256-PAYLOAD-TRAILER
x-amz-trailer: x-amz-checksum-crc32

authorization-code                          // SigV4 headers authorization

2000;chunk-signature=signature-value...\r\n   // Object body chunk 1 (8192 bytes)
```

```
object-bytes\r\n
2000;chunk-signature\r\n                    // Object body chunk 2 (8192 bytes)
object-bytes\r\n
400;chunk-signature\r\n                     // Object body chunk 3 (1024 bytes)
object-bytes\r\n
0;chunk-signature\r\n                       // Completion chunk
x-amz-checksum-crc32:YABb/g==\n\r\n          // Trailer chunk (note optional \n
 character)
trailer-signature\r\n
\r\n                                         // CRLF
```

以下是示例响应：

```
HTTP/1.1 200
ETag: ETag
x-amz-checksum-crc32: YABb/g==
```

# 删除 Amazon S3 对象

您可以使用 Amazon S3 控制台、Amazon SDK、Amazon Command Line Interface (Amazon CLI) 或 REST API 直接从 Amazon S3 删除一个或多个对象。例如，如果您正在收集日志文件，最好在不再需要这些文件时将其删除。可以设置 S3 生命周期规则来自动删除对象（如日志文件）。

要删除对象，可以使用以下 API 操作之一：

- 删除单个对象 – Amazon S3 提供了 DELETE（DeleteObject）API 操作，使您能够删除单个 HTTP 请求中的一个对象。
- 删除多个对象 – Amazon S3 提供了多对象删除（DeleteObjects）API 操作，使您能够在单个 HTTP 请求中删除多达 1000 个对象。

从未启用版本控制的存储桶中删除对象时，只需提供对象键名称。但是，当从启用版本控制的存储桶中删除对象时，可以提供对象的版本 ID，来删除该对象的特定版本。

## 删除对象之前应考虑的最佳实践

在删除对象之前，请考虑以下最佳实践：

- 启用存储桶版本控制。S3 版本控制增加了对简单 DeleteObject 请求的保护，以防止意外删除。对于受版本控制的存储桶，如果您删除对象的当前版本，或删除请求未指定特定版本 ID，则 Amazon S3 不会永久删除该对象。而是 S3 添加一个删除标记，发出对象软删除。然后，删除标记

将成为对象的当前（或最新）版本，具有新版本 ID。有关更多信息，请参阅从启用了版本控制的存储桶中删除对象版本。

- 如果您要删除大量对象，或者要以编程方式根据对象创建日期删除对象，请在存储桶上设置 S3 生命周期配置。要监控这些删除，建议您使用 S3 生命周期事件通知。配置 S3 生命周期通知后，如果删除了存储桶中的对象，`s3:LifecycleExpiration:Delete` 事件类型会通知您。当 S3 生命周期配置永久删除对象版本时，它也会通知您。当 S3 生命周期创建删除标记时，`s3:LifecycleExpiration:DeleteMarkerCreated` 事件类型会通知您。在删除受版本控制的存储桶中对象的当前版本后，将创建删除标记。
- 在对 S3 生命周期配置进行任何更新之前，请确认生命周期已针对所有目标对象完成了操作。有关更多信息，请参阅在存储桶上设置 S3 生命周期配置中的更新、禁用或删除生命周期规则。

> **Note**
>
> S3 生命周期规则必须应用于对象的正确子集，以防止意外删除。在创建生命周期规则时，可以按前缀、对象标签或对象大小筛选对象。

- 考虑限制用户从存储桶中移除或删除对象。要限制用户，您需要在 Amazon S3 存储桶策略中显式拒绝用户执行以下操作的权限：
  - `s3:DeleteObject`、`s3:DeleteObjectVersion`（控制谁可以使用 API 请求删除对象）
  - `s3:PutLifecycleConfiguration`（控制谁可以添加 S3 生命周期到期规则）
- 考虑使用 S3 复制来创建数据的多个副本，并将它们同时复制到多个位置。可以根据需要选择任意数量的目标存储桶。此外，如果无意中删除了某个对象，您仍将拥有该数据的副本。

## 从启用版本控制的存储桶中删除对象

如果存储桶已启用版本控制，则存储桶中可能存在同一对象的多个版本。使用启用了版本控制的存储桶时，`Delete` API 操作将启用以下选项：

- 指定不受版本控制的删除请求 – 仅指定对象的键，而不指定版本 ID。在此情况下，Amazon S3 将在对象的当前版本上创建一个删除标记，并在响应中返回其版本 ID。这将使您的对象从存储桶中消失。有关对象版本控制和删除标记概念的信息，请参阅 使用 S3 版本控制保留对象的多个版本。
- 指定受版本控制的删除请求 – 同时指定键和版本 ID。在此情况下，可能会出现以下结果：
  - 如果版本 ID 映射到特定的对象版本，则 Amazon S3 将删除该特定版本的对象。
  - 如果版本 ID 映射到对象的删除标记，则 Amazon S3 将删除该删除标记。删除了删除标记后，该对象随后会重新出现在存储桶中。

## 从已暂停版本控制的存储桶中删除对象

如果存储桶已暂停版本控制，则 Delete API 操作的行为方式与启用版本控制的存储桶相同（但当前版本的版本 ID 为空时除外）。有关更多信息，请参阅 从已暂停版本控制的存储桶中删除对象。

## 从不受版本控制的存储桶中删除对象

如果存储桶不受版本控制，则可以在 Delete API 操作中指定对象的键，而 Amazon S3 将永久删除该对象。为防止永久删除对象，请启用存储桶版本控制。

## 从启用了 MFA 的存储桶中删除对象

从启用了多重身份验证（MFA）的存储桶中删除对象时，请注意以下内容：

- 如果您提供了无效的 MFA 令牌，请求将始终失败。
- 如果您拥有一个启用了 MFA 的存储桶，并且发送了一个受版本控制的删除请求（您提供了对象键和版本 ID），若您不能提供有效的 MFA 令牌，请求将失败。此外，对启用了 MFA 的存储桶使用多对象 Delete API 操作时，如果任何删除是受版本控制的删除请求（也即，您指定了对象键和版本 ID），若不能提供有效的 MFA 令牌，则整个请求将失败。

但是，在下面的情况下，请求将成功：

- 如果您拥有一个启用了 MFA 的存储桶，并发出一个不受版本控制的删除请求（不删除受版本控制的对象），且您未提供 MFA 令牌，删除会成功。
- 如果您发出一个多对象删除请求，此请求指定从一个启用了 MFA 的存储桶中仅删除不受版本控制的对象，且您未提供 MFA 令牌，这些删除会成功。

有关 MFA 删除的信息，请参阅配置 MFA 删除。

主题

- 删除单个对象
- 删除多个对象

## 删除单个对象

您可以使用 Amazon S3 控制台或 DELETE API 从 S3 存储桶中删除单个现有对象。有关删除 Amazon S3 中的对象的更多信息，请参阅删除 Amazon S3 对象。

由于 S3 存储桶中的所有对象都会产生存储费用，因此您应从中删除不再需要的对象。例如，如果您正在收集日志文件，最好在不再需要这些文件时将其删除。您可以将生命周期规则设置为自动删除对象(如日志文件)。有关更多信息，请参阅 the section called “设置生命周期配置”。

有关 Amazon S3 特征和定价的信息，请参阅 Amazon S3 定价。

使用 S3 控制台

请按照以下步骤使用 Amazon S3 控制台从存储桶中删除单个对象。

> **Warning**
>
> 当您在 Amazon S3 控制台中永久删除对象或指定的对象版本时，删除操作无法撤销。

删除已启用或暂停版本控制的对象

> **Note**
>
> 如果已暂停版本控制的桶中某个对象的版本 ID 标记为 NULL，则 S3 会永久删除该对象，因为不存在之前的版本。然而，如果在暂停了版本控制的桶中为对象列出了有效的版本 ID，则 S3 为已删除的对象创建删除标记，同时保留该对象的先前版本。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶或目录存储桶。
3. 在存储桶列表中，选择要从中删除对象的存储桶的名称。
4. 选择对象，然后选择删除。
5. 要确认删除指定的对象下的对象列表，请在删除对象？文本框中输入 **`delete`**。

永久删除已启用版本控制的桶中的特定对象版本

> **Warning**
>
> 当您永久删除 Amazon S3 中的特定对象版本时，删除操作无法撤销。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Bucket name（存储桶名称）列表中，请选择要从中删除对象的存储桶的名称。
3. 选择您要删除的对象。
4. 选择显示版本开关。
5. 选择对象版本，然后选择删除。
6. 要确认永久删除指定的对象下列出的特定对象版本，请在删除对象？文本框中输入 Permanently delete。Amazon S3 永久删除特定的对象版本。

永久删除未启用版本控制的 Amazon S3 存储桶中的对象

> **Warning**
>
> 当您永久删除 Amazon S3 中的对象时，删除操作无法撤销。此外，对于任何未启用版本控制的桶，删除操作都是永久性的。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在存储桶列表中，选择要从中删除对象的存储桶的名称。
4. 选择对象，然后选择删除。
5. 要确认永久删除指定的对象下列出的对象，请在删除对象？文本框中输入 permanently delete。

> **Note**
>
> 如果您在删除对象时遇到任何问题，请参阅我想永久删除受版本控制的对象。

使用 Amazon CLI

要为每个请求删除一个对象，请使用 DELETE API。有关更多信息，请参阅 DELETE Object。有关使用 CLI 删除对象的更多信息，请参阅 delete-object。

使用 REST API

您可以使用 Amazon SDK 删除对象。然而，如果您的应用程序需要它，则可以直接发送 REST 请求。有关更多信息，请参阅 Amazon Simple Storage Service API 参考中的 DELETE Object。

使用 Amazon 软件开发工具包

以下示例展示了如何使用 Amazon SDK 从存储桶中删除对象。有关更多信息，请参阅 Amazon Simple Storage Service API 参考中的 DELETE Object

如果已对存储桶启用 S3 版本控制，您将可使用以下选项：

- 通过指定版本 ID 来删除特定对象版本。
- 删除对象而不指定版本 ID，在这种情况下，Amazon S3 将向对象添加一个删除标记。

有关 S3 版本控制的更多信息，请参阅使用 S3 版本控制保留对象的多个版本。

有关更多示例以及其它语言的示例，请参阅《Amazon S3 API reference》中的 Use `DeleteObject` with an Amazon SDK or CLI。

Java

Example 示例 1：删除对象（不受版本控制的存储桶）

以下示例假定存储桶不受版本控制且对象没有任何版本 ID。在删除请求中，您仅指定对象键而不是版本 ID。

有关创建和测试有效示例的说明，请参阅《适用于 Java 的 Amazon SDK 开发人员指南》中的入门。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.DeleteObjectRequest;

import java.io.IOException;

public class DeleteObjectNonVersionedBucket {
```

```
    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String keyName = "*** Key name ****";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            s3Client.deleteObject(new DeleteObjectRequest(bucketName, keyName));
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Example 示例 2：删除对象（受版本控制的存储桶）

以下示例将删除受版本控制的存储桶中的对象。该示例通过指定对象键名和版本 ID 来删除特定对象版本。

本示例执行以下操作：

1. 向存储桶添加示例对象。Amazon S3 会返回新添加对象的版本 ID。该示例将在删除请求中使用此版本 ID。
2. 通过指定对象键名和版本 ID 来删除对象版本。如果对象没有其他版本，则 Amazon S3 将完全删除对象。否则，Amazon S3 仅删除指定版本。

> **Note**
>
> 可以通过发送 `ListVersions` 请求来获取对象的版本 ID。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.BucketVersioningConfiguration;
import com.amazonaws.services.s3.model.DeleteVersionRequest;
import com.amazonaws.services.s3.model.PutObjectResult;

import java.io.IOException;

public class DeleteObjectVersionEnabledBucket {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String keyName = "*** Key name ****";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Check to ensure that the bucket is versioning-enabled.
            String bucketVersionStatus =
 s3Client.getBucketVersioningConfiguration(bucketName).getStatus();
            if (!bucketVersionStatus.equals(BucketVersioningConfiguration.ENABLED))
 {
                System.out.printf("Bucket %s is not versioning-enabled.",
 bucketName);
            } else {
                // Add an object.
                PutObjectResult putResult = s3Client.putObject(bucketName, keyName,
                        "Sample content for deletion example.");
                System.out.printf("Object %s added to bucket %s\n", keyName,
 bucketName);

                // Delete the version of the object that we just created.
                System.out.println("Deleting versioned object " + keyName);
```

```
                s3Client.deleteVersion(new DeleteVersionRequest(bucketName, keyName,
 putResult.getVersionId()));
                System.out.printf("Object %s, version %s deleted\n", keyName,
 putResult.getVersionId());
            }
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

以下示例演示如何删除受版本控制和不受版本控制的存储桶中的对象。有关 S3 版本控制的更多信息，请参阅使用 S3 版本控制保留对象的多个版本。

Example 删除不受版本控制的存储桶中的对象

以下 C# 示例将删除不受版本控制的存储桶中的对象。该示例假定对象没有版本 ID，因此您未指定版本 ID。您仅指定了对象键。

有关设置和运行代码示例的信息，请参阅《适用于 .NET 的 Amazon SDK 开发人员指南》中的适用于 .NET 的 Amazon SDK 入门。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class DeleteObjectNonVersionedBucketTest
    {
        private const string bucketName = "*** bucket name ***";
        private const string keyName = "*** object key ***";
        // Specify your bucket region (an example region is shown).
```

```
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;

        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            DeleteObjectNonVersionedBucketAsync().Wait();
        }
        private static async Task DeleteObjectNonVersionedBucketAsync()
        {
            try
            {
                var deleteObjectRequest = new DeleteObjectRequest
                {
                    BucketName = bucketName,
                    Key = keyName
                };

                Console.WriteLine("Deleting an object");
                await client.DeleteObjectAsync(deleteObjectRequest);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 deleting an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 deleting an object", e.Message);
            }
        }
    }
}
```

Example 删除受版本控制的存储桶中的对象

以下 C# 示例将删除受版本控制的存储桶中的对象。它将通过指定对象键名和版本 ID 来删除对象的特定版本。

代码将执行以下任务：

1. 对指定的存储桶启用版本控制（如果已启用 S3 版本控制，则此操作无效）。

2. 向存储桶添加示例对象。作为响应，Amazon S3 将返回新添加的对象的版本 ID。该示例将在删除请求中使用此版本 ID。
3. 通过指定对象键名和版本 ID 来删除示例对象。

> **Note**
>
> 还可以通过发送 `ListVersions` 请求来获取对象的版本 ID。
>
> ```
> var listResponse = client.ListVersions(new ListVersionsRequest { BucketName
>  = bucketName, Prefix = keyName });
> ```

有关设置和运行代码示例的信息，请参阅《适用于 .NET 的 Amazon SDK 开发人员指南》中的适用于 .NET 的 Amazon SDK 入门。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class DeleteObjectVersion
    {
        private const string bucketName = "*** versioning-enabled bucket name ***";
        private const string keyName = "*** Object Key Name ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;

        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            CreateAndDeleteObjectVersionAsync().Wait();
        }

        private static async Task CreateAndDeleteObjectVersionAsync()
        {
            try
```

```
            {
                // Add a sample object.
                string versionID = await PutAnObject(keyName);

                // Delete the object by specifying an object key and a version ID.
                DeleteObjectRequest request = new DeleteObjectRequest
                {
                    BucketName = bucketName,
                    Key = keyName,
                    VersionId = versionID
                };
                Console.WriteLine("Deleting an object");
                await client.DeleteObjectAsync(request);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 deleting an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 deleting an object", e.Message);
            }
        }

        static async Task<string> PutAnObject(string objectKey)
        {
            PutObjectRequest request = new PutObjectRequest
            {
                BucketName = bucketName,
                Key = objectKey,
                ContentBody = "This is the content body!"
            };
            PutObjectResponse response = await client.PutObjectAsync(request);
            return response.VersionId;
        }
    }
}
```

PHP

本示例演示如何使用第 3 版 适用于 PHP 的 Amazon SDK 中的类删除不受版本控制的存储桶中的对象。有关从受版本控制的存储桶中删除对象的信息，请参阅 使用 REST API。

有关适用于 Ruby 的 Amazon 开发工具包 API 的更多信息，请转到适用于 Ruby 的 Amazon 开发工具包 – 版本 2。

下面的 PHP 示例将删除存储桶中的对象。由于此示例演示如何删除不受版本控制的存储桶中的对象，因此它在删除请求中仅提供存储桶名称和对象键（而不是版本 ID）。

```
<?php

require 'vendor/autoload.php';

use Aws\S3\S3Client;
use Aws\S3\Exception\S3Exception;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// 1. Delete the object from the bucket.
try
{
    echo 'Attempting to delete ' . $keyname . '...' . PHP_EOL;

    $result = $s3->deleteObject([
        'Bucket' => $bucket,
        'Key'    => $keyname
    ]);

    if ($result['DeleteMarker'])
    {
        echo $keyname . ' was deleted or does not exist.' . PHP_EOL;
    } else {
        exit('Error: ' . $keyname . ' was not deleted.' . PHP_EOL);
    }
}
catch (S3Exception $e) {
    exit('Error: ' . $e->getAwsErrorMessage() . PHP_EOL);
}

// 2. Check to see if the object was deleted.
```

```
try
{
    echo 'Checking to see if ' . $keyname . ' still exists...' . PHP_EOL;

    $result = $s3->getObject([
        'Bucket' => $bucket,
        'Key'    => $keyname
    ]);

    echo 'Error: ' . $keyname . ' still exists.';
}
catch (S3Exception $e) {
    exit($e->getAwsErrorMessage());
}
```

Javascript

```
import { DeleteObjectCommand } from "@aws-sdk/client-s3";
import { s3Client } from "./libs/s3Client.js" // Helper function that creates Amazon
 S3 service client module.

export const bucketParams = { Bucket: "BUCKET_NAME", Key: "KEY" };

export const run = async () => {
  try {
    const data = await s3Client.send(new DeleteObjectCommand(bucketParams));
    console.log("Success. Object deleted.", data);
    return data; // For unit tests.
  } catch (err) {
    console.log("Error", err);
  }
};
run();
```

## 删除多个对象

由于 S3 存储桶中的所有对象都会产生存储费用，因此您应从中删除不再需要的对象。例如，如果您正在收集日志文件，最好在不再需要这些文件时将其删除。您可以将生命周期规则设置为自动删除对象(如日志文件)。有关更多信息，请参阅 the section called “设置生命周期配置”。

有关 Amazon S3 特征和定价的信息，请参阅 Amazon S3 定价。

您可以使用 Amazon S3 控制台、Amazon SDK 或 REST API 从 S3 存储桶中同时删除多个对象。

使用 S3 控制台

请按照以下步骤使用 Amazon S3 控制台从存储桶中删除多个对象。

> **Warning**
>
> - 删除指定的对象无法撤销。
> - 此操作将删除所有指定的对象。删除文件夹时，请等待删除操作完成，然后再将新对象添加到文件夹。否则，新对象也可能会被删除。
> - 当删除未启用版本控制的存储桶（包括目录存储桶）中的对象时，Amazon S3 将永久删除这些对象。
> - 当删除已启用或已暂停存储桶版本控制的存储桶中的对象时，Amazon S3 将创建删除标记。有关更多信息，请参阅使用删除标记。

删除已启用或暂停版本控制的对象

> **Note**
>
> 如果已暂停版本控制的存储桶中对象的版本 ID 标记为 NULL，则 S3 会永久删除这些对象，因为不存在之前的版本。然而，如果针对已暂停版本控制的存储桶中的对象列出了有效的版本 ID，S3 会为已删除的对象创建删除标记，同时保留这些对象的先前版本。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在存储桶列表中，选择要从中删除对象的存储桶的名称。
4. 选择对象，然后选择删除。
5. 要确认删除指定的对象下的对象列表，请在删除对象？文本框中输入 **`delete`**。

永久删除已启用版本控制的存储桶中的特定对象版本

> **Warning**
>
> 当您永久删除 Amazon S3 中的特定对象版本时，删除操作无法撤销。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在存储桶列表中，选择要从中删除对象的存储桶的名称。
4. 选择您要删除的 对象。
5. 选择显示版本开关。
6. 选择对象版本，然后选择删除。
7. 要确认永久删除指定的对象下列出的特定对象版本，请在删除对象？文本框中输入 Permanently delete。Amazon S3 将永久删除特定对象版本。

永久删除未 启用版本控制的 Amazon S3 存储桶中的对象

> **Warning**
>
> 当您永久删除 Amazon S3 中的对象时，删除操作无法撤销。此外，对于任何未启用版本控制的存储桶（包括目录存储桶），删除操作都是永久性的。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶或目录存储桶。
3. 在存储桶列表中，选择要从中删除对象的存储桶的名称。
4. 选择对象，然后选择删除。
5. 要确认永久删除指定的对象下列出的对象，请在删除对象？文本框中输入 permanently delete。

> **Note**
>
> 如果您在删除对象时遇到任何问题，请参阅我想永久删除受版本控制的对象。

使用 Amazon 软件开发工具包

有关如何使用 Amazon SDK 删除多个对象的示例，请参阅《Amazon S3 API 参考》中的 Code examples。

有关使用不同 Amazon SDK 的一般信息，请参阅《Amazon S3 API 参考》中的 Developing with Amazon S3 using the Amazon SDKs。

使用 REST API

您可以使用 Amazon SDK，通过多个对象删除 API 删除多个对象。然而，如果您的应用程序需要它，则可以直接发送 REST 请求。

有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的删除多个对象。

# 组织、列出和处理对象

在 Amazon S3 中，您可以使用前缀来组织存储。前缀是存储桶中对象的逻辑分组。前缀值类似于允许您将相似数据存储在存储桶内同一目录下的目录名称。以编程方式上传对象时，可以使用前缀来组织数据。

在 Amazon S3 控制台中，前缀称为文件夹。您可以通过导航到存储桶，在 S3 控制台中查看所有对象和文件夹。您还可以查看有关每个对象的信息，包括对象属性。

有关在 Amazon S3 中列出和组织数据的更多信息，请参阅以下主题。

主题

- 使用前缀组织对象
- 以编程方式列出对象键
- 使用文件夹在 Amazon S3 控制台中整理对象
- 在 Amazon S3 控制台中查看对象属性
- 使用标签对存储进行分类

# 使用前缀组织对象

您可以使用前缀来组织存储在 Amazon S3 存储桶中的数据。前缀是对象键名称开头的一串字符串。前缀可以是任意长度，取决于对象键名称的最大长度（1024 个字节）。您可以把前缀视为一种以类似于目录的方式组织数据的方式。但是，前缀不是目录。

按前缀搜索会将结果限制为仅以指定前缀开头的这些键。分隔符导致列表操作将共享公共前缀的所有键汇总到单个汇总列表结果中。

前缀和分隔符参数的目的是帮助您按层次结构组织，然后浏览您的键。要执行此操作，首先为您的存储桶选取一个分隔符，例如，斜杠（/），它不会出现在任何预期的键名中。您可以使用另一个字符作为分隔符。斜杠 (/) 字符没有什么独特之处，它是一个非常常见的前缀分隔符。接下来，通过串联所有包含层次结构的级别，并使用分隔符分隔每个级别来构建您的键名。

例如，如果您正在存储关于城市的信息，您可以按大陆、按国家/区域，然后按省份或州来自然地组织他们。因为这些名称通常不包含标点符号，您可以使用斜杠 (/) 作为分隔符。下面的示例使用斜杠 (/) 分隔符。

- Europe/France/Nouvelle-Aquitaine/Bordeaux
- North America/Canada/Quebec/Montreal
- North America/USA/Washington/Bellevue
- North America/USA/Washington/Seattle

如果您采用此方式来存储世界上每个城市的数据，那么管理平面键命名空间会很困难。通过使用带列表操作的 `Prefix` 和 `Delimiter`，您可以使用已创建的层次结构来列出您的数据。例如，要列出美国的所有州，请设置 `Delimiter='/'` 和 `Prefix='North America/USA/'`。要列出您拥有数据的所有加拿大省份，请设置 `Delimiter='/'` 和 `Prefix='North America/Canada/'`。

有关分隔符、前缀和嵌套文件夹的更多信息，请参阅前缀和嵌套文件夹之间的区别。

## 使用前缀和分隔符列出对象

如果您使用分隔符发布列表请求，您可以仅浏览一个级别的层次结构、跳过或总结嵌套在更深级别的键（可能是数百万）。例如，假设您拥有具有以下键的存储桶 (*amzn-s3-demo-bucket*)：

```
sample.jpg
```

```
photos/2006/January/sample.jpg
```

photos/2006/February/sample2.jpg

photos/2006/February/sample3.jpg

photos/2006/February/sample4.jpg

示例存储桶仅拥有根级 sample.jpg 对象。要仅列出存储桶中的根级对象，您需要向存储桶发送带正斜杠（/）分隔符的 GET 请求。作为响应，Amazon S3 将返回 sample.jpg 对象密钥，因为它不包含 / 分隔符。所有其他键都包含分隔符。Amazon S3 将组合这些密钥，并在指定的分隔符首次出现时，返回带前缀值 photos/ 的单个 CommonPrefixes 元素（它是这些密钥开头的子字符串）。

Example

```
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Name>amzn-s3-demo-bucket</Name>
  <Prefix></Prefix>
  <Marker></Marker>
  <MaxKeys>1000</MaxKeys>
  <Delimiter>/</Delimiter>
  <IsTruncated>false</IsTruncated>
  <Contents>
    <Key>sample.jpg</Key>
    <LastModified>2011-07-24T19:39:30.000Z</LastModified>
    <ETag>&quot;d1a7fb5eab1c16cb4f7cf341cf188c3d&quot;</ETag>
    <Size>6</Size>
    <Owner>
      <ID>75cc57f09aa0c8caeab4f8c24e99d10f8e7faeebf76c078efc7c6caea54ba06a</ID>
      <DisplayName>displayname</DisplayName>
    </Owner>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <CommonPrefixes>
    <Prefix>photos/</Prefix>
  </CommonPrefixes>
</ListBucketResult>
```

有关以编程方式列出对象键的更多信息，请参阅以编程方式列出对象键。

## 以编程方式列出对象键

在 Amazon S3 中，键可以按前缀列出。您可以为相关键的名称选择通用前缀，然后使用分隔层次结构的特殊字符标记这些键。然后，您可以使用列表操作按层次选择和浏览键。这类似于在文件系统的目录中存储文件的方式。

Amazon S3 公开了列表操作，允许您列出包含在存储桶中的键。将按存储桶和前缀选择用于列表的键。例如，假设一个存储桶的名称为“dictionary”，它为每个英语词汇包含了一个键值。您可能会创建一个调用来列出该存储桶中以字母“q”开头的存储桶。列表结果始终以 UTF-8 二进制顺序返回。

SOAP 和 REST 列表操作将返回一个 XML 文档，其中包含匹配键值的名称和有关由每个键值识别的对象的信息。

> **Note**
>
> SOAP API 不适用于新客户，并将于 2025 年 8 月 31 日接近使用寿命终止（EOL）。我们建议您使用 REST API 或 Amazon 软件开发工具包。

出于列表目的，可以根据通用前缀收拢那些共享一个前缀并且以特定分隔符终结的键组。这允许应用程序按层次结构组织和浏览键值，与您在文件系统的目录中组织文件的方式相同。

例如，要扩展字典存储桶以包含除英语单词外的更多内容，您可以使用语言和分隔符为每个单词添加前缀（例如，“French/logical”），从而构成键值。使用此命名方案和层级列表特征，您可以检索仅包含法语词汇的列表。您也可以浏览可用语言的顶级列表，而无需循环浏览所有按字典顺序排列的干预键。有关列表的此方面的更多信息，请参阅 使用前缀组织对象。

REST API

如果您的应用程序需要它，则可以直接发送 REST 请求。您可以发送 GET 请求来返回存储桶中的某些或所有对象，或者您也可以使用选择条件来返回存储桶中对象的子集。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 GET Bucket (List Objects) 版本 2。

列表执行效率

存储桶中的密钥总数不会对列表性能产生重大影响。它也不因是否存在 `prefix`、`marker`、`maxkeys` 或 `delimiter` 参数而受到影响。

循环访问多页结果

由于存储桶可以包含几乎无限数量的键，列表查询的完整结果可能会非常大。为了管理大型结果集，Amazon S3 API 支持分页，以将它们分割为多个响应。每个列出键响应将返回一个拥有多达 1000 个键的页面，同时使用指示器来指示响应是否存在截断。您可以发送一系列的列出键请求，直到您收到了所有的键。AmazonSDK 包装库提供相同的分页。

## 示例

在列出存储桶中的所有对象时，请注意，您必须拥有 `s3:ListBucket` 权限。

CLI

list-objects

以下示例使用 `list-objects` 命令显示指定存储桶中所有对象的名称：

```
aws s3api list-objects --bucket text-content --query 'Contents[].{Key: Key, Size: Size}'
```

该示例使用 `--query` 参数筛选 `list-objects` 的输出，使其范围缩小到每个对象的键值和大小

有关对象的更多信息，请参阅 使用 Amazon S3 中的对象。

- 有关 API 详细信息，请参阅《Amazon CLI 命令参考》中的 ListObjects。

ls

下面的示例通过使用 `ls` 命令列出了存储桶中的所有对象和前缀。

要使用此示例命令，请将 *amzn-s3-demo-bucket* 替换为您存储桶的名称。

```
$ aws s3 ls s3://amzn-s3-demo-bucket
```

- 有关高级命令 `ls` 的更多信息，请参阅《Amazon Command Line Interface 用户指南》中的列出存储桶和对象。

PowerShell

适用于 PowerShell 的工具

示例 1：此命令检索有关存储桶“test-files”中所有项目的信息。

```
Get-S3Object -BucketName amzn-s3-demo-bucket
```

示例 2：此命令从存储桶“test-files”中检索有关项目“sample.txt”的信息。

```
Get-S3Object -BucketName amzn-s3-demo-bucket -Key sample.txt
```

示例 3：此命令从存储桶“test-files”中检索有关前缀为“sample”的所有项目的信息。

```
Get-S3Object -BucketName amzn-s3-demo-bucket -KeyPrefix sample
```

- 有关 API 详细信息，请参阅《Amazon Tools for PowerShell Cmdlet 参考》中的 ListObjects。

## 使用文件夹在 Amazon S3 控制台中整理对象

在 Amazon S3 通用存储桶中，对象是主要资源，并且对象存储在存储桶中。Amazon S3 通用存储桶具有扁平结构，而不是类似于您在文件系统中看到的层次结构。不过，为了实现组织简易性，Amazon S3 控制台支持将文件夹概念作为对象分组手段。控制台通过为分组对象使用共享名称前缀来实现此目的。换句话说，分组对象的名称以一个公用字符串开头。这个公用字符串或共享前缀是文件夹名称。对象名称也称为键名称。

例如，您可以通过控制台在通用存储桶中创建名为 photos 的文件夹，并在其中存储名为 myphoto.jpg 的对象。随后，将使用键名 photos/myphoto.jpg 存储对象，其中 photos/ 为前缀。

以下是另外两个示例：

- 如果通用存储桶中有三个对象：logs/date1.txt、logs/date2.txt 和 logs/date3.txt，则控制台会显示名为 logs 的文件夹。如果您在控制台中打开该文件夹，将看到三个对象：date1.txt、date2.txt 和 date3.txt。
- 如果您有名为 photos/2017/example.jpg 的对象，则控制台会显示名为 photos 的文件夹，其中包含文件夹 2017。文件夹 2017 包含对象 example.jpg。

文件夹中可以有文件夹，但存储桶中不能有存储桶。可以直接将对象上传和复制到一个文件夹中。可以创建和删除文件夹以及将文件夹设为公用，但不能对文件夹进行重命名。可以将对象从一个文件夹复制至另一个文件夹。

> **Important**
>
> 当您在 Amazon S3 控制台中创建文件夹时，S3 将创建一个 0 字节对象。此对象键设置为您提供的文件夹名称加上尾随的正斜杠 (/) 字符。例如，在 Amazon S3 控制台中，如果您在存储桶中创建一个名为 photos 的文件夹，Amazon S3 控制台将使用键 photos/ 创建一个 0 字节的对象。控制台创建这个对象是为了支持文件夹的概念。
>
> 此外，任何使用尾部正斜杠字符 (/) 命名的预先存在的对象都将显示为 Amazon S3 控制台中的文件夹。例如，具有键名称 examplekeyname/ 的对象在 Amazon S3 控制台中显示为文件夹，而不显示为对象。否则，其行为与任何其它对象一样，可以通过 Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 REST API 进行查看和操作。此外，您无法使用

Amazon S3 控制台上传键名称中有尾部正斜杠字符 (/) 字符的对象。但是，通过使用 Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 REST API，可以上传名称中有尾部正斜杠字符 (/) 的对象。
此外，Amazon S3 控制台不像对待其它对象那样显示文件夹对象的内容和元数据。当使用控制台复制名称中有尾部正斜杠字符 (/) 的对象时，将在目标位置创建一个新文件夹，但不会复制对象的数据和元数据。此外，对象键名称中的正斜杠 (/) 可能需要特殊处理。有关更多信息，请参阅 为 Amazon S3 对象命名。

要在目录存储桶中创建文件夹，请上传文件夹。有关更多信息，请参阅 将对象上传到目录存储桶。

主题


- 创建文件夹
- 将文件夹设为公用
- 计算文件夹大小
- 删除文件夹


## 创建文件夹

本部分介绍如何使用 Amazon S3 控制台创建文件夹。

**Important**

如果存储桶策略阻止在没有标签、元数据或访问控制列表（ACL）被授权者的情况下将对象上传到此存储桶，则您无法使用以下过程创建文件夹。而应改为上传空文件夹，并在上传配置中指定以下设置。

如何创建文件夹

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在存储桶列表中，选择要在其中创建文件夹的存储桶的名称。
4. 在对象选项卡上，选择创建文件夹。
5. 输入文件夹的名称（例如，**`favorite-pics`**）。

> **Note**
>
> 文件夹名称受某些限制和准则的约束，并且被视为对象的对象键名称的一部分，该名称限制为 1024 字节。有关更多信息，请参阅 the section called “为对象命名”。

6. （可选）如果存储桶策略要求使用特定的加密密钥对于对象进行加密，则在服务器端加密下，您必须在创建文件夹时选择指定加密密钥并指定相同的加密密钥。否则，文件夹创建将失败。
7. 请选择 Create folder（创建文件夹）。

## 将文件夹设为公用

我们建议禁止所有对 Amazon S3 文件夹和存储桶的公有访问，除非您特别需要公有文件夹或存储桶。当您将文件夹设为公有时，Internet 上的任何人都可以查看该文件夹中分组的所有对象。

在 Amazon S3 控制台中，您可以将文件夹设为公有。您还可以通过创建存储桶策略来将文件夹设为公有，该策略通过前缀限制数据访问权限。有关更多信息，请参阅 Amazon S3 的身份和访问管理。

> **Warning**
>
> 在 Amazon S3 控制台中将文件夹设为公有后，就不能再将其设为私有。而是必须对公有文件夹中的每个单独的对象设置权限，以使对象不具备公有访问。有关更多信息，请参阅 配置 ACL。

主题


- 计算文件夹大小
- 删除文件夹


## 计算文件夹大小

本节介绍如何使用 Amazon S3 控制台计算文件夹的大小。

计算文件夹的大小

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。

3. 在通用存储桶列表中，选择在其中存储文件夹的存储桶的名称。
4. 在对象列表中，选中文件夹名称旁边的复选框。
5. 选择 Actions（操作），然后选择 Calculate total size（计算总大小）。

> **Note**
>
> 在您导航离开该页面后，文件夹信息（包括总大小）不再可用。如果您想再次看到总大小，则必须再次计算该值。

> **Important**
>
> 当您对存储桶中的指定对象或文件夹使用 Calculate total size（计算总大小）操作时，Amazon S3 会计算对象总数和总存储大小。但是，在对象总数或总大小中并不计算未完成或正在进行的分段上传以及以前或非当前的版本。此操作仅针对存储在存储桶中的每个对象的当前或最新版本计算对象总数和总大小。
>
> 例如，如果存储桶中有某个对象的两个版本，则 Amazon S3 中的存储计算器仅将它们计为一个对象。因此，在 Amazon S3 控制台中计算的对象总数可能不同于 S3 Storage Lens 存储统计管理工具中显示的对象计数指标以及 Amazon CloudWatch 指标 `NumberOfObjects` 报告的数量。同样，总存储大小也可能不同于 S3 Storage Lens 存储统计管理工具中显示的 Total Storage（总存储）指标和 CloudWatch 中显示的 `BucketSizeBytes` 指标。

## 删除文件夹

本节介绍如何使用 Amazon S3 控制台从 S3 存储桶中删除文件夹。

有关 Amazon S3 特征和定价的信息，请参阅 Amazon S3。

### 要从 S3 存储桶中删除文件夹

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在通用存储桶列表中，选择要从中删除文件夹的存储桶的名称。
4. 在对象列表中，选中您要删除的文件夹和对象旁的复选框。

5. 选择删除。
6. 在删除对象页面上，验证您选择删除的文件夹和对象的名称是否列在指定的对象下。
7. 在 Delete objects (删除对象) 框中，输入 **`delete`**，然后选择 Delete objects (删除对象)。

> **Warning**
>
> 此操作将删除所有指定的对象。删除文件夹时，请等待删除操作完成，然后再将新对象添加到文件夹。否则，新对象也可能会被删除。

## 在 Amazon S3 控制台中查看对象属性

您可以使用 Amazon S3 控制台查看对象的属性，包括存储类、加密设置、标签和元数据。

查看对象的属性

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶或目录存储桶。
3. 在存储桶列表中，选择包含对象的存储桶的名称。
4. 在 Objects（对象）列表中，请选择要查看其属性的对象的名称。

   对象的 Object overview（对象概述）将打开。您可以向下滚动以查看对象属性。
5. 在对象概述页面上，您可以查看或配置对象的以下属性。

> **Note**
>
> - 如果您更改存储类、加密或元数据属性，则将创建一个新对象来替换旧对象。如果启用 S3 版本控制，则会创建对象的新版本，而现有对象将变为旧版本。更改属性的角色也会成为新对象或（对象版本）的拥有者。
> - 如果您要更改具有用户定义标签的对象的存储类、加密或元数据属性，您必须拥有 `s3:GetObjectTagging` 权限。如果您要对没有用户定义标签但大小超过 16 MB 的对象更改这些属性，您还必须拥有 `s3:GetObjectTagging` 权限。
>
>   如果目标存储桶策略拒绝 `s3:GetObjectTagging` 操作，则将更新对象的这些属性，但将从对象中移除用户定义的标签，并且您将收到错误。

a. Storage class (存储类) – Amazon S3 中的每个对象都有与之关联的存储类。您选择使用的存储类取决于您访问对象的频率。通用存储桶中 S3 对象的默认存储类是 STANDARD。目录存储桶中 S3 对象的默认存储类是 S3 Express One Zone。您可以选择在上传对象使用的存储类。有关存储类的更多信息，请参阅 了解和管理 Amazon S3 存储类。

   要在将对象上传到通用存储桶后更改存储类，请选择存储类。请选择您希望的存储类，然后选择 Save（保存）。

   > **Note**
   >
   > 目录存储桶中对象的存储类无法更改。

b. 服务器端加密设置 – 您可以使用服务器端加密来加密 S3 对象。有关更多信息，请参阅使用 Amazon KMS (SSE-KMS) 指定服务器端加密或指定具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）。

c. 元数据 – Amazon S3 中的每个对象都有一组表示其元数据的名称/值对。有关将元数据添加到 S3 对象的信息，请参阅在 Amazon S3 控制台中编辑对象元数据。

d. 标签：您可以通过向通用存储桶中的 S3 对象添加标签来对存储进行分类。有关更多信息，请参阅 使用标签对存储进行分类。

e. 对象锁定依法保留和保留：您可以防止通用存储桶中的对象被删除。有关更多信息，请参阅使用对象锁定以锁定对象。

## 使用标签对存储进行分类

使用对象标签对存储进行分类。每个标签都是一个键-值对。

您可以将标签添加到新对象（当您上传新对象时），也可以将标签添加到现有对象。

- 您最多可以将 10 个标签与对象关联。与对象关联的标签必须具有唯一的标签键。
- 标签键的长度最大可以为 128 个 Unicode 字符，标签值的长度最大可以为 256 个 Unicode 字符。Amazon S3 对象标签在内部以 UTF-16 表示。请注意，采用 UTF-16 时，字符占用 1 或 2 个字符位置。
- 键和值区分大小写。
- 有关标签限制的更多信息，请参阅《Amazon 账单与成本管理用户指南》中的 User-defined tag restrictions。有关基本标签限制，请参阅《Amazon EC2 用户指南》中的标签限制。

### 示例

请考虑以下标签示例：

#### Example PHI 信息

假设某个对象包含受保护医疗信息 (PHI) 数据。您可以使用以下键/值对标记该对象。

```
PHI=True
```

或

```
Classification=PHI
```

#### Example 项目文件

假设您将项目文件存储在 S3 桶中。您可以使用一个名为 `Project` 的键和一个值标记这些对象，如下所示。

```
Project=Blue
```

#### Example 多个标签

您可以将多个标签添加到一个对象，如下所示。

```
Project=x
Classification=confidential
```

### 键名前缀和标签

您还可以使用对象键名前缀来分类存储。但是，基于前缀的分类是一维的。请考虑以下对象键名：

```
photos/photo1.jpg
project/projectx/document.pdf
project/projecty/document2.pdf
```

这些键名具有前缀 `photos/`、`project/projectx/` 和 `project/projecty/`。这些前缀支持一维分类。即，一个前缀下的一切都属于一个类别。例如，前缀 `project/projectx` 可确定与项目 x 相关的所有文档。

利用标签，您现在获得了另一个维度。如果您希望 photo1 属于项目 x 类别，则可以相应地标记该对象。

其他优势

除了数据分类之外，标签还提供了下列好处：

- 对象标签支持权限的精细访问控制。例如，您可以向用户授予仅读取带有特定标签的对象的权限。
- 对象标签支持精细的对象生命周期管理，在其中，除了在生命周期规则中指定键名前缀之外，还可以指定基于标签的筛选条件。
- 使用 Amazon S3 分析时，您可以配置筛选条件，以便按对象标签、键名前缀或前缀和标签的组合对对象进行分组以进行分析。
- 您还可以自定义 Amazon CloudWatch 指标以按特定标签筛选条件显示信息。以下各节提供了详细信息。

> **Important**
>
> 使用标签来标记包含机密数据（如 personally identifiable information (PII) 或受保护医疗信息 (PHI)）的对象是可以接受的。但标签本身不应包含任何机密信息。

通过单个请求将对象标签集添加到多个 Amazon S3 对象

要使用单个请求向多个 Amazon S3 对象添加对象标签集，您可以使用 S3 分批操作。您为 S3 批量操作提供要操作的对象列表。S3 批量操作调用相应的 API 操作来执行指定的操作。单个批量操作任务可对包含 EB 级数据的数十亿个对象执行指定操作。

S3 批量操作特征包括跟踪进度、发送通知并存储所有操作的详细完成报告，从而提供完全托管、可审核的无服务器体验。您可以通过 Amazon S3 控制台、Amazon CLI、Amazon SDK 或 REST API 使用 S3 批量操作。有关更多信息，请参阅 the section called “批量操作基础知识”。

有关对象标签的更多信息，请参阅 管理对象标签。

## 与对象标签相关的 API 操作

Amazon S3 支持特定于对象标签的以下 API 操作：

对象 API 操作

- PUT 对象标签 – 替换对象上的标签。您可以在请求正文中指定标签。使用此 API 的对象标签管理有两个不同的情形。

- 对象没有标签 - 利用此 API，您可以将一组标签添加到某个对象 (该对象没有以前的标签)。
- 对象有一组现有标签 - 要修改现有标签，您必须先检索现有标签集，在客户端侧修改它，然后使用此 API 替换它。

> **Note**
>
> 如果您发送带有空标签集的此请求，Amazon S3 将删除对象上的现有标签集。如果您使用此方法，则将需为套餐 1 请求 (PUT) 付费。有关更多信息，请参阅 Amazon S3 定价。DELETE 对象标签请求优先进行，因为它可获得相同的结果而不会产生费用。

- GET 对象标签 – 返回与某个对象关联的标签集。Amazon S3 将在响应正文中返回对象标签。
- DELETE 对象标签 – 删除与某个对象关联的标签集。

支持标签的其他 API 操作

- PUT 对象和启动分段上传 – 您可以在创建对象时指定标签。您将使用 `x-amz-tagging` 请求标头指定标签。
- GET 对象 – Amazon S3 不会返回标签集，而会在 `x-amz-tag-count` 标头中返回对象标签计数（仅当请求者有权读取标签时），因为标头响应大小限制为 8000 个字节。如果要查看标签，您应该再发出一个 GET 对象标签 API 操作请求。
- POST 对象 – 您可以在 POST 请求中指定标签。

  只要请求中的标签不超过 8 K 个字节的 HTTP 请求标头大小限制，您就可以使用 PUT Object API 创建带标签的对象。如果您指定的标签超过了标头大小限制，您可以使用将标签包含在正文中的此 POST 方法。

  PUT 对象 – 复制 – 您可以在请求中指定 `x-amz-tagging-directive` 以指示 Amazon S3 复制（默认行为）标签或将标签替换为请求中提供的一组新标签。

请注意以下几点：

- S3 对象标签非常一致。有关更多信息，请参阅 Amazon S3 数据一致性模型。

## 其他配置

本节介绍对象标签如何与其他配置关联。

对象标签和生命周期管理

在桶生命周期配置中，您可以指定筛选条件以选择该规则适用的一部分对象。您可以基于键名前缀、对象标签或两者指定筛选条件。

假设您将照片（原始格式和已完成格式）存储在 Amazon S3 桶中。您可以按下面所示标记这些对象。

```
phototype=raw
or
phototype=finished
```

您可能考虑有时候在创建原始照片后将其存档到 S3 Glacier。您可以在生命周期规则中配置一个筛选条件，用于确定一部分包含特定标签 (photos/) 且带有键名称前缀 (phototype=raw) 的对象。

有关更多信息，请参阅 管理对象的生命周期。

对象标签和复制

如果您在桶上配置了复制，Amazon S3 将复制标签，前提是您向 Amazon S3 授予了读取标签的权限。有关更多信息，请参阅 设置实时复制概述。

对象标记事件通知

您可以设置 Amazon S3 事件通知以在添加对象标签或从对象中删除时接收通知。s3:ObjectTagging:Put 事件类型会在对象上放置标签或现有标签更新时通知您。当从对象中移除标签时，s3:ObjectTagging:Delete 事件类型会通知您。有关更多信息，请参阅 Enabling event notifications（启用事件通知）。

有关对象标签的更多信息，请参阅以下主题：

主题

- 标签和访问控制策略
- 管理对象标签

## 标签和访问控制策略

您还可以使用权限策略（桶和用户策略）管理对象标签相关权限。有关策略操作，请参阅以下主题：

- 对象操作
- 存储桶操作

对象标签支持用于管理权限的精细访问控制。您可以基于对象标签授予条件权限。Amazon S3 支持以下条件键，这些键可用于授予基于对象标签的条件权限：

- `s3:ExistingObjectTag/<tag-key>` - 使用此条件键可验证现有对象标签是否有特定标签键和值。

  > **Note**
  >
  > 当授予 PUT Object 和 DELETE Object 操作的权限时，此条件键不受支持。也就是说，您无法创建这样一个策略：允许或拒绝用户基于对象的现有标签删除或覆盖该对象。

- `s3:RequestObjectTagKeys` - 使用此条件键可限制要在对象上允许的标签键。当使用 PutObjectTagging 和 PutObject 以及 POST 对象请求将标签添加到对象时，这很有用。
- `s3:RequestObjectTag/<tag-key>` - 使用此条件键可限制要在对象上允许的标签键和值。当使用 PutObjectTagging 和 PutObject 以及 POST 桶请求将标签添加到对象时，这很有用。

有关特定于 Amazon S3 服务的条件键的完整列表，请参阅 使用条件键的存储桶策略示例。以下权限策略说明了对象标签如何支持精细访问权限管理。

Example 1：允许用户仅读取具有特定标签和键值的对象

以下权限策略限制用户只能读取具有 `environment: production` 标签键和值的对象。请注意，该策略使用 `s3:ExistingObjectTag` 条件键来指定标签键和值。

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Principal": {
      "AWS": [
        "arn:aws:iam::111122223333:role/JohnDoe"
      ]
    },
    "Effect": "Allow",
    "Action": ["s3:GetObject", "s3:GetObjectVersion"],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
    "Condition": {
      "StringEquals":
        {"s3:ExistingObjectTag/environment": "production"}
    }
  }
```

```
  ]
}
```

Example 2：限制用户可以添加哪些对象标签键

以下权限策略将向用户授予执行 s3:PutObjectTagging 操作的权限，这使用户可以将标签添加到现有对象。条件使用 s3:RequestObjectTagKeys 条件键指定允许的标签键，例如 Owner 或 CreationDate。有关更多信息，请参阅《IAM 用户指南》中的创建测试多个键值的条件。

该策略确保在请求中指定的每个标签键都是授权的标签键。条件中的 ForAnyValue 限定符确保请求中必须至少存在指定的值之一。

```
{
   "Version": "2012-10-17",
  "Statement": [
    {"Principal":{"AWS":[
            "arn:aws:iam::111122223333:role/JohnDoe"
         ]
       },
 "Effect": "Allow",
      "Action": [
        "s3:PutObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {"ForAnyValue:StringEquals": {"s3:RequestObjectTagKeys": [
            "Owner",
            "CreationDate"
          ]
        }
      }
    }
  ]
}
```

Example 3：在允许用户添加对象标签时需要特定的标签键和值

以下示例策略将向用户授予执行 s3:PutObjectTagging 操作的权限，这使用户可以将标签添加到现有对象。条件要求用户包含值设置为 *X* 的特定标签键（如 *Project*）。

```
{
```

```
   "Version": "2012-10-17",
  "Statement": [
    {"Principal":{"AWS":[
       "arn:aws:iam::111122223333:user/JohnDoe"
         ]
       },
      "Effect": "Allow",
      "Action": [
        "s3:PutObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {"StringEquals": {"s3:RequestObjectTag/Project": "X"
        }
      }
    }
  ]
}
```

## 管理对象标签

本节介绍如何使用适用于 Java 和 .NET 的 Amazon 开发工具包或 Amazon S3 控制台管理对象标签。

对象标签为您提供了对通用存储桶中的存储进行分类的方法。每个标签都是遵循以下规则的键值对：

- 您最多可以将 10 个标签与对象关联。与对象关联的标签必须具有唯一的标签键。
- 标签键的长度最大可以为 128 个 Unicode 字符，标签值的长度最大可以为 256 个 Unicode 字符。Amazon S3 对象标签在内部以 UTF-16 表示。请注意，采用 UTF-16 时，字符占用 1 或 2 个字符位置。
- 键和值区分大小写。

有关对象标签的更多信息，请参阅 使用标签对存储进行分类。有关标签限制的更多信息，请参阅《Amazon 账单与成本管理 用户指南》中的用户定义的标签限制。

使用 S3 控制台

向对象添加标签

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。

2. 在左侧导航窗格中，选择通用存储桶。
3. 在存储桶列表中，选择包含对象的存储桶的名称。
4. 选中待更改对象的名称左侧的复选框。
5. 在操作菜单上选择编辑标签。
6. 查看列出的对象，然后选择添加标签。
7. 每个对象标签都是一个键值对。输入 Key (键) 和 Value (值)。要添加另一个标签，请选择 Add Tag (添加标签)。

   您最多可以为一个对象输入 10 个标签。
8. 选择保存更改。

   Amazon S3 会将标签添加给指定对象。

有关更多信息，另请参阅本指南中的 在 Amazon S3 控制台中查看对象属性 和 上传对象。

使用 Amazon 开发工具包

Java

以下示例演示如何使用适用于 Java 的 Amazon SDK为新对象设置标签并检索或替换现有对象的标签。有关对象标签的更多信息，请参阅使用标签对存储进行分类。有关创建和测试有效示例的说明，请参阅《适用于 Java 的 Amazon SDK 开发人员指南》中的入门。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.io.File;
import java.util.ArrayList;
import java.util.List;

public class ManagingObjectTags {

    public static void main(String[] args) {
        Regions clientRegion = Regions.DEFAULT_REGION;
```

```
        String bucketName = "*** Bucket name ***";
        String keyName = "*** Object key ***";
        String filePath = "*** File path ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Create an object, add two new tags, and upload the object to Amazon
 S3.
            PutObjectRequest putRequest = new PutObjectRequest(bucketName, keyName,
 new File(filePath));
            List<Tag> tags = new ArrayList<Tag>();
            tags.add(new Tag("Tag 1", "This is tag 1"));
            tags.add(new Tag("Tag 2", "This is tag 2"));
            putRequest.setTagging(new ObjectTagging(tags));
            PutObjectResult putResult = s3Client.putObject(putRequest);

            // Retrieve the object's tags.
            GetObjectTaggingRequest getTaggingRequest = new
 GetObjectTaggingRequest(bucketName, keyName);
            GetObjectTaggingResult getTagsResult =
 s3Client.getObjectTagging(getTaggingRequest);

            // Replace the object's tags with two new tags.
            List<Tag> newTags = new ArrayList<Tag>();
            newTags.add(new Tag("Tag 3", "This is tag 3"));
            newTags.add(new Tag("Tag 4", "This is tag 4"));
            s3Client.setObjectTagging(new SetObjectTaggingRequest(bucketName,
 keyName, new ObjectTagging(newTags)));
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

以下示例演示如何使用适用于 .NET 的 Amazon SDK为新对象设置标签并检索或替换现有对象的标签。有关对象标签的更多信息，请参阅使用标签对存储进行分类。

有关设置和运行代码示例的信息，请参阅《适用于 .NET 的 Amazon SDK 开发人员指南》中的适用于 .NET 的 Amazon SDK 入门。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    public class ObjectTagsTest
    {
        private const string bucketName = "*** bucket name ***";
        private const string keyName = "*** key name for the new object ***";
        private const string filePath = @"*** file path ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;

        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            PutObjectWithTagsTestAsync().Wait();
        }

        static async Task PutObjectWithTagsTestAsync()
        {
            try
            {
                // 1. Put an object with tags.
                var putRequest = new PutObjectRequest
                {
                    BucketName = bucketName,
```

```
                    Key = keyName,
                    FilePath = filePath,
                    TagSet = new List<Tag>{
                        new Tag { Key = "Keyx1", Value = "Value1"},
                        new Tag { Key = "Keyx2", Value = "Value2" }
                    }
                };

                PutObjectResponse response = await
client.PutObjectAsync(putRequest);
                // 2. Retrieve the object's tags.
                GetObjectTaggingRequest getTagsRequest = new GetObjectTaggingRequest
                {
                    BucketName = bucketName,
                    Key = keyName
                };

                GetObjectTaggingResponse objectTags = await
client.GetObjectTaggingAsync(getTagsRequest);
                for (int i = 0; i < objectTags.Tagging.Count; i++)
                    Console.WriteLine("Key: {0}, Value: {1}",
objectTags.Tagging[i].Key, objectTags.Tagging[i].Value);


                // 3. Replace the tagset.

                Tagging newTagSet = new Tagging();
                newTagSet.TagSet = new List<Tag>{
                    new Tag { Key = "Key3", Value = "Value3"},
                    new Tag { Key = "Key4", Value = "Value4" }
                };


                PutObjectTaggingRequest putObjTagsRequest = new
PutObjectTaggingRequest()
                {
                    BucketName = bucketName,
                    Key = keyName,
                    Tagging = newTagSet
                };
                PutObjectTaggingResponse response2 = await
client.PutObjectTaggingAsync(putObjTagsRequest);

                // 4. Retrieve the object's tags.
```

```
                GetObjectTaggingRequest getTagsRequest2 = new
GetObjectTaggingRequest();
                getTagsRequest2.BucketName = bucketName;
                getTagsRequest2.Key = keyName;
                GetObjectTaggingResponse objectTags2 = await
client.GetObjectTaggingAsync(getTagsRequest2);
                for (int i = 0; i < objectTags2.Tagging.Count; i++)
                    Console.WriteLine("Key: {0}, Value: {1}",
objectTags2.Tagging[i].Key, objectTags2.Tagging[i].Value);

            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine(
                        "Error encountered ***. Message:'{0}' when writing an
object"
                        , e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine(
                    "Encountered an error. Message:'{0}' when writing an object"
                    , e.Message);
            }
        }
    }
}
```

# 使用预签名 URL 下载和上传对象

您可以使用预签名 URL 授予对 Amazon S3 中对象的限时访问权限，而不更新存储桶策略。可以在浏览器中输入预签名 URL，或者程序使用预签名 URL 来下载对象。预签名 URL 使用的凭证是生成该 URL 的 Amazon 用户的凭证。

还可以使用预签名 URL 来允许他人将特定对象上传到您的 Amazon S3 存储桶。这允许在不要求另一方拥有 Amazon 安全凭证或权限的情况下进行上传。如果具有相同键的对象已存在于在预签名 URL 中指定的存储桶中，则 Amazon S3 将现有对象替换为上传的对象。

在到期日期和时间之前，可以多次使用预签名 URL。

创建预签名 URL 时，必须提供您的安全凭证，然后指定以下内容：

- 一个 Amazon S3 存储桶
- 对象键（如果将在您的 Amazon S3 存储桶中下载此对象，则一旦上传，这就是要上传的文件名）
- HTTP 方法（GET 用于下载对象、PUT 用于上传、HEAD 用于读取对象元数据等）
- 过期时间间隔

目前，Amazon S3 预签名 URL 不支持在上传对象时使用以下数据完整性校验和算法（CRC32、CRC32C、SHA-1、SHA-256）。要在上传后验证对象的完整性，您可以在使用预签名 URL 上传对象时提供对象的 MD5 摘要。有关对象完整性的更多信息，请参阅在 Amazon S3 中检查对象完整性。

主题


- 谁可以创建预签名 URL
- 预签名 URL 的到期时间
- 限制预签名 URL 功能
- 使用预签名 URL 共享对象
- 使用预签名 URL 上传对象


## 谁可以创建预签名 URL

具有有效安全凭证的任何人都可以创建预签名 URL。但对于成功地访问对象的人来说，必须由拥有执行预签名 URL 所基于的操作权限的人创建预签名 URL。

以下各个类型的凭证可用于创建预签名 URL：

- IAM 实例配置文件 – 有效期最长 6 小时。
- Amazon Security Token Service – 有效期为最长 36 小时（使用长期安全凭证进行签名时），或为临时凭证的持续时间，以先到者为准。
- IAM 用户 – 使用 Amazon 签名版本 4 时，有效期最长 7 天。

  要创建有效期最长为 7 天的预签名 URL，请首先将 IAM 用户凭证（访问密钥和私有密钥）委托给用于创建预签名 URL 的方法。

> **Note**
>
> 如果您使用临时凭证创建了预签名 URL，则此 URL 将在凭证过期时过期。通常，当您用于创建预签名 URL 的凭证被撤销、删除或停用时，预签名 URL 就会到期。即使创建的 URL 的过期时间更晚，也是如此。有关临时安全凭证生命周期，请参阅《IAM 用户指南》中的比较 Amazon STS API 操作。

## 预签名 URL 的到期时间

预签名 URL 在生成 URL 时指定的时间段内保持有效。如果使用 Amazon S3 控制台创建预签名 URL，过期时间可设置为 1 分钟到 12 小时之间。如果您使用 Amazon CLI 或 Amazon SDK，则过期时间可设置为多达 7 天。

如果您使用临时令牌创建了预签名 URL，则此 URL 将在该令牌到期时到期。通常，当您用于创建预签名 URL 的凭证被撤销、删除或停用时，预签名 URL 就会到期。即使创建的 URL 的过期时间更晚，也是如此。有关您使用的凭证如何影响到期时间的更多信息，请参阅谁可以创建预签名 URL。

在发出 HTTP 请求时，Simple Storage Service (Amazon S3) 会检查签名 URL 的到期日期和时间。例如，如果客户端刚好在到期时间之前开始下载某个大型文件，即使在下载过程中超过到期时间，下载也会继续进行。但如果连接断开，在客户端试图在超过到期时间后重新开始下载，则下载将会失败。

## 限制预签名 URL 功能

预签名 URL 的功能受创建它的用户的权限所限制。预签名 URL 实质上是一种不记名令牌，向持有相关 URL 的人授予了访问权限。因此，我们建议您适当地保护它们。以下是一些可用来限制使用预签名 URL 的方法。

Amazon 签名版本 4（SigV4）

使用 Amazon 签名版本 4（SigV4）对预签名 URL 请求进行身份认证时要强制执行特定的行为，您可以在存储桶策略和接入点策略中使用条件键。例如，以下存储桶策略使用 `s3:signatureAge` 条件，当相关签名的存在时间超过 10 分钟时，拒绝对于 *`amzn-s3-demo-bucket`* 存储桶中对象的任何 Amazon S3 预签名 URL 请求。要使用此示例，请将 *`user input placeholders`* 替换为您自己的信息。

```
{
   "Version": "2012-10-17",
```

```
   "Statement": [
      {
         "Sid": "Deny a presigned URL request if the signature is more than 10 min
 old",
         "Effect": "Deny",
         "Principal": {"AWS":"*"},
         "Action": "s3:*",
         "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
         "Condition": {
            "NumericGreaterThan": {
               "s3:signatureAge": 600000
            }
         }
      }
   ]
}
```

有关策略键相关的 Amazon 签名版本 4 的更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 Amazon 签名版本 4 身份认证。

网络路径限制

如果您想限制使用预签名 URL 和 Amazon S3 对特定网络路径的所有访问权限，则可以编写 Amazon Identity and Access Management（IAM）策略。您可以在进行调用的 IAM 主体、Amazon S3 存储桶或两者上设置这些策略。

对 IAM 主体实施网络路径限制后，要求拥有这些凭证的用户从指定的网络发出请求。对存储桶或接入点实施限制后，要求对该资源的所有请求都必须来自指定的网络。这些限制也适用于预签名 URL 以外的场景。

您使用的 IAM 全局条件键取决于端点的类型。如果您正在对 Amazon S3 使用公有端点，请使用 `aws:SourceIp`。如果您正在使用虚拟私有云（VPC）端点访问 Amazon S3 存储桶，请使用 `aws:SourceVpc` 或 `aws:SourceVpce`。

以下 IAM 策略语句要求主体仅从指定的网络范围访问。Amazon使用此策略语句时，所有访问都必须来自该范围。这包括有人对于 Amazon S3 使用预签名 URL 的情况。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
{
    "Sid": "NetworkRestrictionForIAMPrincipal",
    "Effect": "Deny",
```

```
    "Action": "*",
    "Resource": "*",
    "Condition": {
        "NotIpAddressIfExists": {"aws:SourceIp": "IP-address-range"},
        "BoolIfExists": {"aws:ViaAWSService": "false"}
    }
}
```

## 使用预签名 URL 共享对象

默认情况下，所有 Amazon S3 对象都是私有的，只有对象拥有者才具有访问它们的权限。但是，对象拥有者可以通过创建预签名 URL 与其他人共享对象。预签名 URL 使用安全凭证来授予下载对象的限时权限。可以在浏览器中输入此 URL，或者程序使用此 URL 来下载对象。预签名 URL 使用的凭证是生成该 URL 的 Amazon 用户的凭证。

有关预签名 URL 的一般信息，请参阅使用预签名 URL 下载和上传对象。

您可以使用 Amazon S3 控制台、适用于 Visual Studio 的 Amazon Explorer 或 Amazon Toolkit for Visual Studio Code 创建预签名 URL 来共享对象，而不需要编写任何代码。也可以使用 Amazon Command Line Interface（Amazon CLI）或 Amazon SDK 以编程方式生成预签名 URL。

使用 S3 控制台

您可以使用 Amazon S3 控制台，按照以下步骤生成预签名 URL 来共享对象。使用控制台时，预签名 URL 的最长过期时间为自创建时起 12 小时。

使用 Amazon S3 控制台生成预签名 URL

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 在 Buckets（存储桶）列表中，请选择包含要为其生成预签名 URL 的对象的存储桶的名称。
4. 在 Objects（对象）列表中，选择要为其生成预签名 URL 的对象。
5. 在对象操作菜单上，请选择使用预签名 URL 共享。
6. 指定您希望的预签名 URL 有效时间长度。
7. 请选择 Create presigned URL（创建预签名 URL）。
8. 出现确认时，URL 将自动复制到剪贴板。如果您需要再次复制预签名 URL，您将看到一个按钮，用于复制该 URL。

使用 Amazon CLI

以下示例 Amazon CLI 命令生成一个预签名 URL，以共享 Amazon S3 存储桶中的对象。使用 Amazon CLI 时，预签名 URL 的最长过期时间为自创建时起 7 天。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3 presign s3://amzn-s3-demo-bucket/mydoc.txt --expires-in 604800
```

> **Note**
>
> 对于 2019 年 3 月 20 日之后启动的所有 Amazon Web Services 区域，您需要随请求指定 endpoint-url 和 Amazon Web Services ##。有关所有 Amazon S3 区域和端点的列表，请参阅《Amazon 一般参考》中的区域和端点。

```
aws s3 presign s3://amzn-s3-demo-bucket/mydoc.txt --expires-in 604800 --region af-south-1 --endpoint-url https://s3.af-south-1.amazonaws.com
```

有关更多信息，请参阅 Amazon CLI 命令参考 中的 presign。

使用 Amazon SDK

有关使用 Amazon SDK 生成预签名 URL 来共享对象的示例，请参阅使用 Amazon SDK 为 Amazon S3 创建预签名 URL。

使用 Amazon SDK 生成预签名 URL 时，最长到期时间为创建之时起 7 天。

> **Note**
>
> 对于 2019 年 3 月 20 日之后启动的所有 Amazon Web Services 区域，您需要随请求指定 endpoint-url 和 Amazon Web Services ##。有关所有 Amazon S3 区域和端点的列表，请参阅《Amazon 一般参考》中的区域和端点。

> **Note**
>
> 使用 Amazon SDK 时，Tagging 属性必须是标题而不是查询参数。所有其他属性都可以作为预签名 URL 的参数传递。

使用 Amazon Toolkit for Visual Studio (Windows)

> **Note**
>
> 目前，Amazon Toolkit for Visual Studio 不支持 Visual Studio for Mac。

1. 按照《Amazon Toolkit for Visual Studio User Guide》中的 Installing and setting up the Toolkit for Visual Studio 中的说明安装 Amazon Toolkit for Visual Studio。
2. 使用以下步骤（《Amazon Toolkit for Visual Studio 用户指南》中的连接到 Amazon）连接到 Amazon。
3. 在标有 Amazon 各区服务浏览器的左侧面板中，双击包含您的对象的存储桶。
4. 右键单击要为其生成预签名 URL 的对象，然后选择创建预签名 URL...。
5. 在弹出窗口中，设置预签名 URL 的到期日期和时间。
6. 应根据您选择的对象预填充对象密钥。
7. 选择 GET 可指定此预签名 URL 将用于下载对象。
8. 选择 Generate（生成）按钮。
9. 要将此 URL 复制到剪贴板，请选择 Copy（复制）。
10. 要使用生成的预签名 URL，请将该 URL 粘贴到任何浏览器中。

使用 Amazon Toolkit for Visual Studio Code

如果您使用的是 Visual Studio 代码，可以使用 Amazon Toolkit for Visual Studio Code 生成预签名 URL 来共享对象的，而不需要编写任何代码。有关一般信息，请参阅《Amazon Toolkit for Visual Studio Code 用户指南》中的 Amazon Toolkit for Visual Studio Code。

有关如何安装 Amazon Toolkit for Visual Studio Code 的说明，请参阅《Amazon Toolkit for Visual Studio Code 用户指南》中的安装 Amazon Toolkit for Visual Studio Code。

1. 使用以下步骤（《Amazon Toolkit for Visual Studio Code 用户指南》中的连接到 Amazon Toolkit for Visual Studio Code）连接到 Amazon。
2. 在 Visual Studio 代码中选择左侧面板上的 Amazon 徽标。
3. 在资源管理器下，选择 S3。
4. 选择存储桶和文件，然后打开上下文菜单（右键单击）。
5. 选择生成预签名 URL，然后设置过期时间（以分钟为单位）。
6. 按 Enter，预签名 URL 将复制到剪贴板。

## 使用预签名 URL 上传对象

您可以使用预签名 URL 来允许他人将对象上传到您的 Amazon S3 存储桶。使用预签名 URL 将允许在不要求另一方拥有 Amazon 安全凭证或权限的情况下进行上传。预签名 URL 受创建它的用户的权限所限制。也即，如果您收到预签名 URL 来上传对象，则仅当该 URL 的创建者拥有上传该对象所需的权限时，您才能上传对象。

当有人使用该 URL 上传对象时，Amazon S3 将在指定的存储桶中创建对象。如果存储桶中已存在具有预签名 URL 中指定的相同键的对象，则 Amazon S3 会将现有对象替换为上传的对象。上传后，存储桶拥有者将拥有该对象。

有关预签名 URL 的一般信息，请参阅使用预签名 URL 下载和上传对象。

可以使用适用于 Visual Studio 的 Amazon Explorer 生成预签名 URL 来上传对象，而不需要编写任何代码。也可以使用 Amazon SDK 以编程方式生成预签名 URL。

> **Note**
>
> 目前，Amazon Toolkit for Visual Studio 不支持 Visual Studio for Mac。

使用 Amazon Toolkit for Visual Studio (Windows)

1. 按照《Amazon Toolkit for Visual Studio User Guide》中的 Installing and setting up the Toolkit for Visual Studio 中的说明安装 Amazon Toolkit for Visual Studio。
2. 使用以下步骤（《Amazon Toolkit for Visual Studio 用户指南》中的连接到 Amazon）连接到 Amazon。
3. 在标有 Amazon 各区服务浏览器的左侧面板中，右键单击要向其中上传对象的存储桶。

4. 选择创建预签名 URL...。
5. 在弹出窗口中，设置预签名 URL 的到期日期和时间。
6. 在对象键中，设置要上传的文件的名称。您上传的文件必须与该名称完全匹配。如果具有相同对象键的对象已位于存储桶中，Amazon S3 会将现有对象替换为新上传的对象。
7. 选择 PUT 可指定此预签名 URL 将用于上传对象。
8. 选择 Generate（生成）按钮。
9. 要将此 URL 复制到剪贴板，请选择 Copy（复制）。
10. 要使用此 URL，您可以通过 `curl` 命令发送 PUT 请求。包括您的文件的完整路径以及预签名 URL 本身。

```
curl -X PUT -T "/path/to/file" "presigned URL"
```

使用 Amazon SDK 生成 **PUT** 预签名 URL 来上传文件

您可以生成可在有限时间内执行 S3 操作的预签名 URL。

> **Note**
>
> 如果您使用 Amazon CLI 或 Amazon SDK，则预签名 URL 的到期时间可设置为多达 7 天。有关更多信息，请参阅预签名 URL 的到期时间。

Python

以下 Python 脚本生成一个 PUT 预签名 URL，用于将对象上传到 S3 通用存储桶。

1. 复制脚本的内容并将其保存为“*put-only-url.py*”文件。要使用以下示例，请将*#######*替换为您自己的信息（例如，您的文件名）。

```
import argparse
import boto3
from botocore.exceptions import ClientError

def generate_presigned_url(s3_client, client_method, method_parameters,
 expires_in):
    """
    Generate a presigned Amazon S3 URL that can be used to perform an action.
```

```
    :param s3_client: A Boto3 Amazon S3 client.
    :param client_method: The name of the client method that the URL performs.
    :param method_parameters: The parameters of the specified client method.
    :param expires_in: The number of seconds the presigned URL is valid for.
    :return: The presigned URL.
    """
    try:
        url = s3_client.generate_presigned_url(
            ClientMethod=client_method,
            Params=method_parameters,
            ExpiresIn=expires_in
        )
    except ClientError:
        print(f"Couldn't get a presigned URL for client method
 '{client_method}'.")
        raise
    return url

def main():
    parser = argparse.ArgumentParser()
    parser.add_argument("bucket", help="The name of the bucket.")
    parser.add_argument(
        "key", help="The key (path and filename) in the S3 bucket.",
    )
    args = parser.parse_args()

    # By default, this will use credentials from ~/.aws/credentials
    s3_client = boto3.client("s3")

    # The presigned URL is specified to expire in 1000 seconds
    url = generate_presigned_url(
        s3_client,
        "put_object",
        {"Bucket": args.bucket, "Key": args.key},
        1000
    )
    print(f"Generated PUT presigned URL: {url}")

if __name__ == "__main__":
    main()
```

2. 要生成 PUT 预签名 URL 来上传文件，请使用您的存储桶名称和所需的对象路径运行以下脚本。

   以下命令使用的是示例值。将#######替换为您自己的信息。

```
python put-only-url.py amzn-s3-demo-bucket <object-path>
```

该脚本将输出一个 PUT 预签名 URL：

```
Generated PUT presigned URL: https://amzn-s3-demo-
bucket.s3.amazonaws.com/object.txt?
AmazonAccessKeyId=AKIAIOSFODNN7EXAMPLE&Signature=vjbyNxybdZaMmLa
%2ByT372YEAiv4%3D&Expires=1741978496
```

3. 现在，您可以使用通过 curl 生成的预签名 URL 来上传文件：

```
curl -X PUT -T "path/to/your/local/file" "generated-presigned-url"
```

有关使用 Amazon SDK 生成预签名 URL 来上传对象的更多示例，请参阅 Create a presigned URL for Amazon S3 by using an Amazon SDK。

# 使用 S3 对象 Lambda 转换对象

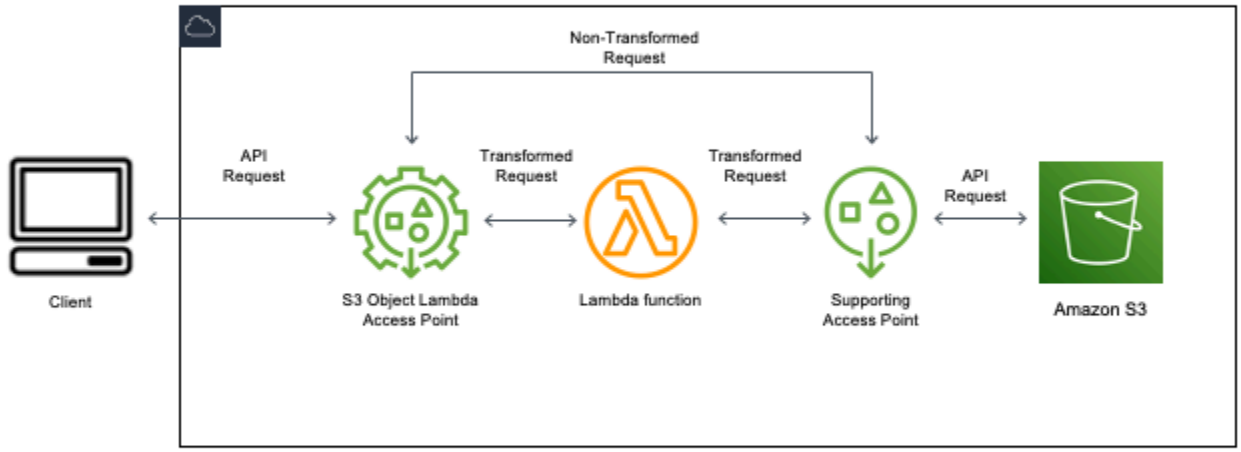
借助 Amazon S3 对象 Lambda，您可以将自己的代码添加到 Amazon S3 GET、LIST 和 HEAD 请求中，以便在数据返回到应用程序时修改和处理数据。您可以使用自定义代码修改由 S3 GET 请求返回的数据，以便执行筛选行、动态调整图像大小和给图像加水印、隐去机密数据等操作。您还可以使用 S3 对象 Lambda 修改 S3 LIST 请求的输出以创建存储桶中所有对象的自定义视图，以及修改 S3 HEAD 请求以修改对象元数据（如对象名称和大小）。您可以使用 S3 对象 Lambda 作为 Amazon CloudFront 分配的来源，以便为最终用户量身定制数据，例如自动调整图像大小、对旧格式进行转码（例如从 JPEG 转码为 WebP）或剥离元数据。有关更多信息，请参阅 Amazon 博客文章将 Amazon S3 对象 Lambda 与 Amazon CloudFront 结合使用。在 Amazon Lambda 函数的支持下，您的代码在完全由 Amazon 管理的基础设施上运行。使用 S3 对象 Lambda 可以减少创建和存储数据的衍生副本或运行代理的需要，所有这些都无需更改应用程序。

S3 对象 Lambda 的工作原理

S3 对象 Lambda 使用 Amazon Lambda 函数来自动处理标准 S3 GET、LIST 或 HEAD 请求的输出。Amazon Lambda 是一种无服务器计算服务，它运行客户定义的代码，而无需管理底层计算资源。您可以编写和运行自己的自定义 Lambda 函数，根据您的特定使用案例定制数据转换。

配置 Lambda 函数后，您可以将其附加到 S3 对象 Lambda 服务端点（称为对象 Lambda 接入点）。对象 Lambda 接入点使用标准 S3 接入点（称为支持接入点）来访问 Amazon S3。

当您向对象 Lambda 接入点发送请求时，Amazon S3 会自动调用您的 Lambda 函数。然后，使用 S3 GET、LIST 或 HEAD 请求通过对象 Lambda 接入点检索的任何数据都会将转换后的结果返回给应用程序。将正常处理所有其他请求，如下图所示。




本节中的主题介绍了如何使用 S3 对象 Lambda。

主题

- 创建对象 Lambda 接入点
- 使用 Amazon S3 对象 Lambda 接入点
- S3 对象 Lambda 接入点的安全注意事项
- 为 S3 对象 Lambda 接入点编写 Lambda 函数
- 使用 Amazon 构建的 Lambda 函数
- S3 对象 Lambda 的最佳实践和指南
- S3 对象 Lambda 教程
- S3 对象 Lambda 调试和故障排除

# 创建对象 Lambda 接入点

对象 Lambda 接入点恰好与一个标准接入点相关联，因此也与一个 Amazon S3 存储桶相关联。要创建对象 Lambda 接入点，您需要以下资源：

- Amazon S3 存储桶。有关创建存储桶的更多信息，请参阅 the section called “创建通用存储桶”。
- 标准 S3 接入点。当您使用对象 Lambda 接入点时，此标准接入点称为支持接入点。有关创建标准接入点的信息，请参阅the section called “创建通用存储桶的接入点”。
- Amazon Lambda 函数。您可以创建自己的 Lambda 函数，也可以使用预构建的函数。有关创建 Lambda 函数的更多信息，请参阅the section called “编写 Lambda 函数”。有关预构建的函数的更多信息，请参阅 使用 Amazon 构建的 Lambda 函数。
- （可选）Amazon Identity and Access Management（IAM）策略。Amazon S3 接入点支持 IAM 资源策略，您可以使用这些策略按资源、用户或其他条件控制接入点的使用。有关创建这些策略的更多信息，请参阅the section called “配置 IAM 策略”。

以下各节介绍如何使用以下方法创建对象 Lambda 接入点：

- 这些区域有：Amazon Web Services Management Console
- Amazon Command Line Interface (Amazon CLI)
- Amazon CloudFormation 模板
- 这些区域有：Amazon Cloud Development Kit (Amazon CDK)

有关如何使用 REST API 创建对象 Lambda 接入点的信息，请参阅《Amazon Simple Storage Service API 参考》中的 `CreateAccessPointForObjectLambda`。

## 创建对象 Lambda 接入点

使用以下过程之一创建对象 Lambda 接入点。

使用 S3 控制台

使用控制台创建对象 Lambda 接入点

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在导航栏中，选择当前所显示 Amazon Web Services 区域的名称。接下来，选择要切换到的区域。

3. 在左侧导航窗格中，选择 Object Lambda 接入点。
4. 在对象 Lambda 接入点页面上，选择创建对象 Lambda 接入点。
5. 对于对象 Lambda 接入点名称，输入要用于接入点的名称。

   与标准接入点一样，对于对象 Lambda 接入点同样具有命名规则。有关更多信息，请参阅 通用存储桶的 Amazon S3 接入点的命名规则。
6. 对于 Supporting Access Point（支持接入点），请输入或浏览到要使用的标准接入点。接入点必须与要变换的对象位于同一 Amazon Web Services 区域 位置。有关创建标准接入点的信息，请参阅the section called “创建通用存储桶的接入点”。
7. 在转换配置下，您可以添加一个函数来转换对象 Lambda 接入点的数据。请执行以下操作之一：

   - 如果您的账户中已经有一个 Amazon Lambda 函数，则可以在 Invoke Lambda function（调用 Lambda 函数）下选择该函数。在这里，您可以在您的 Amazon Web Services 账户中输入 Lambda 函数的 Amazon 资源名称（ARN），也可以从下拉菜单中选择 Lambda 函数。
   - 如果您想使用 Amazon 构建的函数，请在 Amazon 构建的函数下选择函数名称，然后选择创建 Lambda 函数。这将带您进入 Lambda 控制台，您可以在其中将构建的函数部署到您的 Amazon Web Services 账户中。有关构建的函数的更多信息，请参阅使用 Amazon 构建的 Lambda 函数。

   在 S3 APIs（S3 API）下，选择一个或多个要调用的 API 操作。对于所选的每个 API，您必须指定要调用的 Lambda 函数。
8. （可选）在 Payload（有效负载）下，添加要提供给 Lambda 函数作为输入的 JSON 文本。您可以为调用同一 Lambda 函数的不同对象 Lambda 接入点配置具有不同参数的负载，从而扩展 Lambda 函数的灵活性。

   > **Important**
   >
   > 使用对象 Lambda 接入点时，确保负载不包含任何机密信息。
9. （可选）对于 Range and part number（范围和分段编号），如果您要处理带有范围和分段编号标头的 GET 和 HEAD 请求，则必须启用此选项。启用此选项将确认您的 Lambda 函数可以识别和处理这些请求。有关范围标头和分段编号的更多信息，请参阅 使用 Range 和 partNumber 标头。
10. （可选）对于请求指标，请选择启用或禁用，以将 Amazon S3 监控添加到对象 Lambda 接入点。请求指标按标准 Amazon CloudWatch 费率计费。

11. （可选）在对象 Lambda 接入点策略下，设置资源策略。资源策略授予针对指定对象 Lambda 接入点的权限，并可以按资源、用户或其他条件控制接入点的使用。有关对象 Lambda 接入点资源策略的更多信息，请参阅为对象 Lambda 接入点配置 IAM 策略。
12. 在屏蔽此对象 Lambda 接入点的公共访问权限设置下，选择要应用的屏蔽公共访问权限设置。默认情况下，为新的对象 Lambda 接入点启用所有屏蔽公共访问权限设置，建议您将默认设置保留为启用状态。Amazon S3 当前不支持在创建对象 Lambda 接入点之后更改对象 Lambda 接入点的屏蔽公共访问权限设置。

    有关使用 Amazon S3 屏蔽公共访问权限的更多信息，请参阅管理对通用存储桶的接入点的公共访问权限。
13. 请选择创建对象 Lambda 接入点。

使用 Amazon CLI

使用 Amazon CloudFormation 模板创建对象 Lambda 接入点

> **Note**
>
> 要使用以下命令，请将 *user input placeholders* 替换为您自己的信息。

1. 在 S3 对象 Lambda 默认配置中下载 Amazon Lambda 函数部署包 `s3objectlambda_deployment_package.zip`。
2. 运行以下 `put-object` 命令以将文件包上传到 Amazon S3 存储桶。

```
aws s3api put-object --bucket Amazon S3 bucket name --key
 s3objectlambda_deployment_package.zip --body release/
s3objectlambda_deployment_package.zip
```

3. 在 S3 对象 Lambda 默认配置中下载 Amazon CloudFormation 模板 `s3objectlambda_defaultconfig.yaml`。
4. 运行以下 `deploy` 命令以将模板部署到您的 Amazon Web Services 账户。

```
aws cloudformation deploy --template-file s3objectlambda_defaultconfig.yaml \
 --stack-name Amazon CloudFormation stack name \
 --parameter-overrides ObjectLambdaAccessPointName=Object Lambda Access Point name
 \
  SupportingAccessPointName=Amazon S3 access point S3BucketName=Amazon S3 bucket \
```

```
 LambdaFunctionS3BucketName=Amazon S3 bucket containing your Lambda package \
 LambdaFunctionS3Key=Lambda object key LambdaFunctionS3ObjectVersion=Lambda object
version \
 LambdaFunctionRuntime=Lambda function runtime --capabilities capability_IAM
```

您可以将此 Amazon CloudFormation 模板配置为针对 GET、HEAD 和 LIST API 操作调用 Lambda。有关修改模板的默认配置的更多信息，请参阅the section called “使用 Amazon CloudFormation 自动进行 S3 对象 Lambda 设置”。

使用 Amazon CLI 创建对象 Lambda 接入点

> **Note**
>
> 要使用以下命令，请将 *user input placeholders* 替换为您自己的信息。

以下示例为账户 *111122223333* 中的存储桶 *amzn-s3-demo-bucket1* 创建了一个名为 *my-object-lambda-ap* 的对象 Lambda 接入点。此示例假定已创建了名为 *example-ap* 的标准接入点。有关创建标准接入点的信息，请参阅 the section called “创建通用存储桶的接入点”。

此示例使用 Amazon 预构建的函数 decompress。有关预构建的函数的更多信息，请参阅 the section called “使用 Amazon 构建的函数”。

1. 创建存储桶。在此示例中，我们将使用 *amzn-s3-demo-bucket1*。有关创建存储桶的更多信息，请参阅 the section called “创建通用存储桶”。
2. 创建标准接入点并将其附加到存储桶。在此示例中，我们将使用 *example-ap*。有关创建标准接入点的信息，请参阅the section called “创建通用存储桶的接入点”。
3. 请执行以下操作之一：

   - 在您的账户中创建一个 Lambda 函数，用于转换 Amazon S3 对象。有关创建 Lambda 函数的更多信息，请参阅the section called “编写 Lambda 函数”。要将您的自定义函数与 Amazon CLI 结合使用，请参阅《Amazon Lambda 开发人员指南》中的将 Lambda 与 Amazon CLI 结合使用。
   - 使用 Amazon 预构建的 Lambda 函数。有关预构建的函数的更多信息，请参阅 使用 Amazon 构建的 Lambda 函数。
4. 创建一个名为 my-olap-configuration.json 的 JSON 配置文件。在此配置中，为您在前面的步骤中创建的 Lambda 函数提供支持接入点和 Amazon 资源名称（ARN），或者为正在使用的预构建函数提供 ARN。

Example

```
{
    "SupportingAccessPoint" : "arn:aws:s3:us-
east-1:111122223333:accesspoint/example-ap",
    "TransformationConfigurations": [{
        "Actions" : ["GetObject", "HeadObject", "ListObjects", "ListObjectsV2"],
        "ContentTransformation" : {
            "AwsLambda": {
                "FunctionPayload" : "{\"compressionType\":\"gzip\"}",
                "FunctionArn" : "arn:aws:lambda:us-east-1:111122223333:function/
compress"
            }
        }
    }]
}
```

5. 运行 `create-access-point-for-object-lambda` 命令以创建对象 Lambda 接入点。

```
aws s3control create-access-point-for-object-lambda --account-id 111122223333 --
name my-object-lambda-ap --configuration file://my-olap-configuration.json
```

6. （可选）创建名为的 `my-olap-policy.json` JSON 策略文件。

添加对象 Lambda 接入点资源策略可以按资源、用户或其他条件控制接入点的使用。此资源策略为账户 *444455556666* 授予针对指定对象 Lambda 接入点的 `GetObject` 权限。

Example

```
{
    "Version": "2008-10-17",
    "Statement": [
        {
            "Sid": "Grant account 444455556666 GetObject access",
            "Effect": "Allow",
            "Action": "s3-object-lambda:GetObject",
            "Principal": {
                "AWS": "arn:aws:iam::444455556666:root"
            },
            "Resource": "your-object-lambda-access-point-arn"
```

```
        }
    ]
}
```

7. （可选）运行 put-access-point-policy-for-object-lambda 命令以设置资源策略。

```
aws s3control put-access-point-policy-for-object-lambda --account-id 111122223333
 --name my-object-lambda-ap --policy file://my-olap-policy.json
```

8. （可选）指定负载。

有效负载是可选 JSON，您可以将其作为输入提供给 Amazon Lambda 函数。您可以为调用同一 Lambda 函数的不同对象 Lambda 接入点配置具有不同参数的负载，从而扩展 Lambda 函数的灵活性。

以下对象 Lambda 接入点配置显示了带有两个参数的负载。

```
{
 "SupportingAccessPoint": "AccessPointArn",
 "CloudWatchMetricsEnabled": false,
 "TransformationConfigurations": [{
  "Actions": ["GetObject", "HeadObject", "ListObjects", "ListObjectsV2"],
  "ContentTransformation": {
   "AwsLambda": {
    "FunctionArn": "FunctionArn",
    "FunctionPayload": "{\"res-x\": \"100\",\"res-y\": \"100\"}"
   }
  }
 }]
}
```

以下对象 Lambda 接入点配置显示具有一个参数以及启用了 GetObject-Range、GetObject-PartNumber、HeadObject-Range 和 HeadObject-PartNumber 的负载。

```
{
    "SupportingAccessPoint":"AccessPointArn",
    "CloudWatchMetricsEnabled": false,
    "AllowedFeatures": ["GetObject-Range", "GetObject-PartNumber", "HeadObject-
Range", "HeadObject-PartNumber"],
    "TransformationConfigurations": [{
        "Action": ["GetObject", "HeadObject", "ListObjects", "ListObjectsV2"],
        "ContentTransformation": {
```

```
            "AwsLambda": {
                "FunctionArn":"FunctionArn",
                "FunctionPayload": "{\"compression-amount\": \"5\"}"
            }
        }
    }]
}
```

> **Important**
>
> 使用对象 Lambda 接入点时，确保负载不包含任何机密信息。

使用 Amazon CloudFormation 控制台和模板

您可以使用 Amazon S3 提供的默认配置创建对象 Lambda 接入点。您可以从 GitHub 存储库下载 Amazon CloudFormation 模板和 Lambda 函数源代码，并部署这些资源以设置函数对象 Lambda 接入点。

有关修改 Amazon CloudFormation 模板的默认配置的信息，请参阅the section called “使用 Amazon CloudFormation 自动进行 S3 对象 Lambda 设置”。

有关在没有模板的情况下使用 Amazon CloudFormation 配置对象 Lambda 接入点的信息，请参阅《Amazon CloudFormation 用户指南》中的 `AWS::S3ObjectLambda::AccessPoint`。

要上传 Lambda 函数部署软件包

1. 在 S3 对象 Lambda 默认配置中下载 Amazon Lambda 函数部署包 `s3objectlambda_deployment_package.zip`。
2. 将文件包上传到 Amazon S3 存储桶。

使用 Amazon CloudFormation 控制台创建对象 Lambda 接入点

1. 在 S3 对象 Lambda 默认配置中下载 Amazon CloudFormation 模板 `s3objectlambda_defaultconfig.yaml`。
2. 登录 Amazon 管理控制台并通过以下网址打开 Amazon CloudFormation 控制台：https://console.aws.amazon.com/cloudformation。
3. 请执行以下操作之一：

- 如果您以前从未用过 Amazon CloudFormation，请在 Amazon CloudFormation 主页上选择 Create stack（创建堆栈）。
- 如果之前用过 Amazon CloudFormation，请在左侧导航窗格中选择 Stacks（堆栈）。选择 Create stack（创建堆栈），然后选择 With new resources (standard) [使用新资源（标准）]。

4. 对于 Prerequisite - Prepare template（先决条件 - 准备模板），请选择 Template is ready（模板已就绪）。
5. 对于 Specify template（指定模板），选择 Upload a template file（上传模板文件）并上传 `s3objectlambda_defaultconfig.yaml`。
6. 选择下一步。
7. 在 Specify stack details（指定堆栈详细信息）页面上，输入堆栈名称。
8. 在 Parameters（参数）部分中，指定在堆栈模板中定义的以下参数：

   a. 对于 CreateNewSupportingAccessPoint，请执行以下操作之一：

      - 如果对于您上传了模板的 S3 存储桶已经有支持接入点，请选择 false。
      - 如果要为该存储桶创建新的接入点，请选择 true。

   b. 对于 EnableCloudWatchMonitoring，根据您是否要启用 Amazon CloudWatch 请求指标和告警，选择 true 或 false。

   c. （可选）对于 LambdaFunctionPayload，添加要提供给 Lambda 函数作为输入的 JSON 文本。您可以为调用同一 Lambda 函数的不同对象 Lambda 接入点配置具有不同参数的负载，从而扩展 Lambda 函数的灵活性。

      > **Important**
      >
      > 使用对象 Lambda 接入点时，确保负载不包含任何机密信息。

   d. 对于 LambdaFunctionRuntime，输入适用于 Lambda 函数的首选运行时。可用的选项为 `nodejs14.x`、`python3.9`、`java11`。

   e. 对于 LambdaFunctionS3BucketName，输入您在其中上传了部署文件包的 Amazon S3 存储桶名称。

   f. 对于 LambdaFunctionS3Key，输入您在上传部署文件包时使用的 Amazon S3 对象密钥。

   g. 对于 LambdaFunctionS3ObjectVersion，输入您在其中上传了部署文件包的 Amazon S3 对象版本。

   h. 对于 ObjectLambdaAccessPointName，输入对象 Lambda 接入点的名称。

i. 对于 S3BucketName，输入将与对象 Lambda 接入点相关联的 Amazon S3 存储桶名称。

j. 对于 SupportingAccessPointName，输入支持接入点的名称。

> **Note**
>
> 这是与您在上一步中选择的 Amazon S3 存储桶相关联的接入点。如果您没有任何与 Amazon S3 存储桶相关联的接入点，则可以配置模板，以通过为 CreateNewSupportingAccessPoint 选择 true 来为您创建一个此类接入点。

9. 选择 Next(下一步)。
10. 在 配置堆栈选项 页面上，请选择 下一步。

    有关此页面上的可选设置的更多信息，请参阅《Amazon CloudFormation 用户指南》中的设置 Amazon CloudFormation 堆栈选项。
11. 在 Review（查看）页面中，请选择 Create stack（创建堆栈）。

使用 Amazon Cloud Development Kit (Amazon CDK)

有关使用 Amazon CDK 配置对象 Lambda 接入点的更多信息，请参阅《Amazon Cloud Development Kit (Amazon CDK) API 参考》中的 `AWS::S3ObjectLambda` 构造库。

## 使用 CloudFormation 模板自动进行 S3 对象 Lambda 设置

您可以使用 Amazon CloudFormation 模板快速创建 Amazon S3 对象 Lambda 接入点。CloudFormation 模板会自动创建相关资源、配置 Amazon Identity and Access Management（IAM）角色并设置 Amazon Lambda 函数，该函数可通过对象 Lambda 接入点自动处理请求。使用 CloudFormation 模板，您可以实施最佳实践、改善安全状况并减少手动流程导致的错误。

此 GitHub 存储库包含 CloudFormation 模板和 Lambda 函数源代码。有关如何使用模板的说明，请参阅the section called “创建对象 Lambda 接入点”。

模板中提供的 Lambda 函数未运行任何转换。相反，它按原样从 S3 存储桶返回对象。您可以克隆函数并添加自己的转换代码，以便在数据返回到应用程序时修改和处理数据。有关修改函数的更多信息，请参阅the section called “修改 Lambda 函数”和the section called “编写 Lambda 函数”。

修改模板。

创建新的支持接入点

S3 对象 Lambda 使用两个接入点，一个对象 Lambda 接入点和一个标准 S3 接入点（称为支持接入点）。当您向对象 Lambda 接入点发出请求时，S3 会代表您调用 Lambda，或将请求委派给支持接入点，具体取决于 S3 对象 Lambda 配置。在部署模板时，您可以通过将以下参数作为 `aws cloudformation deploy` 命令的一部分来创建一个新的支持接入点。

```
CreateNewSupportingAccessPoint=true
```

配置函数有效负载

在部署模板时，可以通过将以下参数作为 `aws cloudformation deploy` 命令的一部分传递，配置有效负载为 Lambda 函数提供补充数据。

```
LambdaFunctionPayload="format=json"
```

启用 Amazon CloudWatch 监控

您可以在部署模板时通过将以下参数作为 `aws cloudformation deploy` 命令的一部分来启用 CloudWatch 监视。

```
EnableCloudWatchMonitoring=true
```

此参数将为 Amazon S3 请求指标启用对象 Lambda 接入点，并创建两个 CloudWatch 告警来监控客户端和服务器端错误。

> **Note**
>
> Amazon CloudWatch 的使用将产生额外费用。有关 Amazon S3 请求指标的更多信息，请参阅监控和记录通用存储桶的接入点。
> 有关定价详细信息，请参阅 CloudWatch 定价。

配置预配置并发

要减少延迟，您可以通过编辑模板以在 `Resources` 之下包含以下各行，从而为支持对象 Lambda 接入点的 Lambda 函数配置预调配并发。

```
LambdaFunctionVersion:
      Type: AWS::Lambda::Version
      Properties:
        FunctionName: !Ref LambdaFunction
```

```
        ProvisionedConcurrencyConfig:
            ProvisionedConcurrentExecutions: Integer
```

> **Note**
>
> 配置并发将产生额外费用。有关预调配并发的更多信息，请参阅《Amazon Lambda 开发人员指南》中的管理 Lambda 预调配并发。
> 有关定价的详细信息，请参阅 Amazon Lambda 定价。

修改 Lambda 函数

更改 **GetObject** 请求的标头值

默认情况下，Lambda 函数会将所有标头（Content-Length 和 ETag 除外）从预签名 URL 请求转发到 GetObject 客户端。根据 Lambda 函数中的转换代码，您可以选择向 GetObject 客户端发送新的标头值。

您可以更新 Lambda 函数，以通过在 WriteGetObjectResponse API 操作中传递来发送新的标头值。

例如，如果 Lambda 函数将 Amazon S3 对象中的文本转换为另一种语言，则可以在 Content-Language 标头中传递一个新值。您可以通过修改 writeResponse 函数来实现，如下所示：

```
async function writeResponse (s3Client: S3, requestContext: GetObjectContext,
 transformedObject: Buffer,
  headers: Headers): Promise<PromiseResult<{}, AWSError>> {
  const { algorithm, digest } = getChecksum(transformedObject);

  return s3Client.writeGetObjectResponse({
    RequestRoute: requestContext.outputRoute,
    RequestToken: requestContext.outputToken,
    Body: transformedObject,
    Metadata: {
      'body-checksum-algorithm': algorithm,
      'body-checksum-digest': digest
    },
    ...headers,
    ContentLanguage: 'my-new-language'
  }).promise();
}
```

有关受支持标头的完整列表，请参阅 Amazon Simple Storage Service API 参考中的 WriteGetObjectResponse。

返回元数据标头

您可以更新 Lambda 函数，以通过在 WriteGetObjectResponse API 操作请求中传递来发送新的标头值。

```
async function writeResponse (s3Client: S3, requestContext: GetObjectContext,
 transformedObject: Buffer,
  headers: Headers): Promise<PromiseResult<{}, AWSError>> {
  const { algorithm, digest } = getChecksum(transformedObject);

  return s3Client.writeGetObjectResponse({
    RequestRoute: requestContext.outputRoute,
    RequestToken: requestContext.outputToken,
    Body: transformedObject,
    Metadata: {
      'body-checksum-algorithm': algorithm,
      'body-checksum-digest': digest,
      'my-new-header': 'my-new-value'
    },
    ...headers
  }).promise();
}
```

返回新状态码

您可以通过在 WriteGetObjectResponse API 操作请求中进行传递来将自定义状态代码返回至 GetObject 客户端。

```
async function writeResponse (s3Client: S3, requestContext: GetObjectContext,
 transformedObject: Buffer,
  headers: Headers): Promise<PromiseResult<{}, AWSError>> {
  const { algorithm, digest } = getChecksum(transformedObject);

  return s3Client.writeGetObjectResponse({
    RequestRoute: requestContext.outputRoute,
    RequestToken: requestContext.outputToken,
    Body: transformedObject,
    Metadata: {
      'body-checksum-algorithm': algorithm,
      'body-checksum-digest': digest
```

```
    },
    ...headers,
    StatusCode: Integer
  }).promise();
}
```

有关受支持的状态代码的完整列表，请参阅 Amazon Simple Storage Service API 参考中的 WriteGetObjectResponse。

将 **Range** 和 **partNumber** 参数应用于源对象

默认情况下，由 CloudFormation 模板创建的对象 Lambda 接入点可以处理 Range 和 partNumber 参数。Lambda 函数将请求的范围或段编号应用于转换后的对象。为此，此函数必须下载整个对象并运行转换。在某些情况下，转换后的对象范围可能会精确映射到源对象范围。这意味着，在源对象上请求字节范围 A-B 并运行转换，可能会产生与请求整个对象、运行转换以及在转换后的对象上返回字节范围 A-B 相同的结果。

在这种情况下，您可以更改 Lambda 函数实现，以便将范围或段编号直接应用于源对象。这种方法减少了所需的总体函数延迟和内存。有关更多信息，请参阅 the section called “使用 Range 和 partNumber 标头”。

禁用 **Range** 和 **partNumber** 处理

默认情况下，由 CloudFormation 模板创建的对象 Lambda 接入点可以处理 Range 和 partNumber 参数。如果不需要此行为，可以通过从模板中移除以下各行来禁用它。

```
AllowedFeatures:
  - GetObject-Range
  - GetObject-PartNumber
  - HeadObject-Range
  - HeadObject-PartNumber
```

转换大型对象

默认情况下，Lambda 函数会处理内存中的整个对象，然后才能开始将响应流式传输到 S3 对象 Lambda。您可以在执行转换时修改函数以流式传输响应。这样做有助于减少转换延迟和 Lambda 函数内存大小。有关实施示例，请参阅 Stream compressed content example（流式压缩内容示例）。

## 使用 Amazon S3 对象 Lambda 接入点

通过 Amazon S3 对象 Lambda 接入点发出请求与通过其他接入点发出请求的工作方式相同。有关如何通过接入点发出请求的更多信息，请参阅 使用通用存储桶的 Amazon S3 接入点。您可以使用 Amazon

S3 控制台、Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 Amazon S3 REST API，通过对象 Lambda 接入点发出请求。

> **Important**
>
> 对象 Lambda 接入点的 Amazon 资源名称（ARN）使用 `s3-object-lambda` 的服务名称。因此，对象 Lambda 接入点 ARN 以 `arn:aws::s3-object-lambda`（而不是 `arn:aws::s3`）开头，它与其他接入点结合使用。

## 如何查找对象 Lambda 接入点的 ARN

要将对象 Lambda 接入点与 Amazon CLI 或 Amazon SDK 结合使用，您需要知道对象 Lambda 接入点的 Amazon 资源名称（ARN）。以下示例说明如何通过使用 Amazon S3 控制台或 Amazon CLI 查找对象 Lambda 接入点的 ARN。

使用 S3 控制台

使用控制台查找对象 Lambda 接入点的 ARN

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择对象 Lambda 接入点。
3. 选择要复制其 ARN 的对象 Lambda 接入点旁边的选项按钮。
4. 请选择复制 ARN。

使用 Amazon CLI

使用 Amazon CLI 查找对象 Lambda 接入点的 ARN

1. 要检索与 Amazon Web Services 账户 关联的对象 Lambda 接入点的列表，请运行以下命令。在运行命令之前，请将账户 ID *111122223333* 替换为您的 Amazon Web Services 账户 ID。

```
aws s3control list-access-points-for-object-lambda --account-id 111122223333
```

2. 查看命令输出以查找您要使用的对象 Lambda 接入点 ARN。前一个命令的输出内容应类似如下示例。

```
{
```

```
    "ObjectLambdaAccessPointList": [
        {
            "Name": "my-object-lambda-ap",
            "ObjectLambdaAccessPointArn": "arn:aws:s3-object-lambda:us-
east-1:111122223333:accesspoint/my-object-lambda-ap"
        },
        ...
    ]
}
```

## 如何为您的 S3 存储桶对象 Lambda 接入点使用存储桶式别名

当您创建对象 Lambda 接入点时，Amazon S3 会自动为您的对象 Lambda 接入点生成一个唯一的别名。您可以在接入点数据面板操作请求中使用此别名，而不使用 Amazon S3 存储桶名称或对象 Lambda 接入点 Amazon 资源名称（ARN）。有关这些操作的列表，请参阅通用存储桶的接入点兼容性。

对象 Lambda 接入点别名是在与 Amazon S3 存储桶相同的命名空间中创建的。此别名自动生成，无法更改。对于现有对象 Lambda 接入点，会自动分配别名以供使用。对象 Lambda 接入点别名符合有效 Amazon S3 存储桶名称的所有要求，包括以下部分：

*Object Lambda Access Point name prefix*-*metadata*--ol-s3

> **Note**
>
> --ol-s3 后缀是为对象 Lambda 接入点别名预留的，不能用于存储桶或对象 Lambda 接入点名称。有关 Amazon S3 存储桶命名规则的更多信息，请参阅通用存储桶命名规则。

以下示例显示了名为 *my-object-lambda-access-point* 的对象 Lambda 接入点的 ARN 和对象 Lambda 接入点别名。

- ARN – arn:aws:s3-object-lambda:*region*:*account-id*:accesspoint/*my-object-lambda-access-point*
- 对象 Lambda 接入点别名 – *my-object-lambda-acc-1a4n8yjrb3kda96f67zwrwiiuse1a*--ol-s3

当您使用对象 Lambda 接入点时，无需进行大量代码更改，即可使用对象 Lambda 接入点别名。

当您删除对象 Lambda 接入点时，对象 Lambda 接入点别名将变为非活动状态且未调配。

如何查找对象 Lambda 接入点的别名

使用 S3 控制台

使用控制台查找对象 Lambda 接入点的别名

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择对象 Lambda 接入点。
3. 对于要使用的对象 Lambda 接入点，复制对象 Lambda 接入点别名值。

使用 Amazon CLI

创建对象 Lambda 接入点时，Amazon S3 会自动生成对象 Lambda 接入点别名，如以下示例命令所示。要运行此命令，请将 *user input placeholders* 替换为您自己的信息。有关如何使用 Amazon CLI 创建对象 Lambda 接入点的信息，请参阅使用 Amazon CLI 创建对象 Lambda 接入点。

```
aws s3control create-access-point-for-object-lambda --account-id 111122223333 --
name my-object-lambda-access-point --configuration file://my-olap-configuration.json
{
    "ObjectLambdaAccessPointArn": "arn:aws:s3:region:111122223333:accesspoint/my-
access-point",
    "Alias": {
        "Value": "my-object-lambda-acc-1a4n8yjrb3kda96f67zwrwiiuse1a--ol-s3",
        "Status": "READY"
    }
}
```

生成的对象 Lambda 接入点别名有两个字段：

- `Value` 字段是对象 Lambda 接入点的别名值。
- `Status` 字段是对象 Lambda 接入点别名的状态。如果状态为 `PROVISIONING`，则 Amazon S3 正在预调配对象 Lambda 接入点别名，并且该别名尚未准备就绪，无法使用。如果状态为 `READY`，则对象 Lambda 接入点别名已成功调配，并准备就绪可供使用。

有关 REST API 中 `ObjectLambdaAccessPointAlias` 数据类型的更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 CreateAccessPointForObjectLambda 和 ObjectLambdaAccessPointAlias。

如何使用对象 Lambda 接入点别名

您可以使用对象 Lambda 接入点别名，而不是通用存储桶的接入点兼容性中所列的操作的 Amazon S3 存储桶名称。

以下 `get-bucket-location` 命令的 Amazon CLI 示例使用存储桶的接入点别名来返回存储桶所在的 Amazon Web Services 区域。要运行此命令，请将 *`user input placeholders`* 替换为您自己的信息。

```
aws s3api get-bucket-location --bucket my-object-lambda-
acc-w7i37nq6xuzgax3jw3oqtifiusw2a--ol-s3

{
    "LocationConstraint": "us-west-2"
}
```

如果请求中的对象 Lambda 接入点别名无效，则返回错误代码 `InvalidAccessPointAliasError`。有关 `InvalidAccessPointAliasError` 的更多信息，请参阅《Amazon Simple Storage Service API 参考》中的错误代码列表。

对象 Lambda 接入点别名的限制与接入点别名的限制相同。有关接入点别名限制的更多信息，请参阅接入点别名限制。

## S3 对象 Lambda 接入点的安全注意事项

使用 Amazon S3 对象 Lambda，您可以借助使用 Amazon Lambda 作为计算平台的规模和灵活性，在数据离开 Amazon 3 时对其执行自定义转换。S3 和 Lambda 在默认情况下保持安全，但是为了维持这种安全性，Lambda 函数的作者需要特别考虑一些注意事项。S3 对象 Lambda 要求所有访问都由经过身份验证的主体（无匿名访问）和 HTTPS 进行。

为降低安全风险，我们提出以下建议：

- 将 Lambda 执行角色的范围限定为尽可能小的权限集。
- 只要有可能，就确保您的 Lambda 函数通过提供的预签名 URL 访问 Amazon S3。

## 配置 IAM 策略

S3 接入点支持 Amazon Identity and Access Management（IAM）资源策略，这些策略允许您按资源、用户或其他条件控制接入点的使用。有关更多信息，请参阅 为对象 Lambda 接入点配置 IAM 策略。

## 加密行为

由于对象 Lambda 接入点同时使用 Amazon S3 和 Amazon Lambda，因此，加密行为会存在差异。有关默认 S3 加密行为的更多信息，请参阅为 Amazon S3 存储桶设置默认服务器端加密行为。

- 将 S3 服务器端加密与对象 Lambda 接入点结合使用时，需要先将对象解密，然后再将其发送到 Lambda。将对象发送到 Lambda 后，将以未加密方式对其进行处理（如果是 GET 或 HEAD 请求）。
- 为防止密钥被记录，S3 将拒绝针对以下对象的 GET 和 HEAD 请求：使用具有客户提供的密钥的服务器端加密（SSE-C）来加密的对象。但是，如果 Lambda 函数可以访问客户端提供的密钥，它仍可检索这些对象。
- 将 S3 客户端加密与对象 Lambda 接入点结合使用时，请确保 Lambda 有权访问加密密钥，以便它可以解密和重新加密对象。

## 接入点安全性

S3 对象 Lambda 使用两个接入点，一个对象 Lambda 接入点和一个标准 S3 接入点（称为支持接入点）。当您向对象 Lambda 接入点发出请求时，S3 会代表您调用 Lambda，或将请求委派给支持接入点，具体取决于 S3 对象 Lambda 配置。当针对请求调用 Lambda 时，S3 将通过支持接入点，代表您向对象生成一个预签名 URL。您的 Lambda 函数将在调用此函数时接收此 URL 以作为输入。

您可以将 Lambda 函数设置为使用此预签名 URL 来检索原始对象，而不是直接调用 S3。通过使用此模型，您可以为对象应用更好的安全边界。您可以将通过 S3 存储桶或 S3 接入点进行的直接对象访问，限制为一组有限的 IAM 角色或用户。这种方法也可以防止您的 Lambda 函数受到混淆代理问题的影响，发生混淆代理问题时，配置错误的函数具有与调用方不同的权限，可以允许或拒绝对于对象的访问（但原本不应如此）。

## 对象 Lambda 接入点公共访问权限

S3 对象 Lambda 不允许匿名访问和公有访问，因为 Amazon S3 必须向您的身份授权，才能完成任何 S3 对象 Lambda 请求。当通过对象 Lambda 接入点调用请求时，您必须对于已配置的 Lambda 函数拥有 `lambda:InvokeFunction` 权限。同样，当通过对象 Lambda 接入点调用其他 API 操作时，您必须拥有所需的 `s3:*` 权限。

如果不具有这些权限，则调用 Lambda 或委托给 S3 的请求将失败，并出现 HTTP 403 (Forbidden) [HTTP 403（禁止访问）] 错误。必须由经过身份验证的主体进行所有访问。如果您需要公有访问权限，可使用 Lambda@Edge 作为可能的替代方案。有关更多信息，请参阅 Amazon CloudFront 开发人员指南中的使用 Lambda@Edge 在边缘进行自定义。

## 对象 Lambda 接入点 IP 地址

`describe-managed-prefix-lists` 子网支持网关虚拟私有云（VPC）端点，并与 VPC 端点的路由表相关。由于对象 Lambda 接入点不支持网关 VPC，因此其 IP 范围缺失。缺失的范围属于 Amazon S3，但网关 VPC 端点不支持。有关 `describe-managed-prefix-lists` 的更多信息，请参阅《Amazon EC2 API 参考》中的 DescribeManagedPrefixLists 和《Amazon Web Services 一般参考》中的 Amazon IP 地址范围。

## 为对象 Lambda 接入点配置 IAM 策略

Amazon S3 接入点支持 Amazon Identity and Access Management（IAM）资源策略，您可以使用这些策略按资源、用户或其他条件控制接入点的使用。您可以通过对象 Lambda 接入点上的可选资源策略或支持接入点上的资源策略来控制访问权限。有关分步示例，请参阅 教程：使用 S3 对象 Lambda 转换应用程序的数据 和 教程：使用 S3 对象 Lambda 和 Amazon Comprehend 检测和修订 PII 数据。

以下四项资源必须已获得使用对象 Lambda 接入点的权限：

- IAM 身份，例如用户或角色。有关 IAM 身份和最佳实践的更多信息，请参阅《IAM 用户指南》中的 IAM 身份（用户、用户组和角色）。
- 存储桶及其关联的标准接入点。当您使用对象 Lambda 接入点时，此标准接入点称为支持接入点。
- 对象 Lambda 接入点。
- Amazon Lambda 函数。

> **Important**
>
> 在保存策略之前，确保解决来自 Amazon Identity and Access Management Access Analyzer 的安全警告、错误、一般警告和建议。IAM Access Analyzer 将根据 IAM 策略语法和最佳实践运行策略检查，以验证您的策略。这些检查项生成结果并提供可操作的建议，可帮助您编写可操作且符合安全最佳实践的策略。
>
> 要了解有关使用 IAM Access Analyzer 验证策略的更多信息，请参阅《IAM 用户指南》中的 IAM Access Analyzer 策略验证。要查看 IAM Access Analyzer 返回的警告、错误和建议的列表，请参阅 IAM Access Analyzer 策略检查引用。

以下策略示例假设您具有以下资源：

- 具有以下 Amazon 资源名称（ARN）的 Amazon S3 存储桶：

  `arn:aws:s3:::amzn-s3-demo-bucket1`
- 此存储桶上具有以下 ARN 的 Amazon S3 standard 接入点：

  `arn:aws:s3:us-east-1:111122223333:accesspoint/my-access-point`
- 具有以下 ARN 的对象 Lambda 接入点：

  `arn:aws:s3-object-lambda:us-east-1:111122223333:accesspoint/my-object-lambda-ap`
- 具有以下 ARN 的 Amazon Lambda Lambda 函数：

  `arn:aws:lambda:us-east-1:111122223333:function:MyObjectLambdaFunction`

> **Note**
>
> 如果使用您的账户中的 Lambda 函数，则必须在策略声明中包含具体的函数版本。在以下示例 ARN 中，版本由 *1* 表示：
> `arn:aws:lambda:us-east-1:111122223333:function:MyObjectLambdaFunction:1`
> Lambda 不支持向版本 $LATEST 中添加 IAM 策略。有关 Lambda 函数版本的更多信息，请参阅《Amazon Lambda 开发人员指南》中的 Lambda 函数版本。

Example – 将访问控制委派给标准接入点的存储桶策略

下面的 S3 存储桶策略示例将存储桶的访问控制委派给存储桶的标准接入点。此策略允许对存储桶拥有者账户所拥有的所有接入点进行完全访问。因此，对此存储桶的所有访问都由附加到其接入点的策略控制。用户只能通过接入点从存储桶读取，这意味着您只能通过接入点调用操作。有关更多信息，请参阅将访问控制委派到接入点。

```
{
    "Version": "2012-10-17",
    "Statement" : [
    {
        "Effect": "Allow",
        "Principal" : { "AWS":"account-ARN"},
```

```
        "Action" : "*",
        "Resource" : [
            "arn:aws:s3:::amzn-s3-demo-bucket1",
            "arn:aws:s3:::amzn-s3-demo-bucket1/*"
        ],
        "Condition": {
            "StringEquals" : { "s3:DataAccessPointAccount" : "Bucket owner's account
 ID" }
        }
    }]
}
```

Example – 向用户授予使用对象 Lambda 接入点的必需权限的 IAM 策略

以下 IAM 策略授予用户对 Lambda 函数、标准接入点和对象 Lambda 接入点的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowLambdaInvocation",
      "Action": [
        "lambda:InvokeFunction"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:lambda:us-
east-1:111122223333:function:MyObjectLambdaFunction:1",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": [
            "s3-object-lambda.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowStandardAccessPointAccess",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:us-east-1:111122223333:accesspoint/my-access-point/*",
      "Condition": {
```

```
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": [
            "s3-object-lambda.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowObjectLambdaAccess",
      "Action": [
        "s3-object-lambda:Get*",
        "s3-object-lambda:List*"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3-object-lambda:us-east-1:111122223333:accesspoint/my-object-lambda-ap"
    }
  ]
}
```

启用 Lambda 执行角色的权限

当向对象 Lambda 接入点发出 GET 请求时，Lambda 函数需要将数据发送到 S3 对象 Lambda 接入点的权限。可通过对 Lambda 函数的执行角色启用 `s3-object-lambda:WriteGetObjectResponse` 权限来提供此权限。您可以创建新角色，或更新现有角色。

> **Note**
>
> 仅当您发出 GET 请求时，函数才需要 `s3-object-lambda:WriteGetObjectResponse` 权限。

在 IAM 控制台中创建执行角色

1. 通过 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
2. 在左侧导航窗格中，选择 Roles（角色）。
3. 选择 Create role（创建角色）。
4. 在 Common use cases（常用使用案例）下，请选择 Lambda。
5. 选择下一步。

6. 在 Add permissions（添加权限）页面上，搜索 Amazon 托管式策略 AmazonS3ObjectLambdaExecutionRolePolicy，然后选中策略名称旁边的复选框。

   该策略应包含 `s3-object-lambda:WriteGetObjectResponse` 操作。
7. 选择下一步。
8. 在 Name, review, and create（名称、查看和创建）页面上，对于 Role name（角色名称），输入 **`s3-object-lambda-role`**。
9. （可选）为该角色添加描述和标签。
10. 选择 Create role（创建角色）。
11. 应用新创建的 **`s3-object-lambda-role`** 作为 Lambda 函数的执行角色。这可以在 Lambda 控制台中创建 Lambda 函数期间或之后完成。

有关执行角色的更多信息，请参阅 Amazon Lambda 开发人员指南中的 Lambda 执行角色。

将上下文键与对象 Lambda 接入点结合使用

S3 对象 Lambda 将评估与请求的连接或签名相关的上下文键，如 `s3-object-lambda:TlsVersion` 或 `s3-object-lambda:AuthType`。Amazon S3 评估所有其他上下文键，例如 `s3:prefix`。

### 对象 Lambda 接入点 CORS 支持

当 S3 对象 Lambda 收到来自浏览器的请求或包含 `Origin` 标头的请求时，S3 对象 Lambda 始终会添加 `"AllowedOrigins":"*"` 标头字段。

有关更多信息，请参阅 使用跨源资源共享 (CORS)。

## 为 S3 对象 Lambda 接入点编写 Lambda 函数

本节详细介绍如何编写与 Amazon S3 对象 Lambda 接入点结合使用的 Amazon Lambda 函数。

要了解一些 S3 对象 Lambda 任务的完整端到端过程，请参阅以下内容：

- 教程：使用 S3 对象 Lambda 转换应用程序的数据
- 教程：使用 S3 对象 Lambda 和 Amazon Comprehend 检测和修订 PII 数据
- 教程：使用 S3 对象 Lambda 在检索图像时对其动态加水印

主题

- 在 Lambda 中处理 GetObject 请求
- 在 Lambda 中处理 HeadObject 请求
- 在 Lambda 中处理 ListObjects 请求
- 在 Lambda 中处理 ListObjectsV2 请求
- 事件上下文格式和用法
- 使用 Range 和 partNumber 标头

## 在 Lambda 中处理 **GetObject** 请求

本节假设您的对象 Lambda 接入点配置为对于 `GetObject` 调用 Lambda 函数。S3 对象 Lambda 包括 Amazon S3 API 操作 `WriteGetObjectResponse`，该操作可以让 Lambda 函数向 `GetObject` 调用方提供自定义数据和响应标头。

`WriteGetObjectResponse` 可根据您的处理需要，让您对状态代码、响应标头和响应正文进行广泛的控制。您可以使用 `WriteGetObjectResponse` 来响应整个变换对象、变换对象的某些部分或其他基于应用程序上下文的响应。以下部分介绍了使用 `WriteGetObjectResponse` API 操作的独特示例。

- 示例 1：使用 HTTP 状态代码 403（禁止访问）进行响应
- 示例 2： 通过转换后的图像进行响应
- 示例 3： 流式压缩内容

### 示例 1：使用 HTTP 状态代码 403（禁止访问）进行响应

您可以使用 `WriteGetObjectResponse` 根据对象的内容使用 HTTP 状态代码 403（禁止）进行响应。

Java

```
package com.amazon.s3.objectlambda;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.events.S3ObjectLambdaEvent;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3Client;
import com.amazonaws.services.s3.model.WriteGetObjectResponseRequest;
```

```
import java.io.ByteArrayInputStream;
import java.net.URI;
import java.net.http.HttpClient;
import java.net.http.HttpRequest;
import java.net.http.HttpResponse;

public class Example1 {

    public void handleRequest(S3ObjectLambdaEvent event, Context context) throws
 Exception {
        AmazonS3 s3Client = AmazonS3Client.builder().build();

        // Check to see if the request contains all of the necessary information.
        // If it does not, send a 4XX response and a custom error code and message.
        // Otherwise, retrieve the object from S3 and stream it
        // to the client unchanged.
        var tokenIsNotPresent = !
event.getUserRequest().getHeaders().containsKey("requiredToken");
        if (tokenIsNotPresent) {
            s3Client.writeGetObjectResponse(new WriteGetObjectResponseRequest()
                    .withRequestRoute(event.outputRoute())
                    .withRequestToken(event.outputToken())
                    .withStatusCode(403)
                    .withContentLength(0L).withInputStream(new
 ByteArrayInputStream(new byte[0]))
                    .withErrorCode("MissingRequiredToken")
                    .withErrorMessage("The required token was not present in the
 request."));
            return;
        }

        // Prepare the presigned URL for use and make the request to S3.
        HttpClient httpClient = HttpClient.newBuilder().build();
        var presignedResponse = httpClient.send(
                HttpRequest.newBuilder(new URI(event.inputS3Url())).GET().build(),
                HttpResponse.BodyHandlers.ofInputStream());

        // Stream the original bytes back to the caller.
        s3Client.writeGetObjectResponse(new WriteGetObjectResponseRequest()
                .withRequestRoute(event.outputRoute())
                .withRequestToken(event.outputToken())
                .withInputStream(presignedResponse.body()));
    }
```

```
}
```

### Python

```
import boto3
import requests

def handler(event, context):
    s3 = boto3.client('s3')

    """
    Retrieve the operation context object from the event. This object indicates
 where the WriteGetObjectResponse request
    should be delivered and contains a presigned URL in 'inputS3Url' where we can
 download the requested object from.
    The 'userRequest' object has information related to the user who made this
 'GetObject' request to
    S3 Object Lambda.
    """
    get_context = event["getObjectContext"]
    user_request_headers = event["userRequest"]["headers"]

    route = get_context["outputRoute"]
    token = get_context["outputToken"]
    s3_url = get_context["inputS3Url"]

    # Check for the presence of a 'CustomHeader' header and deny or allow based on
 that header.
    is_token_present = "SuperSecretToken" in user_request_headers

    if is_token_present:
        # If the user presented our custom 'SuperSecretToken' header, we send the
 requested object back to the user.
        response = requests.get(s3_url)
        s3.write_get_object_response(RequestRoute=route, RequestToken=token,
 Body=response.content)
    else:
        # If the token is not present, we send an error back to the user.
        s3.write_get_object_response(RequestRoute=route, RequestToken=token,
 StatusCode=403,
        ErrorCode="NoSuperSecretTokenFound", ErrorMessage="The request was not
 secret enough.")
```

```
    # Gracefully exit the Lambda function.
    return { 'status_code': 200 }
```

Node.js

```
const { S3 } = require('aws-sdk');
const axios = require('axios').default;

exports.handler = async (event) => {
    const s3 = new S3();

    // Retrieve the operation context object from the event. This object indicates
 where the WriteGetObjectResponse request
    // should be delivered and contains a presigned URL in 'inputS3Url' where we can
 download the requested object from.
    // The 'userRequest' object has information related to the user who made this
 'GetObject' request to S3 Object Lambda.
    const { userRequest, getObjectContext } = event;
    const { outputRoute, outputToken, inputS3Url } = getObjectContext;

    // Check for the presence of a 'CustomHeader' header and deny or allow based on
 that header.
    const isTokenPresent = Object
        .keys(userRequest.headers)
        .includes("SuperSecretToken");

    if (!isTokenPresent) {
        // If the token is not present, we send an error back to the user. The
 'await' in front of the request
        // indicates that we want to wait for this request to finish sending before
 moving on.
        await s3.writeGetObjectResponse({
            RequestRoute: outputRoute,
            RequestToken: outputToken,
            StatusCode: 403,
            ErrorCode: "NoSuperSecretTokenFound",
            ErrorMessage: "The request was not secret enough.",
        }).promise();
    } else {
        // If the user presented our custom 'SuperSecretToken' header, we send the
 requested object back to the user.
        // Again, note the presence of 'await'.
        const presignedResponse = await axios.get(inputS3Url);
```

```
        await s3.writeGetObjectResponse({
            RequestRoute: outputRoute,
            RequestToken: outputToken,
            Body: presignedResponse.data,
        }).promise();
    }

    // Gracefully exit the Lambda function.
    return { statusCode: 200 };
}
```

示例 2：通过转换后的图像进行响应

执行图像转换时，您可能会发现需要源对象的所有字节，然后才能开始处理它们。在这种情况下，您的 `WriteGetObjectResponse` 请求会在一次调用中将整个对象返回给请求的应用程序。

Java

```
package com.amazon.s3.objectlambda;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.events.S3ObjectLambdaEvent;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3Client;
import com.amazonaws.services.s3.model.WriteGetObjectResponseRequest;

import javax.imageio.ImageIO;
import java.awt.image.BufferedImage;
import java.awt.Image;
import java.io.ByteArrayInputStream;
import java.io.ByteArrayOutputStream;
import java.net.URI;
import java.net.http.HttpClient;
import java.net.http.HttpRequest;
import java.net.http.HttpResponse;

public class Example2 {

    private static final int HEIGHT = 250;
    private static final int WIDTH = 250;
```

```
    public void handleRequest(S3ObjectLambdaEvent event, Context context) throws
 Exception {
        AmazonS3 s3Client = AmazonS3Client.builder().build();
        HttpClient httpClient = HttpClient.newBuilder().build();

        // Prepare the presigned URL for use and make the request to S3.
        var presignedResponse = httpClient.send(
                HttpRequest.newBuilder(new URI(event.inputS3Url())).GET().build(),
                HttpResponse.BodyHandlers.ofInputStream());

        // The entire image is loaded into memory here so that we can resize it.
        // Once the resizing is completed, we write the bytes into the body
        // of the WriteGetObjectResponse request.
        var originalImage = ImageIO.read(presignedResponse.body());
        var resizingImage = originalImage.getScaledInstance(WIDTH, HEIGHT,
 Image.SCALE_DEFAULT);
        var resizedImage = new BufferedImage(WIDTH, HEIGHT,
 BufferedImage.TYPE_INT_RGB);
        resizedImage.createGraphics().drawImage(resizingImage, 0, 0, WIDTH, HEIGHT,
 null);

        var baos = new ByteArrayOutputStream();
        ImageIO.write(resizedImage, "png", baos);

        // Stream the bytes back to the caller.
        s3Client.writeGetObjectResponse(new WriteGetObjectResponseRequest()
                .withRequestRoute(event.outputRoute())
                .withRequestToken(event.outputToken())
                .withInputStream(new ByteArrayInputStream(baos.toByteArray())));
    }
}
```

Python

```
import boto3
import requests
import io
from PIL import Image

def handler(event, context):
    """
    Retrieve the operation context object from the event. This object indicates
 where the WriteGetObjectResponse request
```

```
    should be delivered and has a presigned URL in 'inputS3Url' where we can
 download the requested object from.
    The 'userRequest' object has information related to the user who made this
 'GetObject' request to
    S3 Object Lambda.
    """
    get_context = event["getObjectContext"]
    route = get_context["outputRoute"]
    token = get_context["outputToken"]
    s3_url = get_context["inputS3Url"]

    """
    In this case, we're resizing .png images that are stored in S3 and are
 accessible through the presigned URL
    'inputS3Url'.
    """
    image_request = requests.get(s3_url)
    image = Image.open(io.BytesIO(image_request.content))
    image.thumbnail((256,256), Image.ANTIALIAS)

    transformed = io.BytesIO()
    image.save(transformed, "png")

    # Send the resized image back to the client.
    s3 = boto3.client('s3')
    s3.write_get_object_response(Body=transformed.getvalue(), RequestRoute=route,
 RequestToken=token)

    # Gracefully exit the Lambda function.
    return { 'status_code': 200 }
```

Node.js

```
const { S3 } = require('aws-sdk');
const axios = require('axios').default;
const sharp = require('sharp');

exports.handler = async (event) => {
    const s3 = new S3();

    // Retrieve the operation context object from the event. This object indicates
 where the WriteGetObjectResponse request
```

```
    // should be delivered and has a presigned URL in 'inputS3Url' where we can
 download the requested object from.
    const { getObjectContext } = event;
    const { outputRoute, outputToken, inputS3Url } = getObjectContext;

    // In this case, we're resizing .png images that are stored in S3 and are
 accessible through the presigned URL
    // 'inputS3Url'.
    const { data } = await axios.get(inputS3Url, { responseType: 'arraybuffer' });

    // Resize the image.
    const resized = await sharp(data)
        .resize({ width: 256, height: 256 })
        .toBuffer();

    // Send the resized image back to the client.
    await s3.writeGetObjectResponse({
        RequestRoute: outputRoute,
        RequestToken: outputToken,
        Body: resized,
    }).promise();

    // Gracefully exit the Lambda function.
    return { statusCode: 200 };
}
```

示例 3： 流式压缩内容

压缩对象时，压缩数据是以增量方式生成的。因此，您可以使用您的 `WriteGetObjectResponse` 请求在压缩数据准备就绪后立即返回压缩的数据。如本示例所示，您不需要知道已完成转换的长度。

Java

```
package com.amazon.s3.objectlambda;

import com.amazonaws.services.lambda.runtime.events.S3ObjectLambdaEvent;
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3Client;
import com.amazonaws.services.s3.model.WriteGetObjectResponseRequest;

import java.net.URI;
```

```
import java.net.http.HttpClient;
import java.net.http.HttpRequest;
import java.net.http.HttpResponse;

public class Example3 {

    public void handleRequest(S3ObjectLambdaEvent event, Context context) throws
 Exception {
        AmazonS3 s3Client = AmazonS3Client.builder().build();
        HttpClient httpClient = HttpClient.newBuilder().build();

        // Request the original object from S3.
        var presignedResponse = httpClient.send(
                HttpRequest.newBuilder(new URI(event.inputS3Url())).GET().build(),
                HttpResponse.BodyHandlers.ofInputStream());

        // Consume the incoming response body from the presigned request,
        // apply our transformation on that data, and emit the transformed bytes
        // into the body of the WriteGetObjectResponse request as soon as they're
 ready.
        // This example compresses the data from S3, but any processing pertinent
        // to your application can be performed here.
        var bodyStream = new GZIPCompressingInputStream(presignedResponse.body());

        // Stream the bytes back to the caller.
        s3Client.writeGetObjectResponse(new WriteGetObjectResponseRequest()
                .withRequestRoute(event.outputRoute())
                .withRequestToken(event.outputToken())
                .withInputStream(bodyStream));
    }

}
```

Python

```
import boto3
import requests
import zlib
from botocore.config import Config


"""
```

```
A helper class to work with content iterators. Takes an interator and compresses the
 bytes that come from it. It
implements 'read' and '__iter__' so that the SDK can stream the response.
"""
class Compress:
    def __init__(self, content_iter):
        self.content = content_iter
        self.compressed_obj = zlib.compressobj()

    def read(self, _size):
        for data in self.__iter__()
            return data

    def __iter__(self):
        while True:
            data = next(self.content)
            chunk = self.compressed_obj.compress(data)
            if not chunk:
                break

            yield chunk

        yield self.compressed_obj.flush()


def handler(event, context):
    """
    Setting the 'payload_signing_enabled' property to False allows us to send a
 streamed response back to the client.
    in this scenario, a streamed response means that the bytes are not buffered into
 memory as we're compressing them,
    but instead are sent straight to the user.
    """
    my_config = Config(
        region_name='eu-west-1',
        signature_version='s3v4',
        s3={
            "payload_signing_enabled": False
        }
    )
    s3 = boto3.client('s3', config=my_config)

    """
```

```
    Retrieve the operation context object from the event. This object indicates
 where the WriteGetObjectResponse request
    should be delivered and has a presigned URL in 'inputS3Url' where we can
 download the requested object from.
    The 'userRequest' object has information related to the user who made this
 'GetObject' request to S3 Object Lambda.
    """
    get_context = event["getObjectContext"]
    route = get_context["outputRoute"]
    token = get_context["outputToken"]
    s3_url = get_context["inputS3Url"]

    # Compress the 'get' request stream.
    with requests.get(s3_url, stream=True) as r:
        compressed = Compress(r.iter_content())

        # Send the stream back to the client.
        s3.write_get_object_response(Body=compressed, RequestRoute=route,
 RequestToken=token, ContentType="text/plain",
                                     ContentEncoding="gzip")

    # Gracefully exit the Lambda function.
    return {'status_code': 200}
```

Node.js

```
const { S3 } = require('aws-sdk');
const axios = require('axios').default;
const zlib = require('zlib');

exports.handler = async (event) => {
    const s3 = new S3();

    // Retrieve the operation context object from the event. This object indicates
 where the WriteGetObjectResponse request
    // should be delivered and has a presigned URL in 'inputS3Url' where we can
 download the requested object from.
    const { getObjectContext } = event;
    const { outputRoute, outputToken, inputS3Url } = getObjectContext;

    // Download the object from S3 and process it as a stream, because it might be a
 huge object and we don't want to
```

```
    // buffer it in memory. Note the use of 'await' because we want to wait for
 'writeGetObjectResponse' to finish
    // before we can exit the Lambda function.
    await axios({
        method: 'GET',
        url: inputS3Url,
        responseType: 'stream',
    }).then(
        // Gzip the stream.
        response => response.data.pipe(zlib.createGzip())
    ).then(
        // Finally send the gzip-ed stream back to the client.
        stream => s3.writeGetObjectResponse({
            RequestRoute: outputRoute,
            RequestToken: outputToken,
            Body: stream,
            ContentType: "text/plain",
            ContentEncoding: "gzip",
        }).promise()
    );

    // Gracefully exit the Lambda function.
    return { statusCode: 200 };
}
```

> **Note**
>
> 虽然 S3 对象 Lambda 允许使用长达 60 秒的时间通过 `WriteGetObjectResponse` 请求来将完整响应发送给发起人，但实际可用时间可能会减少。例如，Lambda 函数超时可能少于 60 秒。在其他情况下，发起人可能会有更严格的超时。

要使原始调用方能够收到非 HTTP 状态代码 500（内部服务器错误）响应，必须完成 `WriteGetObjectResponse` 调用。如果 Lambda 函数返回时引发了异常或其他情况，则在调用 `WriteGetObjectResponse` API 操作之前，原始调用方将收到 500（内部服务器错误）响应。在完成响应所需的时间内引发的异常将导致截断对发起人的响应。如果 Lambda 函数从 `WriteGetObjectResponse` API 调用收到 HTTP 状态代码 200（OK）响应，即表示原始调用方已经发送了完整的请求。S3 对象 Lambda 会忽略 Lambda 函数的响应，无论是否抛出异常。

调用 WriteGetObjectResponse API 操作时，Amazon S3 需要事件上下文中的路由和请求令牌。有关更多信息，请参阅 事件上下文格式和用法。

将 WriteGetObjectResult 请求与原始调用方连接起来需要这些路由和请求令牌参数。尽管重试 500（内部服务器错误）响应始终是适当的，但请注意，由于请求令牌是一个单一用途令牌，后续尝试使用它可能会导致 HTTP 状态代码 400（错误请求）响应。虽然使用路由和请求令牌调用 WriteGetObjectResponse 不需要从被调用的 Lambda 函数发出，但它必须由同一账户中的身份发出。还必须在 Lambda 函数完成执行之前完成调用。

## 在 Lambda 中处理 **HeadObject** 请求

本节假设您的对象 Lambda 接入点配置为对于 HeadObject 调用 Lambda 函数。Lambda 将收到一个 JSON 有效负载，其中包含名为 headObjectContext 的密钥。在上下文中，有一个名为 inputS3Url 的属性，它是 HeadObject 的支持接入点的预签名 URL。

预签名 URL 将包含以下属性（如果已指定）：

- versionId（在查询参数中）
- requestPayer（在 x-amz-request-payer 标头中）
- expectedBucketOwner（在 x-amz-expected-bucket-owner 标头中）

其他属性未预签名，因此不会包含在内。当调用在 userRequest 标头中找到的预签名 URL 时，可以手动将作为标头发送的未签名选项添加到请求中。对于 HeadObject，不支持服务器端加密选项。

有关请求语法 URI 参数，请参阅《Amazon Simple Storage Service API 参考》中的 HeadObject。

以下示例显示了 HeadObject 的 Lambda JSON 输入有效负载。

```
{
  "xAmzRequestId": "requestId",
  "**headObjectContext**": {
    "**inputS3Url**": "https://my-s3-ap-111122223333.s3-accesspoint.us-
east-1.amazonaws.com/example?X-Amz-Security-Token=<snip>"
  },
  "configuration": {
        "accessPointArn": "arn:aws:s3-object-lambda:us-
east-1:111122223333:accesspoint/example-object-lambda-ap",
        "supportingAccessPointArn": "arn:aws:s3:us-
east-1:111122223333:accesspoint/example-ap",
        "payload": "{}"
  },
```

```
  "userRequest": {
       "url": "https://object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com/example",
       "headers": {
           "Host": "object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com",
           "Accept-Encoding": "identity",
           "X-Amz-Content-SHA256": "e3b0c44298fc1example"
       }
   },
   "userIdentity": {
       "type": "AssumedRole",
       "principalId": "principalId",
       "arn": "arn:aws:sts::111122223333:assumed-role/Admin/example",
       "accountId": "111122223333",
       "accessKeyId": "accessKeyId",
       "sessionContext": {
            "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "Wed Mar 10 23:41:52 UTC 2021"
       },
       "sessionIssuer": {
            "type": "Role",
            "principalId": "principalId",
            "arn": "arn:aws:iam::111122223333:role/Admin",
            "accountId": "111122223333",
            "userName": "Admin"
            }
       }
    },
  "protocolVersion": "1.00"
}
```

您的 Lambda 函数应返回一个 JSON 对象，其中包含将针对 `HeadObject` 调用返回的标头和值。

下面的示例显示 `HeadObject` 的 Lambda 响应 JSON 的结构。

```
{
    "statusCode": <number>; // Required
    "errorCode": <string>;
    "errorMessage": <string>;
    "headers": {
        "Accept-Ranges": <string>,
        "x-amz-archive-status": <string>,
```

```
        "x-amz-server-side-encryption-bucket-key-enabled": <boolean>,
        "Cache-Control": <string>,
        "Content-Disposition": <string>,
        "Content-Encoding": <string>,
        "Content-Language": <string>,
        "Content-Length": <number>, // Required
        "Content-Type": <string>,
        "x-amz-delete-marker": <boolean>,
        "ETag": <string>,
        "Expires": <string>,
        "x-amz-expiration": <string>,
        "Last-Modified": <string>,
        "x-amz-missing-meta": <number>,
        "x-amz-object-lock-mode": <string>,
        "x-amz-object-lock-legal-hold": <string>,
        "x-amz-object-lock-retain-until-date": <string>,
        "x-amz-mp-parts-count": <number>,
        "x-amz-replication-status": <string>,
        "x-amz-request-charged": <string>,
        "x-amz-restore": <string>,
        "x-amz-server-side-encryption": <string>,
        "x-amz-server-side-encryption-customer-algorithm": <string>,
        "x-amz-server-side-encryption-aws-kms-key-id": <string>,
        "x-amz-server-side-encryption-customer-key-MD5": <string>,
        "x-amz-storage-class": <string>,
        "x-amz-tagging-count": <number>,
        "x-amz-version-id": <string>,
        <x-amz-meta-headers>: <string>, // user-defined metadata
        "x-amz-meta-meta1": <string>, // example of the user-defined metadata header,
 it will need the x-amz-meta prefix
        "x-amz-meta-meta2": <string>
        ...
    };
}
```

以下示例显示如何在返回 JSON 之前根据需要修改标头值，以使用预签名 URL 来填充您的响应。

Python

```
import requests

def lambda_handler(event, context):
    print(event)
```

```
    # Extract the presigned URL from the input.
    s3_url = event["headObjectContext"]["inputS3Url"]

    # Get the head of the object from S3.
    response = requests.head(s3_url)

    # Return the error to S3 Object Lambda (if applicable).
    if (response.status_code >= 400):
        return {
            "statusCode": response.status_code,
            "errorCode": "RequestFailure",
            "errorMessage": "Request to S3 failed"
    }

    # Store the headers in a dictionary.
    response_headers = dict(response.headers)

    # This obscures Content-Type in a transformation, it is optional to add
    response_headers["Content-Type"] = ""

    # Return the headers to S3 Object Lambda.
    return {
        "statusCode": response.status_code,
        "headers": response_headers
        }
```

## 在 Lambda 中处理 **ListObjects** 请求

本节假设您的对象 Lambda 接入点配置为对于 `ListObjects` 调用 Lambda 函数。Lambda 将收到带有名为 `listObjectsContext` 的新对象的 JSON 有效负载。`listObjectsContext` 包含单个属性 `inputS3Url`，它是 `ListObjects` 的支持接入点的预签名 URL。

与 `GetObject` 和 `HeadObject` 不同，预签名 URL 将包含以下属性（如果已指定）：

- 所有查询参数
- `requestPayer`（在 `x-amz-request-payer` 标头中）
- `expectedBucketOwner`（在 `x-amz-expected-bucket-owner` 标头中）

有关请求语法 URI 参数，请参阅《Amazon Simple Storage Service API 参考》中的 `ListObjects`。

> **Important**
>
> 我们建议您在开发应用程序时使用较新的版本 ListObjectsV2。为了向后兼容，Amazon S3 仍继续支持 `ListObjects`。

以下示例显示了 `ListObjects` 的 Lambda JSON 输入有效负载。

```
{
    "xAmzRequestId": "requestId",
     "**listObjectsContext**": {
     "**inputS3Url**": "https://my-s3-ap-111122223333.s3-accesspoint.us-
east-1.amazonaws.com/?X-Amz-Security-Token=<snip>",
     },
    "configuration": {
        "accessPointArn": "arn:aws:s3-object-lambda:us-
east-1:111122223333:accesspoint/example-object-lambda-ap",
        "supportingAccessPointArn": "arn:aws:s3:us-
east-1:111122223333:accesspoint/example-ap",
        "payload": "{}"
    },
    "userRequest": {
        "url": "https://object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com/example",
        "headers": {
            "Host": "object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com",
            "Accept-Encoding": "identity",
            "X-Amz-Content-SHA256": "e3b0c44298fc1example"
        }
    },
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "principalId",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/example",
        "accountId": "111122223333",
        "accessKeyId": "accessKeyId",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "Wed Mar 10 23:41:52 UTC 2021"
            },
            "sessionIssuer": {
```

```
                "type": "Role",
                "principalId": "principalId",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            }
        }
    },
  "protocolVersion": "1.00"
}
```

您的 Lambda 函数应返回一个 JSON 对象，其中包含将从 S3 对象 Lambda 返回的状态码、列表 XML 结果或错误信息。

S3 对象 Lambda 不处理或验证 `listResultXml`，而是将其转发给 `ListObjects` 调用方。对于 `listBucketResult`，S3 对象 Lambda 期望某些属性属于特定类型，如果它无法解析它们，则会引发异常。无法同时提供 `listResultXml` 和 `listBucketResult`。

以下示例演示如何使用预签名 URL 调用 Amazon S3 并使用结果填充响应，包括错误检查。

Python

```
import requests
import xmltodict

def lambda_handler(event, context):
    # Extract the presigned URL from the input.
    s3_url = event["listObjectsContext"]["inputS3Url"]


    # Get the head of the object from Amazon S3.
    response = requests.get(s3_url)

    # Return the error to S3 Object Lambda (if applicable).
    if (response.status_code >= 400):
        error = xmltodict.parse(response.content)
        return {
            "statusCode": response.status_code,
            "errorCode": error["Error"]["Code"],
            "errorMessage": error["Error"]["Message"]
        }

    # Store the XML result in a dict.
```

```
    response_dict = xmltodict.parse(response.content)

    # This obscures StorageClass in a transformation, it is optional to add
    for item in response_dict['ListBucketResult']['Contents']:
        item['StorageClass'] = ""

    # Convert back to XML.
    listResultXml = xmltodict.unparse(response_dict)

    # Create response with listResultXml.
    response_with_list_result_xml = {
        'statusCode': 200,
        'listResultXml': listResultXml
    }

    # Create response with listBucketResult.
    response_dict['ListBucketResult'] =
 sanitize_response_dict(response_dict['ListBucketResult'])
    response_with_list_bucket_result = {
        'statusCode': 200,
        'listBucketResult': response_dict['ListBucketResult']
    }

    # Return the list to S3 Object Lambda.
    # Can return response_with_list_result_xml or response_with_list_bucket_result
    return response_with_list_result_xml

# Converting the response_dict's key to correct casing
def sanitize_response_dict(response_dict: dict):
    new_response_dict = dict()
    for key, value in response_dict.items():
        new_key = key[0].lower() + key[1:] if key != "ID" else 'id'
        if type(value) == list:
            newlist = []
            for element in value:
                if type(element) == type(dict()):
                    element = sanitize_response_dict(element)
                newlist.append(element)
            value = newlist
        elif type(value) == dict:
            value = sanitize_response_dict(value)
        new_response_dict[new_key] = value
    return new_response_dict
```

下面的示例显示 `ListObjects` 的 Lambda 响应 JSON 的结构。

```
{
  "statusCode": <number>; // Required
  "errorCode": <string>;
  "errorMessage": <string>;
  "listResultXml": <string>; // This can also be Error XML string in case S3 returned
 error response when calling the pre-signed URL

  "listBucketResult": {  // listBucketResult can be provided instead of listResultXml,
 however they can not both be provided in the JSON response
        "name": <string>,  // Required for 'listBucketResult'
        "prefix": <string>,
        "marker": <string>,
        "nextMarker": <string>,
        "maxKeys": <int>,   // Required for 'listBucketResult'
        "delimiter": <string>,
        "encodingType": <string>
        "isTruncated": <boolean>,  // Required for 'listBucketResult'
        "contents": [  {
            "key": <string>,  // Required for 'content'
            "lastModified": <string>,
            "eTag": <string>,
            "checksumAlgorithm": <string>,   // CRC32,  CRC32C,  SHA1,  SHA256
            "size": <int>,   // Required for 'content'
            "owner": {
                "displayName": <string>,  // Required for 'owner'
                "id": <string>,  // Required for 'owner'
            },
            "storageClass": <string>
            },
        ...
        ],
        "commonPrefixes": [  {
            "prefix": <string>   // Required for 'commonPrefix'
        },
        ...
        ],
    }
}
```

## 在 Lambda 中处理 **ListObjectsV2** 请求

本节假设您的对象 Lambda 接入点配置为对于 `ListObjectsV2` 调用 Lambda 函数。Lambda 将收到带有名为 `listObjectsV2Context` 的新对象的 JSON 有效负载。`listObjectsV2Context` 包含单个属性 `inputS3Url`，它是 `ListObjectsV2` 的支持接入点的预签名 URL。

与 `GetObject` 和 `HeadObject` 不同，预签名 URL 将包含以下属性（如果已指定）：

- 所有查询参数
- `requestPayer`（在 `x-amz-request-payer` 标头中）
- `expectedBucketOwner`（在 `x-amz-expected-bucket-owner` 标头中）

有关请求语法 URI 参数，请参阅《Amazon Simple Storage Service API 参考》中的 `ListObjectsV2`。

以下示例显示了 `ListObjectsV2` 的 Lambda JSON 输入有效负载。

```
{
    "xAmzRequestId": "requestId",
     "**listObjectsV2Context**": {
     "**inputS3Url**": "https://my-s3-ap-111122223333.s3-accesspoint.us-
east-1.amazonaws.com/?list-type=2&X-Amz-Security-Token=<snip>",
     },
    "configuration": {
        "accessPointArn": "arn:aws:s3-object-lambda:us-
east-1:111122223333:accesspoint/example-object-lambda-ap",
        "supportingAccessPointArn": "arn:aws:s3:us-
east-1:111122223333:accesspoint/example-ap",
        "payload": "{}"
    },
    "userRequest": {
        "url": "https://object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com/example",
        "headers": {
            "Host": "object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com",
            "Accept-Encoding": "identity",
            "X-Amz-Content-SHA256": "e3b0c44298fc1example"
        }
    },
    "userIdentity": {
```

```
        "type": "AssumedRole",
        "principalId": "principalId",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/example",
        "accountId": "111122223333",
        "accessKeyId": "accessKeyId",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "Wed Mar 10 23:41:52 UTC 2021"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "principalId",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            }
        }
    },
  "protocolVersion": "1.00"
}
```

您的 Lambda 函数应返回一个 JSON 对象，其中包含将从 S3 对象 Lambda 返回的状态码、列表 XML 结果或错误信息。

S3 对象 Lambda 不处理或验证 `listResultXml`，而是将其转发给 `ListObjectsV2` 调用方。对于 `listBucketResult`，S3 对象 Lambda 期望某些属性属于特定类型，如果它无法解析它们，则会引发异常。无法同时提供 `listResultXml` 和 `listBucketResult`。

以下示例演示如何使用预签名 URL 调用 Amazon S3 并使用结果填充响应，包括错误检查。

Python

```
import requests
import xmltodict

def lambda_handler(event, context):
    # Extract the presigned URL from the input.
    s3_url = event["listObjectsV2Context"]["inputS3Url"]


    # Get the head of the object from Amazon S3.
    response = requests.get(s3_url)
```

```
    # Return the error to S3 Object Lambda (if applicable).
    if (response.status_code >= 400):
        error = xmltodict.parse(response.content)
        return {
            "statusCode": response.status_code,
            "errorCode": error["Error"]["Code"],
            "errorMessage": error["Error"]["Message"]
        }

    # Store the XML result in a dict.
    response_dict = xmltodict.parse(response.content)

    # This obscures StorageClass in a transformation, it is optional to add
    for item in response_dict['ListBucketResult']['Contents']:
        item['StorageClass'] = ""

    # Convert back to XML.
    listResultXml = xmltodict.unparse(response_dict)

    # Create response with listResultXml.
    response_with_list_result_xml = {
        'statusCode': 200,
        'listResultXml': listResultXml
    }

    # Create response with listBucketResult.
    response_dict['ListBucketResult'] =
 sanitize_response_dict(response_dict['ListBucketResult'])
    response_with_list_bucket_result = {
        'statusCode': 200,
        'listBucketResult': response_dict['ListBucketResult']
    }

    # Return the list to S3 Object Lambda.
    # Can return response_with_list_result_xml or response_with_list_bucket_result
    return response_with_list_result_xml

# Converting the response_dict's key to correct casing
def sanitize_response_dict(response_dict: dict):
    new_response_dict = dict()
    for key, value in response_dict.items():
        new_key = key[0].lower() + key[1:] if key != "ID" else 'id'
        if type(value) == list:
```

```
            newlist = []
            for element in value:
                if type(element) == type(dict()):
                    element = sanitize_response_dict(element)
                newlist.append(element)
            value = newlist
        elif type(value) == dict:
            value = sanitize_response_dict(value)
        new_response_dict[new_key] = value
    return new_response_dict
```

下面的示例显示 `ListObjectsV2` 的 Lambda 响应 JSON 的结构。

```
{
    "statusCode": <number>; // Required
    "errorCode": <string>;
    "errorMessage": <string>;
    "listResultXml": <string>; // This can also be Error XML string in case S3 returned
 error response when calling the pre-signed URL

    "listBucketResult": {  // listBucketResult can be provided instead of
 listResultXml, however they can not both be provided in the JSON response
        "name": <string>, // Required for 'listBucketResult'
        "prefix": <string>,
        "startAfter": <string>,
        "continuationToken": <string>,
        "nextContinuationToken": <string>,
        "keyCount": <int>, // Required for 'listBucketResult'
        "maxKeys": <int>, // Required for 'listBucketResult'
        "delimiter": <string>,
        "encodingType": <string>
        "isTruncated": <boolean>, // Required for 'listBucketResult'
        "contents": [ {
            "key": <string>, // Required for 'content'
            "lastModified": <string>,
            "eTag": <string>,
            "checksumAlgorithm": <string>, // CRC32, CRC32C, SHA1, SHA256
            "size": <int>, // Required for 'content'
            "owner": {
                "displayName": <string>, // Required for 'owner'
                "id": <string>, // Required for 'owner'
            },
```

```
            "storageClass": <string>
            },
            ...
        ],
        "commonPrefixes": [ {
            "prefix": <string> // Required for 'commonPrefix'
            },
        ...
        ],
    }
}
```

## 事件上下文格式和用法

Amazon S3 对象 Lambda 提供了有关在传递给 Amazon Lambda 函数的事件中发出的请求的上下文。以下屏幕截图显示一个示例请求。示例后面包含对各个字段的描述。

```
{
    "xAmzRequestId": "requestId",
    "getObjectContext": {
        "inputS3Url": "https://my-s3-ap-111122223333.s3-accesspoint.us-
east-1.amazonaws.com/example?X-Amz-Security-Token=<snip>",
        "outputRoute": "io-use1-001",
        "outputToken": "OutputToken"
    },
    "configuration": {
        "accessPointArn": "arn:aws:s3-object-lambda:us-
east-1:111122223333:accesspoint/example-object-lambda-ap",
        "supportingAccessPointArn": "arn:aws:s3:us-
east-1:111122223333:accesspoint/example-ap",
        "payload": "{}"
    },
    "userRequest": {
        "url": "https://object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com/example",
        "headers": {
            "Host": "object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com",
            "Accept-Encoding": "identity",
            "X-Amz-Content-SHA256": "e3b0c44298fc1example"
        }
    },
    "userIdentity": {
```

```
        "type": "AssumedRole",
        "principalId": "principalId",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/example",
        "accountId": "111122223333",
        "accessKeyId": "accessKeyId",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "Wed Mar 10 23:41:52 UTC 2021"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "principalId",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            }
        }
    },
    "protocolVersion": "1.00"
}
```

请求中包含以下字段：

- `xAmzRequestId` – 此请求的 Amazon S3 请求 ID。我们建议您记录此值以帮助调试。
- `getObjectContext` – 连接到 Amazon S3 和 S3 对象 Lambda 的输入和输出详细信息。
  - `inputS3Url` – 可用于从 Amazon S3 获取原始对象的预签名 URL。URL 是使用原始调用方的身份进行签名的，使用 URL 时该用户的权限将适用。如果 URL 中有签名标头，则 Lambda 函数必须将这些标头包含在对 Amazon S3 的调用中，`Host` 标头除外。
  - `outputRoute` – 在 Lambda 函数调用 `WriteGetObjectResponse` 时添加到 S3 对象 Lambda URL 的路由令牌。
  - `outputToken` – S3 对象 Lambda 使用的不透明令牌，用于将 `WriteGetObjectResponse` 调用与原始调用方相匹配。
- `configuration` – 有关对象 Lambda 接入点的配置信息。
  - `accessPointArn` – 收到此请求的对象 Lambda 接入点的 Amazon 资源名称（ARN）。
  - `supportingAccessPointArn` – 在对象 Lambda 接入点配置中指定的支持接入点的 ARN。
  - `payload` – 应用于对象 Lambda 接入点配置的自定义数据。S3 对象 Lambda 将此数据视为不透明字符串，因此在使用前可能需要对其进行解码。

- `userRequest` – 有关对 S3 对象 Lambda 的原始调用的信息。
  - `url` – S3 对象 Lambda 接收的请求的解码 URL，不包括任何与授权相关的查询参数。
  - `headers` – 字符串到字符串的映射，包含原始调用中的 HTTP 标头及其值，不包括任何与授权相关的标头。如果同一个标头多次出现，会将相同标头的每个实例中的值组合成一个以逗号分隔的列表。此映射中会保留原始标头的大小写。
- `userIdentity` – 有关对 S3 对象 Lambda 发出调用的身份的详细信息。有关更多信息，请参阅 Amazon CloudTrail 用户指南中的记录数据事件以便跟踪。
  - `type` – 身份的类型。
  - `accountId` – 身份所属的 Amazon Web Services 账户。
  - `userName` – 已发出调用的身份的友好名称。
  - `principalId` – 已发出调用的身份的唯一标识符。
  - `arn` – 已发出调用的主体的 ARN。ARN 的最后一个部分包含已发出调用的用户或角色。
  - `sessionContext` – 如果已使用临时安全证书发出请求，此元素提供有关已为这些证书创建的会话的信息。
  - `invokedBy` – 发出请求的 Amazon Web Services 服务 的名称，例如 Amazon EC2 Auto Scaling 或 Amazon Elastic Beanstalk。
  - `sessionIssuer` – 如果已使用临时安全证书发出请求，此元素提供有关证书获取方式的信息。
- `protocolVersion` – 提供的上下文的版本 ID。此字段的格式为 `{Major Version}.{Minor Version}`。次要版本号始终是两位数字。对字段的语义进行任何删除或更改都将导致主要版本冲突，并且需要主动选择加入。Amazon S3 可以随时添加新字段，此时您可能会遇到次要版本冲突。由于软件部署的性质，您可能会同时看到多个次要版本处于使用状态。

## 使用 Range 和 partNumber 标头

在 Amazon S3 对象 Lambda 中使用大型对象时，您可以使用 `Range` HTTP 标头从对象中下载指定的字节范围。要从相同对象中提取不同的字节范围，您可以使用到 Amazon S3 的并发连接。还可以指定 `partNumber` 参数（1 到 10000 之间的整数），它对于对象的指定分段执行范围内的请求。

由于您可能希望通过多种方法来处理包括 `Range` 或 `partNumber` 参数的请求，S3 对象 Lambda 不会将这些参数应用于转换后的对象。相反，您的 Amazon Lambda 函数必须根据应用程序的需要实施此功能。

要对 S3 对象 Lambda 使用 `Range` 和 `partNumber` 参数，请执行以下操作：

- 在对象 Lambda 接入点配置中启用这些参数。

- 编写一个 Lambda 函数，以处理包含这些参数的请求。

以下步骤介绍了如何完成此操作。

步骤 1：配置对象 Lambda 接入点

默认情况下，对象 Lambda 接入点会对在标头或查询参数中包含 Range 或 partNumber 参数的任何 GetObject 或 HeadObject 请求响应 HTTP 状态代码 501（未实施）错误。

要使对象 Lambda 接入点能够接受此类请求，您必须在对象 Lambda 接入点配置的 AllowedFeatures 部分中加入 GetObject-Range、GetObject-PartNumber、HeadObject-Range 或 HeadObject-PartNumber。有关更新对象 Lambda 接入点配置的更多信息，请参阅创建对象 Lambda 接入点。

步骤 2：在 Lambda 函数中实施 **Range** 或 **partNumber** 处理

当对象 Lambda 接入点使用范围内的 GetObject 或 HeadObject 请求调用 Lambda 函数时，Range 或 partNumber 参数将包含在事件上下文中。如下表所述，参数在事件上下文中的位置取决于使用的参数以及如何将其包含在对于对象 Lambda 接入点的原始请求中。

| 参数 | 事件上下文位置 |
| --- | --- |
| Range（标头） | userRequest.headers.Range |
| Range（查询参数） | userRequest.url （查询参数 Range） |
| partNumber | userRequest.url （查询参数 partNumber ） |

> **Important**
>
> 为对象 Lambda 接入点提供的预签名 URL 不包含原始请求中的 Range 或 partNumber 参数。请参阅以下选项，了解如何在 Amazon Lambda 函数中处理这些参数。

在您提取 Range 或 partNumber 值后，您可以根据应用程序的需要采取以下方法之一：

A. 将请求的 **Range** 或 **partNumber** 映射到转换后的对象（建议）。

处理 Range 或 partNumber 请求的最可靠方法是执行以下操作：

- 从 Amazon S3 中检索完整的对象。
- 转换对象。
- 将请求的 Range 或 partNumber 参数应用于转换的对象。

为此，请使用提供的预签名 URL 从 Amazon S3 获取整个对象，然后根据需要处理该对象。对于 Lambda 函数以此方式处理 Range 函数的示例，请参阅 Amazon Samples GitHub 存储库中的此示例。

B. 将请求的 **Range** 映射到预签名的 URL。

在某些情况下，您的 Lambda 函数可以将请求的 Range 直接映射到预签名 URL，以便仅从 Amazon S3 中检索对象的一部分。仅当您的转换符合以下两个条件时，此方法才适用：

1. 您的转换函数可以应用于部分对象范围。
2. 在转换函数之前或之后应用 Range 参数会得到相同的已转换对象。

例如，将 ASCII 编码对象中的所有字符转换为大写的转换函数符合上述两个条件。转换可以应用于对象的一部分，在转换之前应用 Range 参数获得的结果与在转换后应用此参数相同。

相比之下，反转 ASCII 编码对象中的字符的函数不符合这些条件。这样的函数符合标准 1，因为它可以应用于部分对象范围。但是，它不符合标准 2，因为在转换之前应用 Range 参数达到的结果与在转换后应用参数不同。

考虑请求将函数应用于包含内容 abcdefg 的对象的前三个字符。在转换前应用 Range 参数将仅检索 abc，然后反转数据，从而返回 cba。但是，如果在转换之后应用该参数，则函数将检索整个对象，将其反转，然后应用 Range 参数，以返回 gfe。由于这些结果不同，此函数在从 Amazon S3 中检索对象时不应应用 Range 参数。相反，它应该检索整个对象，执行转换，然后仅应用 Range 参数。

> **Warning**
>
> 在很多情况下，向预签名 URL 应用 Range 参数将导致 Lambda 函数或发出请求的客户端出现意外行为。除非您确定应用程序在从 Amazon S3 中仅检索部分对象时能够正常工作，否则我们建议您按照前面的方法 A 中所述检索和转换完整对象。

如果您的应用程序符合前面在方法 B 中介绍的条件，您可以简化您的 Amazon Lambda 函数，方法是仅获取所请求的对象范围，然后在该范围内运行转换。

以下 Java 代码示例演示如何执行以下操作：

- 从 `GetObject` 请求中检索 `Range` 标头。
- 将 `Range` 标头添加到预签名 URL 中，Lambda 可以使用此标头从 Amazon S3 中检索请求的范围。

```
private HttpRequest.Builder applyRangeHeader(ObjectLambdaEvent event,
 HttpRequest.Builder presignedRequest) {
    var header = event.getUserRequest().getHeaders().entrySet().stream()
            .filter(e -> e.getKey().toLowerCase(Locale.ROOT).equals("range"))
            .findFirst();

    // Add check in the query string itself.
    header.ifPresent(entry -> presignedRequest.header(entry.getKey(),
 entry.getValue()));
    return presignedRequest;
}
```

## 使用 Amazon 构建的 Lambda 函数

Amazon 提供了一些预构建的 Amazon Lambda 函数，您可以将这些函数与 S3 对象 Lambda 结合使用，以检测和编辑个人身份信息（PII）以及解压缩 S3 对象。这些 Lambda 函数可在 Amazon Serverless Application Repository 中使用。您可以在创建对象 Lambda 接入点时通过 Amazon Web Services Management Console选择这些函数。

有关如何从 Amazon Serverless Application Repository 部署无服务器应用程序的更多信息，请参阅《Amazon Serverless Application Repository 开发人员指南》中的部署应用程序。

> **Note**
>
> 以下示例只能与 `GetObject` 请求结合使用。

### 示例 1：PII 访问控制

此 Lambda 函数使用 Amazon Comprehend，这是一项自然语言处理（NLP）服务，它使用机器学习发现文本中的见解和关系。此函数自动从 Amazon S3 存储桶的文档中检测个人身份信息（PII），例如姓名、地址、日期、信用卡号和社会保障号码。如果存储桶中具有包含 PII 的文档，则可以将 PII 访问控制函数配置为检测这些 PII 实体类型并限制未授权用户进行访问。

要开始使用，请在您的账户中部署以下 Lambda 函数，然后向对象 Lambda 接入点配置中添加此函数的 Amazon 资源名称（ARN）。

以下是此函数的示例 ARN：

```
arn:aws:serverlessrepo:us-east-1:111122223333:applications/
ComprehendPiiAccessControlS3ObjectLambda
```

您可以使用以下 Amazon Serverless Application Repository 链接在 Amazon Web Services Management Console上添加或查看此函数：ComprehendPiiAccessControlS3ObjectLambda。

要在 GitHub 上查看此函数，请参阅 Amazon Comprehend S3 对象 Lambda。

### 示例 2：PII 编辑

此 Lambda 函数使用 Amazon Comprehend，这是一项自然语言处理（NLP）服务，它使用机器学习发现文本中的见解和关系。此函数自动从 Amazon S3 存储桶的文档中编辑个人身份信息（PII），例如姓名、地址、日期、信用卡号和社会保障号码。

如果存储桶中具有包含信用卡号或银行账户信息等信息的文档，则可以将 PII Redction S3 对象 Lambda 函数配置为检测 PII，然后返回这些文档的副本，在这些文档中，已对 PII 实体类型进行了编辑。

要开始使用，请在您的账户中部署以下 Lambda 函数，然后向对象 Lambda 接入点配置中添加此函数的 ARN。

以下是此函数的示例 ARN：

```
arn:aws:serverlessrepo:us-east-1:111122223333::applications/
ComprehendPiiRedactionS3ObjectLambda
```

您可以使用以下 Amazon Web Services Management Console 链接在 Amazon Serverless Application Repository上添加或查看此函数：ComprehendPiiRedactionS3ObjectLambda。

要在 GitHub 上查看此函数，请参阅 Amazon Comprehend S3 对象 Lambda。

要了解 PII 编辑中某些 S3 对象 Lambda 任务的完整端到端过程，请参阅教程：使用 S3 对象 Lambda 和 Amazon Comprehend 检测和修订 PII 数据。

### 示例 3：Decompression

Lambda 函数 `S3ObjectLambdaDecompression` 可以将存储在 Amazon S3 中的对象解压缩为六种压缩文件格式之一：`bzip2`、`gzip`、`snappy`、`zlib`、`zstandard` 和 `ZIP`。

要开始使用，请在您的账户中部署以下 Lambda 函数，然后向对象 Lambda 接入点配置中添加此函数的 ARN。

以下是此函数的示例 ARN：

```
arn:aws:serverlessrepo:us-east-1:111122223333::applications/S3ObjectLambdaDecompression
```

您可以使用以下 Amazon Web Services Management Console 链接在 Amazon Serverless Application Repository上添加或查看此函数：S3ObjectLambdaDecompression。

要在 GitHub 上查看此函数，请参阅 S3 对象 Lambda 解压缩。

## S3 对象 Lambda 的最佳实践和指南

使用 S3 对象 Lambda 时，请遵循以下最佳实践和指南来优化操作和性能。

主题

- 使用 S3 对象 Lambda
- 与 S3 对象 Lambda 结合使用的 Amazon Web Services 服务
- Range 和 partNumber 标头
- 转换 expiry-date
- 使用 Amazon CLI 和 Amazon SDK

### 使用 S3 对象 Lambda

S3 对象 Lambda 仅支持处理 `GET`、`LIST` 和 `HEAD` 请求。任何其他请求都不会调用 Amazon Lambda，而是返回标准的未转换 API 响应。每个 Amazon Web Services 账户、每个区域最多可以创建 1000 个对象 Lambda 接入点。您使用的 Amazon Lambda 函数必须与对象 Lambda 接入点位于同一 Amazon Web Services 账户和区域中。

S3 对象 Lambda 允许使用长达 60 秒的时间将完整的响应流式传输到发起人。您的函数还受 Amazon Lambda 默认限额的约束。有关更多信息，请参阅《Amazon Lambda 开发人员指南》中的 Lambda 配额。

当 S3 对象 Lambda 调用您指定的 Lambda 函数时，您有责任确保指定的 Lambda 函数或应用程序从 Amazon S3 中覆盖或删除的任何数据都符合预期且正确。

您只能使用 S3 对象 Lambda 对于对象执行操作。您不能使用 S3 对象 Lambda 执行其他 Amazon S3 操作，例如修改或删除存储桶。有关支持接入点的 S3 操作的完整列表，请参阅通用存储桶的接入点与 S3 操作的兼容性。

除此列表外，对象 Lambda 接入点不支持 `POST Object`、`CopyObject`（作为源）和 `SelectObjectContent` API 操作。

## 与 S3 对象 Lambda 结合使用的 Amazon Web Services 服务

S3 对象 Lambda 可以连接 Amazon S3 和 Amazon Lambda，也可以连接您选择的其他 Amazon Web Services 服务，以交付与发出请求的应用程序相关的对象。与 S3 对象 Lambda 结合使用的所有 Amazon Web Services 服务将继续受其各自服务水平协议（SLA）管控。例如，如有任何 Amazon Web Services 服务不遵守其服务承诺，您将有资格获得该服务的 SLA 中介绍的服务积分。

## **Range** 和 **partNumber** 标头

使用大型对象时，您可以使用 `Range` HTTP 标头从对象中下载指定的字节范围。当您使用 `Range` 标头时，您的请求仅提取对象的指定部分。您还可以使用 `partNumber` 标头对于对象中的指定分段执行范围内的请求。

有关更多信息，请参阅使用 Range 和 partNumber 标头。

## 转换 **expiry-date**

您可以在 Amazon Web Services Management Console上从对象 Lambda 接入点打开或下载转换后的对象。这些对象必须未过期。如果您的 Lambda 函数转换了对象的 `expiry-date`，您可能会看到无法打开或下载的过期对象。此行为仅适用于 S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 还原的对象。

## 使用 Amazon CLI 和 Amazon SDK

不支持将 Amazon Command Line Interface（Amazon CLI）S3 子命令（`cp`、`mv` 和 `sync`）和 适用于 Java 的 Amazon SDK `TransferManager` 类与 S3 对象 Lambda 结合使用。

# S3 对象 Lambda 教程

以下教程提供了一些 S3 对象 Lambda 任务的完整端到端过程。

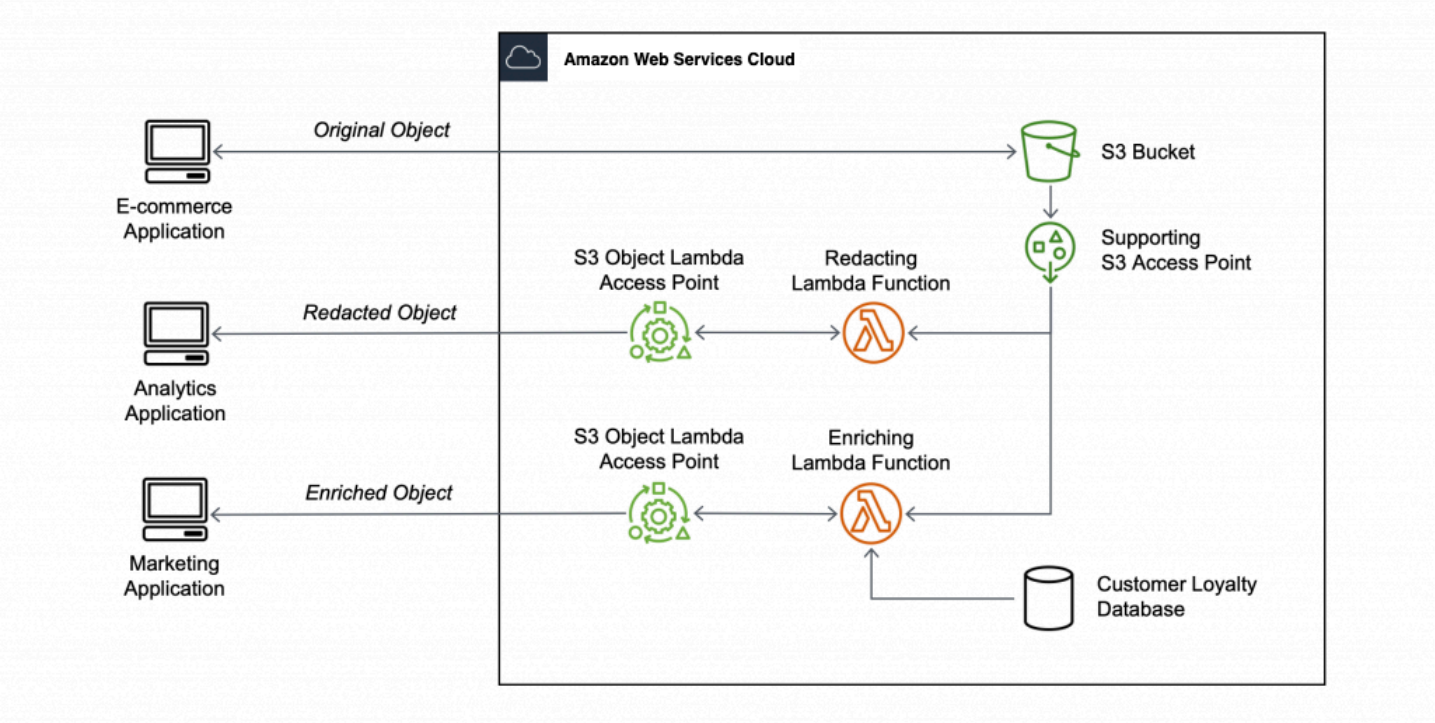
采用 S3 对象 Lambda，可以添加自己的代码处理从 S3 检索的数据，然后再将其返回应用程序。以下每个教程都将在从 Amazon S3 检索出数据时对数据进行修改，而无需更改现有对象或维护数据的多个副本。第一个教程将演练如何向 S3 GET 请求添加 Amazon Lambda 函数，来修改从 S3 中检索到的对象。第二个教程演示如何使用由 Amazon Comprehend 支持的预构建 Lambda 函数，在将从 S3 检索到的个人身份信息（PII）返回给应用程序之前为其提供保护。第三个教程使用 S3 对象 Lambda，在从 Amazon S3 检索到图像时为其添加水印。

- 教程：使用 S3 对象 Lambda 转换应用程序的数据
- 教程：使用 S3 对象 Lambda 和 Amazon Comprehend 检测和修订 PII 数据
- 教程：使用 S3 对象 Lambda 在检索图像时对其动态加水印

## 教程：使用 S3 对象 Lambda 转换应用程序的数据

在 Amazon S3 中存储数据时，您可以轻松共享数据供多个应用程序使用。但是，每个应用程序可能具有独特的数据格式要求，可能需要针对特定用例修改或处理您的数据。例如，由电子商务应用程序创建的数据集可能包括个人识别信息（PII）。处理相同的数据以进行分析时，不需要此 PII，应该进行修订。但是，如果将同一数据集用于营销活动，可能需要使用其他详细信息来丰富数据，例如来自客户忠诚度数据库的信息。

采用 S3 对象 Lambda，可以添加自己的代码处理从 S3 检索的数据，然后再将其返回应用程序。具体来说，您可以配置 Amazon Lambda 函数并将其附加到 S3 对象 Lambda 接入点。当应用程序通过 S3 对象 Lambda 接入点发送标准 S3 GET 请求时，将调用指定的 Lambda 函数，以处理通过支持的 S3 接入点从 S3 存储桶检索到的任何数据。然后，S3 对象 Lambda 接入点将转换后的结果返回给应用程序。您可以创作和执行自己的自定义 Lambda 函数，根据您的特定用例定制 S3 对象 Lambda 数据转换，所有这些都不需要更改您的应用程序。




目标

在本教程中，您将了解如何将自定义代码添加到标准 S3 GET 请求中，修改从 S3 检索到的请求对象，从而使该对象适合请求客户端或应用程序的需要。具体而言，您将学习如何通过 S3 对象 Lambda 将存储在 S3 中的原始对象中所有文本转换为大写。

> **Note**
>
> 本教程使用 Python 代码来转换数据，有关使用其它 Amazon SDK 的示例，请参阅 Amazon SDK 代码示例库中的 Transform data for your application with S3 Object Lambda。

主题


- 先决条件
- 步骤 1：创建 S3 存储桶
- 步骤 2：将文件上传到 S3 存储桶。
- 步骤 3：创建 S3 接入点
- 步骤 4：创建 Lambda 函数
- 步骤 5：为 Lambda 函数的执行角色配置 IAM 策略

- 步骤 6：创建 S3 对象 Lambda 接入点
- 步骤 7：查看转换的数据
- 第 8 步：清除
- 后续步骤

先决条件

在开始本教程之前，您必须具有 Amazon Web Services 账户，您可使用具有正确权限的 Amazon Identity and Access Management（IAM）用户登录此账户。您还必须安装 Python 3.8 或更高版本。

分步

- 在您的 Amazon Web Services 账户 中创建具有权限的 IAM 用户（控制台）
- 在本地计算机上安装 Python 3.8 或更高版本

在您的 Amazon Web Services 账户 中创建具有权限的 IAM 用户（控制台）

您可以为此教程创建 IAM 用户。要完成本教程，您的 IAM 用户必须附加以下 IAM 策略才能访问相关 Amazon 资源并执行特定操作。有关如何创建 IAM 用户的更多信息，请参阅 《IAM 用户指南》中的创建 IAM 用户（控制台）。

您的 IAM 用户需要以下策略：

- AmazonS3FullAccess - 授予对所有 Amazon S3 操作的权限，包括创建和使用对象 Lambda 接入点的权限。
- AWSLambda_FullAccess - 对所有 Lambda 操作授予权限。
- IAMFullAccess - 对所有 IAM 操作授予权限。
- IAMAccessAnalyzerReadOnlyAccess - 授予读取 IAM Access Analyzer 提供的所有访问信息的权限。
- CloudWatchLogsFullAccess – 授予对 CloudWatch Logs 的完全访问权限。

> **Note**
>
> 为简单起见，本教程创建并使用 IAM 用户。完成本教程后，请记住 删除 IAM 用户。对于生产用途，我们建议您遵循《IAM 用户指南》中的 IAM 中的安全最佳实践。最佳实践要求人类用户将联合身份验证与身份提供商结合使用，以使用临时凭证访问 Amazon。另一项最佳

实践是要求工作负载使用带有 IAM 角色的临时凭证访问 Amazon。要了解如何使用 Amazon IAM Identity Center 创建具有临时凭证的用户，请参阅《Amazon IAM Identity Center 用户指南》中的入门。
本教程还使用完全访问 Amazon 托管式策略。对于生产用途，建议您根据安全最佳实践仅授予用例所需的最低权限。

在本地计算机上安装 Python 3.8 或更高版本

使用以下过程在本地计算机上安装 Python 3.8 或更高版本。有关安装说明的更多信息，请参阅《Python 初学者指南》中的下载 Python 页面。

1. 打开本地终端或 shell 并运行以下命令以确定是否已安装 Python，如果已安装，确定已安装的版本。

```
python --version
```

2. 如果没有 Python 3.8 或更高版本，则下载适合您的本地计算机的官方安装。
3. 双击下载的文件运行安装程序，然后按照步骤完成安装。

   对于 Windows 用户，在安装向导中选择将 Python 3.X 添加到 PATH，然后选择立即安装。
4. 通过关闭并重新打开终端来重新启动它。
5. 运行以下命令以验证是否正确安装了 Python 3.8或更高版本。

   对于 macOS 用户，运行以下命令：

```
python3 --version
```

   对于 Windows 用户，运行此命令：

```
python --version
```

6. 运行以下命令验证是否安装了 pip3 包管理器。如果您在命令响应中看到 pip 版本号和 python 3.8 或更高版本，则意味着 pi3 软件包管理器已成功安装。

```
pip --version
```

### 步骤 1：创建 S3 存储桶

创建存储桶来存储您计划转换的原始数据。

创建存储桶

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 选择创建存储桶。

   此时将打开创建存储桶页面。
4. 对于存储桶名称，输入您的存储桶名称（例如，**tutorial-bucket**）。

   有关 Amazon S3 存储桶命名的更多信息，请参阅 通用存储桶命名规则。
5. 对于区域，选择要放置存储桶的 Amazon Web Services 区域。

   有关存储桶区域的更多信息，请参阅 通用存储桶概述。
6. 对于此存储桶的屏蔽公共访问权限设置，保留默认值（屏蔽所有公共访问权限已启用）。

   除非您需要为您的用例关闭一个或多个屏蔽公共访问权限设置，否则建议您将所有这些设置保持为启用状态。有关屏蔽公共访问权限的更多信息，请参阅 阻止对您的 Amazon S3 存储的公有访问。
7. 对于其余设置，保留默认值。

   （可选）如果要为您的特定用例配置其他存储桶设置，请参阅 创建通用存储桶。
8. 选择创建存储桶。

### 步骤 2：将文件上传到 S3 存储桶。

将文本文件上传到 S3 存储桶。此文本文件包含本教程稍后将转换为大写的原始数据。

例如，您可以上传包含以下文本的 `tutorial.txt`文件：

```
Amazon S3 Object Lambda Tutorial:
You can add your own code to process data retrieved from S3 before
returning it to an application.
```

要上传文件到存储桶

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 在存储桶列表中，选择您在步骤 1中创建的存储桶名称（例如，**tutorial-bucket**）上传您的文件。
4. 在存储桶的对象 选项卡上，选择上传。
5. 在上传页面的文件和文件夹下，选择添加文件。
6. 选择要上传的文件，然后选择打开。例如，您可以上传之前提到的 `tutorial.txt` 文件示例。
7. 选择上传。

## 步骤 3：创建 S3 接入点

要使用 S3 对象 Lambda 接入点访问和转换原始数据，您必须创建一个 S3 接入点，并将其与您在步骤 1 中创建的 S3 存储桶关联。接入点必须与要变换的对象位于同一 Amazon Web Services 区域 位置。

在本教程的后面部分，您将使用此接入点作为对象 Lambda 接入点的支持接入点。

创建接入点

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择接入点。
3. 在接入点页面上，选择创建接入点。
4. 在接入点名称字段中输入接入点名称（例如，**tutorial-access-point**）。

   有关命名接入点的更多信息，请参阅通用存储桶的 Amazon S3 接入点的命名规则。
5. 在存储桶名称字段中，输入您在步骤 1中创建的存储桶名称（例如，**tutorial-bucket**)。S3 将接入点附加到存储桶。

   您也可以选择浏览 S3 浏览和搜索账户中的存储桶。如果选择浏览 S3，请选择所需的存储桶，然后选择选择路径使用该存储桶的名称填充存储桶名称字段。
6. 适用于网络源中，选择互联网。

   有关接入点的网络源的更多信息，请参阅创建限制到虚拟私有云的通用存储桶的接入点。

7. 默认情况下，为您的接入点启用所有屏蔽公共访问权限设置。我们建议您将屏蔽所有 公共访问权限保留为启用状态。

   有关更多信息，请参阅 管理对通用存储桶的接入点的公共访问权限。
8. 对于所有其他接入点设置，保留默认设置。

   （可选）您可以修改接入点设置以支持您的用例。在本教程中，我们建议您保留默认设置。

   （可选）如果需要管理对接入点的访问，可以指定接入点策略。有关更多信息，请参阅 通用存储桶的接入点的策略示例。
9. 选择 Create access point（创建接入点）。

### 步骤 4：创建 Lambda 函数

要转换原始数据，请创建 Lambda 函数以与 S3 对象 Lambda 接入点结合使用。

分步

- 编写 Lambda 函数代码并使用虚拟环境创建部署包
- 使用执行角色创建 Lambda 函数（控制台）
- 用 .zip 文件归档部署 Lambda 函数代码，并配置 Lambda 函数（控制台）

#### 编写 Lambda 函数代码并使用虚拟环境创建部署包

1. 在本地计算机上，使用文件夹名称 `object-lambda` 创建一个文件夹，供本教程稍后使用。
2. 在 `object-lambda` 文件夹中，使用 Lambda 函数创建一个文件，该函数将原始对象中的所有文本更改为大写。例如，您可以使用 Python 编写的以下函数。将此函数保存在名为的文件 `transform.py` 中。

```
import boto3
import requests
from botocore.config import Config

# This function capitalizes all text in the original object
def lambda_handler(event, context):
    object_context = event["getObjectContext"]
    # Get the presigned URL to fetch the requested original object
    # from S3
    s3_url = object_context["inputS3Url"]
    # Extract the route and request token from the input context
```

```
    request_route = object_context["outputRoute"]
    request_token = object_context["outputToken"]

    # Get the original S3 object using the presigned URL
    response = requests.get(s3_url)
    original_object = response.content.decode("utf-8")

    # Transform all text in the original object to uppercase
    # You can replace it with your custom code based on your use case
    transformed_object = original_object.upper()

    # Write object back to S3 Object Lambda
    s3 = boto3.client('s3', config=Config(signature_version='s3v4'))
    # The WriteGetObjectResponse API sends the transformed data
    # back to S3 Object Lambda and then to the user
    s3.write_get_object_response(
        Body=transformed_object,
        RequestRoute=request_route,
        RequestToken=request_token)

    # Exit the Lambda function: return the status code
    return {'status_code': 200}
```

> **Note**
>
> 前面的示例 Lambda 函数将整个请求的对象加载到内存中，然后再将其转换为客户端。您还可以从 S3 流式传输对象，避免将整个对象加载到内存中。这种方法在处理大型对象时非常有用。有关使用对象 Lambda 接入点流式处理响应的详细信息，请参阅在 Lambda 中处理 GetObject 请求中的流式处理示例。

编写 Lambda 函数以用于 S3 对象 Lambda 接入点时，该函数基于 S3 对象 Lambda 提供给 Lambda 函数的输入事件上下文。事件上下文提供有关在从 S3 对象 Lambda 传递到 Lambda 的事件中发出请求的信息。它包含用于创建 Lambda 函数的参数。

用于创建前面的 Lambda 函数的字段如下所示：

字段 `getObjectContext` 表示与 Amazon S3 和 S3 对象 Lambda连接的输入和输出详细信息。它具有以下字段：

- `inputS3Url` - Lambda 函数可用于从支持接入点下载原始对象的预签名 URL。通过使用预签名 URL，Lambda 函数无需具有 Amazon S3 读取权限即可检索原始对象，只能访问每次调用处理的对象。
- `outputRoute` - 当 Lambda 函数调用 `WriteGetObjectResponse` 以发回转换后的对象时，添加到 S3 对象 Lambda URL 的路由令牌。
- `outputToken` - S3 对象 Lambda 在发送回转换对象时用于将 `WriteGetObjectResponse` 调用与原始调用方匹配的令牌。

有关事件上下文中所有字段的更多信息，请参阅 事件上下文格式和用法 和 为 S3 对象 Lambda 接入点编写 Lambda 函数。

3. 在您的本地终端上，输入以下命令来安装 `virtualenv` 包：

```
python -m pip install virtualenv
```

4. 在您的本地终端中，打开之前创建的 `object-lambda` 文件夹，然后输入以下命令创建并初始化名为的虚拟环境 `venv`。

```
python -m virtualenv venv
```

5. 要激活虚拟环境，请输入以下命令，以执行环境的文件夹中的 `activate` 文件：

对于 macOS 用户，运行以下命令：

```
source venv/bin/activate
```

对于 Windows 用户， 运行此命令：

```
.\venv\Scripts\activate
```

现在，命令提示符更改为显示 (venv)，表示虚拟环境处于活动状态。

6. 要安装所需的库，请在 `venv` 虚拟环境中运行下列命令行。

这些命令会安装您 `lambda_handler` Lambda 函数依赖关系的更新版本。这些依赖关系是 Amazon SDK for Python (Boto3) 和请求模块。

```
pip3 install boto3
```

```
pip3 install requests
```

7. 要停用虚拟环境，运行以下命令：

```
deactivate
```

8. 要在 object-lambda 目录的根目录下，将已安装的库作为 .zip 文件（文件名为 lambda.zip）来创建部署程序包，请在本地终端中逐行运行以下命令。

> **Tip**
>
> 可能需要调整以下命令才能在您的特定环境中工作。例如，库可能出现在 site-packages 或 dist-packages 中，第一个文件夹可能是 lib 或者 lib64。另外，python 文件夹可能会使用不同的 Python 版本命名。您可以使用 pip show 命令定位特定包。

适用于 macOS 用户，运行以下命令：

```
cd venv/lib/python3.8/site-packages
```

```
zip -r ../../../../lambda.zip .
```

对于 Windows 用户，运行以下命令：

```
cd .\venv\Lib\site-packages\
```

```
powershell Compress-Archive * ../../../lambda.zip
```

最后一个命令将部署程序包保存到 object-lambda 目录的根目录中。

9. 将函数代码文件 transform.py 添加到部署程序包的根目录中。

适用于 macOS 用户，运行以下命令：

```
cd ../../../../
```

```
zip -g lambda.zip transform.py
```

对于 Windows 用户，运行以下命令：

```
cd ..\..\..\
```

```
powershell Compress-Archive -update transform.py lambda.zip
```

完成此步骤后，文件目录结构应如下：

```
lambda.zip$
  # transform.py
  # __pycache__
  | boto3/
  # certifi/
  # pip/
  # requests/
  ...
```

使用执行角色创建 Lambda 函数（控制台）

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Lambda 控制台：https://console.aws.amazon.com/lambda/。
2. 在左侧导航窗格中，选择函数。
3. 选择 Create function (创建函数)。
4. 选择从头开始创作。
5. 在基本信息中，执行以下操作：
   a. 对于 Function name（函数名称），请输入 **tutorial-object-lambda-function**。
   b. 适用于运行时间中，选择 Python 3.8 或更高版本。
6. 展开更改默认执行角色部分。在执行角色中，选择创建具有基本 Lambda 权限的新角色。

   在步骤 5 中，在本教程的后面，您将 AmazonS3ObjectLambdaExecutionRolePolicy 附加到 Lambda 函数的执行角色上。
7. 对于其余设置，保留默认值。

8. 选择 Create function（创建函数）。

用 .zip 文件归档部署 Lambda 函数代码，并配置 Lambda 函数（控制台）

1. 在 Amazon Lambda 控制台位于 https://console.aws.amazon.com/lambda/ 中，选择左侧导航窗格中的 Functions（函数）。
2. 选择您之前创建的 Lambda 函数（例如 **`tutorial-object-lambda-function`**）。
3. 在 Lambda 函数的详细信息页面上，选择代码选项卡。在代码源部分，选择上传，然后选择 .zip 文件。
4. 选择上传以选择本地 `.zip` 文件。
5. 选择您之前创建的 `lambda.zip` 文件，然后选择打开。
6. 选择保存。
7. 在运行时间设置部分，选择编辑。
8. 在存储库的编辑运行时设置页面上，确认运行时设置为 Python 3.8 或更高版本。
9. 要告诉 Lambda 运行时要调用 Lambda 函数代码中的哪个处理程序方法，请输入 **`transform.lambda_handler`** 的处理程序。

   当您在 Python 中配置函数时，处理程序设置的值是文件名，也是处理程序模块的名称（由点分隔）。例如，`transform.lambda_handler` 调用在 `transform.py` 文件中定义的 `lambda_handler` 方法。
10. 选择保存。
11. （可选）在 Lambda 函数的详细信息页面上，选择配置选项卡。在左侧导航窗格中，选择常规配置，然后选择编辑。在超时字段中，输入 **`1`** 分钟 **`0`** 秒。对于其余设置，保留默认值，然后选择保存。

    超时 –是 Lambda 允许函数在停止调用之前为调用运行的时长。默认值为 3 秒。S3 对象 Lambda 使用的 Lambda 函数的最大持续时间为 60 秒。定价基于配置的内存量和代码运行的时间量。

步骤 5：为 Lambda 函数的执行角色配置 IAM 策略

要使 Lambda 函数能够提供自定义的数据和响应标头 `GetObject` 调用者，Lambda 函数的执行角色必须具有 IAM 权限才能调用 `WriteGetObjectResponse` API。

将 IAM 策略附加到 Lambda 函数角色

1. 在 Amazon Lambda 控制台位于 https://console.aws.amazon.com/lambda/ 中，选择左侧导航窗格中的 Functions（函数）。
2. 选择您在步骤 4 中创建的函数（例如，**tutorial-object-lambda-function**）。
3. 在 Lambda 函数的详细信息页面上，选择配置选项卡，然后选择Permissions（权限）在左侧导航窗格中。
4. Unts执行角色中，选择 Role name（角色名称）。打开 IAM 控制台。
5. 在 IAM 控制台上对应于 Lambda 函数的执行角色的 Summary（摘要）页面上，选择 Permissions（权限）选项卡。然后，从 Add Permissions（添加权限）菜单中选择 Attach policies（附加策略）。
6. 在附加权限策略页的搜索字段中输入 **AmazonS3ObjectLambdaExecutionRolePolicy** 策略的名称。选中 AmazonS3ObjectLambdaExecutionRolePolicy 政策名称旁边的复选框。
7. 选择附加策略。

### 步骤 6：创建 S3 对象 Lambda 接入点

S3 对象 Lambda 接入点提供了直接从 S3 GET 请求调用 Lambda 函数的灵活性，以便该函数可以处理从 S3 接入点检索的数据。创建和配置 S3 对象 Lambda 接入点时，必须指定 Lambda 函数以调用并提供 JSON 格式的事件上下文作为 Lambda 要使用的自定义参数。

创建 S3 对象 Lambda 接入点

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Object Lambda 接入点。
3. 在对象 Lambda 接入点页面上，选择创建对象 Lambda 接入点。
4. 对于对象 Lambda 接入点名称，输入想要用于对象 Lambda 接入点的名称（例如 **tutorial-object-lambda-accesspoint**）。
5. 适用于支持接入点中，输入或浏览到您在步骤 3（例如，**tutorial-access-point**），然后选择选择支持的接入点。
6. 对于 S3 APIs（S3 API），要从 S3 存储桶中检索对象以便 Lambda 函数进行处理，请选择 GetObject。
7. 对于调用 Lambda 函数，您可以为本教程选择以下两个选项之一。
   - 选择从您的账户中的函数选择，然后在 Lambda 函数下拉列表选择您在步骤 4中创建的 Lambda 函数（例如，**tutorial-object-lambda-function**）。

- 选择输入 ARN，然后输入您在步骤 4 中创建的 Lambda 函数的 Amazon 资源名称（ARN）。

8. 适用于Lambda 函数版本，选择$LATEST（您在步骤 4中创建的最新版 Lambda 函数)。
9. （可选）如果您需要 Lambda 函数识别和处理带有范围和分段编号标头的 GET 请求，请选择 Lambda 函数支持使用范围的请求和 Lambda 函数支持使用零件编号的请求。否则，请清除这两个复选框。

   有关如何将范围或分段编号与 S3 对象 Lambda 结合使用的更多信息，请参阅 使用 Range 和 partNumber 标头。
10. （可选）在 Payload（负载）- 可选下，添加 JSON 文本，向 Lambda 函数提供其他信息。

    负载是可选 JSON 文本，您可以将其作为来自特定 S3 对象 Lambda 接入点的所有调用的输入提供给 Lambda 函数。要自定义调用同一 Lambda 函数的多个对象 Lambda 接入点的行为，您可以使用不同的参数配置负载，从而扩展 Lambda 函数的灵活性。

    更多有关路径模式的信息，请参阅 事件上下文格式和用法。
11. （可选）对于请求指标 - 可选，选择禁用或启用以将 Amazon S3 监控添加到对象 Lambda 接入点。请求指标按标准 Amazon CloudWatch 费率计费。有关更多信息，请参阅 CloudWatch 定价。
12. 在对象 Lambda 接入点策略 - 可选下，保留默认设置。

    （可选）您可以设置资源策略。此资源策略授予 `GetObject` API 权限，以便使用指定的对象 Lambda 接入点。
13. 对于其余设置，保留默认值，然后选择创建对象 Lambda 接入点。

### 步骤 7：查看转换的数据

现在，S3 对象 Lambda 已准备好为您的使用案例转换您的数据。在本教程中，S3 对象 Lambda 将对象中的所有文本转换为大写。

分步

- 在 S3 对象 Lambda 接入点中查看转换后的数据
- 运行 Python 脚本以打印原始数据和转换数据

### 在 S3 对象 Lambda 接入点中查看转换后的数据

当您请求通过 S3 对象 Lambda 接入点检索文件时，您需要对 S3 对象 Lambda 进行 `GetObject` API 调用。S3 对象 Lambda 调用 Lambda 函数来转换您的数据，然后返回转换后的数据作为对标准 S3 的响应 `GetObject` API 调用。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择对象 Lambda 接入点。
3. 在对象 Lambda 接入点页面上，选择您在步骤 6 中创建的 S3 对象 Lambda 接入点（例如，**tutorial-object-lambda-accesspoint**）。
4. 在 S3 对象 Lambda 接入点的对象选项卡中，选择具有相同名称的文件（例如 `tutorial.txt`）作为您在步骤 2 中上传到 S3 存储桶的文件。

   此文件应包含所有转换的数据。
5. 要查看转换后的数据，请选择打开或者下载。

### 运行 Python 脚本以打印原始数据和转换数据

您可以将 S3 对象 Lambda 与现有应用程序结合使用。为此，请更新应用程序配置，以使用在步骤 6 中创建的新 S3 对象 Lambda 接入点 ARN 从 S3 检索数据。

以下示例 Python 脚本既打印来自 S3 存储桶的原始数据，也打印来自 S3 对象 Lambda 接入点的转换数据。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择对象 Lambda 接入点。
3. 在对象 Lambda 接入点页面上，选择在步骤 6 中创建的 S3 对象 Lambda 接入点左侧的单选按钮（例如，**tutorial-object-lambda-accesspoint**）。
4. 选择复制 ARN。
5. 保存 ARN 以供稍后使用。
6. 在本地计算机上编写 Python 脚本，以从 S3 存储桶中打印原始数据（例如，`tutorial.txt`）并从 S3 对象 Lambda 接入点中打印转换后的数据（例如 `tutorial.txt`）。您可以使用以下示例脚本。

```
import boto3
from botocore.config import Config

s3 = boto3.client('s3', config=Config(signature_version='s3v4'))

def getObject(bucket, key):
    objectBody = s3.get_object(Bucket = bucket, Key = key)
```

```
    print(objectBody["Body"].read().decode("utf-8"))
    print("\n")

print('Original object from the S3 bucket:')
# Replace the two input parameters of getObject() below with
# the S3 bucket name that you created in Step 1 and
# the name of the file that you uploaded to the S3 bucket in Step 2
getObject("tutorial-bucket",
          "tutorial.txt")

print('Object transformed by S3 Object Lambda:')
# Replace the two input parameters of getObject() below with
# the ARN of your S3 Object Lambda Access Point that you saved earlier and
# the name of the file with the transformed data (which in this case is
# the same as the name of the file that you uploaded to the S3 bucket
# in Step 2)
getObject("arn:aws:s3-object-lambda:us-west-2:111122223333:accesspoint/tutorial-
object-lambda-accesspoint",
          "tutorial.txt")
```

7. 使用自定义名称将 Python 脚本（例如，`tutorial_print.py`）保存您在步骤 4中本地计算机上中创建的文件夹中（例如，`object-lambda`）。

8. 在您的本地终端上，在步骤 4中创建的根目录下运行以下命令（例如，`object-lambda`）。

```
python3 tutorial_print.py
```

您应该通过终端同时看到原始数据和转换后的数据（所有文本均为大写）。如，您应看到类似于以下的文本。

```
Original object from the S3 bucket:
Amazon S3 Object Lambda Tutorial:
You can add your own code to process data retrieved from S3 before
returning it to an application.

Object transformed by S3 Object Lambda:
AMAZON S3 OBJECT LAMBDA TUTORIAL:
YOU CAN ADD YOUR OWN CODE TO PROCESS DATA RETRIEVED FROM S3 BEFORE
RETURNING IT TO AN APPLICATION.
```

## 第 8 步：清除

如果您仅出于练习目的通过 S3 对象 Lambda 创建静态网站，则删除您所分配的 Amazon 资源，使其不再产生费用。

分步

- 删除对象 Lambda 接入点
- 删除 S3 接入点
- 删除您的 Lambda 函数的执行角色。
- 删除 Lambda 函数
- 删除 CloudWatch 日志组
- 删除 S3 源存储桶中的原始文件
- 删除 S3 源存储桶
- 删除 IAM 用户

### 删除对象 Lambda 接入点

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择对象 Lambda 接入点。
3. 在对象 Lambda 接入点页面上，选择在步骤 6 中创建的 S3 对象 Lambda 接入点左侧的单选按钮（例如，**`tutorial-object-lambda-accesspoint`**）。
4. 选择删除。
5. 通过在显示的文本字段中输入对象 Lambda 接入点的名称，确认要删除的对象 Lambda 接入点，然后选择删除。

### 删除 S3 接入点

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择接入点。
3. 导航到您在步骤 3创建的接入点（例如，**`tutorial-access-point`**），然后选择接入点名称旁的单选按钮。

4. 选择删除。
5. 在显示的文本字段中输入接入点名称，然后选择删除，确认您要删除接入点。

删除您的 Lambda 函数的执行角色。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Lambda 控制台：https://console.aws.amazon.com/lambda/。
2. 在左侧导航窗格中，选择函数。
3. 选择您在步骤 4 中创建的函数（例如，**tutorial-object-lambda-function**）。
4. 在 Lambda 函数的详细信息页面上，选择配置选项卡，然后选择Permissions（权限）在左侧导航窗格中。
5. Unts执行角色中，选择 Role name（角色名称）。打开 IAM 控制台。
6. 在 Lambda 函数的执行角色 IAM 控制台的摘要页面上，选择删除角色。
7. 在 Delete role（删除角色）对话框中，选择 Yes, delete（是的，删除）。

删除 Lambda 函数

1. 在 Amazon Lambda 控制台（位于 https://console.aws.amazon.com/lambda/）中，选择左侧导航窗格中的 Functions（函数）。
2. 选择您在步骤4中创建的函数名称左侧的复选框（例如，**tutorial-object-lambda-function**）。
3. 选择操作，然后选择删除。
4. 在删除函数对话框中，选择删除。

删除 CloudWatch 日志组

1. 通过 https://console.aws.amazon.com/cloudwatch/ 打开 CloudWatch 控制台。
2. 在左侧导航窗格中，选择日志组。
3. 查找名称以步骤4中创建的 Lambda 函数结尾的日志组（例如，**tutorial-object-lambda-function**）。
4. 选择日志组名称左侧的复选框。
5. 选择操作，然后选择删除日志组。
6. 在删除日志组对话框中，选择删除。

删除 S3 源存储桶中的原始文件

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 在存储桶名称列表中，选择您在步骤 2中将原始文件上传到的存储桶名称（例如，**tutorial-bucket**）。
4. 选中要删除的对象名称左侧的复选框（例如，`tutorial.txt`）。
5. 选择删除。
6. 在永久删除对象？的删除对象页面上，在文本框中输入 **permanently delete** 确认您希望删除此对象。
7. 选择删除对象。

删除 S3 源存储桶

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 在存储桶列表中，选择您在步骤 1中创建的存储桶名称旁的单选按钮（例如，**tutorial-bucket**）。
4. 选择删除。
5. 在删除存储桶页面上，通过在文本字段中输入存储桶名称来确认要删除存储桶，然后选择删除存储桶。

删除 IAM 用户

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在左侧导航窗格中，选择用户，然后选中要删除的用户旁的复选框。
3. 在页面的顶部，选择删除。
4. 在删除**###**?对话框中，在文本输入字段中输入用户名以确认删除用户。选择删除。

### 后续步骤

完成本教程后，您可以为您的用例自定义 Lambda 函数，以便修改标准 S3 GET 请求返回的数据。

以下是 S3 对象 Lambda 的常见用例列表：

- 屏蔽敏感数据以确保安全性和合规性。

  有关更多信息，请参阅 教程：使用 S3 对象 Lambda 和 Amazon Comprehend 检测和修订 PII 数据。
- 筛选某些数据行以提供特定信息。
- 使用来自其他服务或数据库的信息增加数据。
- 跨数据格式转换，例如将 XML 转换为 JSON 以实现应用程序兼容性。
- 在下载文件时压缩或解压缩文件。
- 调整图像大小和水印图像。

  有关更多信息，请参阅教程：使用 S3 对象 Lambda 在检索图像时对其动态加水印。
- 实施自定义授权规则以访问数据。

有关 S3 对象 Lambda 的更多信息，请参阅 使用 S3 对象 Lambda 转换对象。

## 教程：使用 S3 对象 Lambda 和 Amazon Comprehend 检测和修订 PII 数据

将 Amazon S3 用于多个应用程序和用户访问的共享数据集时，请务必将特权信息（如个人身份信息 (PII)）限制为仅授权实体。例如，当营销应用程序使用某些包含 PII 的数据时，可能需要首先掩盖 PII 数据以满足数据隐私要求。此外，分析应用程序使用生产订单清单数据集时，可能需要首先编辑客户信用卡信息，防止意外的数据泄露。

用 S3 对象 Lambda 和预构建的 Amazon Lambda 函数，您可以在将从 S3 检索 Amazon Comprehend 的 PII 数据返回到应用程序之前进行保护。具体来说，您可以使用预构建的 Lambda 函数作为编校函数，并将其附加到 S3 对象 Lambda 接入点。应用程序（例如，分析应用程序）发送标准 S3 GET 请求时，这些通过 S3 对象 Lambda 接入点发出的请求将调用预构建的编校 Lambda 函数，以检测和编校通过支持的 S3 接入点从 S3 存储桶检索到的 PII 数据。然后，S3 对象 Lambda 接入点将编校的结果返回到应用程序。

在此过程中，无论 PII 在文本中的存在方式如何（例如，数字或单词和数字的组合），预构建的 Lambda 函数均使用 Amazon Comprehend，这是一种自然语言处理 (NLP) 服务，用于捕获 PII 表示方式的变化。Amazon Comprehend 甚至可以用文本中的上下文来了解 4 位数字是否是 PIN、社会保

险号 (SSN) 的最后四个数字还是年份。Amazon Comprehend 处理 UTF-8 格式的任何文本文件，并可以大规模保护 PII，而不会影响准确性。有关更多信息，请参阅 《Amazon Comprehend 开发人员指南》中的什么是 Amazon Comprehend？

目标

在本教程中，您将学习如何将 S3 对象 Lambda 与预构建的 Lambda 函数一起使用 `ComprehendPiiRedactionS3ObjectLambda`。此函数使用 Amazon Comprehend 来检测 PII 实体。然后，通过用星号替换这些实体来修订它们。通过修订 PII，您可以隐藏敏感数据，这有助于提高安全性和合规性。

您还可以了解在 Amazon Serverless Application Repository 中如何使用和配置预构建的 Amazon Lambda 函数与 S3 对象 Lambda 一起使用便于部署。

主题


- 先决条件：创建具有权限的 IAM 用户
- 步骤 1：创建 S3 存储桶
- 步骤 2：将文件上传到 S3 存储桶。
- 步骤 3：创建 S3 接入点
- 步骤 4：配置和部署预构建的 Lambda 函数
- 步骤 5：创建 S3 对象 Lambda 接入点
- 步骤 6：使用 S3 对象 Lambda 接入点检索编校的文件
- 步骤 7：清除
- 后续步骤


## 先决条件：创建具有权限的 IAM 用户

在开始本教程之前，您必须具有 Amazon 账户，您可使用具有正确权限的 Amazon Identity and Access Management 用户（IAM 用户）登录此账户。

您可以为此教程创建 IAM 用户。要完成本教程，您的 IAM 用户必须附加以下 IAM 策略才能访问相关 Amazon 资源并执行特定操作。

> **Note**
>
> 为简单起见，本教程创建并使用 IAM 用户。完成本教程后，请记住 删除 IAM 用户。对于生产用途，我们建议您遵循《IAM 用户指南》中的 IAM 中的安全最佳实践。最佳实践要求人

类用户将联合身份验证与身份提供商结合使用，以使用临时凭证访问 Amazon。另一项最佳实践是要求工作负载使用带有 IAM 角色的临时凭证访问 Amazon。要了解如何使用 Amazon IAM Identity Center 创建具有临时凭证的用户，请参阅《Amazon IAM Identity Center 用户指南》中的入门。
本教程还使用完全访问策略。对于生产用途，我们建议您根据安全最佳实践仅授予用例所需的最低权限。

您的 IAM 用户需要以下 Amazon 托管策略：

- AmazonS3FullAccess - 授予对所有 Amazon S3 操作的权限，包括创建和使用对象 Lambda 接入点的权限。
- AWSLambda_FullAccess - 对所有 Lambda 操作授予权限。
- AWSCloudFormationFullAccess - 为所有 Amazon CloudFormation 操作授予权限。
- IAMFullAccess - 对所有 IAM 操作授予权限。
- IAMAccessAnalyzerReadOnlyAccess - 授予读取 IAM Access Analyzer 提供的所有访问信息的权限。

您可以在创建 IAM 用户时直接附加这些现有策略。有关如何创建 IAM 用户的更多信息，请参阅 《IAM 用户指南》中的创建 IAM 用户（控制台）。

此外，您的 IAM 用户需要客户托管策略。将 IAM 用户权限授予所有 Amazon Serverless Application Repository 资源和操作，您必须创建 IAM 策略并将此策略附加给 IAM 用户。

创建一个 IAM 策略并将其附加到 IAM 用户

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在左侧导航窗格中，选择 Policies（策略）。
3. 选择创建策略。
4. 在可视化编辑器选项卡上，服务，选择服务。然后，选择 Serverless Application Repository。
5. 对于操作，在手动操作中，选择此教程中所有 Serverless Application Repository 操作（serverlessrepo:*）。

   作为安全最佳实践，您应根据用例仅允许用户所需的操作和资源的权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM 安全最佳实践。

6. 对于资源中，选择本教程中的所有资源。

   作为最佳实践，您应仅为特定账户中的特定资源定义权限。您也可以使用条件键授予最低权限。有关更多信息，请参阅 《IAM 用户指南》 中的授予最低权限。

7. 选择下一步：标签。
8. 选择下一步：审核。
9. 在查看策略页面上，为创建的策略输入名称（例如，**tutorial-serverless-application-repository**）和描述（可选）。查看策略摘要以确保您授予了所需的权限，然后选择创建策略以保存新策略。
10. 在左侧导航窗格中，选择 用户。然后，为本教程选择 IAM 用户。
11. 在所选用户的摘要页面上，选择权限选项卡，然后选择添加权限。
12. 在 Grant permissions (授予权限) 下，选择 Attach existing policies directly (直接挂载现有策略)。
13. 选择刚创建的策略旁边的复选框（例如，**tutorial-serverless-application-repository**），然后选择下一步：审查。
14. 在策略摘要下，查看摘要确保附加了预期的策略。然后选择 添加权限。

### 步骤 1：创建 S3 存储桶

创建存储桶来存储您计划转换的原始数据。

#### 创建存储桶

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 选择创建存储桶。

   此时将打开创建存储桶页面。

4. 对于存储桶名称，输入您的存储桶名称（例如，**tutorial-bucket**）。

   有关 Amazon S3 存储桶命名的更多信息，请参阅 通用存储桶命名规则。

5. 对于区域，选择要放置存储桶的 Amazon Web Services 区域。

   有关存储桶区域的更多信息，请参阅 通用存储桶概述。

6. 对于此存储桶的屏蔽公共访问权限设置，保留默认值（屏蔽所有公共访问权限已启用）。

除非您需要为您的用例关闭一个或多个屏蔽公共访问权限设置，否则建议您将所有这些设置保持为启用状态。有关屏蔽公共访问权限的更多信息，请参阅 阻止对您的 Amazon S3 存储的公有访问。

7. 对于其余设置，保留默认值。

（可选）如果要为您的特定用例配置其他存储桶设置，请参阅 创建通用存储桶。

8. 选择创建存储桶。

步骤 2：将文件上传到 S3 存储桶。

将包含各种类型的已知 PII 数据（如姓名、银行信息、电话号码和SSN）的文本文件作为原始数据上传到 S3 存储桶中，您将在本教程稍后部分对PII进行修订。

例如，您可以上传 `tutorial.txt` 文件。这是 Amazon Comprehend 的示例输入文件。

```
Hello Zhang Wei, I am John. Your AnyCompany Financial Services,
LLC credit card account 1111-0000-1111-0008 has a minimum payment
of $24.53 that is due by July 31st. Based on your autopay settings,
we will withdraw your payment on the due date from your
bank account number XXXXXX1111 with the routing number XXXXX0000.

Your latest statement was mailed to 100 Main Street, Any City,
WA 98121.
After your payment is received, you will receive a confirmation
text message at 206-555-0100.
If you have questions about your bill, AnyCompany Customer Service
is available by phone at 206-555-0199 or
email at support@anycompany.com.
```

要上传文件到存储桶

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 在存储桶列表中，选择您在步骤 1中创建的存储桶名称（例如，**`tutorial-bucket`**）上传您的文件。
4. 在存储桶的对象 选项卡上，选择上传。
5. 在上传页面的文件和文件夹下，选择添加文件。

6. 选择要上传的文件，然后选择打开。例如，您可以上传之前提到的 `tutorial.txt` 文件示例。
7. 选择上传。

### 步骤 3：创建 S3 接入点

要使用 S3 对象 Lambda 接入点访问和转换原始数据，您必须创建一个 S3 接入点，并将其与您在步骤 1 中创建的 S3 存储桶关联。接入点必须与要转换的对象位于同一 Amazon Web Services 区域中。

在本教程的后面部分，您将使用此接入点作为对象 Lambda 接入点的支持接入点。

#### 创建接入点

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择接入点。
3. 在接入点页面上，选择创建接入点。
4. 在接入点名称字段中输入接入点名称（例如，**`tutorial-pii-access-point`**）。

   有关命名接入点的更多信息，请参阅通用存储桶的 Amazon S3 接入点的命名规则。
5. 在存储桶名称字段中，输入您在步骤 1中创建的存储桶名称（例如，**`tutorial-bucket`**)。S3 将接入点附加到存储桶。

   您也可以选择浏览 S3 浏览和搜索账户中的存储桶。如果选择浏览 S3，请选择所需的存储桶，然后选择选择路径使用该存储桶的名称填充存储桶名称字段。
6. 适用于网络源中，选择互联网。

   有关接入点的网络源的更多信息，请参阅创建限制到虚拟私有云的通用存储桶的接入点。
7. 默认情况下，为接入点启用所有屏蔽公共访问权限设置。我们建议您将屏蔽所有 公共访问权限保留为启用状态。有关更多信息，请参阅 管理对通用存储桶的接入点的公共访问权限。
8. 对于所有其他接入点设置，保留默认设置。

   （可选）您可以修改接入点设置以支持您的用例。在本教程中，我们建议您保留默认设置。

   （可选）如果需要管理对接入点的访问，可以指定接入点策略。有关更多信息，请参阅 通用存储桶的接入点的策略示例。
9. 选择 Create access point（创建接入点）。

### 步骤 4：配置和部署预构建的 Lambda 函数

要编校 PII 数据，请配置和部署预构建的 Amazon Lambda 函数 `ComprehendPiiRedactionS3ObjectLambda` 以便与 S3 对象 Lambda 接入点结合使用。

要配置和部署 Lambda 函数

1. 登录到 Amazon Web Services Management Console，然后查看 Amazon Serverless Application Repository 中的 `ComprehendPiiRedactionS3ObjectLambda` 函数。
2. 对于应用程序设置，在应用程序名称下，请保留本教程默认值 (`ComprehendPiiRedactionS3ObjectLambda`)。

   （可选）您可以输入要为此应用程序提供的名称。如果计划为同一共享数据集的不同访问需求配置多个 Lambda 函数，则可能需要执行此操作。
3. 对于 MaskCharacter，请保留默认值 (*)。掩码字符将替换已修订的 PII 实体中的每个字符。
4. 对于 MaskMode，请保留默认值 (MASK)。MaskMode 值指定 PII 实体是否使用 `MASK` 字符或 `PII_ENTITY_TYPE` 值。
5. 要修订数据指定类型，对于 PiiEntityTypes，请保留默认值 ALL。PiiEntityTypes 值指定要考虑修订的 PII 实体类型。

   有关支持的 PII 实体类型列表的更多信息，请参阅 《Amazon Comprehend 开发人员指南》中的检测个人身份信息 (PII)。
6. 对于其余设置，保留默认值。

   （可选）如果要为特定用例配置其他设置，请参阅页面左侧的自述文件部分。
7. 选中 I acknowledge that this app creates custom IAM roles (我确认此应用程序创建自定义 IAM 角色) 旁边的复选框。
8. 选择部署。
9. 在新应用程序的页面上，在资源下，选择Lambda 函数的逻辑 ID，在 Lambda 函数页面上部署的 Lambda 函数。

### 步骤 5：创建 S3 对象 Lambda 接入点

S3 对象 Lambda 接入点提供了直接从 S3 GET 请求调用 Lambda 函数的灵活性，以便该函数可以编校从 S3 接入点检索的 PII 数据。创建和配置 S3 对象 Lambda 接入点时，必须指定要调用的编校 Lambda 函数，并以 JSON 格式提供事件上下文作为供 Lambda 使用的自定义参数。

事件上下文提供有关在从 S3 对象 Lambda 传递到 Lambda 的事件中发出请求的信息。有关事件上下文中所有字段的更多信息，请参阅 事件上下文格式和用法。

创建 S3 对象 Lambda 接入点

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Object Lambda 接入点。
3. 在对象 Lambda 接入点页面上，选择创建对象 Lambda 接入点。
4. 对于对象 Lambda 接入点名称，输入想要用于对象 Lambda 接入点的名称（例如 **tutorial-pii-object-lambda-accesspoint**）。
5. 适用于支持接入点中，输入或浏览到您在步骤 3（例如，**tutorial-pii-access-point**），然后选择选择支持的接入点。
6. 对于 S3 APIs（S3 API），要从 S3 存储桶中检索对象以便 Lambda 函数进行处理，请选择 GetObject。
7. 对于调用 Lambda 函数，您可以为本教程选择以下两个选项之一。
   - 选择从您的账户中的函数中选择，选择您在步骤 4中部署的来自 Lambda 函数下拉列表的 Lambda 函数（例如，**serverlessrepo-ComprehendPiiRedactionS3ObjectLambda**）。
   - 选择输入 ARN，然后输入您在步骤 4 中创建的 Lambda 函数的 Amazon 资源名称（ARN）。
8. 对于 Lambda 函数版本中，选择$LATEST（您在步骤 4中部署的最新版本 Lambda 函数)。
9. （可选）如果您需要 Lambda 函数识别和处理带有范围和分段编号标头的 GET 请求，选择 Lambda 函数支持，使用范围的请求和 Lambda 函数支持带零件编号的请求。否则，请清除这两个复选框。

   有关如何将范围或分段编号与 S3 对象 Lambda 结合使用的更多信息，请参阅 使用 Range 和 partNumber 标头。
10. （可选）在 Payload（负载）- 可选下，添加 JSON 文本，向 Lambda 函数提供其他信息。

    负载是可选 JSON 文本，您可以将其作为来自特定 S3 对象 Lambda 接入点的所有调用的输入提供给 Lambda 函数。要自定义调用同一 Lambda 函数的多个对象 Lambda 接入点的行为，您可以使用不同的参数配置负载，从而扩展 Lambda 函数的灵活性。

    更多有关路径模式的信息，请参阅 事件上下文格式和用法。
11. （可选）对于请求指标 - 可选，选择禁用或启用以将 Amazon S3 监控添加到对象 Lambda 接入点。请求指标按标准 Amazon CloudWatch 费率计费。有关更多信息，请参阅 CloudWatch 定价。

12. 在对象 Lambda 接入点策略 - 可选下，保留默认设置。

    （可选）您可以设置资源策略。此资源策略授予 `GetObject` API 权限，以便使用指定的对象 Lambda 接入点。

13. 对于其余设置，保留默认值，选择创建对象 Lambda 接入点。

### 步骤 6：使用 S3 对象 Lambda 接入点检索编校的文件

现在，S3 对象 Lambda 已准备好从原始文件修订 PII 数据。

#### 使用 S3 对象 Lambda 接入点检索编校的文件

当您请求通过 S3 对象 Lambda 接入点检索文件时，您需要对 S3 对象 Lambda 进行 `GetObject` API 调用。S3 对象 Lambda 调用 Lambda 函数来编辑 PII 数据，并将转换后的数据作为对标准 S3 `GetObject` API调用的响应返回。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择对象 Lambda 接入点。
3. 在对象 Lambda 接入点页面上，选择您在步骤 5 中创建的 S3 对象 Lambda 接入点（例如，**`tutorial-pii-object-lambda-accesspoint`**）。
4. 在 S3 对象 Lambda 接入点的对象选项卡中，选择具有相同名称的文件（例如 `tutorial.txt`）作为您在步骤 2 中上传到 S3 存储桶的文件。

   此文件应包含所有转换的数据。

5. 要查看转换后的数据，请选择打开或者下载。

   您应该能够看到修订的文件，如以下示例所示。

```
Hello *********. Your AnyCompany Financial Services,
LLC credit card account ****************** has a minimum payment
of $24.53 that is due by *********. Based on your autopay settings,
we will withdraw your payment on the due date from your
bank account ********** with the routing number *********.

Your latest statement was mailed to ********************************.
After your payment is received, you will receive a confirmation
text message at ************.
If you have questions about your bill, AnyCompany Customer Service
is available by phone at ************ or
```

```
email at **********************.
```

步骤 7：清除

如果您仅作为学习练习通过 S3 对象 Lambda 修订数据，请删除分配的 Amazon 资源，以便不再累积费用。

分步

- 删除对象 Lambda 接入点
- 删除 S3 接入点
- 删除 Lambda 函数
- 删除 CloudWatch 日志组
- 删除 S3 源存储桶中的原始文件
- 删除 S3 源存储桶
- 删除您的 Lambda 函数的 IAM 角色
- 删除 IAM 用户的客户托管策略
- 删除 IAM 用户

删除对象 Lambda 接入点

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择对象 Lambda 接入点。
3. 在对象 Lambda 接入点页面上，选择在步骤 5 中创建的 S3 对象 Lambda 接入点（例如，**`tutorial-pii-object-lambda-accesspoint`**）左侧的选项按钮。
4. 选择删除。
5. 通过在显示的文本字段中输入对象 Lambda 接入点的名称，确认要删除的对象 Lambda 接入点，然后选择删除。

删除 S3 接入点

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。

2. 在左侧导航窗格中，选择接入点。
3. 导航到您在步骤 3中创建的接入点（例如，**tutorial-pii-access-point**），然后选择接入点名称旁边的选项按钮。
4. 选择删除。
5. 在显示的文本字段中输入接入点名称，然后选择删除，确认您要删除接入点。

### 删除 Lambda 函数

1. 在 Amazon Lambda 控制台左侧导航窗格中 https://console.aws.amazon.com/lambda/ 中，选择函数。
2. 选择您在步骤 4 中创建的函数（例如，**serverlessrepo-ComprehendPiiRedactionS3ObjectLambda**）。
3. 选择操作，然后选择删除。
4. 在删除函数对话框中，选择删除。

### 删除 CloudWatch 日志组

1. 通过 https://console.aws.amazon.com/cloudwatch/ 打开 CloudWatch 控制台。
2. 在左侧导航窗格中，选择日志组。
3. 查找名称以步骤4中创建的 Lambda 函数结尾的日志组（例如，**serverlessrepo-ComprehendPiiRedactionS3ObjectLambda**）。
4. 选择操作，然后选择删除日志组。
5. 在删除日志组对话框中，选择删除。

### 删除 S3 源存储桶中的原始文件

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 在存储桶名称列表中，选择您在步骤 2中将原始文件上传到的存储桶名称（例如，**tutorial-bucket**）。
4. 选中要删除的对象名称左侧的复选框（例如，`tutorial.txt`）。
5. 选择删除。

6. 在永久删除对象？的删除对象页面上，在文本框中输入 **permanently delete** 确认您希望删除此对象。
7. 选择删除对象。

### 删除 S3 源存储桶

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 在存储桶列表中，选择您在步骤 1中创建存储桶名称旁边的选项按钮（例如，**tutorial-bucket**）。
4. 选择删除。
5. 在删除存储桶页面上，通过在文本字段中输入存储桶名称来确认要删除存储桶，然后选择删除存储桶。

### 删除您的 Lambda 函数的 IAM 角色

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在左侧导航窗格中，选择角色，然后选中要删除的角色旁的复选框。角色名称以您在步骤 4中部署的 Lambda 函数名称开头（例如，**serverlessrepo-ComprehendPiiRedactionS3ObjectLambda**）。
3. 选择删除。
4. 在删除对话框中，在文本输入字段中输入角色名称以确认删除。然后选择 Delete(删除)。

### 删除 IAM 用户的客户托管策略

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在左侧导航窗格中，选择 Policies（策略）。
3. 在策略页面上，输入您在搜索框中先决条件中创建的客户托管策略名称（例如，**tutorial-serverless-application-repository**) 以筛选策略列表。选择要删除的策略名称旁边的选项按钮。
4. 选择操作，然后选择删除。

5. 在出现的文本字段中输入此策略的名称，确认要删除此策略，然后选择删除。

### 删除 IAM 用户

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在左侧导航窗格中，选择用户，然后选中要删除的用户旁的复选框。
3. 在页面的顶部，选择删除。
4. 在删除###?对话框中，在文本输入字段中输入用户名以确认删除用户。选择删除。

### 后续步骤

完成本教程后，您可以进一步探索以下相关用例：

- 您可以创建多个 S3 对象 Lambda 接入点，并使用预构建的 Lambda 函数启用这些接入点，根据数据访问者的业务需要，将以不同方式配置这些函数，以编校特定类型的 PII。

  每种类型的用户都代入一个 IAM 角色，且只能访问一个 S3 对象 Lambda 接入点（通过 IAM 策略进行托管）。然后，将为不同编校使用案例配置的每个 `ComprehendPiiRedactionS3ObjectLambda` Lambda 函数附加到不同的 S3 对象 Lambda 接入点。对于每个 S3 对象 Lambda 接入点，您可以拥有一个支持的 S3 接入点，以便从存储共享数据集的 S3 存储桶读取数据。

  有关如何创建 S3 存储桶策略（仅允许用户通过 S3 接入点读取存储桶）的详细信息，请参阅 配置 IAM 策略以使用通用存储桶的接入点。

  有关如何授予用户访问 Lambda 函数、S3 接入点和 S3 对象 Lambda 接入点的权限的更多信息，请参阅为对象 Lambda 接入点配置 IAM 策略。
- 您可以构建自己的 Lambda 函数，并将 S3 对象 Lambda 与自定义的 Lambda 函数结合使用，满足您的特定数据需求。

  例如，要探索各种数据值，您可以使用 S3 对象 Lambda 和自己的 Lambda 函数，该函数使用其他 Amazon Comprehend 特征（例如实体识别、关键短语识别、情绪分析和文档分类）来处理数据。您也可以使用 S3 对象 Lambda 与 Amazon Comprehend Medical（符合 HIPAA 条件的 NLP 服务），用于以上下文感知的方式分析和提取数据。

  有关如何使用 S3 对象 Lambda 和自己的 Lambda 函数转换数据的详细信息，请参阅 教程：使用 S3 对象 Lambda 转换应用程序的数据。

## S3 对象 Lambda 调试和故障排除

当 Lambda 函数调用或执行出现问题时，对 Amazon S3 对象 Lambda 接入点的请求可能会导致新的错误响应。这些错误的格式与标准 Amazon S3 错误的格式相同。有关 S3 对象 Lambda 错误的信息，请参阅 Amazon Simple Storage Service API 参考中的 S3 对象 Lambda 错误代码列表。

有关常规 Lambda 函数调试的更多信息，请参阅 Amazon Lambda 开发人员指南中的监控和排查 Lambda 应用程序故障。

有关标准 Amazon S3 错误的信息，请参阅 Amazon Simple Storage Service API 参考中的错误响应。

您可以在 Amazon CloudWatch 中为对象 Lambda 接入点启用请求指标。这些指标可帮助您监控接入点的运行性能。您可以在创建对象 Lambda 接入点期间或之后启用请求指标。有关更多信息，请参阅 CloudWatch 中的 S3 对象 Lambda 请求指标。

要获取有关向对象 Lambda 接入点发出的请求的更精细的日志记录，您可以启用 Amazon CloudTrail 数据事件。有关更多信息，请参阅 Amazon CloudTrail 用户指南中的记录数据事件以便跟踪。

有关 S3 对象 Lambda 教程，请参阅以下内容：

- 教程：使用 S3 对象 Lambda 转换应用程序的数据
- 教程：使用 S3 对象 Lambda 和 Amazon Comprehend 检测和修订 PII 数据
- 教程：使用 S3 对象 Lambda 在检索图像时对其动态加水印

有关标准接入点的更多信息，请参阅 通过接入点管理对通用存储桶中共享数据集的访问。

有关使用存储桶的信息，请参阅 通用存储桶概述。有关使用对象的信息，请参阅 Amazon S3 对象概述。

# 使用批量操作批量执行对象操作

您可以使用 S3 批量操作对 Amazon S3 对象执行大规模批量操作。S3 批量操作可以对您指定的 Amazon S3 对象列表执行单个操作。单个任务可对数十亿个包含 EB 级数据的对象执行指定操作。Amazon S3 跟踪进度、发送通知并存储所有操作的详细完成报告，从而提供完全托管、可审核的无服务器体验。可以通过 Amazon S3 控制台、Amazon CLI、Amazon SDK 或 Amazon S3 REST API 使用 S3 批量操作。

使用 S3 批量操作复制对象并设置对象标签或访问控制列表（ACL）。您还可以从 S3 Glacier Flexible Retrieval 启动对象还原，或者调用 Amazon Lambda 函数以使用您的对象执行自定义操作。您可以对

自定义的对象列表执行这些操作，也可以使用 Amazon S3 清单报告来轻松生成对象列表。Amazon S3 批量操作使用的 Amazon S3 API 操作与您已在 Amazon S3 中使用的操作相同。

> **Note**
>
> 有关将 Amazon S3 Express One Zone 存储类与目录存储桶配合使用的更多信息，请参阅 S3 Express One Zone 和使用目录存储桶。有关将批量操作与 S3 Express One Zone 和目录存储桶配合使用的更多信息，请参阅对目录存储桶使用批量操作。

## S3 批量操作基础知识

您可以使用 S3 批量操作对 Amazon S3 对象执行大规模批量操作。S3 批量操作可以对您指定的 Amazon S3 对象列表运行单个操作。

### 术语

本节使用的术语清单、任务、操作 和任务 定义如下：

清单

清单是一种 Amazon S3 对象，其中包含您希望 Amazon S3 采取操作的对象键。如果要创建批量操作任务，必须提供清单。用户生成的清单必须包括存储桶名称、对象键以及（可选）每个对象的对象版本。如果您提供用户生成的清单，清单必须采用 Amazon S3 清单报告或 CSV 文件的形式。

还可以让 Amazon S3 根据您在创建任务时指定的对象筛选条件自动生成清单。此选项适用于您在 Amazon S3 控制台中创建的 S3 批量复制任务，也适用于您使用 Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 Amazon S3 REST API 创建的任何任务类型。

作业

任务是 S3 批量操作的基本工作单位。任务包含对清单中所列对象运行指定操作所需的全部信息。在您提供此信息并请求任务开始后，任务将对清单中的每个对象执行操作。

操作

操作是您希望批量操作任务运行的 API 操作的类型，例如复制对象。对于清单中指定的所有对象，每个任务执行单一类型的操作。

任务

任务是任务的执行单元。任务表示为了对单个对象执行任务的操作而对 Amazon S3 或 Amazon Lambda API 操作进行的单个调用。在任务的生命周期内，S3 批量操作将为清单中指定的每个对象创建一个任务。

### S3 批量操作任务的工作原理

任务是 S3 批量操作的基本工作单位。任务包含要对对象列表运行指定操作所需的全部信息。要创建任务，您需要向 S3 批量操作提供对象列表并指定要对这些对象执行的操作。

有关 S3 批量操作支持的操作的信息，请参阅 S3 分批操作支持的操作。

批量任务将对其清单 中包含的每个对象执行指定的操作。清单列出了您希望批处理任务进行处理的对象并将其作为对象存储在存储桶中。您可以使用逗号分隔值（CSV）格式的 使用 S3 清单对数据进行编目和分析 报告作为清单，这样便于轻松创建位于存储桶中的大型对象列表。您还可以指定采用简单的 CSV 格式的清单，这样您便可对单个存储桶中包含的对象的自定义列表执行批量操作。

在您创建任务后，Amazon S3 将处理清单中的对象列表并对每个对象运行指定的操作。在任务运行时，您能够通过编程方式或通过 Amazon S3 控制台监控其进度。您还可以对任务进行配置，以便在其完成时生成完成报告。完成报告会描述任务已执行的每个任务的结果。有关监控任务的更多信息，请参阅 管理 S3 分批操作任务。

S3 批量操作会产生成本。您需要为创建批量操作作业（包括在完成之前取消的作业）付费。有关更多信息，请参阅 Amazon S3 定价。

单个 S3 批量操作任务可处理多达 40 亿个对象。每个 Amazon 账户最多只能有 6 个活动的批量操作任务。要开始创建批量操作任务，请参阅创建 S3 批量操作任务。

## S3 批量操作教程

以下教程提供了一些批量操作任务的完整端到端过程。

- 教程：使用 S3 批量操作对视频进行批量转码

## 授予批处理操作的权限

在创建和运行 S3 分批操作任务之前，您必须授予所需的权限。要创建 Amazon S3 分批操作任务，需要 `s3:CreateJob` 用户权限。创建任务的同一个实体也必须具有 `iam:PassRole` 权限，以便将为此任务指定的 Amazon Identity and Access Management（IAM）角色传递到批量操作。

有关指定 IAM 资源的一般信息，请参阅 IAM 用户指南中的 IAM JSON 策略 – 资源元素。以下各节提供了有关创建 IAM 角色和附加策略的信息。

主题

- 创建 S3 分批操作 IAM 角色
- 附加权限策略

## 创建 S3 分批操作 IAM 角色

Amazon S3 必须具有权限才能代表您执行 S3 分批操作。您通过 Amazon Identity and Access Management (IAM) 角色授予这些权限。此部分提供您在创建 IAM 角色时使用的信任和权限策略的示例。有关更多信息，请参阅 IAM 用户指南中的 IAM 角色。有关示例，请参阅 使用任务标签控制批量操作的权限 和 使用 S3 分批操作复制对象。

在 IAM 策略中，您还可以使用条件键筛选 S3 分批操作任务的访问权限。有关更多信息和 Amazon S3 特定条件键的完整列表，请参阅《Service Authorization Reference》中的 Actions, resources, and condition keys for Amazon S3。

有关按 S3 资源类型对 S3 API 操作的权限的更多信息，请参阅 Amazon S3 API 操作所需的权限。

信任策略

要允许 S3 分批操作服务委托人担任 IAM 角色，您可将以下信任策略附加到该角色。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"batchoperations.s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

## 附加权限策略

根据操作的类型，您可以附加以下策略之一。

在配置权限之前，请注意以下事项：

- 不论执行什么操作，Amazon S3 都需要权限来从您的 S3 存储桶读取清单对象并（可选）将报告写入您的存储桶。因此，所有以下策略均包含这些权限。
- 对于 Amazon S3 清单报告清单，S3 分批操作需要读取 manifest.json 对象以及所有关联的 CSV 数据文件的权限。
- 当您指定对象的版本 ID 时，只需要版本特定的权限，如 `s3:GetObjectVersion`。
- 如果您在加密对象上运行 S3 分批操作，则 IAM 角色还必须拥有对用于加密这些对象的 Amazon KMS 密钥的访问权限。
- 如果您提交使用 Amazon KMS 加密的清单报告清单，则 IAM 策略必须包含对于 manifest.json 对象以及所有关联 CSV 数据文件的 `"kms:Decrypt"` 和 `"kms:GenerateDataKey"` 权限。
- 如果批量操作任务在已启用访问控制列表（ACL）且位于其它 Amazon Web Services 账户内的存储桶中生成清单，则您必须在为该批量任务配置的 IAM 角色的 IAM 策略中授予 `s3:PutObjectAcl` 权限。如果没有包含此权限，则批量任务会失败，并显示错误 `Error occurred when preparing manifest: Failed to write manifest`。

复制对象：PutObject

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectTagging",
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
```

```
                "arn:aws:s3:::amzn-s3-demo-source-bucket",
                "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
            ]
        }
    ]
}
```

替换对象标记：PutObjectTagging

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObjectTagging",
        "s3:PutObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
```

```
        "s3:GetObjectVersion"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObject"
      ],
      "Resource":[
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
      ]
    }
  ]
}
```

删除对象标记：DeleteObjectTagging

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
              "s3:DeleteObjectTagging",
              "s3:DeleteObjectVersionTagging"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
            ]
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
            ]
        }
    ]
}
```

替换访问控制列表：PutObjectAcl

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObjectAcl",
        "s3:PutObjectVersionAcl"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObject"
      ],
      "Resource":[
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
      ]
```

```
    }
  ]
}
```

### 还原对象：RestoreObject

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
          "s3:RestoreObject"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObject"
      ],
      "Resource":[
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
      ]
    }
  ]
}
```

### 应用对象锁定保留：PutObjectRetention

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": "s3:GetBucketObjectLockConfiguration",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-destination-bucket"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObjectRetention",
                "s3:BypassGovernanceRetention"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
            ]
        }
    ]
}
```

应用对象锁定法定保留：PutObjectLegalHold

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:GetBucketObjectLockConfiguration",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-destination-bucket"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "s3:PutObjectLegalHold",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
            ]
        }
    ]
}
```

复制现有对象：InitiateReplication（使用 S3 生成的清单）

如果您使用和存储 S3 生成的清单，请使用此策略。有关使用批量操作来复制现有对象的更多信息，请参阅[使用批量复制以复制现有对象]。

```
{
```

```
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[
            "s3:InitiateReplication"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
         ]
      },
      {
         "Action":[
            "s3:GetReplicationConfiguration",
            "s3:PutInventoryConfiguration"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket"
         ]
      },
      {
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*",
            "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
         ]
      }
   ]
}
```

复制现有对象：InitiateReplication（使用用户清单）

如果您使用用户提供的清单，请使用此策略。有关使用批量操作来复制现有对象的更多信息，请参阅使用批量复制以复制现有对象。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[
            "s3:InitiateReplication"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
         ]
      },
      {
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
         ]
      }
   ]
}
```

## 创建 S3 批量操作任务

借助 Amazon S3 批量操作，您可以对特定 Amazon S3 对象的列表执行大规模批量操作。本节介绍创建 S3 批量操作任务所需的信息以及 `CreateJob` 请求的结果。它还提供说明，讲解如何通过使用

Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）和 适用于 Java 的 Amazon SDK 创建批量操作任务。

当您创建 S3 批量操作任务时，可以为全部任务或仅失败任务请求完成报告。只要成功调用了至少一个任务，S3 批量操作即会为已完成、已失败或已取消的任务生成报告。有关更多信息，请参阅 示例：S3 分批操作完成报告。

主题

- 批量操作任务请求元素
- 指定清单

## 批量操作任务请求元素

要创建 S3 批量操作任务，您必须提供以下信息：

操作

指定希望 S3 批量操作对清单中的对象运行的操作。每种操作类型都接受特定于该操作的参数。借助批量操作功能，您可以批量执行操作，其结果与对每个对象逐个执行该操作相同。

清单

清单是您希望 S3 批量操作对其运行指定操作的所有对象的列表。您可以使用以下方法为批量操作任务指定清单。

- 手动创建您自己自定义的 CSV 格式的对象列表。
- 选择现有的 CSV 格式的 使用 S3 清单对数据进行编目和分析 报告。
- 直接批量操作功能可根据您在创建任务时指定的对象筛选条件自动生成清单。此选项适用于您在 Amazon S3 控制台中创建的批量复制任务，也适用于您使用 Amazon CLI、Amazon SDK 或 Amazon S3 REST API 创建的任何任务类型。

> **Note**
>
> - 无论您如何指定清单，列表本身都必须存储在通用存储桶中。批量操作无法从目录存储桶中导入现有清单，也无法将生成的清单保存到目录存储桶。但是，清单中描述的对象可以存储在目录存储桶中。有关更多信息，请参阅目录存储桶。
> - 如果清单中的对象位于受版本控制的存储桶中，指定对象的版本 ID 时，批量操作将在特定版本上执行此操作。如果未指定版本 ID，则批量操作将针对最新对象版本执行该操作。如果您的清单包含版本 ID 字段，则必须为清单中的所有对象提供版本 ID。

有关更多信息，请参阅 指定清单。

优先级

使用任务优先级指示此任务相对于在您账户中运行的其他任务的优先级。数字越大，优先级越高。

任务优先级仅相对于为同一账户和区域中的其他任务设置的优先级有意义。您可以选择适合您的编号系统。例如，您可能希望将所有还原（`RestoreObject`）任务的优先级指定为 1，将所有复制（`CopyObject`）任务的优先级指定为 2，并将所有替换访问控制列表（ACL）（`PutObjectAcl`）任务的优先级指定为 3。

S3 批量操作根据优先级编号确定任务的优先级，但不严格保证顺序。因此，任务优先级并不用来确保任何一个任务会在其他任何任务之前开始或完成。如果您需要确保严格的顺序，请等到一个任务完成后，再开始下一个任务。

RoleArn

指定将运行任务的 Amazon Identity and Access Management (IAM) 角色。您使用的 IAM 角色必须具有足够的权限来执行任务中指定的操作。例如，要运行 `CopyObject` 任务，IAM 角色必须具有针对源存储桶的 `s3:GetObject` 权限和针对目标存储桶的 `s3:PutObject` 权限。该角色还需要读取清单和写入任务完成报告的权限。

有关 IAM 角色的更多信息，请参阅《IAM 用户指南》中的 IAM 角色。

有关 Amazon S3 权限的更多信息，请参阅 Amazon S3 的策略操作。

> **Note**
>
> 对目录存储桶执行操作的批量操作任务需要特定的权限。有关更多信息，请参阅适用于 S3 Express One Zone 的 Amazon Identity and Access Management（IAM）。

报告

指定您是否希望 S3 批量操作生成完成报告。如果您请求任务完成报告，还必须在此元素中提供报告参数。必要的信息包括：

- 您希望存储报告的存储桶

> **Note**
>
> 报告必须存储在通用存储桶中。批量操作功能无法将报告保存到目录存储桶中。有关更多信息，请参阅目录存储桶。

- 报告的格式
- 您希望报告包含所有任务的详细信息还是只包含失败的任务
- 可选的前缀字符串

> **Note**
>
> 完成报告始终使用具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）来进行加密。

标签（可选）

您可以通过添加标签来标记和控制对 S3 批量操作任务的访问。您可以使用标签来标识谁负责批量操作任务，或者控制用户与批量操作任务的交互方式。任务标签的存在可授予或限制用户取消任务、激活处于确认状态的任务或更改任务优先级的能力。例如，您可以授予用户调用 `CreateJob` 操作的权限，前提是使用标签 `"Department=Finance"` 创建此任务。

您可以创建附加了标签的任务，并且可以在创建任务后向任务添加标签。

有关更多信息，请参阅 the section called “使用标签”。

Description（可选）

要跟踪和监控任务，您还可以提供最多包含 256 个字符的描述。只要返回有关任务的信息或在 Amazon S3 控制台中显示任务详细信息，Amazon S3 便会包含此描述。随后您便可以根据自己分配的描述轻松地对任务进行排序和筛选。描述不一定是唯一的，因此您可以使用描述作为类别（例如“每周日志复制任务”）来帮助您跟踪多组相似的任务。

## 指定清单

清单是一种 Amazon S3 对象，其中包含您希望 Amazon S3 采取操作的对象键。您可以通过下列方式之一提供清单：

- 手动创建新的清单文件。

- 使用现有的清单。
- 直接批量操作功能可根据您在创建任务时指定的对象筛选条件自动生成清单。此选项适用于您在 Amazon S3 控制台中创建的批量复制任务，也适用于您使用 Amazon CLI、Amazon SDK 或 Amazon S3 REST API 创建的任何任务类型。

> **Note**
>
> - Amazon S3 批量操作不支持跨区域清单生成。
> - 无论您如何指定清单，列表本身都必须存储在通用存储桶中。批量操作无法从目录存储桶中导入现有清单，也无法将生成的清单保存到目录存储桶。但是，清单中描述的对象可以存储在目录存储桶中。有关更多信息，请参阅目录存储桶。

创建清单文件

要手动创建清单文件，您需要采用 CSV 格式列表的形式，指定清单对象键、ETag（实体键）和可选的版本 ID。清单的内容必须是 URL 编码的。

默认情况下，Amazon S3 自动使用具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）对上传到 Amazon S3 存储桶的清单进行加密。不支持使用具有客户提供密钥（SSE-C）的服务器端加密的清单。仅当使用 CSV 格式的清单报告时，才支持使用具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）的清单。不支持将手动创建的清单与 Amazon KMS 一起使用。

您的清单必须包括存储桶名称、对象键以及（可选）每个对象的对象版本。S3 批量操作不使用清单中的任何其他字段。

> **Note**
>
> 如果清单中的对象位于受版本控制的存储桶中，指定对象的版本 ID 时，批量操作将在特定版本上执行此操作。如果未指定版本 ID，则批量操作将针对最新对象版本执行该操作。如果您的清单包含版本 ID 字段，则必须为清单中的所有对象提供版本 ID。

下面是 CSV 格式的没有版本 ID 的清单示例。

```
amzn-s3-demo-bucket1,objectkey1
```

```
amzn-s3-demo-bucket1,objectkey2
amzn-s3-demo-bucket1,objectkey3
amzn-s3-demo-bucket1,photos/jpgs/objectkey4
amzn-s3-demo-bucket1,photos/jpgs/newjersey/objectkey5
amzn-s3-demo-bucket1,object%20key%20with%20spaces
```

下面是 CSV 格式的包含版本 ID 的清单示例。

```
amzn-s3-demo-bucket1,objectkey1,PZ9ibn9D5lP6p298B7S9_ceqx1n5EJ0p
amzn-s3-demo-bucket1,objectkey2,YY_ouuAJByNW1LRBfFMfxMge7XQWxMBF
amzn-s3-demo-bucket1,objectkey3,jbo9_jhdPEyB4RrmOxWS0kU0EoNrU_oI
amzn-s3-demo-bucket1,photos/jpgs/objectkey4,6EqlikJJxLTsHsnbZbSRffn24_eh5Ny4
amzn-s3-demo-bucket1,photos/jpgs/newjersey/objectkey5,imHf3FAiRsvBW_EHB8GOu.NHunHO1gVs
amzn-s3-demo-bucket1,object%20key%20with%20spaces,9HkPvDaZY5MVbMhn6TMn1YTb5ArQAo3w
```

指定现有的清单文件

您可以使用以下两种格式之一，在创建任务请求中指定清单文件：

- Amazon S3 清单报告 – 必须是 CSV 格式的 Amazon S3 清单报告。您必须指定与清单报告关联的 `manifest.json` 文件。有关清单报告的更多信息，请参阅 使用 S3 清单对数据进行编目和分析。如果清单报告包括版本 ID，S3 批量操作将对特定对象版本进行操作。

  > **Note**
  >
  > - S3 批量操作支持用 SSE-KMS 加密的 CSV 格式清单报告。
  > - 如果您提交使用 SSE-KMS 加密的清单报告清单，则 IAM 策略必须包含对于 `manifest.json` 对象以及所有关联 CSV 数据文件的 `"kms:Decrypt"` 和 `"kms:GenerateDataKey"` 权限。

- CSV 文件 – 文件中的每一行必须包括存储桶名称和对象键，还可选择包括对象版本。对象键必须进行 URL 编码，如以下示例所示。清单必须包含所有对象的版本 ID 或忽略所有对象的版本 ID。有关 CSV 清单格式的更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 JobManifestSpec。

  > **Note**
  >
  > S3 批量操作不支持使用 SSE-KMS 加密的 CSV 清单文件。

> **Important**
>
> 当您使用手动创建的清单和受版本控制的存储桶时，我们建议您指定对象的版本 ID。创建任务时，S3 批量操作会在运行任务之前解析整个清单。不过，它不会获取存储桶状态的“快照”。由于清单可以包含数十亿个对象，因此任务可能需要很长时间才能运行完，这可能会影响任务所针对的对象版本。假设您在任务运行时用新版本覆盖某个对象，但未指定该对象的版本 ID。在这种情况下，Amazon S3 将对该对象的最新版本（而不是在创建作业时存在的版本）执行操作。避免此行为的唯一方式是为清单中列出的对象指定版本 ID。

### 自动生成清单

您可以指示 Amazon S3 批量操作根据创建任务时指定的对象筛选条件自动生成清单。此选项适用于您在 Amazon S3 控制台中创建的批量复制任务，也适用于您使用 Amazon CLI、Amazon SDK 或 Amazon S3 REST API 创建的任何任务类型。有关分批复制的更多信息，请参阅 使用批量复制以复制现有对象。

要自动生成清单，请在任务创建请求中指定以下元素：

- 有关包含您的源对象的存储桶的信息，包括存储桶拥有者和 Amazon 资源名称（ARN）
- 有关清单输出的信息，包括用于创建清单文件的标志、输出存储桶拥有者、ARN、前缀、文件格式和加密类型
- 按对象的创建日期、键名称、大小和存储类来筛选对象的可选标准。对于复制任务，还可以使用标签来筛选对象。

### 对象筛选标准

要筛选要包含在自动生成的清单中的对象列表，您可以指定以下标准。有关更多信息，请参阅《Amazon S3 API 参考》中的 JobManifestGeneratorFilter。

CreatedAfter

如果提供，则生成的清单仅包含在此时间之后创建的源存储桶对象。

CreatedBefore

如果提供，则生成的清单仅包含在此时间之前创建的源存储桶对象。

EligibleForReplication

如果提供，则生成的清单仅包含根据源存储桶上的复制配置而符合复制条件的对象。

KeyNameConstraint

如果提供，则生成的清单仅包含下面这样的源存储桶对象：其对象密钥与 MatchAnySubstring、MatchAnyPrefix 和 MatchAnySuffix 所指定的字符串约束相匹配。

MatchAnySubstring – 如果提供，则当指定的字符串出现在对象密钥字符串中的任何位置时，生成的清单将包含对象。

MatchAnyPrefix – 如果提供，则当指定的字符串出现在对象密钥字符串的开头时，生成的清单将包含对象。

MatchAnySuffix – 如果提供，则当指定的字符串出现在对象密钥字符串的末尾时，生成的清单将包含对象。

MatchAnyStorageClass

如果提供，则生成的清单仅包含以指定存储类存储的源存储桶对象。

ObjectReplicationStatuses

如果提供，则生成的清单仅包含具有指定复制状态之一的源存储桶对象。

ObjectSizeGreaterThanBytes

如果提供，则生成的清单仅包含文件大小大于指定字节数的源存储桶对象。

ObjectSizeLessThanBytes

如果提供，则生成的清单仅包含文件大小小于指定字节数的源存储桶对象。

> **Note**
>
> 您无法克隆大多数自动生成清单的任务。可以克隆批量复制任务，除非它们使用 `KeyNameConstraint`、`MatchAnyStorageClass`、`ObjectSizeGreaterThanBytes` 或 `ObjectSizeLessThanBytes` 清单筛选标准。

指定清单标准的语法因您用于创建任务的方法而异。有关示例，请参阅 创建作业。

创建作业

您可以使用 Amazon S3 控制台、Amazon CLI、Amazon SDK 或 Amazon S3 REST API 创建 S3 批量操作任务。

有关创建任务请求的更多信息，请参阅 批量操作任务请求元素。

先决条件

在创建批量操作任务之前，请确认您已配置相关权限。有关更多信息，请参阅 授予批处理操作的权限。

使用 S3 控制台

创建批量任务

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在页面顶部的导航栏中，选择当前所显示 Amazon Web Services 区域的名称。接下来，选择要在其中创建任务的区域。

   > **Note**
   >
   > 对于复制操作，必须在目标存储桶所在的同一区域中创建任务。对于所有其它操作，必须在与清单中的对象相同的区域中创建任务。

3. 在 Amazon S3 控制台的左侧导航窗格中选择批量操作。
4. 请选择创建任务。
5. 查看要在其中创建任务的 Amazon Web Services 区域。
6. 在 Manifest format (清单格式) 下，请选择要使用的清单对象的类型。

   - 如果您选择 S3 inventory report (S3 清单报告)，请输入 Amazon S3 在 CSV 格式的清单报告中生成的 manifest.json 对象的路径，以及（可选）输入清单对象的版本 ID（如果您要使用的版本不是最新版本）。
   - 如果您选择 CSV，请输入 CSV 格式清单对象的路径。清单对象必须遵循控制台中描述的格式。如果您希望使用并非最新的对象版本，则可以选择包含清单对象的版本 ID。

   > **Note**
   >
   > Amazon S3 控制台仅支持对批量复制任务自动生成清单。对于其他所有任务类型，如果您希望 Amazon S3 根据您指定的筛选标准自动生成清单，则必须使用 Amazon CLI、Amazon SDK 或 Amazon S3 REST API 配置您的任务。

7. 请选择 Next（下一步）。

8. 在 Operation (操作) 下，请选择您希望对清单中列出的所有对象执行的操作。填写您所选操作的信息，然后选择下一步。
9. 填写配置额外选项的信息，然后选择下一步。
10. 对于审核，验证设置。如果需要进行更改，请选择 Previous。否则，请选择创建任务。

使用 Amazon CLI

要使用 Amazon CLI 创建批量操作任务，请根据您是指定现有清单还是自动生成清单，选择以下示例之一。

Specify manifest

以下示例说明如何使用 Amazon CLI 来创建 S3 批量操作 `S3PutObjectTagging` 任务，以便处理现有清单文件中列出的对象。

通过指定清单来创建批量操作 **`S3PutObjectTagging`** 任务

1. 使用以下命令创建 Amazon Identity and Access Management（IAM）角色，然后创建一个 IAM 策略来分配相关权限。以下角色和策略授予 Amazon S3 添加对象标签的权限，您在后续步骤中创建任务时将需要用到该权限。

   a. 使用以下示例命令创建 IAM 角色供批量操作使用。要使用此示例命令，请将 *`S3BatchJobRole`* 替换为要为角色指定的名称。

```
aws iam create-role \
 --role-name S3BatchJobRole \
 --assume-role-policy-document '{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"batchoperations.s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}'
```

   记下角色的 Amazon 资源名称（ARN）。创建任务时，您需要该 ARN。

b. 使用以下示例命令创建具有必要权限的 IAM 策略，并将其附加到您在上一步中创建的 IAM 角色。有关必要权限的更多信息，请参阅授予批处理操作的权限。

> **Note**
>
> 对目录存储桶执行操作的批量操作任务需要特定的权限。有关更多信息，请参阅适用于 S3 Express One Zone 的 Amazon Identity and Access Management（IAM）。

要使用此示例命令，请按如下方式替换 *user input placeholders*：

- 将 *S3BatchJobRole* 替换为您的 IAM 角色的名称。请确保此名称与您之前使用的名称一致。
- 将 *PutObjectTaggingBatchJobPolicy* 替换为要为 IAM 策略指定的名称。
- 将 *amzn-s3-demo-destination-bucket* 替换为包含要应用标签的对象的存储桶的名称。
- 将 *amzn-s3-demo-manifest-bucket* 替换为包含清单的存储桶的名称。
- 将 *amzn-s3-demo-completion-report-bucket* 替换为要将完成报告交付到的存储桶的名称。

```
aws iam put-role-policy \
  --role-name S3BatchJobRole \
  --policy-name PutObjectTaggingBatchJobPolicy \
  --policy-document '{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObjectTagging",
        "s3:PutObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    },
    {
      "Effect": "Allow",
      "Action": [
```

```
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket",
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "Resource":[
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
      ]
    }
  ]
}'
```

2. 使用以下示例命令创建 S3PutObjectTagging 任务。

manifest.csv 文件提供存储桶和对象键值的列表。任务将指定的标签应用到清单中标识的对象。ETag 是 manifest.csv 对象的 ETag，可以从 Amazon S3 控制台获取。此请求指定了 no-confirmation-required 参数，这样您就可以运行任务，而不必使用 update-job-status 命令进行确认。有关更多信息，请参阅 Amazon CLI 命令参考 中的 create-job。

要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。将 *IAM-role* 替换为您之前创建的 IAM 角色的 ARN。

```
aws s3control create-job \
    --region us-west-2 \
    --account-id acct-id \
    --operation '{"S3PutObjectTagging": { "TagSet": [{"Key":"keyOne",
 "Value":"ValueOne"}] }}' \
    --manifest '{"Spec":{"Format":"S3BatchOperations_CSV_20180820","Fields":
["Bucket","Key"]},"Location":{"ObjectArn":"arn:aws:s3:::amzn-s3-demo-manifest-
bucket/manifest.csv","ETag":"60e460c9d1046e73f7dde5043ac3ae85"}}' \
```

```
    --report '{"Bucket":"arn:aws:s3:::amzn-s3-demo-
completion-report-bucket","Prefix":"final-reports",
 "Format":"Report_CSV_20180820","Enabled":true,"ReportScope":"AllTasks"}' \
    --priority 42 \
    --role-arn IAM-role \
    --client-request-token $(uuidgen) \
    --description "job description" \
    --no-confirmation-required
```

作为响应，Amazon S3 返回任务 ID（例如 `00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c`）。您需要使用任务 ID 来识别、监控和修改任务。

### Generate manifest

以下示例说明如何创建 S3 批量操作 `S3DeleteObjectTagging` 任务，该任务会根据您的对象筛选标准自动生成清单。此标准包括创建日期、密钥名称、大小、存储类和标签。

通过生成清单来创建批量操作 **`S3DeleteObjectTagging`** 任务

1. 使用以下命令创建 Amazon Identity and Access Management（IAM）角色，然后创建一个 IAM 策略来分配权限。以下角色和策略授予 Amazon S3 删除对象标签的权限，您在后续步骤中创建任务时将需要用到该权限。

   a. 使用以下示例命令创建 IAM 角色供批量操作使用。要使用此示例命令，请将 *`S3BatchJobRole`* 替换为要为角色指定的名称。

```
aws iam create-role \
 --role-name S3BatchJobRole \
 --assume-role-policy-document '{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"batchoperations.s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}'
```

记下角色的 Amazon 资源名称（ARN）。创建任务时，您需要该 ARN。

b. 使用以下示例命令创建具有必要权限的 IAM 策略，并将其附加到您在上一步中创建的 IAM 角色。有关必要权限的更多信息，请参阅授予批处理操作的权限。

> **Note**
>
> 对目录存储桶执行操作的批量操作任务需要特定的权限。有关更多信息，请参阅适用于 S3 Express One Zone 的 Amazon Identity and Access Management（IAM）。

要使用此示例命令，请按如下方式替换 *user input placeholders*：

- 将 *S3BatchJobRole* 替换为您的 IAM 角色的名称。请确保此名称与您之前使用的名称一致。
- 将 *DeleteObjectTaggingBatchJobPolicy* 替换为要为 IAM 策略指定的名称。
- 将 *amzn-s3-demo-destination-bucket* 替换为包含要应用标签的对象的存储桶的名称。
- 将 *amzn-s3-demo-manifest-bucket* 替换为您想用于保存清单的存储桶的名称。
- 将 *amzn-s3-demo-completion-report-bucket* 替换为要将完成报告交付到的存储桶的名称。

```
aws iam put-role-policy \
  --role-name S3BatchJobRole \
  --policy-name DeleteObjectTaggingBatchJobPolicy \
  --policy-document '{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    },
    {
```

```
      "Effect":"Allow",
      "Action":[
        "s3:PutInventoryConfiguration"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket",
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Resource":[
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    }
  ]
}'
```

2. 使用以下命令创建 S3DeleteObjectTagging 任务。

   在此示例中，--report 部分中的值指定了将生成的任务报告的存储桶、前缀、格式和范围。该 --manifest-generator 部分指定了有关包含任务将处理的对象的源存储桶的信息、有关将为任务生成的清单输出列表的信息，以及按创建日期、名称限制、大小和存储类来缩小要包含在清单中的对象范围的筛选标准。该命令还指定任务的优先级、IAM 角色和 Amazon Web Services 区域。

   有关更多信息，请参阅 Amazon CLI 命令参考 中的 create-job。

要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。将 *IAM-role* 替换为您之前创建的 IAM 角色的 ARN。

```
aws s3control create-job \
    --account-id 012345678901 \
    --operation '{
        "S3DeleteObjectTagging": {}
    }' \
    --report '{
        "Bucket":"arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
        "Prefix":"reports",
        "Format":"Report_CSV_20180820",
        "Enabled":true,
        "ReportScope":"AllTasks"
    }' \
    --manifest-generator '{
        "S3JobManifestGenerator": {
          "ExpectedBucketOwner": "012345678901",
          "SourceBucket": "arn:aws:s3:::amzn-s3-demo-source-bucket",
          "EnableManifestOutput": true,
          "ManifestOutputLocation": {
            "ExpectedManifestBucketOwner": "012345678901",
            "Bucket": "arn:aws:s3:::amzn-s3-demo-manifest-bucket",
            "ManifestPrefix": "prefix",
            "ManifestFormat": "S3InventoryReport_CSV_20211130"
          },
          "Filter": {
            "CreatedAfter": "2023-09-01",
            "CreatedBefore": "2023-10-01",
            "KeyNameConstraint": {
              "MatchAnyPrefix": [
                "prefix"
              ],
              "MatchAnySuffix": [
                "suffix"
              ]
            },
            "ObjectSizeGreaterThanBytes": 100,
            "ObjectSizeLessThanBytes": 200,
            "MatchAnyStorageClass": [
              "STANDARD",
              "STANDARD_IA"
```

```
            ]
          }
        }
      }' \
    --priority 2 \
    --role-arn IAM-role \
    --region us-east-1
```

作为响应，Amazon S3 返回任务 ID（例如 `00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c`）。您将需要此任务 ID 来识别、监控或修改任务。

使用 适用于 Java 的 Amazon SDK

要使用 适用于 Java 的 Amazon SDK 创建批量操作任务，请根据您是指定现有清单还是自动生成清单，选择以下示例之一。

Specify manifest

以下示例说明如何创建 S3 批量操作 `S3PutObjectTagging` 任务，以便处理现有清单文件中列出的对象。要使用此示例，请将 *`user input placeholders`* 替换为您自己的信息。

Example

```
package aws.example.s3control;



import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.*;

import java.util.UUID;
import java.util.ArrayList;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class CreateJob {
    public static void main(String[] args) {
        String accountId = "Account ID";
```

```
        String iamRoleArn = "IAM Role ARN";
        String reportBucketName = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
        String uuid = UUID.randomUUID().toString();

        ArrayList tagSet = new ArrayList<S3Tag>();
        tagSet.add(new S3Tag().withKey("keyOne").withValue("ValueOne"));


        try {
            JobOperation jobOperation = new JobOperation()
                    .withS3PutObjectTagging(new S3SetObjectTaggingOperation()
                            .withTagSet(tagSet)
                    );

            JobManifest manifest = new JobManifest()
                    .withSpec(new JobManifestSpec()
                            .withFormat("S3BatchOperations_CSV_20180820")
                            .withFields(new String[]{
                                    "Bucket", "Key"
                            }))
                    .withLocation(new JobManifestLocation()
                            .withObjectArn("arn:aws:s3:::my_manifests/manifest.csv")
                            .withETag("60e460c9d1046e73f7dde5043ac3ae85"));
            JobReport jobReport = new JobReport()
                    .withBucket(reportBucketName)
                    .withPrefix("reports")
                    .withFormat("Report_CSV_20180820")
                    .withEnabled(true)
                    .withReportScope("AllTasks");

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.createJob(new CreateJobRequest()
                    .withAccountId(accountId)
                    .withOperation(jobOperation)
                    .withManifest(manifest)
                    .withReport(jobReport)
                    .withPriority(42)
                    .withRoleArn(iamRoleArn)
                    .withClientRequestToken(uuid)
```

```
                    .withDescription("job description")
                    .withConfirmationRequired(false)
            );

        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

### Generate manifest

以下示例说明如何创建 S3 批量操作 s3PutObjectCopy 任务，以便根据对象筛选标准（包括创建日期、密钥名称和大小）自动生成清单。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

#### Example

```
        package aws.example.s3control;

    import com.amazonaws.AmazonServiceException;
    import com.amazonaws.SdkClientException;
    import com.amazonaws.auth.profile.ProfileCredentialsProvider;
    import com.amazonaws.services.s3control.AWSS3Control;
    import com.amazonaws.services.s3control.AWSS3ControlClient;
    import com.amazonaws.services.s3control.model.CreateJobRequest;
    import com.amazonaws.services.s3control.model.CreateJobResult;
    import com.amazonaws.services.s3control.model.JobManifestGenerator;
    import com.amazonaws.services.s3control.model.JobManifestGeneratorFilter;
    import com.amazonaws.services.s3control.model.JobOperation;
    import com.amazonaws.services.s3control.model.JobReport;
    import com.amazonaws.services.s3control.model.KeyNameConstraint;
    import com.amazonaws.services.s3control.model.S3JobManifestGenerator;
    import com.amazonaws.services.s3control.model.S3ManifestOutputLocation;
    import com.amazonaws.services.s3control.model.S3SetObjectTaggingOperation;
    import com.amazonaws.services.s3control.model.S3Tag;

    import java.time.Instant;
```

```
    import java.util.Date;
    import java.util.UUID;
    import java.util.ArrayList;

    import static com.amazonaws.regions.Regions.US_WEST_2;

    public class test {
        public static void main(String[] args) {
            String accountId = "012345678901";
            String iamRoleArn = "arn:aws:iam::012345678901:role/ROLE";
            String sourceBucketName = "arn:aws:s3:::amzn-s3-demo-source-bucket";
            String reportBucketName = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
            String manifestOutputBucketName = "arn:aws:s3:::amzn-s3-demo-manifest-
bucket";
            String uuid = UUID.randomUUID().toString();
            long minimumObjectSize = 100L;

            ArrayList<S3Tag> tagSet = new ArrayList<>();
            tagSet.add(new S3Tag().withKey("keyOne").withValue("ValueOne"));

            ArrayList<String> prefixes = new ArrayList<>();
            prefixes.add("s3KeyStartsWith");

            try {
                JobOperation jobOperation = new JobOperation()
                        .withS3PutObjectTagging(new S3SetObjectTaggingOperation()
                                .withTagSet(tagSet)
                        );
                S3ManifestOutputLocation manifestOutputLocation = new
 S3ManifestOutputLocation()
                        .withBucket(manifestOutputBucketName)
                        .withManifestPrefix("manifests")
                        .withExpectedManifestBucketOwner(accountId)
                        .withManifestFormat("S3InventoryReport_CSV_20211130");

                JobManifestGeneratorFilter jobManifestGeneratorFilter = new
 JobManifestGeneratorFilter()
                        .withEligibleForReplication(true)
                        .withKeyNameConstraint(
                                new KeyNameConstraint()
                                        .withMatchAnyPrefix(prefixes))
                        .withCreatedBefore(Date.from(Instant.now()))
                        .withObjectSizeGreaterThanBytes(minimumObjectSize);
```

```
                S3JobManifestGenerator s3JobManifestGenerator = new
S3JobManifestGenerator()
                        .withEnableManifestOutput(true)
                        .withManifestOutputLocation(manifestOutputLocation)
                        .withFilter(jobManifestGeneratorFilter)
                        .withSourceBucket(sourceBucketName);

                JobManifestGenerator jobManifestGenerator = new
JobManifestGenerator()
                        .withS3JobManifestGenerator(s3JobManifestGenerator);

                JobReport jobReport = new JobReport()
                        .withBucket(reportBucketName)
                        .withPrefix("reports")
                        .withFormat("Report_CSV_20180820")
                        .withEnabled(true)
                        .withReportScope("AllTasks");

                AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                        .withCredentials(new ProfileCredentialsProvider())
                        .withRegion(US_WEST_2)
                        .build();

                CreateJobResult createJobResult = s3ControlClient.createJob(new
CreateJobRequest()
                        .withAccountId(accountId)
                        .withOperation(jobOperation)
                        .withManifestGenerator(jobManifestGenerator)
                        .withReport(jobReport)
                        .withPriority(42)
                        .withRoleArn(iamRoleArn)
                        .withClientRequestToken(uuid)
                        .withDescription("job description")
                        .withConfirmationRequired(true)
                );

                System.out.println("Created job " + createJobResult.getJobId());

            } catch (AmazonServiceException e) {
                // The call was transmitted successfully, but Amazon S3 couldn't
process
                // it and returned an error response.
                e.printStackTrace();
```

```
            } catch (SdkClientException e) {
                // Amazon S3 couldn't be contacted for a response, or the client
                // couldn't parse the response from Amazon S3.
                e.printStackTrace();
            }
        }
    }
```

使用 REST API

您可以使用 REST API 创建批量操作任务。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 CreateJob。

任务响应

如果 `CreateJob` 请求成功，Amazon S3 将返回一个任务 ID。任务 ID 是 Amazon S3 自动生成的唯一标识符，以便于您标识批量操作任务并监控其状态。

通过 Amazon CLI、Amazon SDK 或 REST API 创建任务时，您可以设置 S3 批量操作以开始自动处理任务。任务在准备就绪后立即开始运行，而不是等待后面较高优先级的任务。

当您通过 Amazon S3 控制台创建任务时，在批量操作开始处理该任务之前，您必须查看任务详细信息并确认希望运行它。如果任务保持暂停状态超过 30 天，则它将失败。

## S3 分批操作支持的操作

您可以使用 S3 批量操作对 Amazon S3 对象执行大规模批量操作。S3 批量操作可以对您指定的 Amazon S3 对象列表执行单个操作。单个任务可对数十亿个包含 EB 级数据的对象执行指定操作。Amazon S3 跟踪进度、发送通知并存储所有操作的详细完成报告，从而提供完全托管、可审核的无服务器体验。可以通过 Amazon S3 控制台、Amazon CLI、Amazon SDK 或 Amazon S3 REST API 使用 S3 批量操作。

S3 批处理操作支持以下操作：

### 复制对象

可以使用 Amazon S3 批量操作对 Amazon S3 对象执行大规模批量操作。批量操作复制操作会复制清单中指定的每个对象。可以将对象复制到相同 Amazon Web Services 区域中的存储桶或不同区域中的存储桶。S3 分批操作支持 Amazon S3 所提供用于复制对象的大部分选项。这些选项包括设置对象元数据、设置权限以及更改对象的存储类。

可以使用复制操作来复制现有的未加密对象，并将其作为加密的对象写入到同一存储桶。有关更多信息，请参阅使用 Amazon S3 分批操作加密对象。

复制对象时，可以更改用于计算对象校验和的校验和算法。如果对象没有额外的已计算校验和，您还可以通过指定 Amazon S3 要使用的校验和算法来添加一个校验和。有关更多信息，请参阅 在 Amazon S3 中检查对象完整性。

有关复制 Amazon S3 中的对象以及必需参数和可选参数的更多信息，请参阅本指南中的复制、移动和重命名对象和《Amazon Simple Storage Service API 参考》中的 CopyObject。

限制和局限性

当您使用批量操作复制操作时，以下限制和局限性适用：

- 所有源对象必须位于一个存储桶中。
- 所有目标对象必须位于一个存储桶中。
- 您必须具有源存储桶的读取权限和目标存储桶的写入权限。
- 复制的对象大小最多为 5 GB。
- 如果您尝试将对象从 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 类复制到 S3 Standard 存储类，则必须先还原这些对象。有关更多信息，请参阅 恢复已归档的对象。
- 必须在目标区域（即您打算将对象复制到的区域）中创建批量操作复制任务。
- 除了针对实体标签（ETag）的条件检查和具有客户提供的加密密钥的服务器端加密（SSE-C）之外，所有 `CopyObject` 选项都受支持。
- 如果目标存储桶不受版本控制，您将覆盖任何具有相同键名称的对象。
- 不必以对象在清单中出现的相同顺序复制这些对象。对于受版本控制的存储桶，如果保留当前或非当前版本顺序很重要，则首先复制所有非当前版本。然后，在第一个任务完成后，在后续任务中复制当前版本。
- 不支持将对象复制到低冗余存储（RRS）类。

使用 S3 分批操作复制对象

可以使用 Amazon S3 批量操作对 Amazon S3 对象执行大规模批量操作。可以使用 S3 批量操作创建复制 (`CopyObject`) 任务，以便在同一账户内复制对象或将对象复制到不同的目标账户。

以下示例说明了如何存储和使用位于不同账户中的清单。第一个示例说明了如何使用 Amazon S3 清单将清单报告发送到目标账户，以便在创建任务期间使用。第二个示例说明了如何在源账户或目标账户

中使用逗号分隔值（CSV）清单。第三个示例说明了如何使用复制操作为现有对象启用 S3 存储桶密钥，而这些对象已使用具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）进行加密。

复制操作示例

- 使用清单报告跨 Amazon Web Services 账户 复制对象
- 使用 CSV 清单跨 Amazon Web Services 账户 复制对象
- 使用批量操作为 SSE-KMS 启用 S3 存储桶密钥

使用清单报告跨 Amazon Web Services 账户 复制对象

可以使用 Amazon S3 批量操作对 Amazon S3 对象执行大规模批量操作。可以使用 S3 批量操作创建复制 (`CopyObject`) 任务，以便在同一账户内复制对象或将对象复制到不同的目标账户。

可以使用 Amazon S3 清单创建清单报告，然后使用该报告创建要使用 S3 批量操作复制的对象列表（清单）。有关在源账户或目标账户中使用 CSV 清单的信息，请参阅 the section called “使用 CSV 清单跨 Amazon Web Services 账户 复制对象”。

Amazon S3 清单生成桶中的对象的清单。生成的列表将发布到输出文件。进行清点的桶称为源桶，其中存储清单报告文件的桶称为目标桶。

Amazon S3 清单报告可配置为传输到另一个 Amazon Web Services 账户。如果这样做，则在目标账户中创建任务时，将支持 S3 批量操作读取清单报告。

有关 Amazon S3 清单源桶和目标桶的更多信息，请参阅 源存储桶和目标存储桶。

设置清单的最简单方法是使用 Amazon S3 控制台，不过您也可以使用 Amazon S3 REST API、Amazon Command Line Interface (Amazon CLI) 或 Amazon SDK。

以下控制台过程包含用于设置 S3 分批操作任务的权限的概要步骤。在此过程中，您将对象从源账户复制到目标账户，并将清单报告存储在目标账户中。

为由不同账户拥有的源桶和目标桶设置 Amazon S3 清单

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 确定（或创建）用于存储清单报告的目标清单存储桶。在此过程中，目标账户 是同时拥有目标清单桶和对象要复制到的桶的账户。

4. 为源存储桶配置清单报告。有关如何使用控制台配置清单或如何加密清单列表文件的信息，请参阅配置 Amazon S3 清单。

   配置清单报告时，请指定要将该列表存储在其中的目标存储桶。源桶的清单报告将发布到目标桶。在此过程中，源账户 是拥有源桶的账户。

   为输出格式选择 CSV。

   输入目标桶的信息时，请选择 Buckets in another account（另一个账户中的桶）。然后，输入目标清单桶的名称。或者，可以输入目标账户的账户 ID。

   在保存清单配置后，控制台会显示类似于以下内容的一条消息：

   Amazon S3 无法在目标桶上创建桶策略。要求目标桶拥有者添加以下桶策略，以允许 Amazon S3 在该桶中放置数据。

   然后，控制台会显示可用于目标桶的桶策略。

5. 复制显示在控制台上的目标桶策略。
6. 在目标账户中，将复制的桶策略添加到存储清单报告所在的目标清单桶。
7. 在目标账户中创建一个基于 S3 分批操作信任策略的角色。有关该信任策略的更多信息，请参阅信任策略。

   有关创建角色的更多信息，请参阅《IAM 用户指南》中的创建向 Amazon Web Services 服务委派权限的角色。

   输入角色的名称（以下示例角色使用名称 *BatchOperationsDestinationRoleCOPY*）。选择 S3 服务，然后选择 S3 批量操作使用案例，这会将信任策略应用于该角色。

   然后选择 Create policy (创建策略) 以将以下策略附加到该角色。要使用这一策略，请将 *user input placeholders* 替换为您自己的信息。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowBatchOperationsDestinationObjectCOPY",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectVersionAcl",
```

```
        "s3:PutObjectAcl",
        "s3:PutObjectVersionTagging",
        "s3:PutObjectTagging",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-source-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    }
  ]
}
```

该角色使用策略授予 batchoperations.s3.amazonaws.com 权限来读取目标桶中的清单。该角色还授予 GET 源对象存储桶中对象、访问控制列表（ACL）、标签和版本的权限。并且，该角色还授予将对象、ACL、标签和版本 PUT 到目标对象存储桶中的权限。

8. 在源账户中，为源存储桶创建存储桶策略，该策略向您在上一步中创建的角色授予 GET 源存储桶中对象、ACL、标签和版本的权限。此步骤允许 S3 分批操作通过可信角色获取源桶中的对象。

   以下是源账户的桶策略的示例。要使用这一策略，请将 *user input placeholders* 替换为您自己的信息。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowBatchOperationsSourceObjectCOPY",
      "Effect": "Allow",
      "Principal": {
        "AWS":
 "arn:aws:iam::DestinationAccountNumber:role/BatchOperationsDestinationRoleCOPY"
      },
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
```

```
        "s3:GetObjectTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
    }
  ]
}
```

9. 在清单报告可用后，在目标账户中创建一个 S3 批量操作复制 (CopyObject) 任务，并从目标清单存储桶中选择清单报告。您需要您在目标账户中创建的 IAM 角色的 ARN。

   有关创建任务的一般信息，请参阅 创建 S3 批量操作任务。

   有关使用控制台创建任务的信息，请参阅创建 S3 批量操作任务。

使用 CSV 清单跨 Amazon Web Services 账户 复制对象

可以使用 Amazon S3 批量操作对 Amazon S3 对象执行大规模批量操作。可以使用 S3 批量操作创建复制 (CopyObject) 任务，以便在同一账户内复制对象或将对象复制到不同的目标账户。

可以使用存储在源账户中的 CSV 清单，通过 S3 批量操作跨 Amazon Web Services 账户复制对象。要使用 S3 清单报告作为清单，请参阅the section called “使用清单报告跨 Amazon Web Services 账户复制对象”。

有关清单文件的 CSV 格式的示例，请参阅the section called “创建清单文件”。

以下过程显示了当使用 S3 批量操作任务通过存储在源账户中的 CSV 清单文件将对象从源账户复制到目标账户时，如何设置权限。

使用 CSV 清单跨 Amazon Web Services 账户复制对象

1. 在目标账户中创建一个基于 S3 批量操作信任策略的 Amazon Identity and Access Management（IAM）角色。在此过程中，目标账户是对象要复制到的账户。

   有关信任策略的更多信息，请参阅信任策略。

   有关创建角色的更多信息，请参阅《IAM 用户指南》中的创建向 Amazon Web Services 服务委派权限的角色。

如果您使用控制台来创建角色，请输入角色的名称（以下示例角色使用名称 *BatchOperationsDestinationRoleCOPY*）。选择 S3 服务，然后选择 S3 批量操作使用案例，这会将信任策略应用于该角色。

然后选择 Create policy (创建策略) 以将以下策略附加到该角色。要使用这一策略，请将 *user input placeholders* 替换为您自己的信息。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowBatchOperationsDestinationObjectCOPY",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectVersionAcl",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionTagging",
        "s3:PutObjectTagging",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": [
        "arn:aws-cn:s3:::amzn-s3-demo-destination-bucket/*",
        "arn:aws-cn:s3:::amzn-s3-demo-source-bucket/*",
        "arn:aws-cn:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    }
  ]
}
```

使用策略，该角色将授予 batchoperations.s3.amazonaws.com 权限以读取源清单存储桶中的清单。该角色授予对源对象存储桶中的 GET 对象、访问控制列表（ACL）、标签和版本的权限。它还授予对目标对象存储桶中的 PUT 对象、ACL、标签和版本的权限。

2. 在源账户中，为包含清单的存储桶创建存储桶策略，来向您在上一步中创建的角色授予对源清单存储桶中 GET 对象和版本的权限。

此步骤可让 S3 批量操作通过使用可信角色来读取清单。将存储桶策略应用于包含清单的存储桶。

以下是要应用于源清单存储桶的存储桶策略的示例。要使用这一策略，请将 *user input placeholders* 替换为您自己的信息。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowBatchOperationsSourceManfiestRead",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws-cn:iam::DestinationAccountNumber:user/ConsoleUserCreatingJob",
          "arn:aws-
cn:iam::DestinationAccountNumber:role/BatchOperationsDestinationRoleCOPY"
        ]
      },
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws-cn:s3:::amzn-s3-demo-manifest-bucket/*"
    }
  ]
}
```

此策略还授予权限来允许要在目标账户中创建任务的控制台用户通过相同的存储桶策略具有源清单存储桶中的相同权限。

3. 在源账户中，为源存储桶创建存储桶策略，该策略向您创建的角色授予对源对象存储桶中 GET 对象、ACL、标签和版本的权限。然后，S3 分批操作可以通过可信角色获取源存储桶中的对象。

   以下是包含源对象的存储桶的存储桶策略示例。要使用这一策略，请将 *user input placeholders* 替换为您自己的信息。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowBatchOperationsSourceObjectCOPY",
      "Effect": "Allow",
```

```
      "Principal": {
        "AWS": "arn:aws-
cn:iam::DestinationAccountNumber:role/BatchOperationsDestinationRoleCOPY"
      },
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws-cn:s3:::amzn-s3-demo-source-bucket/*"
    }
  ]
}
```

4. 在目标账户中创建 S3 分批操作任务。您需要您在目标账户中创建的角色的 Amazon Resource Name (ARN)。有关创建作业的更多信息，请参阅创建 S3 批量操作任务。

使用批量操作为 SSE-KMS 启用 S3 存储桶密钥

S3 存储桶密钥通过减少从 Amazon S3 到 Amazon KMS 的请求流量，降低了具有 Amazon Key Management Service（Amazon KMS）的服务器端加密（SSE-KMS）的成本。有关更多信息，请参阅使用 Amazon S3 存储桶密钥降低 SSE-KMS 的成本和将存储桶配置为将 S3 存储桶密钥与 SSE-KMS 结合使用于新对象。当您使用 REST API、Amazon SDK 或 Amazon CLI 执行 `CopyObject` 操作时，可以通过添加带有 `true` 或 `false` 值的 `x-amz-server-side-encryption-bucket-key-enabled` 请求标头，在对象级别启用或禁用 S3 存储桶密钥。

当您使用 `CopyObject` 操作为对象配置 S3 存储桶密钥时，Amazon S3 仅更新该对象的设置。目标存储桶的 S3 存储桶密钥设置不会发生变化。如果您向启用了 S3 存储桶密钥的存储桶提交对于 Amazon KMS 加密对象的 `CopyObject` 请求，对象级操作将自动使用 S3 存储桶密钥，则除非您在请求标头中禁用这些密钥。如果您未为对象指定 S3 存储桶密钥，则 Amazon S3 会将目标存储桶的 S3 存储桶密钥设置应用于该对象。

要加密现有 Amazon S3 对象，可以使用 S3 批量操作。您可以使用批量操作复制操作复制现有的未加密对象，并将其作为加密对象写回同一存储桶。有关更多信息，请参阅 Amazon 存储博客上的 Encrypting objects with Amazon S3 Batch Operations。

在以下示例中，使用批量操作复制操作在现有对象上启用 S3 存储桶密钥。有关更多信息，请参阅 the section called “为对象配置 S3 存储桶密钥”。

主题


- 使用 S3 批量操作通过已启用的 S3 存储桶密钥加密对象的注意事项
- 先决条件
- 第 1 步：使用 Amazon S3 清单获取对象列表
- 第 2 步：使用 S3 Select 筛选对象列表
- 第 3 步：设置并运行 S3 分批操作任务


## 使用 S3 批量操作通过已启用的 S3 存储桶密钥加密对象的注意事项

使用 S3 批量操作通过已启用的 S3 存储桶密钥加密对象时，请考虑以下问题：

- 除了与 S3 批量操作代表您执行的操作关联的任何费用之外（包括数据传输、请求等费用），您还需要为 S3 批量操作任务、对象和请求付费。有关更多信息，请参阅 Amazon S3 定价。
- 如果您使用受版本控制的桶，则执行的每个 S3 分批操作任务都会创建对象的新加密版本。另外，无需配置 S3 桶密钥即可维护以前的版本。要删除旧版本，请为非当前版本设置 S3 生命周期过期策略，如 生命周期配置元素。
- 复制操作会创建具有新创建日期的新对象，这会影响生命周期操作（如归档）。如果您复制桶中的所有对象，所有新副本均具有相同或相似的创建日期。要进一步识别这些对象并为各种数据子集创建不同的生命周期规则，请考虑使用对象标签。

## 先决条件

在将对象配置为使用 S3 存储桶密钥之前，请查看启用 S3 存储桶密钥之前需要注意的更改。

要使用此示例，您必须具有 Amazon Web Services 账户和至少一个 S3 存储桶来存放工作文件和加密的结果。您可能还会发现许多有用的现有 S3 分批操作文档，包括以下主题：

- S3 批量操作基础知识
- 创建 S3 批量操作任务
- S3 分批操作支持的操作
- 管理 S3 分批操作任务

## 第 1 步：使用 Amazon S3 清单获取对象列表

要开始操作，请确定包含要加密对象的 S3 Bucket，并获取其内容列表。Amazon S3 清单报告是完成此操作的最方便且最经济的方式。报告提供存储桶中对象的列表及其关联的元数据。在此步骤中，源存

储桶是进行清点的存储桶，目标存储桶是您存储清单报告文件的存储桶。有关 Amazon S3 清单源桶和目标桶的更多信息，请参阅 使用 S3 清单对数据进行编目和分析。

设置清单最简单的方法是使用 Amazon Web Services Management Console。但您也可以使用 REST API、Amazon Command Line Interface (Amazon CLI) 或 Amazon 开发工具包。执行以下步骤之前，请务必登录控制台，并通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。如果遇到权限拒绝错误，请在目标桶中添加桶策略。有关更多信息，请参阅 向 S3 清单和 S3 分析功能授予权限。

使用 S3 清单获取对象列表

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶，然后选择包含要加密的对象的存储桶。
3. 在 Management (管理) 选项卡导航至 Inventory configurations (清单配置) 部分，然后选择 Create inventory configuration (创建清单配置)。
4. 为您的新清单命名，输入目标 S3 Bucket 的名称，并可选择为 Amazon S3 创建目标前缀，以便在该桶中分配对象。
5. 为 Output format (输出格式) 选择 CSV。
6. （可选）在其他字段 – 可选部分中，选择加密以及您感兴趣的任何其他报告字段。将报告发送频率设置为 Daily（每天），以便更快将第一个报告发送到您的桶。
7. 选择 Create (创建) 以保存您的配置。

Amazon S3 可能需要长达 48 小时才能交付第一个报告，所以当第一个报告到达时请予以查看。收到第一个报告后，请转入下一步来筛选 S3 清单报告的内容。如果您不再希望接收此桶的清单报告，请删除您的 S3 清单配置。否则，Amazon S3 会继续按每日或每周计划提供报告。

清单列表并非所有对象的单个时间点视图。清单列表是桶项的滚动快照，最终是一致的（例如，列表可能不包含最近添加或删除的对象）。当您使用静态对象或两天乃至更多天之前创建的对象集时，将 S3 清单和 S3 分批操作结合使用效果最佳。要处理最新数据，请使用 ListObjectsV2（GET 存储桶）API 操作来手动构建对象列表。如有需要，请在接下来的几天内重复该过程，或直到清单报告显示所有对象的理想状态。

第 2 步：使用 S3 Select 筛选对象列表

收到 S3 清单报告后，可以筛选报告的内容，以仅列出未使用已启用的 S3 存储桶密钥进行加密的对象。如果您希望使用已启用的 S3 存储桶密钥来加密存储桶的所有对象，则可以忽略此步骤。但是，在

此阶段筛选 S3 清单报告，则对于先前使用已启用的 S3 存储桶密钥加密的对象，可以节省对其重新加密的时间和费用。

尽管以下步骤介绍的是如何使用 Amazon S3 Select 进行筛选，但也可以使用 Amazon Athena。要决定使用哪个工具，请查看 S3 清单报告的 `manifest.json` 文件。此文件列出了与该报告关联的数据文件的数量。如果数量较大，请使用 Amazon Athena，因为其运行在多个 S3 对象之间，而 S3 Select 一次仅适用一个对象。有关将 Amazon S3 和 Athena 结合使用的更多信息，请参阅使用 Amazon Athena 查询 Amazon S3 清单以及 Amazon 存储博客文章 Encrypting objects with Amazon S3 Batch Operations 中的“Using Athena”。

使用 S3 Select 筛选 S3 清单报告

1. 打开清单报告中的 `manifest.json` 文件，然后查看 JSON 中的 `fileSchema` 部分。这将通知您的数据运行查询。

   以下 JSON 是一个示例 `manifest.json` 文件，用于查看已启用版本控制的桶上的 CSV 格式清单。根据您配置库存报告的方式，您的清单可能会有所不同。

   ```
     {
       "sourceBucket": "batchoperationsdemo",
       "destinationBucket": "arn:aws:s3:::amzn-s3-demo-destination-bucket",
       "version": "2021-05-22",
       "creationTimestamp": "1558656000000",
       "fileFormat": "CSV",
       "fileSchema": "Bucket, Key, VersionId, IsLatest, IsDeleteMarker,
    BucketKeyStatus",
       "files": [
         {
           "key": "demoinv/batchoperationsdemo/DemoInventory/data/009a40e4-
   f053-4c16-8c75-6100f8892202.csv.gz",
           "size": 72691,
           "MD5checksum": "c24c831717a099f0ebe4a9d1c5d3935c"
         }
       ]
     }
   ```

   如果桶未激活版本控制，或者您选择运行最新版本报告，则 `fileSchema` 是 `Bucket`、`Key` 和 `BucketKeyStatus`。

如果激活了版本控制，根据您设置清单报告的方式，fileSchema 可能包括：Bucket、Key、VersionId、IsLatest、IsDeleteMarker、BucketKeyStatus。因此，当您运行查询时，请注意第 1、2、3 和 6 栏。

除了搜索依据字段（即 BucketKeyStatus）外，S3 批量操作还需要输入桶、密钥和版本 ID 以执行任务。您不需要 VersionID 字段，但在对受版本控制的存储桶进行操作时，指定 VersionID 字段很有用。有关更多信息，请参阅 使用启用版本控制的存储桶中的对象。

2. 找到清单报告的数据文件。manifest.json 对象列出了文件夹下的数据文件。
3. 在 S3 控制台中找到并选择数据文件后，选择 Actions (操作)，然后选择 Query with S3 Select (使用 S3 Select 进行查询)。
4. 保留预设 CSV、逗号 和 GZIP 字段，然后选择 Next (下一步)。
5. 如需在继续操作之前检查清单报告格式，请选择 Show file preview (显示文件预览)。
6. 在 SQL 表达式字段中输入要引用的列，然后选择 Run SQL（运行 SQL）。以下表达式为未配置 S3 桶密钥的所有对象返回列 1-3。

```
select s._1, s._2, s._3 from s3object s where s._6 = 'DISABLED'
```

以下是示例结果。

```
      batchoperationsdemo,0100059%7Ethumb.jpg,lsrtIxksLu0R0ZkYPL.LhgD5caTYn6vu
      batchoperationsdemo,0100074%7Ethumb.jpg,sd2M60g6Fdazoi6D5kNARIE7KzUibmHR
      batchoperationsdemo,0100075%7Ethumb.jpg,TLYESLnl1mXD5c4BwiOIinqFrktddkoL
      batchoperationsdemo,0200147%7Ethumb.jpg,amufzfMi_fEw0Rs99rxR_HrDFlE.l3Y0
      batchoperationsdemo,0301420%7Ethumb.jpg,9qGU2SEscL.C.c_sK89trmXYIwooABSh
      batchoperationsdemo,0401524%7Ethumb.jpg,ORnEWNuB1QhHrrYAGFsZhbyvEYJ3DUor
      batchoperationsdemo,200907200065HQ
%7Ethumb.jpg,d8LgvIVjbDR5mUVwW6pu9ahTfReyn5V4
      batchoperationsdemo,200907200076HQ
%7Ethumb.jpg,XUT25d7.gK40u_GmnupdaZg3BVx2jN40
      batchoperationsdemo,201103190002HQ
%7Ethumb.jpg,z.2sVRh0myqVi0BuIrngWlsRPQdb7qOS
```

7. 下载结果，将其保存为 CSV 格式，然后将其作为 S3 分批操作任务的对象列表上传至 Amazon S3。
8. 如果您有多个清单文件，也请对它们运行 Query with S3 Select (使用 S3 Select 进行查询)。根据结果的大小，您可以合并列表并运行单个 S3 分批操作任务，或将每个列表作为单独任务运行。要决定要运行的任务数量，请考虑运行每个 S3 批量操作任务的价格。

第 3 步：设置并运行 S3 分批操作任务

现在，您有了 S3 对象的筛选 CSV 列表，可以开始 S3 批量操作任务，以使用已启用的 S3 存储桶密钥来加密对象。

任务指提供的对象列表（清单）、执行的操作以及指定的参数的统称。使用已启用的 S3 存储桶密钥加密此对象集的最简单方法是使用复制操作，并指定与清单中列出的对象相同的目标前缀。在不受版本控制的存储桶中，此操作会覆盖现有对象。在开启了版本控制的存储桶中，此操作将创建对象的较新的加密版本。

作为复制对象的一部分，指定 Amazon S3 应使用 SSE-KMS 加密来为对象进行加密。此任务会复制这些对象，因此，所有对象在完成时都显示更新后的创建日期，无论最初是何时将其添加到 Amazon S3 的。另外，在 S3 分批操作任务中指定对象集的其他属性，包括对象标记和存储类。

分步

- 设置 IAM 策略
- 设置分批操作 IAM 角色
- 为现有存储桶启用 S3 存储桶密钥
- 创建分批操作任务
- 运行您的分批操作任务

设置 IAM 策略

1. 通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在左侧导航窗格中，选择策略，然后选择创建策略。
3. 选择 JSON 选项卡。选择 Edit Policy (编辑策略)，然后添加出现在以下代码块中的示例 IAM 策略。

   将策略示例复制到 IAM 控制台后，请替换以下内容：

   a. 将 *amzn-s3-demo-source-bucket* 替换为要从中复制对象的源存储桶的名称。
   b. 将 *amzn-s3-demo-destination-bucket* 替换为要向其中复制对象的目标存储桶的名称。
   c. 将 *amzn-s3-demo-manifest-bucket*/*manifest-key* 替换为清单对象的名称。
   d. 将 *amzn-s3-demo-completion-report-bucket* 替换为要用于保存完成报告的存储桶的名称。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CopyObjectsToEncrypt",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectTagging",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionTagging",
        "s3:PutObjectVersionAcl",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-source-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      ]
    },
    {
      "Sid": "ReadManifest",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/manifest-key"
    },
    {
      "Sid": "WriteReport",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
    }
  ]
```

```
}
```

4. 选择 Next: Tags (下一步：标签)。
5. 添加您想要的所有标签（可选），然后选择 Next: Review (下一步：审核)。
6. 添加策略名称，可添加描述，然后选择 Create Policy (创建策略)。
7. 选择 Review policy (查看策略) 和 Save changes (保存更改)。
8. 您的 S3 分批操作策略现已完成，控制台会将您返回到 IAM Policies (策略) 页面。筛选策略名称，选择策略名称左侧的按钮，选择 Policy actions (策略操作)，然后选择 Attach (附加)。

   如需将新创建的策略附加到 IAM 角色，请在账户中选择相应的用户、组或角色，然后选择 Attach policy (附加策略)。系统会带您返回 IAM 控制台。

设置分批操作 IAM 角色

1. 在 IAM 控制台的导航窗格中，选择角色，然后选择创建角色。
2. 选择 Amazon Web Services 服务、S3 和 S3 批量操作。然后选择 Next: Permissions (下一步：权限)。
3. 输入您刚刚创建的 IAM 策略的名称。根据出现的策略名称选中相应名称，然后选择 Next: Tags (下一步：标签)。
4. （可选）为本次练习添加标签或将密钥和值字段保留为空。选择 Next: Review (下一步：审核)。
5. 输入角色名称，然后接受默认说明或添加您自己的说明。选择 Create role (创建角色)。
6. 确保创建任务的用户具有以下示例中的权限。

   将 *account-id* 替换为您的 Amazon Web Services 账户 ID，并将 *IAM-role-name* 替换为您计划应用于稍后将在批量操作任务创建步骤中创建的 IAM 角色的名称。有关更多信息，请参阅 授予批处理操作的权限。

```
{
"Sid": "AddIamPermissions",
"Effect": "Allow",
"Action": [
"iam:GetRole",
"iam:PassRole"
],
"Resource": "arn:aws:iam::account-id:role/IAM-role-name"
}
```

为现有存储桶启用 S3 存储桶密钥

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在桶列表中，选择要为其启用 S3 桶密钥的桶。
3. 选择 Properties (属性)。
4. 在 Default encryption (默认加密) 下，请选择 Edit (编辑)。
5. 在加密类型下，您可以在 Amazon S3 托管式密钥（SSE-S3）和 Amazon Key Management Service 密钥（SSE-KMS）之间进行选择。
6. 如果您选择了 Amazon Key Management Service 密钥（SSE-KMS），则在 Amazon KMS key 之下，您可以通过以下选项之一指定 Amazon KMS 密钥。

   - 要从可用的 KMS 密钥列表中进行选择，请选择从您的 Amazon KMS 密钥中进行选择。从可用密钥的列表中，选择与桶位于同一区域的对称加密 KMS 密钥。Amazon 托管式密钥（aws/s3）和您的客户自主管理型密钥都显示在列表中。
   - 要输入 KMS 密钥 ARN，请选择输入 Amazon KMS 密钥 ARN，然后在显示的字段中输入您的 KMS 密钥 ARN。
   - 要在 Amazon KMS 控制台中创建新的客户自主管理型密钥，请选择创建 KMS 密钥。
7. 在 Bucket Key（桶密钥）中，选择 Enable（启用），然后选择 Save changes（保存更改）。

现在，S3 存储桶密钥已在存储桶级别启用，默认情况下，上传、修改或复制到此存储桶中的对象将继承此加密配置。这包括使用 Amazon S3 批量操作复制的对象。

创建分批操作任务

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在导航窗格中，选择 Batch Operations (分批操作)，然后选择 Create Job (创建任务)。
3. 选择您存储对象的 Region (区域)，然后选择 CSV 作为清单类型。
4. 输入路径或导航至您之前从 S3 Select（或 Athena）结果创建的 CSV 清单文件。如果您的清单包含版本 ID，请选中该框。选择 Next (下一步)。
5. 选择 Copy 操作，然后选择复制目标桶。您可以保持禁用服务器端加密。只要桶目标启用了 S3 桶密钥，复制操作将在目标桶上应用 S3 桶密钥。
6. （可选）根据需要选择存储类和其他参数。您在此步骤中指定的参数将应用于清单中列出的对象执行的所有操作。选择下一步。
7. 要配置服务器端加密，请执行以下步骤：

   a. 在服务器端加密下，选择以下选项之一：

- 要在将对象存储在 Amazon S3 中时保留适用于对象原定设置服务器端加密的桶设置，请选择不要指定加密密钥。只要桶目标启用了 S3 桶密钥，复制操作就将在目标桶上应用 S3 桶密钥。

> **Note**
>
> 如果指定的目标的桶策略要求在将对象存储到 Amazon S3 之前对其进行加密，则必须指定加密密钥。否则，将对象复制到目标将失败。

- 要在将对象存储到 Amazon S3 之前对其进行加密，请选择指定加密密钥。

b. 在加密设置下，如果您选择指定加密密钥，则必须选择使用用于原定设置加密的目标桶设置或覆盖用于原定设置加密的目标桶设置。

c. 如果您选择覆盖用于原定设置加密的目标桶设置，则必须配置以下加密设置。

i. 在加密类型下，您必须选择 Amazon S3 托管式密钥（SSE-S3）或 Amazon Key Management Service 密钥（SSE-KMS）。SSE-S3 使用最强的数据块密码之一 [即 256 位高级加密标准（AES-256）] 来加密每个对象。SSE-KMS 为您提供了对密钥的更多控制。有关更多信息，请参阅使用具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）和使用具有 Amazon KMS 密钥的服务器端加密（SSE-KMS）。

ii. 如果您选择 Amazon Key Management Service 密钥（SSE-KMS），则在 Amazon KMS key 之下，您可以通过以下选项之一指定 Amazon KMS key。

- 要从可用 KMS 密钥列表中进行选择，请选择从您的 Amazon KMS keys 中进行选择，然后选择与桶位于同一区域的对称加密 KMS 密钥。Amazon 托管式密钥（`aws/s3`）和您的客户自主管理型密钥都显示在列表中。
- 要输入 KMS 密钥 ARN，请选择输入 Amazon KMS 密钥 ARN，然后在显示的字段中输入您的 KMS 密钥 ARN。
- 要在 Amazon KMS 控制台中创建新的客户自主管理型密钥，请选择创建 KMS 密钥。

iii. 在 Bucket Key（存储桶密钥）下，请选择 Enable（启用）。复制操作将在目标桶应用 S3 桶密钥。

8. 提供任务说明（或保留默认值），设置其优先级，选择报告类型，然后指定 Path to completion report destination (完成报告目标的路径)。
9. 在 Permissions (权限) 部分，请确保选择您之前定义的分批操作 IAM 角色。选择 Next (下一步)。
10. 在 Review (审核) 中验证设置。如果需要进行更改，请选择 Previous (上一步)。确认分批操作设置后，选择 Create job (创建任务)。

有关更多信息，请参阅 创建 S3 批量操作任务。

运行您的分批操作任务

安装向导将自动将您返回 Amazon S3 控制台的 S3 分批操作部分。随着 S3 开始此过程，您的新任务将从 New (新建) 状态变为 Preparing (准备中) 状态。在 Preparing (准备中) 状态下，S3 会读取任务清单，检查是否存在错误，并计算对象数量。

1. 在 Amazon S3 控制台中选择刷新按钮以检查进度。根据清单的大小，读取可能需要几分钟或几小时。
2. S3 读取任务清单后，任务将转移至 Awaiting your confirmation (待确认) 状态。选择任务 ID 左侧的选项按钮，然后选择 Run job (运行任务)。
3. 检查任务设置，然后选择右下角的 Run job (运行任务)。

   任务开始运行后，您可以选择刷新按钮通过控制台控制面板视图或选择特定任务来检查进度。
4. 任务完成后，您可以查看 Successful (成功) 和 Failed (失败) 对象数量以确认所有任务均按预期执行。如果您启用了任务报告，请检查任务报告，了解失败操作的确切原因。

   还可以使用 Amazon CLI、Amazon SDK 或 Amazon S3 REST API 来执行这些步骤。有关追踪任务状态和完成报告的更多信息，请参阅 跟踪任务状态和完成报告。

有关说明使用 Amazon CLI 和 适用于 Java 的 Amazon SDK 对标签进行复制操作的示例，请参阅 使用用于标记的任务标签创建分批操作任务。

## 调用 Amazon Lambda 函数

可以使用 Amazon S3 批量操作对 Amazon S3 对象执行大规模批量操作。批量操作调用 Amazon Lambda 函数操作将启动 Amazon Lambda 函数，来对清单中列出的对象执行自定义操作。本部分介绍如何创建 Lambda 函数来与 S3 批量操作结合使用，以及如何创建任务来调用该函数。S3 批量操作任务使用 `LambdaInvoke` 操作对清单中列出的每个对象运行 Lambda 函数。

可以使用 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 Amazon S3 REST API 处理 S3 批量操作。有关使用 Lambda 的更多信息，请参阅《Amazon Lambda 开发人员指南》中的入门Amazon Lambda。

以下部分说明如何开始将 S3 批量操作与 Lambda 结合使用。

主题

- 将 Lambda 与批量操作结合使用
- 创建与 S3 批量操作一起使用的 Lambda 函数
- 创建调用 Lambda 函数的 S3 批量操作任务
- 在 Lambda 清单中提供任务级信息
- S3 批量操作教程

### 将 Lambda 与批量操作结合使用

将 S3 批量操作与 Amazon Lambda 结合使用时，您必须创建专门用于 S3 批量操作的新 Lambda 函数。您无法在 S3 批量操作中重复使用基于事件的现有 Amazon S3 函数。事件函数只能接收消息；不返回消息。与 S3 批量操作结合使用的 Lambda 函数必须接受并返回消息。有关将 Lambda 与 Amazon S3 事件结合使用的更多信息，请参阅《Amazon Lambda 开发人员指南》中的将 Amazon Lambda 与 Amazon S3 结合使用。

创建调用 Lambda 函数的 S3 批量操作任务。此任务在清单中列出的所有对象上运行相同的 Lambda 函数。在处理清单中的对象时，您可以控制要使用的 Lambda 函数版本。S3 批量操作支持非限定的 Amazon Resource Name（ARN）、别名和特定版本。有关更多信息，请参阅《Amazon Lambda 开发人员指南》中的Amazon Lambda 版本控制简介。

如果您提供的 S3 批量操作任务包含使用别名或 `$LATEST` 限定符的函数 ARN，并更新它们各自所指向的版本，S3 批量操作开始调用 Lambda 函数的新版本。如果您希望通过大型任务更新此方法的功能部分，这会非常有用。如果您不希望 S3 批量操作更改所使用的版本，请在创建任务时在 `FunctionARN` 参数中提供特定版本。

### 将 Lambda 和批量操作用于目录存储桶

目录存储桶是一种 Amazon S3 存储桶类型，专为需要一致的个位数毫秒延迟的工作负载或性能至关重要的应用程序而设计。有关更多信息，请参阅目录存储桶。

使用批量操作来调用处理目录存储桶的 Lambda 函数有特殊要求。例如，必须使用更新后的 JSON 架构来构建 Lambda 请求，并在创建任务时指定 InvocationSchemaVersion 2.0（而不是 1.0）。此更新后的架构允许您为 UserArguments 指定可选的键值对，您可以使用这些键值对修改现有 Lambda 函数的某些参数。有关更多信息，请参阅 Amazon 存储博客中的 Automate object processing in Amazon S3 directory buckets with S3 Batch Operations and Amazon Lambda。

### 响应和结果代码

S3 批量操作使用一个或多个键调用 Lambda 函数，每个键都有一个与之关联的 `TaskID`。S3 批量操作需要 Lambda 函数提供每个键的结果代码。对于在请求中发送的任何任务 ID，如果没有为它们返回

每个键的结果代码，则将从 treatMissingKeysAs 字段中提供结果代码。treatMissingKeysAs 是可选的请求字段，默认为 TemporaryFailure。下表包含 treatMissingKeysAs 字段的其它可能的结果代码和值。

| 响应代码 | 描述 |
| --- | --- |
| Succeeded | 任务正常完成。如果您请求了任务完成报告，报告中将包含任务的结果字符串。 |
| TemporaryFailure | 任务暂时失败，将在任务完成前重新启动。忽略结果字符串。如果是最后一次重新启动，最终报告将包含错误消息。 |
| PermanentFailure | 任务永久失败。如果您请求了任务完成报告，任务将被标记为 Failed 并包含错误消息字符串。忽略失败任务的结果字符串。 |

创建与 S3 批量操作一起使用的 Lambda 函数

此部分提供使用 Lambda 函数必须具有的 Amazon Identity and Access Management (IAM) 权限示例。它还包含一个与 S3 批量操作一起使用的示例 Lambda 函数。如果您之前从未创建过 Lambda 函数，请参阅《Amazon Lambda 开发人员指南》中的教程：将 Amazon Lambda 与 Amazon S3 结合使用。

您必须创建专门与 S3 批量操作一起使用的 Lambda 函数。您无法重用基于 Amazon S3 事件的现有 Lambda 函数，因为用于 S3 批量操作的 Lambda 函数必须接受并返回特殊数据字段。

> **Important**
>
> 用 Java 编写的 Amazon Lambda 函数接受 RequestHandler 或 RequestStreamHandler 处理程序接口。但是，为了支持 S3 批量操作请求和响应格式，Amazon Lambda 需要 RequestStreamHandler 接口来对请求和响应进行自定义序列化和反序列化。此接口允许 Lambda 将 InputStream 和 OutputStream 传递给 Java handleRequest 方法。
> 将 Lambda 函数与 S3 批量操作结合使用时，请务必使用 RequestStreamHandler 接口。如果您使用 RequestHandler 接口，则批处理任务会失败，并在完成报告中显示“Lambda 负载中返回无效的 JSON”。
> 有关更多信息，请参阅《Amazon Lambda 用户指南》中的处理程序接口。

### IAM 权限示例

以下是将 Lambda 函数与 S3 批量操作结合使用所需的 IAM 权限示例。

#### Example – S3 批量操作信任策略

以下是您可用于批量操作 IAM 角色的信任策略示例。当您创建任务并授予批量操作代入 IAM 角色的权限时，会指定此 IAM 角色。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "batchoperations.s3.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

#### Example – Lambda IAM 策略

以下是提供 S3 批量操作权限以调用 Lambda 函数和读取输入清单的 IAM 策略示例。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "BatchOperationsLambdaPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion",
                "s3:PutObject",
                "lambda:InvokeFunction"
            ],
            "Resource": "*"
        }
    ]
}
```

### 示例请求和响应

本节内容提供 Lambda 函数的请求和响应示例。

#### Example 请求

以下是 Lambda 函数的请求的 JSON 示例。

```
{
    "invocationSchemaVersion": "1.0",
    "invocationId": "YXNkbGZqYWRmaiBhc2RmdW9hZHNmZGpmaGFzbGtkaGZza2RmaAo",
    "job": {
        "id": "f3cc4f60-61f6-4a2b-8a21-d07600c373ce"
    },
    "tasks": [
        {
            "taskId": "dGFza2lkZ29lc2hlcmUK",
            "s3Key": "customerImage1.jpg",
            "s3VersionId": "1",
            "s3BucketArn": "arn:aws:s3:us-east-1:0123456788:amzn-s3-demo-bucket1"
        }
    ]
}
```

#### Example 响应

以下是 Lambda 函数的响应的 JSON 示例。

```
{
  "invocationSchemaVersion": "1.0",
  "treatMissingKeysAs" : "PermanentFailure",
  "invocationId" : "YXNkbGZqYWRmaiBhc2RmdW9hZHNmZGpmaGFzbGtkaGZza2RmaAo",
  "results": [
    {
      "taskId": "dGFza2lkZ29lc2hlcmUK",
      "resultCode": "Succeeded",
      "resultString": "[\"Mary Major", \"John Stiles\"]"
    }
  ]
}
```

### S3 批量操作的 Lambda 函数示例

以下示例中，Python Lambda 从受版本控制的对象中移除删除标记。

如示例所示，S3 批量操作中的键采用 URL 编码。要将 Amazon S3 与其他 Amazon 服务结合使用，请务必对从 S3 批量操作传递的键进行 URL 解码。

```
import logging
from urllib import parse
import boto3
from botocore.exceptions import ClientError

logger = logging.getLogger(__name__)
logger.setLevel("INFO")

s3 = boto3.client("s3")


def lambda_handler(event, context):
    """
    Removes a delete marker from the specified versioned object.

    :param event: The S3 batch event that contains the ID of the delete marker
                  to remove.
    :param context: Context about the event.
    :return: A result structure that Amazon S3 uses to interpret the result of the
             operation. When the result code is TemporaryFailure, S3 retries the
             operation.
    """
    # Parse job parameters from Amazon S3 batch operations
    invocation_id = event["invocationId"]
    invocation_schema_version = event["invocationSchemaVersion"]

    results = []
    result_code = None
    result_string = None

    task = event["tasks"][0]
    task_id = task["taskId"]

    try:
        obj_key = parse.unquote(task["s3Key"], encoding="utf-8")
        obj_version_id = task["s3VersionId"]
        bucket_name = task["s3BucketArn"].split(":")[-1]

        logger.info(
```

```
            "Got task: remove delete marker %s from object %s.", obj_version_id,
obj_key
        )

        try:
            # If this call does not raise an error, the object version is not a delete
            # marker and should not be deleted.
            response = s3.head_object(
                Bucket=bucket_name, Key=obj_key, VersionId=obj_version_id
            )
            result_code = "PermanentFailure"
            result_string = (
                f"Object {obj_key}, ID {obj_version_id} is not " f"a delete marker."
            )

            logger.debug(response)
            logger.warning(result_string)
        except ClientError as error:
            delete_marker = error.response["ResponseMetadata"]["HTTPHeaders"].get(
                "x-amz-delete-marker", "false"
            )
            if delete_marker == "true":
                logger.info(
                    "Object %s, version %s is a delete marker.", obj_key,
obj_version_id
                )
                try:
                    s3.delete_object(
                        Bucket=bucket_name, Key=obj_key, VersionId=obj_version_id
                    )
                    result_code = "Succeeded"
                    result_string = (
                        f"Successfully removed delete marker "
                        f"{obj_version_id} from object {obj_key}."
                    )
                    logger.info(result_string)
                except ClientError as error:
                    # Mark request timeout as a temporary failure so it will be
retried.
                    if error.response["Error"]["Code"] == "RequestTimeout":
                        result_code = "TemporaryFailure"
                        result_string = (
                            f"Attempt to remove delete marker from  "
                            f"object {obj_key} timed out."
```

```
                    )
                    logger.info(result_string)
                else:
                    raise
        else:
            raise ValueError(
                f"The x-amz-delete-marker header is either not "
                f"present or is not 'true'."
            )
    except Exception as error:
        # Mark all other exceptions as permanent failures.
        result_code = "PermanentFailure"
        result_string = str(error)
        logger.exception(error)
    finally:
        results.append(
            {
                "taskId": task_id,
                "resultCode": result_code,
                "resultString": result_string,
            }
        )
    return {
        "invocationSchemaVersion": invocation_schema_version,
        "treatMissingKeysAs": "PermanentFailure",
        "invocationId": invocation_id,
        "results": results,
    }
```

创建调用 Lambda 函数的 S3 批量操作任务

创建 S3 批量操作任务以调用 Lambda 函数时，必须提供以下信息：

- Lambda 函数的 ARN（可能包含函数别名或特定版本号）
- 具有调用此函数的权限的 IAM 角色
- 操作参数 `LambdaInvokeFunction`

有关创建 S3 批量操作任务的更多信息，请参阅 创建 S3 批量操作任务 和 S3 分批操作支持的操作。

以下示例使用 Amazon CLI 创建用于调用 Lambda 函数的 S3 批量操作任务。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control create-job
    --account-id account-id
    --operation  '{"LambdaInvoke": { "FunctionArn": "arn:aws:lambda:region:account-
id:function:LambdaFunctionName" } }'
    --manifest '{"Spec":{"Format":"S3BatchOperations_CSV_20180820","Fields":
["Bucket","Key"]},"Location":{"ObjectArn":"arn:aws:s3:::amzn-s3-demo-manifest-
bucket","ETag":"ManifestETag"}}'
    --report '{"Bucket":"arn:aws:s3:::amzn-s3-demo-
bucket","Format":"Report_CSV_20180820","Enabled":true,"Prefix":"ReportPrefix","ReportScope":"Al
    --priority 2
    --role-arn arn:aws:iam::account-id:role/BatchOperationsRole
    --region region
    --description "Lambda Function"
```

在 Lambda 清单中提供任务级信息

当您将 Amazon Lambda 函数与 S3 批量操作结合使用时，对于所运行的各个任务或键，可能会需要附带额外的数据。例如，您可能希望同时提供源对象键和新的对象键。然后，您的 Lambda 函数可以将源键以新名称复制到新 S3 存储桶。默认情况下，通过批量操作，可以仅在任务的输入清单中指定目标存储桶以及源键的列表。下面的示例介绍了如何在清单中包含额外的数据，以便运行更复杂的 Lambda 函数。

要在 S3 批量操作清单中指定各个键的参数以在 Lambda 函数代码中使用，请使用以下 URL 编码的 JSON 格式。key 字段采用类似于 Amazon S3 对象键的方式传递到您的 Lambda 函数。但是，Lambda 函数可以解释此字段来包含其它值或多个键，如下示例所示。

> **Note**
>
> 清单中 key 字段的最大字符数为 1024。

Example – 清单将“Amazon S3 密钥”替换为 JSON 字符串

必须向 S3 批量操作提供 URL 编码的版本。

```
amzn-s3-demo-bucket,{"origKey": "object1key", "newKey": "newObject1Key"}
amzn-s3-demo-bucket,{"origKey": "object2key", "newKey": "newObject2Key"}
amzn-s3-demo-bucket,{"origKey": "object3key", "newKey": "newObject3Key"}
```

Example – URL 编码的清单

必须向 S3 批量操作提供此 URL 编码的版本。非 URL 编码的版本不起作用。

```
amzn-s3-demo-bucket,%7B%22origKey%22%3A%20%22object1key%22%2C%20%22newKey%22%3A
%20%22newObject1Key%22%7D
amzn-s3-demo-bucket,%7B%22origKey%22%3A%20%22object2key%22%2C%20%22newKey%22%3A
%20%22newObject2Key%22%7D
amzn-s3-demo-bucket,%7B%22origKey%22%3A%20%22object3key%22%2C%20%22newKey%22%3A
%20%22newObject3Key%22%7D
```

Example – 具有清单格式的 Lambda 函数将结果写入任务报告

这个 URL 编码的清单示例包含以竖线分隔的对象键，供以下 Lambda 函数进行解析。

```
amzn-s3-demo-bucket,object1key%7Clower
amzn-s3-demo-bucket,object2key%7Cupper
amzn-s3-demo-bucket,object3key%7Creverse
amzn-s3-demo-bucket,object4key%7Cdelete
```

此 Lambda 函数显示了如何解析编码到 S3 批量操作清单中的以竖线分隔的任务。该任务指示应用于指定对象的修订操作。

```
import logging
from urllib import parse
import boto3
from botocore.exceptions import ClientError

logger = logging.getLogger(__name__)
logger.setLevel("INFO")

s3 = boto3.resource("s3")


def lambda_handler(event, context):
    """
    Applies the specified revision to the specified object.

    :param event: The Amazon S3 batch event that contains the ID of the object to
                  revise and the revision type to apply.
    :param context: Context about the event.
    :return: A result structure that Amazon S3 uses to interpret the result of the
             operation.
```

```
    """
    # Parse job parameters from Amazon S3 batch operations
    invocation_id = event["invocationId"]
    invocation_schema_version = event["invocationSchemaVersion"]

    results = []
    result_code = None
    result_string = None

    task = event["tasks"][0]
    task_id = task["taskId"]
    # The revision type is packed with the object key as a pipe-delimited string.
    obj_key, revision = parse.unquote(task["s3Key"], encoding="utf-8").split("|")
    bucket_name = task["s3BucketArn"].split(":")[-1]

    logger.info("Got task: apply revision %s to %s.", revision, obj_key)

    try:
        stanza_obj = s3.Bucket(bucket_name).Object(obj_key)
        stanza = stanza_obj.get()["Body"].read().decode("utf-8")
        if revision == "lower":
            stanza = stanza.lower()
        elif revision == "upper":
            stanza = stanza.upper()
        elif revision == "reverse":
            stanza = stanza[::-1]
        elif revision == "delete":
            pass
        else:
            raise TypeError(f"Can't handle revision type '{revision}'.")

        if revision == "delete":
            stanza_obj.delete()
            result_string = f"Deleted stanza {stanza_obj.key}."
        else:
            stanza_obj.put(Body=bytes(stanza, "utf-8"))
            result_string = (
                f"Applied revision type '{revision}' to " f"stanza {stanza_obj.key}."
            )

        logger.info(result_string)
        result_code = "Succeeded"
    except ClientError as error:
        if error.response["Error"]["Code"] == "NoSuchKey":
```

```
            result_code = "Succeeded"
            result_string = (
                f"Stanza {obj_key} not found, assuming it was deleted "
                f"in an earlier revision."
            )
            logger.info(result_string)
        else:
            result_code = "PermanentFailure"
            result_string = (
                f"Got exception when applying revision type '{revision}' "
                f"to {obj_key}: {error}."
            )
            logger.exception(result_string)
    finally:
        results.append(
            {
                "taskId": task_id,
                "resultCode": result_code,
                "resultString": result_string,
            }
        )
    return {
        "invocationSchemaVersion": invocation_schema_version,
        "treatMissingKeysAs": "PermanentFailure",
        "invocationId": invocation_id,
        "results": results,
    }
```

S3 批量操作教程

以下教程提供了使用 Lambda 的一些批量操作任务的完整端到端过程。在本教程中，您将了解如何将批量操作设置为调用 Lambda 函数，来对存储在 S3 源存储桶中的视频进行批量转码。Lambda 函数调用 AWS Elemental MediaConvert 来对视频进行转码。

- 教程：使用 S3 批量操作对视频进行批量转码

## 替换所有对象标签

可以使用 Amazon S3 批量操作对 Amazon S3 对象执行大规模批量操作。替换所有对象标签操作将替换清单中列出的每个对象上的对象标签。 对象标签是一个字符串的键/值对，您可用它来存储有关对象的元数据。

要创建替换所有对象标签任务，您需要提供要应用的标签集。S3 分批操作将相同的标签集应用于每个对象。您提供的标签集替换已与清单中的对象关联的任何标签集。S3 批量操作不支持在保留现有标签的同时向对象添加标签。

如果清单中的对象位于受版本控制的存储桶中，您可将标签集应用到每个对象的特定版本。为此，请为清单中的每个对象指定版本 ID。如果您没有包括任何对象的版本 ID，则 S3 批量操作将标签集应用到每个对象的最新版本。有关分批操作清单的更多信息，请参阅 指定清单。

有关对象标记的更多信息，请参阅本指南中的使用标签对存储进行分类，并参阅《Amazon Simple Storage Service API 参考》中的 PutObjectTagging、GetObjectTagging 和 DeleteObjectTagging。

要使用控制台创建替换所有对象标签任务，请参阅创建 S3 批量操作任务。

限制和局限性

使用批量操作来替换对象标签时，以下限制和局限性适用：

- 您指定用于运行批量操作任务的 Amazon Identity and Access Management（IAM）角色必须有权执行基础 `PutObjectTagging` 操作。有关所需权限的更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 PutObjectTagging。
- S3 批量操作使用 Amazon S3 PutObjectTagging 操作，来将标签应用到清单中的每个对象。适用于基础操作的所有限制也适用于 S3 分批操作任务。

## 删除所有对象标签

可以使用 Amazon S3 批量操作对 Amazon S3 对象执行大规模批量操作。删除所有对象标签操作将删除当前与清单中列出的对象关联的所有 Amazon S3 对象标签集。S3 批量操作不支持在保留其它标签的同时删除对象中的标签。

如果清单中的对象位于受版本控制的存储桶中，则可以从对象的特定版本中删除标签集。为此，必须为清单中的每个对象指定版本 ID。如果您没有包括对象的版本 ID，S3 分批操作将从每个对象的最新版本中删除该标签集。有关分批操作清单的更多信息，请参阅 指定清单。

有关对象标记的详细信息，请参阅本指南中的使用标签对存储进行分类，以及《Amazon Simple Storage Service API 参考》中的 PutObjectTagging、GetObjectTagging 和 DeleteObjectTagging。

> **Warning**
>
> 运行此任务将删除清单中列出的每个对象上的所有对象标签集。

要使用控制台创建删除所有对象标签任务，请参阅创建 S3 批量操作任务。

限制和局限性

使用批量操作来删除对象标签时，以下限制和局限性适用：

- 您指定用于运行该任务的 Amazon Identity and Access Management（IAM）角色必须有权执行基础 Amazon S3 `DeleteObjectTagging` 操作。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 DeleteObjectTagging。
- S3 批量操作使用 Amazon S3 DeleteObjectTagging 操作从清单中的每个对象移除标签集。适用于基础操作的所有限制也适用于 S3 分批操作任务。

## 替换访问控制列表（ACL）

可以使用 Amazon S3 批量操作对 Amazon S3 对象执行大规模批量操作。替换访问控制列表（ACL）操作会替换在清单中列出的每个对象的访问控制列表（ACL）。使用 ACL，您可以定义谁可以访问某个对象，以及他们可以执行哪些操作。

> **Note**
>
> Amazon S3 中的大多数现代使用案例不再需要使用 ACL。我们建议您将 ACL 保持为禁用状态，除非有需要单独控制每个对象的访问权限的特殊情况。禁用 ACL 后，您可以使用策略来控制对存储桶中所有对象的访问权限，无论是谁将对象上传到您的存储桶。有关更多信息，请参阅 为您的存储桶控制对象所有权和禁用 ACL。。

S3 批量操作支持您定义的自定义 ACL 以及 Amazon S3 随预定义的访问权限集提供的标准 ACL。

如果清单中的对象位于受版本控制的存储桶中，您可将 ACL 应用到每个对象的特定版本。为此，请为清单中的每个对象指定版本 ID。如果您没有包括任何对象的版本 ID，S3 批量操作将 ACL 应用到对象的最新版本。

有关 Amazon S3 中 ACL 的更多信息，请参阅访问控制列表 (ACL) 概述。

S3 阻止公有访问

如果您要限制对存储桶中所有对象的公共访问权限，建议您使用 Amazon S3 屏蔽公共访问权限，而不是使用 S3 批量操作来应用 ACL。阻止公有访问可以在各个存储桶或整个账户的范围进行，并且只需一个简单的操作，立即生效。当您的目标是控制对某个存储桶或账户中所有对象的公共访问权限时，此行为使 Amazon S3 屏蔽公共访问权限成为更好的选择。仅当您需要将自定义 ACL 应用到清单中的每个对象时，才使用 S3 批量操作。有关 S3 阻止公有访问的更多信息，请参阅 阻止对您的 Amazon S3 存储的公有访问。

S3 对象所有权

如果清单中的对象位于存储桶中，而该存储桶对于对象所有权使用强制存储桶拥有者设置，则替换访问控制列表（ACL）操作只能指定向存储桶拥有者授予完全控制权限的对象 ACL。在这种情况下，替换访问控制列表（ACL）操作无法将对象 ACL 权限授予其它 Amazon Web Services 账户或组。有关更多信息，请参阅 为您的存储桶控制对象所有权和禁用 ACL。。

限制和局限性

使用批量操作来替换 ACL 时，以下限制和局限性适用：

- 您指定用于运行替换访问控制列表（ACL）任务的 Amazon Identity and Access Management（IAM）角色必须有权执行基础 Amazon S3 `PutObjectAcl` 操作。有关所需权限的更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 PutObjectAcl。
- S3 分批操作使用 Amazon S3 `PutObjectAcl` 操作，将指定的 ACL 应用到清单中的每个对象。因此，适用于基础 `PutObjectAcl` 操作的所有限制和局限性也适用于 S3 批量操作替换访问控制列表（ACL）任务。

## 使用批量操作还原对象

可以使用 Amazon S3 批量操作对 Amazon S3 对象执行大规模批量操作。还原操作启动对清单中列出的已归档 Amazon S3 对象的还原请求。必须先还原以下归档对象，然后才能实时访问这些对象：

- 在 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储类中归档的对象
- 通过归档访问层或深度归档访问层中的 S3 Intelligent-Tiering 存储类归档的对象

在 S3 批量操作任务中使用还原（S3InitiateRestoreObjectOperation）操作，会导致针对在清单中指定的每个对象发出 `RestoreObject` 请求。

> **Important**
>
> 还原任务仅启动 还原对象的请求。在为每个对象启动请求后，S3 分批操作将对象的任务报告为完成。还原对象时，Amazon S3 不会更新任务或以其他方式通知您。不过，当对象在 Amazon S3 中可用时，您可以使用 S3 事件通知来接收通知。有关更多信息，请参阅 Amazon S3 事件通知。

当您创建还原任务时，可以使用以下参数：

ExpirationInDays

此参数用于指定 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 对象在 Amazon S3 中保持可用的时长。以 S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 对象为目标的还原任务要求您将 `ExpirationInDays` 设置为 1 或更大的值。

> **Important**
>
> 在创建以 S3 Intelligent-Tiering 归档访问和深度归档访问层对象为目标的还原操作任务时，请勿设置 `ExpirationInDays`。S3 Intelligent-Tiering 归档访问层中的对象不受还原到期的限制，因此指定 `ExpirationInDays` 会导致 `RestoreObject` 请求失败。

GlacierJobTier

Amazon S3 可以使用三个不同的检索层之一还原对象：`EXPEDITED`、`STANDARD` 和 `BULK`。但是，S3 分批操作功能仅支持 `STANDARD` 和 `BULK` 检索层。有关各检索层之间的差异的更多信息，请参阅了解归档检索选项。

有关每层定价的更多信息，请参阅 Amazon S3 定价页面上的请求和数据检索部分。

从 S3 Glacier 和 S3 Intelligent-Tiering 还原时的区别

从 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储类还原归档文件与从归档访问层或深度归档访问层中的 S3 Intelligent-Tiering 存储类恢复文件不同。

- 当您从 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 中还原时，将创建对象的临时副本。Amazon S3 会在 `ExpirationInDays` 参数中指定的值过期后删除此副本。删除此临时副本后，您必须提交额外的还原请求才能访问该对象。

- 还原归档的 S3 Intelligent-Tiering 对象时，请勿指定 `ExpirationInDays` 参数。当您从 S3 Intelligent-Tiering 归档访问层或深度归档访问层还原对象时，此对象会转换回 S3 Intelligent-Tiering 频繁访问层中。在至少连续 90 天无访问后，对象会自动转换到归档访问层。在至少连续 180 天无访问后，对象会自动移动到深度归档访问层。
- 批量操作任务既可以在 S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 存储类对象上运行，也可以在 S3 Intelligent-Tiering 归档访问和深度归档访问存储层对象上运行。批量操作不能在同一个任务中对两种类型的归档对象进行操作。要还原两种类型的对象，必须创建单独的分批操作任务。

### 重叠还原

如果 S3InitiateRestoreObjectOperation 任务尝试还原已处于还原过程中的对象，S3 批量操作的过程如下所示。

如果满足以下任意条件，对象的还原操作将成功：

- 与已在进行的还原请求相比，此任务的 `ExpirationInDays` 值相同，而其 `GlacierJobTier` 值更快。
- 之前的还原请求已完成，对象当前已可用。在这种情况下，批量操作会更新已还原对象的过期日期，以便与在正在进行的还原请求中指定的 `ExpirationInDays` 值匹配。

如果满足以下任意条件，对象的还原操作失败：

- 已在进行的还原请求尚未完成，并且此任务的还原持续时间（由 `ExpirationInDays` 值指定）不同于在正在进行的还原请求中指定的还原持续时间。
- 此任务的还原层（由 `GlacierJobTier` 值指定）与在正进行的还原请求中指定的还原层速度相同或更慢。

### 限制

`S3InitiateRestoreObjectOperation` 任务具有以下限制：

- 您必须在与归档对象相同的区域中创建任务。
- S3 批量操作不支持 `EXPEDITED` 检索层。

有关还原对象的更多信息，请参阅 恢复已归档的对象。

## S3 对象锁定保留

可以使用 Amazon S3 批量操作对 Amazon S3 对象执行大规模批量操作。可以使用对象锁定保留操作，通过监管模式或合规模式来为对象应用保留日期。这些保留模式会应用不同级别的保护。可将任一保留模式应用于任意对象版本。与依法保留类似，保留日期可防止覆盖或删除对象。Amazon S3 存储在对象的元数据中指定的保留到期日，并保护指定的对象版本，直到保留期到期。

可以将 S3 批量操作与对象锁定结合使用，以便同时管理许多 Amazon S3 对象的保留日期。可以在清单中指定目标对象的列表，并将该清单提交到批量操作以完成操作。有关更多信息，请参阅 S3 对象锁定the section called “保留期限”。

具有保留日期的任务 S3 分批操作将持续运行，直至达到完成、取消或失败状态。当要通过单个请求添加、更改或移除许多对象的保留日期时，建议使用 S3 批量操作和 S3 对象锁定保留。

在处理清单中的任何密钥之前，分批操作会验证是否已在您的存储桶上启用对象锁定。要执行操作和验证，批量操作需要 Amazon Identity and Access Management（IAM）角色中的 `s3:GetBucketObjectLockConfiguration` 和 `s3:PutObjectRetention` 权限，来支持批量操作代表您调用对象锁定。有关更多信息，请参阅 the section called “对象锁定注意事项”。

有关将此操作与 REST API 结合使用的信息，请参阅《Amazon Simple Storage Service API 参考》的 CreateJob 操作中的 `S3PutObjectRetention`。

有关使用此操作的 Amazon Command Line Interface（Amazon CLI）示例，请参阅the section called “使用分批操作与对象锁定保留”。有关 适用于 Java 的 Amazon SDK 示例，请参阅the section called “使用分批操作与对象锁定保留”。

### 限制和局限性

使用批量操作来应用对象锁定保留期时，以下限制和局限性适用：

- S3 批量操作不会进行任何存储桶级别的更改。
- 必须在执行任务的存储桶上配置版本控制和 S3 对象锁定。
- 清单中列出的所有对象都必须位于同一个存储桶中。
- 除非清单中明确指定了版本，否则该操作将适用于最新版本的对象。
- 您需要在 IAM 角色中拥有 `s3:PutObjectRetention` 权限，才能使用对象锁定保留任务。
- 需要 `s3:GetBucketObjectLockConfiguration` IAM 权限，才能确认为您正在对其执行任务的 S3 存储桶启用了对象锁定。
- 只能在应用 `COMPLIANCE` 模式保留日期的情况下延长对象的保留期，并且不能缩短此保留期。

## S3 对象锁定依法保留

可以使用 Amazon S3 批量操作对 Amazon S3 对象执行大规模批量操作。可以使用对象锁定法定保留操作来对于对象版本实施法定保留。与设置保留期限相似，依法保留可防止对象版本被覆盖或删除。但是，法定保留没有关联的保留期，在移除之前将一直有效。

您可以将 S3 分批操作与对象锁定一起使用，以便同时添加对很多 Amazon S3 对象的依法保留。为此，请在清单中指定目标对象的列表，并将该列表提交给批量操作。S3 批量操作对象锁定法定保留任务将持续运行，直至完成、取消或达到失败状态。

在处理清单中的任何对象之前，S3 批量操作会验证是否已在您的 S3 存储桶上启用对象锁定。要执行对象操作和存储桶级别验证，S3 批量操作需要 Amazon Identity and Access Management（IAM）角色中的 `s3:PutObjectLegalHold` 和 `s3:GetBucketObjectLockConfiguration`。这些权限可让 S3 批量操作代表您调用 S3 对象锁定。

当您创建 S3 批量操作任务来移除法定保留时，只需将 `Off` 指定为法定保留状态。有关更多信息，请参阅 the section called “对象锁定注意事项”。

有关如何将此操作与 Amazon S3 REST API 结合使用的信息，请参阅《Amazon Simple Storage Service API 参考》的 CreateJob 操作中的 `S3PutObjectLegalHold`。

有关使用此操作的示例，请参阅使用适用于 Java 的 Amazon 开发工具包。

限制和局限性

使用批量操作来应用或移除对象锁定法定保留时，以下限制和局限性适用：

- S3 批量操作不会进行任何存储桶级别的更改。
- 清单中列出的所有对象都必须位于同一个存储桶中。
- 必须在执行任务的存储桶上配置版本控制和 S3 对象锁定。
- 除非在清单中明确指定了版本，否则对象锁定法定保留操作将适用于最新版本的对象。
- IAM 角色需要 `s3:PutObjectLegalHold` 权限，才能在对象中添加或移除法定保留。
- 需要 `s3:GetBucketObjectLockConfiguration` IAM 权限，才能确认为在其中执行任务的 S3 存储桶启用了 S3 对象锁定。

- 复制对象
- 调用 Amazon Lambda 函数

- 替换所有对象标签
- 删除所有对象标签
- 替换访问控制列表（ACL）
- 使用批量操作还原对象
- S3 对象锁定保留
- S3 对象锁定依法保留
- 使用批量复制以复制现有对象

## 管理 S3 分批操作任务

Amazon S3 提供一组功能强大的工具，帮助您在创建 S3 分批操作任务后管理任务。本节介绍了可以通过 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 Amazon S3 REST API 来管理和跟踪任务的操作。

主题

- 使用 Amazon S3 控制台管理 S3 分批操作任务
- 列出任务
- 查看任务详细信息
- 分配任务优先级

### 使用 Amazon S3 控制台管理 S3 分批操作任务

使用控制台，您可以管理 S3 分批操作任务。例如，您可以：

- 查看活动任务和已排队的任务
- 更改工作的优先级
- 确认并运行任务
- 克隆任务
- 取消任务

要使用控制台管理分批操作

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。

2. 在左侧导航窗格中，请选择分批操作。
3. 请选择您想要管理的特定任务。

## 列出任务

您可以检索 S3 分批操作任务的列表。此列表包含您尚未完成的任务，以及您在过去 90 天内完成的任务。该任务列表包含每个任务的信息，如其 ID、描述、优先级、当前状态以及成功和失败的任务数。您可以按状态筛选任务列表。当您通过控制台检索任务列表时，还可以按描述或 ID 搜索任务并按 Amazon Web Services 区域 对其进行筛选。

获取 **`Active`** 和 **`Complete`** 任务的列表

以下 Amazon CLI 示例获取 `Active` 和 `Complete` 任务的列表。要使用此示例，请将 *`user input placeholders`* 替换为您自己的信息。

```
aws s3control list-jobs \
    --region us-west-2 \
    --account-id account-id \
    --job-statuses '["Active","Complete"]' \
    --max-results 20
```

有关更多信息和示例，请参阅 Amazon CLI 命令参考中的 list-jobs。

## 查看任务详细信息

如果您需要有关 Amazon S3 批量操作任务的信息比通过列出任务可检索到的信息更多，则可查看单个任务的所有详细信息。您可以查看您尚未完成的作业或者过去 90 天内完成的作业的详细信息。除了任务列表中返回的信息之外，单个任务的详细信息还包含其他项目，例如：

- 操作参数
- 有关清单的详细信息
- 有关完成报告的信息（如果您在创建任务时配置了完成报告）
- 您分配用于运行任务的 Amazon Identity and Access Management（IAM）用户角色的 Amazon 资源名称（ARN）

通过查看单个任务的详细信息，可以访问任务的整个配置。要查看任务的详细信息，您可以使用 Amazon S3 控制台或 Amazon Command Line Interface（Amazon CLI）。

在 Amazon S3 控制台中获取 S3 批量操作任务的描述

使用控制台查看批量操作任务的描述

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择批量操作。
3. 选择特定任务的任务 ID，以查看其详细信息。

在 Amazon CLI 中获取 S3 批量操作任务的描述

以下示例使用 Amazon CLI 获取 S3 批量操作任务的描述。要使用以下示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control describe-job \
--region us-west-2 \
--account-id account-id \
--job-id 00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c
```

有关更多信息和示例，请参阅 Amazon CLI 命令参考中的 describe-job。

## 分配任务优先级

可以为每个 Amazon S3 批量操作任务分配一个数字优先级，该优先级可以是任意正整数。S3 批量操作根据分配的优先级确定任务的优先次序。系统将首先评估具有较高优先级（或者优先级参数的数值较高）的任务。优先级按降序确定。例如，优先级值为 10 的任务队列将会比优先级值为 1 的任务队列优先计划。

可以在任务正在运行时更改其优先级。如果您在任务运行时提交优先级更高的新任务，则优先级较低的任务可以暂停，以允许优先级高的任务运行。

更改任务的优先级不会影响任务的处理速度。

> **Note**
>
> S3 批量操作尽最大努力遵循任务优先级。尽管优先级高的任务通常优先于优先级低的任务，但 Amazon S3 无法保证任务的严格顺序。

使用 S3 控制台

如何在 Amazon S3 控制台中更新任务优先级

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，请选择分批操作。
3. 请选择您想要管理的特定任务。
4. 请选择 Action（操作）。请在下拉列表中，选择 Update priority（更新优先级）。

使用 Amazon CLI

以下示例使用 Amazon CLI 更新任务优先级。数字越大，执行优先级越高。要使用以下示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control update-job-priority \
    --region us-west-2 \
    --account-id account-id \
    --priority 98 \
    --job-id 00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c
```

使用 适用于 Java 的 Amazon SDK

以下示例使用 适用于 Java 的 Amazon SDK 更新 S3 分批操作任务的优先级。

有关任务优先级的更多信息，请参阅 分配任务优先级。

Example

```
package aws.example.s3control;


import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.UpdateJobPriorityRequest;
```

```
import static com.amazonaws.regions.Regions.US_WEST_2;

public class UpdateJobPriority {
    public static void main(String[] args) {
        String accountId = "Account ID";
        String jobId = "00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c";

        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.updateJobPriority(new UpdateJobPriorityRequest()
                    .withAccountId(accountId)
                    .withJobId(jobId)
                    .withPriority(98));

        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

## 跟踪任务状态和完成报告

借助 S3 分批操作，您可以查看和更新任务状态、添加通知和日志记录、跟踪任务失败以及生成完成报告。

主题


- 任务状态
- 更新任务状态
- 通知和日志记录
- 跟踪任务失败
- 完成报告

- 示例：通过 Amazon CloudTrail 在 Amazon EventBridge 中跟踪 S3 分批操作任务。
- 示例：S3 分批操作完成报告

## 任务状态

在您创建和运行任务之后，该任务会逐步经过一系列状态。下表描述了状态以及状态之间可能的转换。

| 状态 | 说明 | 转换 |
| --- | --- | --- |
| New | 在您创建任务时，任务首先处于 New 状态。 | Amazon S3 开始处理清单对象时，任务自动转入 Preparing 状态。 |
| Preparing | Amazon S3 正在处理清单对象及其他任务参数，以设置和运行任务。 | Amazon S3 完成清单和其他参数的处理之后，任务自动转入 Ready 状态。然后，任务随时可以在清单中列出的对象上开始运行指定的操作。<br><br>如果任务要求在运行之前确认，就像您在使用 Amazon S3 控制台创建任务时那样，则任务从 Preparing 转换为 Suspended 。在您确认希望运行之前，任务将保持在 Suspended 状态。 |
| Suspended | 任务需要确认，但您尚未确认您想要运行该任务。只有使用 Amazon S3 控制台创建的任务需要确认。使用控制台创建的任务在 Preparing 之后立即进入 Suspended 状态。在您确认希望运行任务并且任务成为 Ready 状态之后，它不会再返回 Suspended 状态。 | 在您确认希望运行任务之后，其状态将更改为 Ready。 |

| 状态 | 说明 | 转换 |
| --- | --- | --- |
| Ready | Amazon S3 已准备好开始运行请求的对象操作。 | Amazon S3 开始运行任务时，任务自动转入 Active 状态。任务保持在 Ready 状态的时间长度取决于您是否已经在运行具有较高优先级的任务，以及完成这些任务需要多长时间。 |
| Active | Amazon S3 正在对清单中列出的对象执行请求的操作。当任务处于 Active 状态时，您可使用 Amazon S3 控制台，或者通过 REST API、Amazon CLI 或 Amazon 开发工具包使用 DescribeJob 操作监控其进度。 | 当任务不再在对象上运行操作时，该任务就移出 Active 状态。此行为自动发生，例如在任务成功完成或失败时。或者，此行为也可作为用户操作的结果发生，例如取消某个任务。任务转入的状态取决于发生转换的原因。 |
| Pausing | 任务从其他状态转换为 Paused。 | Paused 阶段完成时，任务自动转入 Pausing 状态。 |
| Paused | 在当前任务正在运行时，如果您提交了具有更高优先级的其他任务，任务可以进入 Paused 状态。 | 对于处于 Paused 状态的任务，如果阻止了该任务的任何较高优先级的任务执行完成、失败或暂停，则该任务自动返回 Active 状态。 |
| Complete | 任务已完成对清单中所有对象执行请求的操作。对于每个对象，操作可能成功或失败。如果您配置任务生成完成报告，则在任务处于 Complete 状态之后报告立即可用。 | Complete 是最终状态。任务一旦进入 Complete 状态，就不会转换为任何其它状态。 |
| Cancelling | 任务转换为 Cancelled 状态。 | Cancelled 阶段完成时，任务自动转入 Cancelling 状态。 |

| 状态 | 说明 | 转换 |
| --- | --- | --- |
| Cancelled | 您请求取消任务，而 S3 批量操作已成功取消了任务。任务将不会向 Amazon S3 提交任何新请求。 | Cancelled 是最终状态。任务进入 Cancelled 状态之后，就不会转换为任何其它状态。 |
| Failing | 任务转换为 Failed 状态。 | Failed 阶段完成后，任务自动转入 Failing 状态。 |
| Failed | 任务已失败，不再运行。有关任务失败的更多信息，请参阅跟踪任务失败。 | Failed 是最终状态。任务进入 Failed 状态之后，就不会转换为任何其它状态。 |

## 更新任务状态

以下 Amazon CLI 和适用于 Java 的 Amazon SDK 示例更新批量操作任务的状态。有关使用 Amazon S3 控制台管理批量操作任务的更多信息，请参阅使用 Amazon S3 控制台管理 S3 分批操作任务。

使用 Amazon CLI

要使用以下示例命令，请将 *user input placeholders* 替换为您自己的信息。

- 如果未在 create-job 命令中指定 --no-confirmation-required 参数，则任务将保持为暂停状态，直至通过将其状态设置为 Ready 来确认任务。然后，Amazon S3 会使任务符合执行的条件。

```
aws s3control update-job-status \
    --region us-west-2 \
    --account-id 123456789012 \
    --job-id 00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c \
    --requested-job-status 'Ready'
```

- 通过将任务状态设置为 Cancelled 来取消任务。

```
aws s3control update-job-status \
     --region us-west-2 \
     --account-id 123456789012 \
     --job-id 00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c \
     --status-update-reason "No longer needed" \
     --requested-job-status Cancelled
```

使用适用于 Java 的 Amazon 开发工具包

以下示例使用适用于 Java 的 Amazon SDK 来更新 S3 批量操作任务的状态。

有关任务状态的更多信息，请参阅 跟踪任务状态和完成报告。

Example

```
package aws.example.s3control;


import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.UpdateJobStatusRequest;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class UpdateJobStatus {
    public static void main(String[] args) {
        String accountId = "Account ID";
        String jobId = "00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c";

        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.updateJobStatus(new UpdateJobStatusRequest()
                    .withAccountId(accountId)
                    .withJobId(jobId)
                    .withRequestedJobStatus("Ready"));

        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
```

```
            e.printStackTrace();
        }
    }
}
```

## 通知和日志记录

除了请求完成报告外，还可以使用 Amazon CloudTrail 捕获、查看和审计批量操作活动。由于批量操作使用现有的 Amazon S3 API 操作来执行任务，因此，这些任务还会发出与您直接调用这些操作时相同的事件。因此，可以使用相同的通知、日志记录和审计工具以及已用于 Amazon S3 的过程，来跟踪和记录任务及其所有工作的进度。有关更多信息，请参阅以下部分中的示例。

> **Note**
>
> 批量操作会在任务执行期间在 CloudTrail 中同时生成管理事件和数据事件。这些事件的数量随每个任务的清单中的键数量而扩展。有关更多信息，请参阅 CloudTrail 定价页面，其中包括定价如何根据您在账户中配置的跟踪数量而变化的示例。要了解如何配置和记录事件以满足您的需求，请参阅《Amazon CloudTrail 用户指南》中的创建您的第一个跟踪。

有关 Amazon S3 事件的更多信息，请参阅 Amazon S3 事件通知。

## 跟踪任务失败

如果 S3 分批操作任务遇到的问题使其无法成功运行（如无法读取指定清单），则该任务失败。任务失败时，系统会生成一个或多个故障代码或失败原因。S3 批量操作将故障代码和原因与任务一起存储，便于您通过请求任务的详细信息来查看它们。如果您请求任务的完成报告，同时还会显示故障代码和原因。

为防止任务运行大量不成功的操作，Amazon S3 会对每个分批操作任务施加任务失败阈值。当任务已运行至少 1000 项工作时，Amazon S3 将监控工作失败率。在任何时刻，如果失败率（失败的任务数占已运行任务总数的比例）超过 50%，则任务失败。如果任务由于超过了任务失败阈值而失败，您可以确定造成失败的原因。例如，您可能在清单中意外地包括了一些指定存储桶中不存在的对象。修复错误之后，您可以重新提交任务。

> **Note**
>
> S3 批量操作异步进行操作，而工作并不一定按照清单中列出对象的顺序来运行。因此您不能使用清单顺序来确定哪些对象的任务成功，哪些对象的任务失败。而是可以通过查看任务的完成报告（如果已请求）或查看 Amazon CloudTrail 事件日志来帮助确定失败原因。

## 完成报告

在创建任务时，您可以请求完成报告。只要 S3 批量操作成功调用至少一项工作，Amazon S3 便会在任务完成运行工作、失败或被取消后生成完成报告。可对完成报告进行配置，以包含所有任务或只包含失败的任务。

完成报告包含任务配置、状态以及每项工作的信息，包括对象键和版本、状态、错误代码以及有关任何错误的描述。完成报告提供了以合并格式查看任务结果的简单途径，且无需进行任何附加设置。完成报告使用具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）来进行加密。有关完成报告的示例，请参阅 示例：S3 分批操作完成报告。

如果您未配置完成报告，则仍可使用 CloudTrail 和 Amazon CloudWatch 监控并审计您的任务及其各项工作。有关更多信息，请参阅以下主题：

主题

- 示例：通过 Amazon CloudTrail 在 Amazon EventBridge 中跟踪 S3 分批操作任务。
- 示例：S3 分批操作完成报告

## 示例：通过 Amazon CloudTrail 在 Amazon EventBridge 中跟踪 S3 分批操作任务。

Amazon S3 分批操作任务活动在 Amazon CloudTrail 中记录为事件。您可以在 Amazon EventBridge 中创建自定义规则，然后将这些事件发送到您选择的目标通知资源，例如 Amazon Simple Notification Service (Amazon SNS)。

> **Note**
>
> Amazon EventBridge 是管理事件的首选方式。Amazon CloudWatch Events 和 EventBridge 是相同的底层服务和 API，但 EventBridge 提供了更多功能。您在 CloudWatch 或 EventBridge 中所作的更改将显示在每个控制台中。有关更多信息，请参阅 Amazon EventBridge 用户指南。

跟踪示例

- 在 CloudTrail 中记录的 S3 分批操作事件
- 用于跟踪 S3 分批操作任务事件的 EventBridge 规则

### 在 CloudTrail 中记录的 S3 分批操作事件

创建分批操作任务后，它将作为 `JobCreated` 事件记录在 CloudTrail 中。在任务运行时，它会在处理过程中更改状态，并且其他 `JobStatusChanged` 事件将记录到 CloudTrail 中。您可以在 CloudTrail 控制台中查看这些事件。有关 CloudTrail 的更多信息，请参阅《Amazon CloudTrail 用户指南》。

> **Note**
>
> CloudTrail 中只记录 S3 分批操作任务 `status-change` 事件。

Example — CloudTrail 记录的 S3 批处理操作作业完成事件

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "s3.amazonaws.com"
    },
    "eventTime": "2020-02-05T18:25:30Z",
    "eventSource": "s3.amazonaws.com",
    "eventName": "JobStatusChanged",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "s3.amazonaws.com",
    "userAgent": "s3.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "f907577b-bf3d-4c53-b9ed-8a83a118a554",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "123412341234",
    "serviceEventDetails": {
        "jobId": "d6e58ec4-897a-4b6d-975f-10d7f0fb63ce",
        "jobArn": "arn:aws:s3:us-west-2:181572960644:job/
d6e58ec4-897a-4b6d-975f-10d7f0fb63ce",
        "status": "Complete",
```

```
        "jobEventId": "b268784cf0a66749f1a05bce259804f5",
        "failureCodes": [],
        "statusChangeReason": []
    }
}
```

用于跟踪 S3 分批操作任务事件的 EventBridge 规则

以下示例说明如何在 Amazon EventBridge 中创建规则，以便将 Amazon CloudTrail 记录的 S3 分批操作事件捕获到您选择的目标。

为此，您可以按照创建用于响应事件的 EventBridge 规则中的所有步骤来创建规则。粘贴以下 S3 分批操作自定义事件模式策略（如果适用），然后选择所需的目标服务。

S3 批处理操作自定义事件模式策略

```
{
    "source": [
        "aws.s3"
    ],
    "detail-type": [
        "Amazon Service Event via CloudTrail"
    ],
    "detail": {
        "eventSource": [
            "s3.amazonaws.com"
        ],
        "eventName": [
            "JobCreated",
            "JobStatusChanged"
        ]
    }
}
```

以下示例是从 EventBridge 事件规则发送到 Amazon Simple Queue Service (Amazon SQS) 的两个分批操作事件。由于分批操作任务在处理期间会经历多种不同的状态（`New`、`Preparing`、`Active` 等），因此对于每个任务，您都将收到多条消息。

Example — JobCreated 示例事件

```
{
    "version": "0",
```

```
    "id": "51dc8145-541c-5518-2349-56d7dffdf2d8",
    "detail-type": "Amazon Service Event via CloudTrail",
    "source": "aws.s3",
    "account": "123456789012",
    "time": "2020-02-27T15:25:49Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "11112223334444",
            "invokedBy": "s3.amazonaws.com"
        },
        "eventTime": "2020-02-27T15:25:49Z",
        "eventSource": "s3.amazonaws.com",
        "eventName": "JobCreated",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "s3.amazonaws.com",
        "userAgent": "s3.amazonaws.com",
        "eventID": "7c38220f-f80b-4239-8b78-2ed867b7d3fa",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "jobId": "e849b567-5232-44be-9a0c-40988f14e80c",
            "jobArn": "arn:aws:s3:us-east-1:181572960644:job/
e849b567-5232-44be-9a0c-40988f14e80c",
            "status": "New",
            "jobEventId": "f177ff24f1f097b69768e327038f30ac",
            "failureCodes": [],
            "statusChangeReason": []
        }
    }
}
```

### Example — JobStatusChanged 任务完成事件

```
{
  "version": "0",
  "id": "c8791abf-2af8-c754-0435-fd869ce25233",
  "detail-type": "Amazon Service Event via CloudTrail",
  "source": "aws.s3",
  "account": "123456789012",
  "time": "2020-02-27T15:26:42Z",
```

```
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "eventVersion": "1.05",
    "userIdentity": {
      "accountId": "1111222233334444",
      "invokedBy": "s3.amazonaws.com"
    },
    "eventTime": "2020-02-27T15:26:42Z",
    "eventSource": "s3.amazonaws.com",
    "eventName": "JobStatusChanged",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "s3.amazonaws.com",
    "userAgent": "s3.amazonaws.com",
    "eventID": "0238c1f7-c2b0-440b-8dbd-1ed5e5833afb",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "serviceEventDetails": {
      "jobId": "e849b567-5232-44be-9a0c-40988f14e80c",
      "jobArn": "arn:aws:s3:us-east-1:181572960644:job/
e849b567-5232-44be-9a0c-40988f14e80c",
      "status": "Complete",
      "jobEventId": "51f5ac17dba408301d56cd1b2c8d1e9e",
      "failureCodes": [],
      "statusChangeReason": []
    }
  }
}
```


## 示例：S3 分批操作完成报告

当您创建 S3 分批操作任务时，可以为全部任务或仅失败任务请求完成报告。只要成功调用了至少一个任务，S3 分批操作即会为已完成、已失败或已取消的任务生成报告。

完成报告包含每个任务的其他信息，包括对象键名称和版本、版本、错误代码以及任何错误的描述。每个失败任务的错误的描述可用于诊断在任务创建期间发生的问题，如权限。

> **Note**
>
> 完成报告始终使用 Amazon S3 托管式密钥（SSE-S3）进行加密。

Example — 顶级清单结果文件

顶级 manifest.json 文件包含每个成功报告的位置以及（如果任务有任何失败）失败报告的位置，如以下示例所示。

```
{
    "Format": "Report_CSV_20180820",
    "ReportCreationDate": "2019-04-05T17:48:39.725Z",
    "Results": [
        {
            "TaskExecutionStatus": "succeeded",
            "Bucket": "my-job-reports",
            "MD5Checksum": "83b1c4cbe93fc893f54053697e10fd6e",
            "Key": "job-f8fb9d89-a3aa-461d-bddc-ea6a1b131955/
results/6217b0fab0de85c408b4be96aeaca9b195a7daa5.csv"
        },
        {
            "TaskExecutionStatus": "failed",
            "Bucket": "my-job-reports",
            "MD5Checksum": "22ee037f3515975f7719699e5c416eaa",
            "Key": "job-f8fb9d89-a3aa-461d-bddc-ea6a1b131955/results/
b2ddad417e94331e9f37b44f1faf8c7ed5873f2e.csv"
        }
    ],
    "ReportSchema": "Bucket, Key, VersionId, TaskStatus, ErrorCode, HTTPStatusCode,
 ResultMessage"
}
```

Example — 失败任务报告

失败的任务报告包含所有失败 任务的以下信息：

- Bucket
- Key
- VersionId
- TaskStatus
- ErrorCode
- HTTPStatusCode
- ResultMessage

以下示例报告显示 Amazon Lambda 函数超时，从而导致失败以超出失败阈值的情况。然后，它会标记为 PermanentFailure。

```
amzn-s3-demo-bucket1,image_14975,,failed,200,PermanentFailure,"Lambda returned
 function error: {""errorMessage"":""2019-04-05T17:35:21.155Z 2845ca0d-38d9-4c4b-
abcf-379dc749c452 Task timed out after 3.00 seconds""}"
amzn-s3-demo-bucket1,image_15897,,failed,200,PermanentFailure,"Lambda returned
 function error: {""errorMessage"":""2019-04-05T17:35:29.610Z 2d0a330b-de9b-425f-
b511-29232fde5fe4 Task timed out after 3.00 seconds""}"
amzn-s3-demo-bucket1,image_14819,,failed,200,PermanentFailure,"Lambda returned
 function error: {""errorMessage"":""2019-04-05T17:35:22.362Z fcf5efde-74d4-4e6d-b37a-
c7f18827f551 Task timed out after 3.00 seconds""}"
amzn-s3-demo-bucket1,image_15930,,failed,200,PermanentFailure,"Lambda returned
 function error: {""errorMessage"":""2019-04-05T17:35:29.809Z 3dd5b57c-4a4a-48aa-8a35-
cbf027b7957e Task timed out after 3.00 seconds""}"
amzn-s3-demo-bucket1,image_17644,,failed,200,PermanentFailure,"Lambda
 returned function error: {""errorMessage"":""2019-04-05T17:35:46.025Z
 10a764e4-2b26-4d8c-9056-1e1072b4723f Task timed out after 3.00 seconds""}"
amzn-s3-demo-bucket1,image_17398,,failed,200,PermanentFailure,"Lambda returned
 function error: {""errorMessage"":""2019-04-05T17:35:44.661Z 1e306352-4c54-4eba-
aee8-4d02f8c0235c Task timed out after 3.00 seconds""}"
```

Example — 成功任务报告

成功任务报告包含成功 任务的以下各项内容：

- Bucket
- Key
- VersionId
- TaskStatus
- ErrorCode
- HTTPStatusCode
- ResultMessage

在以下示例中，Lambda 函数将 Amazon S3 对象成功复制到其他存储桶。返回的 Amazon S3 响应会传回到 S3 分批操作，然后写入最终完成报告。

```
amzn-s3-demo-bucket1,image_17775,,succeeded,200,,"{u'CopySourceVersionId':
 'xVR78haVKlRnurYofbTfYr3ufYbktF8h', u'CopyObjectResult': {u'LastModified':
```

```
 datetime.datetime(2019, 4, 5, 17, 35, 39, tzinfo=tzlocal()), u'ETag':
 '""fe66f4390c50f29798f040d7aae72784""'}, 'ResponseMetadata': {'HTTPStatusCode':
 200, 'RetryAttempts': 0, 'HostId': 'nXNaClIMxEJzWNmeMNQV2KpjbaCJLn0OGoXWZpuVOFS/
iQYWxb3QtTvzX9SVfx2lA3oTKLwImKw=', 'RequestId': '3ED5852152014362', 'HTTPHeaders':
 {'content-length': '234', 'x-amz-id-2': 'nXNaClIMxEJzWNmeMNQV2KpjbaCJLn0OGoXWZpuVOFS/
iQYWxb3QtTvzX9SVfx2lA3oTKLwImKw=', 'x-amz-copy-source-version-id':
 'xVR78haVKlRnurYofbTfYr3ufYbktF8h', 'server': 'AmazonS3', 'x-amz-request-id':
 '3ED5852152014362', 'date': 'Fri, 05 Apr 2019 17:35:39 GMT', 'content-type':
 'application/xml'}}}"
amzn-s3-demo-bucket1,image_17763,,succeeded,200,,"{u'CopySourceVersionId':
 '6HjOUSim4Wj6BTcbxToXW44pSZ.40pwq', u'CopyObjectResult': {u'LastModified':
 datetime.datetime(2019, 4, 5, 17, 35, 39, tzinfo=tzlocal()),
 u'ETag': '""fe66f4390c50f29798f040d7aae72784""'}, 'ResponseMetadata':
 {'HTTPStatusCode': 200, 'RetryAttempts': 0, 'HostId': 'GiCZNYr8LHd/
Thyk6beTRP96IGZk2sYxujLe13TuuLpq6U2RD3we0YoluuIdm1PRvkMwnEW1aFc=', 'RequestId':
 '1BC9F5B1B95D7000', 'HTTPHeaders': {'content-length': '234', 'x-amz-id-2':
 'GiCZNYr8LHd/Thyk6beTRP96IGZk2sYxujLe13TuuLpq6U2RD3we0YoluuIdm1PRvkMwnEW1aFc=', 'x-
amz-copy-source-version-id': '6HjOUSim4Wj6BTcbxToXW44pSZ.40pwq', 'server': 'AmazonS3',
 'x-amz-request-id': '1BC9F5B1B95D7000', 'date': 'Fri, 05 Apr 2019 17:35:39 GMT',
 'content-type': 'application/xml'}}}"
amzn-s3-demo-bucket1,image_17860,,succeeded,200,,"{u'CopySourceVersionId':
 'm.MDD0g_QsUnYZ8TBzVFrp.TmjN8PJyX', u'CopyObjectResult': {u'LastModified':
 datetime.datetime(2019, 4, 5, 17, 35, 40, tzinfo=tzlocal()), u'ETag':
 '""fe66f4390c50f29798f040d7aae72784""'}, 'ResponseMetadata': {'HTTPStatusCode':
 200, 'RetryAttempts': 0, 'HostId': 'F9ooZOgpE5g9sNgBZxjdiPHqB4+0DNWgj3qbsir
+sKai4fv7rQEcF2fBN1VeeFc2WH45a9ygb2g=', 'RequestId': '8D9CA56A56813DF3', 'HTTPHeaders':
 {'content-length': '234', 'x-amz-id-2': 'F9ooZOgpE5g9sNgBZxjdiPHqB4+0DNWgj3qbsir
+sKai4fv7rQEcF2fBN1VeeFc2WH45a9ygb2g=', 'x-amz-copy-source-version-id':
 'm.MDD0g_QsUnYZ8TBzVFrp.TmjN8PJyX', 'server': 'AmazonS3', 'x-amz-request-id':
 '8D9CA56A56813DF3', 'date': 'Fri, 05 Apr 2019 17:35:40 GMT', 'content-type':
 'application/xml'}}}"
```

## 使用标签控制访问和标记任务

您可以通过添加标签来标记和控制对 S3 分批操作任务的访问。标签可用于确定谁负责分批操作任务。任务标签的存在可授予或限制用户取消任务、激活处于确认状态的任务或更改任务优先级的能力。可以创建附加了标签的任务，并且可以在创建任务后向任务添加标签。每个标签都是一个键值对，可以在创建任务或稍后更新时包含该键值对。

> **Warning**
>
> 确保任务标签中不包含任何机密信息或个人数据。

考虑以下标记示例：假设您希望您的财务部门创建一个分批操作任务。您可以编写允许用户调用 `CreateJob` 的 Amazon Identity and Access Management (IAM) 策略，前提是创建任务时使用分配了 `Finance` 值的 `Department` 标签。此外，您可以将该策略附加到作为财务部门成员的所有用户。

继续使用此示例，您可以编写一个策略，允许用户更新具有所需标签的任何任务的优先级，或者取消具有这些标签的任何任务。有关更多信息，请参阅 the section called “控制权限”。

您可以在创建新的 S3 分批操作任务时向其添加标签，也可以将向现有任务添加标签。

注意以下标签限制：

- 只要任务具有唯一的标签键，就可以将最多 50 个标签与该任务关联。
- 标签键的长度最大可以为 128 个 Unicode 字符，标签值的长度最大可以为 256 个 Unicode 字符。
- 键和值区分大小写。

有关标签限制的更多信息，请参阅《Amazon 账单与成本管理 用户指南》中的用户定义的标签限制。

## 与 S3 分批操作任务标记相关的 API 操作

Amazon S3 支持以下特定于 S3 分批操作任务标记的 API 操作：

- GetJobTagging – 返回与批量操作任务关联的标签集。
- PutJobTagging – 替换与任务关联的标签集。使用此 API 操作进行 S3 分批操作任务标签管理有两种不同的方案：
  - 任务没有标签 – 可以向任务添加一组标签（任务之前没有标签）。
  - 任务具有一组现有标签 – 要修改现有标签集，您可以完全替换现有标签集，或者通过使用 GetJobTagging 检索现有标签集来在现有标签集中进行更改，修改该标签集，然后使用此 API 操作来将此标签集替换为您已修改的标签集。

    > **Note**
    >
    > 如果您发送带有空标签集的此请求，S3 分批操作将删除对象上的现有标签集。如果您使用此方法，则需为套餐 1 请求 (PUT) 付费。有关更多信息，请参阅 Amazon S3 定价。
    > 要删除分批操作任务的现有标签，首选执行 `DeleteJobTagging` 操作，因为该操作在不产生费用的情况下实现相同的结果。

- DeleteJobTagging – 删除与批量操作任务关联的标签集。

## 使用用于标记的任务标签创建分批操作任务

可以通过添加标签 来标注 Amazon S3 批量操作任务和控制对任务的访问。标签可用于确定谁负责分批操作任务。您可以创建附加了标签的任务，并且可以在创建任务后向任务添加标签。有关更多信息，请参阅 the section called “使用标签”。

使用 Amazon CLI

以下 Amazon CLI 示例创建了 S3 分批操作 S3PutObjectCopy 任务，其中使用任务标签作为该任务的标签。

1. 请选择您希望分批操作任务执行的操作或 OPERATION，然后选择您的 TargetResource。

```
read -d '' OPERATION <<EOF
{
  "S3PutObjectCopy": {
    "TargetResource": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
  }
}
EOF
```

2. 确定您需要用于此任务的任务 TAGS。在这种情况下，您应用两个标签 department 和 FiscalYear，值分别为 Marketing 和 2020。

```
read -d '' TAGS <<EOF
[
  {
    "Key": "department",
    "Value": "Marketing"
  },
  {
    "Key": "FiscalYear",
    "Value": "2020"
  }
]
EOF
```

3. 为分批操作任务指定 MANIFEST。

```
read -d '' MANIFEST <<EOF
{
  "Spec": {
```

```
    "Format": "EXAMPLE_S3BatchOperations_CSV_20180820",
    "Fields": [
      "Bucket",
      "Key"
    ]
  },
  "Location": {
    "ObjectArn": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/example_manifest.csv",
    "ETag": "example-5dc7a8bfb90808fc5d546218"
  }
}
EOF
```

4. 为分批操作任务配置 REPORT。

```
read -d '' REPORT <<EOF
{
  "Bucket": "arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
  "Format": "Example_Report_CSV_20180820",
  "Enabled": true,
  "Prefix": "reports/copy-with-replace-metadata",
  "ReportScope": "AllTasks"
}
EOF
```

5. 运行 `create-job` 操作以使用在上述步骤中设置的输入创建分批操作任务。

```
aws \
    s3control create-job \
    --account-id 123456789012 \
    --manifest "${MANIFEST//$'\n'}" \
    --operation "${OPERATION//$'\n'/}" \
    --report "${REPORT//$'\n'}" \
    --priority 10 \
    --role-arn arn:aws:iam::123456789012:role/batch-operations-role \
    --tags "${TAGS//$'\n'/}" \
    --client-request-token "$(uuidgen)" \
    --region us-west-2 \
    --description "Copy with Replace Metadata";
```

使用适用于 Java 的 Amazon 开发工具包

Example

以下示例使用 适用于 Java 的 Amazon SDK 创建带有标签的 S3 分批操作任务。

```
public String createJob(final AWSS3ControlClient awss3ControlClient) {
    final String manifestObjectArn = "arn:aws:s3:::amzn-s3-demo-manifest-bucket/
manifests/10_manifest.csv";
    final String manifestObjectVersionId = "example-5dc7a8bfb90808fc5d546218";

    final JobManifestLocation manifestLocation = new JobManifestLocation()
            .withObjectArn(manifestObjectArn)
            .withETag(manifestObjectVersionId);

    final JobManifestSpec manifestSpec =
            new
 JobManifestSpec().withFormat(JobManifestFormat.S3InventoryReport_CSV_20161130);

    final JobManifest manifestToPublicApi = new JobManifest()
            .withLocation(manifestLocation)
            .withSpec(manifestSpec);

    final String jobReportBucketArn = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
    final String jobReportPrefix = "example-job-reports";

    final JobReport jobReport = new JobReport()
            .withEnabled(true)
            .withReportScope(JobReportScope.AllTasks)
            .withBucket(jobReportBucketArn)
            .withPrefix(jobReportPrefix)
            .withFormat(JobReportFormat.Report_CSV_20180820);

    final String lambdaFunctionArn = "arn:aws:lambda:us-
west-2:123456789012:function:example-function";

    final JobOperation jobOperation = new JobOperation()
            .withLambdaInvoke(new
 LambdaInvokeOperation().withFunctionArn(lambdaFunctionArn));

    final S3Tag departmentTag = new
 S3Tag().withKey("department").withValue("Marketing");
    final S3Tag fiscalYearTag = new S3Tag().withKey("FiscalYear").withValue("2020");
```

```
    final String roleArn = "arn:aws:iam::123456789012:role/example-batch-operations-
role";
    final Boolean requiresConfirmation = true;
    final int priority = 10;

    final CreateJobRequest request = new CreateJobRequest()
            .withAccountId("123456789012")
            .withDescription("Test lambda job")
            .withManifest(manifestToPublicApi)
            .withOperation(jobOperation)
            .withPriority(priority)
            .withRoleArn(roleArn)
            .withReport(jobReport)
            .withTags(departmentTag, fiscalYearTag)
            .withConfirmationRequired(requiresConfirmation);

    final CreateJobResult result = awss3ControlClient.createJob(request);

    return result.getJobId();
}
```

## 从 S3 分批操作任务中删除标签

可以使用这些示例从 Amazon S3 批量操作任务中删除标签。

### 使用 Amazon CLI

以下示例使用 Amazon CLI 从分批操作任务中删除标签。

```
aws \
    s3control delete-job-tagging \
    --account-id 123456789012 \
    --job-id Example-e25a-4ed2-8bee-7f8ed7fc2f1c \
    --region us-east-1
```

### 删除分批操作任务的任务标签

### Example

以下示例使用 适用于 Java 的 Amazon SDK 删除 S3 分批操作任务的标签。

```
public void deleteJobTagging(final AWSS3ControlClient awss3ControlClient,
                             final String jobId) {
```

```
    final DeleteJobTaggingRequest deleteJobTaggingRequest = new
 DeleteJobTaggingRequest()
            .withJobId(jobId);

    final DeleteJobTaggingResult deleteJobTaggingResult =
                awss3ControlClient.deleteJobTagging(deleteJobTaggingRequest);
}
```

## 向现有批量操作任务添加任务标签

可以使用 PutJobTagging API 操作向现有 Amazon S3 批量操作任务添加任务标签。有关更多信息，请参阅以下示例。

使用 Amazon CLI

以下是使用 Amazon CLI 通过 `s3control put-job-tagging` 向 S3 批量操作任务添加任务标签的示例。要使用这些示例，请将 *`user input placeholders`* 替换为您自己的信息。

> **Note**
>
> 如果您发送带有空标签集的此请求，批量操作将删除对象上的现有标签集。但是，如果您使用此方法，则需为套餐 1 请求 (PUT) 付费。有关更多信息，请参阅 Amazon S3 定价。
> 相反，要删除批量操作任务的现有标签，建议使用 `DeleteJobTagging` 操作，因为该操作可在不产生费用的情况下实现相同的结果。

1. 确定您需要用于此任务的任务 TAGS。在这种情况下，您应用两个标签 *`department`* 和 *`FiscalYear`*，值分别为 *`Marketing`* 和 *`2020`*。

```
read -d '' TAGS <<EOF
[
  {
    "Key": "department",
    "Value": "Marketing"
  },
  {
    "Key": "FiscalYear",
    "Value": "2020"
  }
]
EOF
```

2. 使用所需参数运行以下 put-job-tagging 命令：

```
aws \
    s3control put-job-tagging \
    --account-id 123456789012 \
    --tags "${TAGS//$'\n'/}" \
    --job-id Example-e25a-4ed2-8bee-7f8ed7fc2f1c \
    --region us-east-1
```

使用适用于 Java 的 Amazon SDK

Example

以下示例使用适用于 Java 的 Amazon SDK 放置 S3 批量操作任务的标签。

```
public void putJobTagging(final AWSS3ControlClient awss3ControlClient,
                          final String jobId) {
    final S3Tag departmentTag = new
 S3Tag().withKey("department").withValue("Marketing");
    final S3Tag fiscalYearTag = new S3Tag().withKey("FiscalYear").withValue("2020");

    final PutJobTaggingRequest putJobTaggingRequest = new PutJobTaggingRequest()
            .withJobId(jobId)
            .withTags(departmentTag, fiscalYearTag);

    final PutJobTaggingResult putJobTaggingResult =
 awss3ControlClient.putJobTagging(putJobTaggingRequest);
}
```

## 获取 S3 分批操作任务的标签

要检索 Amazon S3 批量操作任务的标签，可以使用 GetJobTagging API 操作。有关更多信息，请参阅以下示例。

使用 Amazon CLI

以下示例使用 Amazon CLI 获取分批操作任务的标签。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
aws \
    s3control get-job-tagging \
```

```
    --account-id 123456789012 \
    --job-id Example-e25a-4ed2-8bee-7f8ed7fc2f1c \
    --region us-east-1
```

使用适用于 Java 的 Amazon 开发工具包

Example

以下示例使用 适用于 Java 的 Amazon SDK 获取 S3 分批操作任务的标签。

```
public List<S3Tag> getJobTagging(final AWSS3ControlClient awss3ControlClient,
                                 final String jobId) {
    final GetJobTaggingRequest getJobTaggingRequest = new GetJobTaggingRequest()
            .withJobId(jobId);

    final GetJobTaggingResult getJobTaggingResult =
            awss3ControlClient.getJobTagging(getJobTaggingRequest);

    final List<S3Tag> tags = getJobTaggingResult.getTags();

    return tags;
}
```

## 使用任务标签控制批量操作的权限

为了协助您管理 Amazon S3 批量操作任务，可以添加任务标签。借助任务标签，您可以控制对 S3 分批操作任务的访问，并强制在创建任何任务时应用标签。

您最多可以为每个分批操作任务应用 50 个任务标签。通过使用标签，可以设置精细的策略，来限制可以编辑任务的用户集。任务标签可授予或限制用户取消任务、激活处于确认状态的任务或更改任务优先级的能力。此外，您可以强制将标签应用于所有新任务，并为标签指定允许的键值对。可以使用 Amazon Identity and Access Management（IAM）策略语言来表达所有这些条件。有关更多信息，请参阅《Service Authorization Reference》中的 Actions, resources, and condition keys for Amazon S3。

有关按 S3 资源类型对 S3 API 操作的权限的更多信息，请参阅 Amazon S3 API 操作所需的权限。

以下示例显示如何使用 S3 分批操作任务标签仅向用户授予创建和编辑在特定部门（例如，财务或合规性部门）内运行的任务的权限。您还可以根据与任务相关的开发阶段分配任务，例如 QA 或生产。

在此示例中，您在 IAM 策略中使用 S3 批量操作任务标签，来向用户授予创建和编辑只能在其部门内运行的任务的权限。您可以根据与任务相关的开发阶段分配任务，例如 QA 或生产。

下面的示例使用以下部门，每个部门使用批量操作的方式均不同：

- 财务
- 合规性
- 商业智能
- 工程

主题


- 通过向用户和资源分配标签来控制访问
- 按阶段标记分批操作任务并对任务优先级实施限制


通过向用户和资源分配标签来控制访问

在这种情况下，管理员正在使用基于属性的访问控制 (ABAC)。ABAC 是一种 IAM 授权策略，它通过向用户和 Amazon 资源附加标签来定义权限。

为用户和任务分配以下部门标签之一：

键：值

- `department : Finance`
- `department : Compliance`
- `department : BusinessIntelligence`
- `department : Engineering`

> **Note**
>
> 任务标签键和值区分大小写。

使用 ABAC 访问控制策略，您可以授予“财务”部门中的用户在其部门内创建和管理 S3 批量操作任务的权限，方法是将标签 `department=Finance` 与其用户关联。

此外，您可以将托管策略附加到 IAM 用户，此策略允许公司中的任何用户在其各自部门内创建或修改 S3 分批操作任务。

此示例中的策略包括三个策略语句：

- 策略中的第一个语句允许用户创建分批操作任务，前提是任务创建请求包含与其各自部门匹配的任务标签。这使用 "${aws:PrincipalTag/department}" 语法表示，该语法在策略评估时被用户的部门标签所取代。当在请求 ("aws:RequestTag/department") 中为部门标签提供的值与用户的部门匹配时，该条件将得到满足。
- 策略中的第二个语句允许用户更改任务的优先级或更新任务的状态，前提是用户正在更新的任务与用户的部门匹配。
- 第三个语句允许用户随时通过 PutJobTagging 请求更新分批操作任务的标签，只要 (1) 其部门标签被保留，并且 (2) 他们正在更新的任务位于其部门内。

```
{
      "Version": "2012-10-17",
      "Statement": [
            {
                  "Effect": "Allow",
                  "Action": "s3:CreateJob",
                  "Resource": "*",
                  "Condition": {
                        "StringEquals": {
                              "aws:RequestTag/department": "${aws:PrincipalTag/
department}"
                }
            }
        },
            {
                  "Effect": "Allow",
                  "Action": [
                        "s3:UpdateJobPriority",
                        "s3:UpdateJobStatus"
            ],
                  "Resource": "*",
                  "Condition": {
                        "StringEquals": {
                              "aws:ResourceTag/department": "${aws:PrincipalTag/
department}"
                }
            }
        },
            {
                  "Effect": "Allow",
                  "Action": "s3:PutJobTagging",
                  "Resource": "*",
```

```
                "Condition": {
                      "StringEquals": {
                            "aws:RequestTag/department": "${aws:PrincipalTag/
department}",
                            "aws:ResourceTag/department": "${aws:PrincipalTag/
department}"
                }
             }
        }
    ]
}
```

按阶段标记分批操作任务并对任务优先级实施限制

所有 S3 分批操作任务都具有数字优先级，Amazon S3 使用此优先级来决定以何种顺序运行任务。对于此示例，您可以限制大多数用户可以分配给任务的最大优先级，并为有限的特权用户集保留更高的优先级范围，如下所示：

- QA 阶段优先级范围（低）：1-100
- 生产阶段优先级范围（高）：1-300

为此，请引入一个代表任务阶段 的新标签集：

键 : 值

- `stage : QA`
- `stage : Production`

在部门内创建和更新低优先级任务

除了基于部门的限制外，此策略还对 S3 分批操作任务创建和更新引入了两个新的限制：

- 它允许用户在其部门中创建或更新任务，而一个新条件要求任务包含标签 `stage=QA`。
- 它允许用户创建或更新任务的优先级，新的最大优先级为 100。

```
{
        "Version": "2012-10-17",
        "Statement": [
        {
```

```
        "Effect": "Allow",
        "Action": "s3:CreateJob",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:RequestTag/department": "${aws:PrincipalTag/department}",
                "aws:RequestTag/stage": "QA"
            },
            "NumericLessThanEquals": {
                "s3:RequestJobPriority": 100
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "s3:UpdateJobStatus"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/department": "${aws:PrincipalTag/department}"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": "s3:UpdateJobPriority",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/department": "${aws:PrincipalTag/department}",
                "aws:ResourceTag/stage": "QA"
            },
            "NumericLessThanEquals": {
                "s3:RequestJobPriority": 100
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": "s3:PutJobTagging",
        "Resource": "*",
        "Condition": {
```

```
            "StringEquals": {
                "aws:RequestTag/department" : "${aws:PrincipalTag/department}",
                "aws:ResourceTag/department": "${aws:PrincipalTag/department}",
                "aws:RequestTag/stage": "QA",
                "aws:ResourceTag/stage": "QA"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": "s3:GetJobTagging",
        "Resource": "*"
    }
    ]
}
```

在部门内创建和更新高优先级任务

少数用户可能需要在 QA 或 生产 中创建高优先级任务的能力。为了满足这一需求，您可以创建一个根据上一节中的低优先级策略改写的托管策略。

该策略执行以下操作：

- 允许用户使用标签 `stage=QA` 或 `stage=Production` 在其部门中创建或更新任务。
- 允许用户创建或更新任务的优先级，最高为 300。

```
{
      "Version": "2012-10-17",
      "Statement": [
          {
                "Effect": "Allow",
                "Action": "s3:CreateJob",
                "Resource": "*",
                "Condition": {
                      "ForAnyValue:StringEquals": {
                            "aws:RequestTag/stage": [
                                  "QA",
                                  "Production"
                    ]
                },
                      "StringEquals": {
```

```
                        "aws:RequestTag/department": "${aws:PrincipalTag/
department}"
                },
                      "NumericLessThanEquals": {
                            "s3:RequestJobPriority": 300
                }
            }
        },
          {
                "Effect": "Allow",
                "Action": [
                      "s3:UpdateJobStatus"
            ],
                "Resource": "*",
                "Condition": {
                      "StringEquals": {
                            "aws:ResourceTag/department": "${aws:PrincipalTag/
department}"
                }
            }
        },
          {
                "Effect": "Allow",
                "Action": "s3:UpdateJobPriority",
                "Resource": "*",
                "Condition": {
                      "ForAnyValue:StringEquals": {
                            "aws:ResourceTag/stage": [
                                  "QA",
                                  "Production"
                    ]
                },
                      "StringEquals": {
                            "aws:ResourceTag/department": "${aws:PrincipalTag/
department}"
                },
                      "NumericLessThanEquals": {
                            "s3:RequestJobPriority": 300
                }
            }
        },
          {
                "Effect": "Allow",
                "Action": "s3:PutJobTagging",
```

```
                "Resource": "*",
                "Condition": {
                      "StringEquals": {
                            "aws:RequestTag/department": "${aws:PrincipalTag/
department}",
                            "aws:ResourceTag/department": "${aws:PrincipalTag/
department}"
                },
                      "ForAnyValue:StringEquals": {
                            "aws:RequestTag/stage": [
                                  "QA",
                                  "Production"
                    ],
                            "aws:ResourceTag/stage": [
                                  "QA",
                                  "Production"
                    ]
                }
            }
        }
    ]
}
```

## 使用 S3 分批操作管理 S3 对象锁定

您可以使用 S3 批量操作对 Amazon S3 对象执行大规模批量操作。S3 批量操作可以对您指定的 Amazon S3 对象列表执行单个操作。单个任务可对数十亿个包含 EB 级数据的对象执行指定操作。Amazon S3 跟踪进度、发送通知并存储所有操作的详细完成报告，从而提供完全托管、可审核的无服务器体验。可以通过 Amazon S3 控制台、Amazon CLI、Amazon SDK 或 Amazon S3 REST API 使用 S3 批量操作。

S3 对象锁定还可以对对象版本进依法保留。与设置保留期限相似，依法保留可防止对象版本被覆盖或删除。但是，法定保留没有关联的保留期，在移除法定保留之前将保持有效。有关更多信息，请参阅 S3 对象锁定依法保留。

要将 S3 批量操作与对象锁定结合使用，以便同时对许多 Amazon S3 对象添加法定保留，请参阅以下主题。

主题

- 使用 S3 分批操作启用 S3 对象锁定
- 使用分批操作设置对象锁定保留

- 将 S3 分批操作与 S3 对象锁定保留合规模式结合使用
- 将 S3 分批操作与 S3 对象锁定保留监管模式结合使用
- 使用 S3 批量操作关闭 S3 对象锁定法定保留

## 使用 S3 分批操作启用 S3 对象锁定

可以将 Amazon S3 批量操作与 S3 对象锁定结合使用，以便同时为许多 Amazon S3 对象管理保留或启用法定保留。您可以在清单中指定目标对象的列表并将该列表提交到分批操作以完成操作。有关更多信息，请参阅the section called “对象锁定保留”和the section called “对象锁定依法保留”。

以下示例说明如何创建具有 S3 批量操作权限的 Amazon Identity and Access Management（IAM）角色并更新角色权限，来创建启用对象锁定的任务。还必须有一个 CSV 清单来标识 S3 批量操作任务的对象。有关更多信息，请参阅 the section called “指定清单”。

要使用以下示例，请将 *user input placeholders* 替换为您自己的信息。

使用 Amazon CLI

1. 创建 IAM 角色并为 S3 分批操作分配运行权限。

   所有 S3 分批操作任务都必须执行此步骤。

```
export AWS_PROFILE='aws-user'

read -d '' batch_operations_trust_policy <<EOF
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "batchoperations.s3.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
EOF
aws iam create-role --role-name batch_operations-objectlock \
```

```
--assume-role-policy-document "${batch_operations_trust_policy}"
```

2. 设置要运行的 S3 分批操作和 S3 对象锁定。

   在此步骤中，允许角色执行以下操作：

   a. 在包含您希望在其上运行分批操作的目标对象的 S3 存储桶上运行对象锁定。

   b. 读取清单 CSV 文件和对象所在的 S3 存储桶。

   c. 将 S3 分批操作任务的结果写入报告存储桶。

```
read -d '' batch_operations_permissions <<EOF
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:GetBucketObjectLockConfiguration",
            "Resource": [
                "arn:aws:s3:::{{amzn-s3-demo-manifest-bucket}}"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::{{amzn-s3-demo-manifest-bucket}}/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::{{amzn-s3-demo-completion-report-bucket}}/*"
            ]
        }
```

```
    ]
}
EOF

aws iam put-role-policy --role-name batch_operations-objectlock \
--policy-name object-lock-permissions \
--policy-document "${batch_operations_permissions}"
```

使用适用于 Java 的 Amazon 开发工具包

以下示例说明如何使用适用于 Java 的 Amazon SDK 创建具有 S3 批量操作权限的 IAM 角色并更新角色权限，来创建启用对象锁定的任务。您还必须有一个 CSV 清单来标识 S3 分批操作任务的对象。有关更多信息，请参阅 the section called “指定清单”。

执行以下步骤：

1. 创建 IAM 角色并为 S3 分批操作分配运行权限。所有 S3 分批操作任务都必须执行此步骤。
2. 设置要运行的 S3 分批操作和 S3 对象锁定。

   允许角色执行以下操作：

   1. 在包含您希望在其上运行分批操作的目标对象的 S3 存储桶上运行对象锁定。
   2. 读取清单 CSV 文件和对象所在的 S3 存储桶。
   3. 将 S3 分批操作任务的结果写入报告存储桶。

```
public void createObjectLockRole() {
    final String roleName = "batch_operations-object-lock";

    final String trustPolicy = "{" +
            "  \"Version\": \"2012-10-17\", " +
            "  \"Statement\": [ " +
            "    { " +
            "      \"Effect\": \"Allow\", " +
            "      \"Principal\": { " +
            "        \"Service\": [" +
            "          \"batchoperations.s3.amazonaws.com\"" +
            "        ]" +
            "      }, " +
            "      \"Action\": \"sts:AssumeRole\" " +
            "    } " +
```

```
            "  ]" +
            "}";

    final String bopsPermissions = "{" +
            "    \"Version\": \"2012-10-17\"," +
            "    \"Statement\": [" +
            "        {" +
            "            \"Effect\": \"Allow\"," +
            "            \"Action\": \"s3:GetBucketObjectLockConfiguration\"," +
            "            \"Resource\": [" +
            "                \"arn:aws:s3:::amzn-s3-demo-manifest-bucket\"" +
            "            ]" +
            "        }," +
            "        {" +
            "            \"Effect\": \"Allow\"," +
            "            \"Action\": [" +
            "                \"s3:GetObject\"," +
            "                \"s3:GetObjectVersion\"," +
            "                \"s3:GetBucketLocation\"" +
            "            ]," +
            "            \"Resource\": [" +
            "                \"arn:aws:s3:::amzn-s3-demo-manifest-bucket/*\"" +
            "            ]" +
            "        }," +
            "        {" +
            "            \"Effect\": \"Allow\"," +
            "            \"Action\": [" +
            "                \"s3:PutObject\"," +
            "                \"s3:GetBucketLocation\"" +
            "            ]," +
            "            \"Resource\": [" +
            "                \"arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*\""
+
            "            ]" +
            "        }" +
            "    ]" +
            "}";

    final AmazonIdentityManagement iam =
            AmazonIdentityManagementClientBuilder.defaultClient();

    final CreateRoleRequest createRoleRequest = new CreateRoleRequest()
            .withAssumeRolePolicyDocument(bopsPermissions)
            .withRoleName(roleName);
```

```
    final CreateRoleResult createRoleResult = iam.createRole(createRoleRequest);

    final PutRolePolicyRequest putRolePolicyRequest = new PutRolePolicyRequest()
            .withPolicyDocument(bopsPermissions)
            .withPolicyName("batch_operations-permissions")
            .withRoleName(roleName);

    final PutRolePolicyResult putRolePolicyResult =
 iam.putRolePolicy(putRolePolicyRequest);
}
```

## 使用分批操作设置对象锁定保留

可以将 Amazon S3 批量操作与 S3 对象锁定结合使用，以便同时管理许多 Amazon S3 对象的保留。您可以在清单中指定目标对象的列表并将该列表提交到分批操作以完成操作。有关更多信息，请参阅the section called “对象锁定保留”和the section called “对象锁定依法保留”。

以下示例说明如何创建具有 S3 批量操作权限的 Amazon Identity and Access Management（IAM）角色，并更新角色权限来包含 `s3:PutObjectRetention` 权限，以便您可以对清单存储桶中的对象运行 S3 对象锁定保留。还必须有一个 CSV 清单来标识 S3 批量操作任务的对象。有关更多信息，请参阅the section called “指定清单”。

要使用以下示例，请将 *user input placeholders* 替换为您自己的信息。

### 使用 Amazon CLI

以下 Amazon CLI 示例说明如何使用批量操作跨多个对象应用 S3 对象锁定保留。

```
export AWS_PROFILE='aws-user'

read -d '' retention_permissions <<EOF
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObjectRetention"
            ],
            "Resource": [
                "arn:aws:s3:::{{amzn-s3-demo-manifest-bucket}}/*"
```

```
            ]
        }
    ]
}
EOF

aws iam put-role-policy --role-name batch_operations-objectlock --policy-
name retention-permissions --policy-document "${retention_permissions}"
```

使用适用于 Java 的 Amazon SDK

以下适用于 Java 的 Amazon SDK 示例说明如何使用批量操作跨多个对象应用 S3 对象锁定保留。

```
public void allowPutObjectRetention() {
    final String roleName = "batch_operations-object-lock";

    final String retentionPermissions = "{" +
            "    \"Version\": \"2012-10-17\"," +
            "    \"Statement\": [" +
            "        {" +
            "            \"Effect\": \"Allow\"," +
            "            \"Action\": [" +
            "                \"s3:PutObjectRetention\"" +
            "            ]," +
            "            \"Resource\": [" +
            "                \"arn:aws:s3:::amzn-s3-demo-manifest-bucket*\"" +
            "            ]" +
            "        }" +
            "    ]" +
            "}";

    final AmazonIdentityManagement iam =
            AmazonIdentityManagementClientBuilder.defaultClient();

    final PutRolePolicyRequest putRolePolicyRequest = new PutRolePolicyRequest()
            .withPolicyDocument(retentionPermissions)
            .withPolicyName("retention-permissions")
            .withRoleName(roleName);

    final PutRolePolicyResult putRolePolicyResult =
 iam.putRolePolicy(putRolePolicyRequest);
}
```

## 将 S3 分批操作与 S3 对象锁定保留合规模式结合使用

以下示例基于上述创建信任策略以及在对象上设置 S3 分批操作和 S3 对象锁定配置权限的示例而构建。此示例将保留模式设置为 COMPLIANCE，并将 retain until date 设置为 2025 年 1 月 1 日。此示例将创建一个任务，该任务以清单存储桶中的对象为目标，并在您标识的报告存储桶中报告结果。

要使用以下示例，请将 *user input placeholders* 替换为您自己的信息。

使用 Amazon CLI

以下 Amazon CLI 示例说明如何使用批量操作跨多个对象应用 S3 对象锁定保留合规模式。

Example — 跨多个对象设置 S3 对象锁定保留合规模式

```
export AWS_PROFILE='aws-user'
export AWS_DEFAULT_REGION='us-west-2'
export ACCOUNT_ID=123456789012
export ROLE_ARN='arn:aws:iam::123456789012:role/batch_operations-objectlock'

read -d '' OPERATION <<EOF
{
  "S3PutObjectRetention": {
    "Retention": {
      "RetainUntilDate":"2025-01-01T00:00:00",
      "Mode":"COMPLIANCE"
    }
  }
}
EOF

read -d '' MANIFEST <<EOF
{
  "Spec": {
    "Format": "S3BatchOperations_CSV_20180820",
    "Fields": [
      "Bucket",
      "Key"
    ]
  },
  "Location": {
    "ObjectArn": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/compliance-objects-
manifest.csv",
    "ETag": "Your-manifest-ETag"
```

```
  }
}
EOF

read -d '' REPORT <<EOF
{
  "Bucket": "arn:aws:s3:::ReportBucket",
  "Format": "Report_CSV_20180820",
  "Enabled": true,
  "Prefix": "amzn-s3-demo-completion-report-bucket/compliance-objects-batch-
operations",
  "ReportScope": "AllTasks"
}
EOF

aws \
    s3control create-job \
    --account-id "${ACCOUNT_ID}" \
    --manifest "${MANIFEST//$'\n'}" \
    --operation "${OPERATION//$'\n'/}" \
    --report "${REPORT//$'\n'}" \
    --priority 10 \
    --role-arn "${ROLE_ARN}" \
    --client-request-token "$(uuidgen)" \
    --region "${AWS_DEFAULT_REGION}" \
    --description "Set compliance retain-until to 1 Jul 2030";
```

Example — 将 **COMPLIANCE** 模式的 **retain until date** 延长至 2025 年 1 月 15 日

以下示例将 COMPLIANCE 模式的 `retain until date` 延长至 2025 年 1 月 15 日。

```
export AWS_PROFILE='aws-user'
export AWS_DEFAULT_REGION='us-west-2'
export ACCOUNT_ID=123456789012
export ROLE_ARN='arn:aws:iam::123456789012:role/batch_operations-objectlock'

read -d '' OPERATION <<EOF
{
  "S3PutObjectRetention": {
    "Retention": {
      "RetainUntilDate":"2025-01-15T00:00:00",
      "Mode":"COMPLIANCE"
    }
  }
```

```
}
EOF

read -d '' MANIFEST <<EOF
{
  "Spec": {
    "Format": "S3BatchOperations_CSV_20180820",
    "Fields": [
      "Bucket",
      "Key"
    ]
  },
  "Location": {
    "ObjectArn": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/compliance-objects-
manifest.csv",
    "ETag": "Your-manifest-ETag"
  }
}
EOF

read -d '' REPORT <<EOF
{
  "Bucket": "arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
  "Format": "Report_CSV_20180820",
  "Enabled": true,
  "Prefix": "reports/compliance-objects-batch_operations",
  "ReportScope": "AllTasks"
}
EOF

aws \
    s3control create-job \
    --account-id "${ACCOUNT_ID}" \
    --manifest "${MANIFEST//$'\n'}" \
    --operation "${OPERATION//$'\n'/}" \
    --report "${REPORT//$'\n'}" \
    --priority 10 \
    --role-arn "${ROLE_ARN}" \
    --client-request-token "$(uuidgen)" \
    --region "${AWS_DEFAULT_REGION}" \
    --description "Extend compliance retention to 15 Jan 2025";
```

使用适用于 Java 的 Amazon 开发工具包

以下 适用于 Java 的 Amazon SDK 示例说明如何使用批量操作跨多个对象应用 S3 对象锁定保留合规模式。

Example — 将保留模式设置为 COMPLIANCE（合规），并将“保留到期日”设置为 2025 年 1 月 1 日

```
public String createComplianceRetentionJob(final AWSS3ControlClient awss3ControlClient)
 throws ParseException {
    final String manifestObjectArn = "arn:aws:s3:::amzn-s3-demo-manifest-bucket/
compliance-objects-manifest.csv";
    final String manifestObjectVersionId = "your-object-version-Id";

    final JobManifestLocation manifestLocation = new JobManifestLocation()
            .withObjectArn(manifestObjectArn)
            .withETag(manifestObjectVersionId);

    final JobManifestSpec manifestSpec =
            new JobManifestSpec()
                    .withFormat(JobManifestFormat.S3BatchOperations_CSV_20180820)
                    .withFields("Bucket", "Key");

    final JobManifest manifestToPublicApi = new JobManifest()
            .withLocation(manifestLocation)
            .withSpec(manifestSpec);

    final String jobReportBucketArn = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
    final String jobReportPrefix = "reports/compliance-objects-bops";

    final JobReport jobReport = new JobReport()
            .withEnabled(true)
            .withReportScope(JobReportScope.AllTasks)
            .withBucket(jobReportBucketArn)
            .withPrefix(jobReportPrefix)
            .withFormat(JobReportFormat.Report_CSV_20180820);

    final SimpleDateFormat format = new SimpleDateFormat("dd/MM/yyyy");
    final Date janFirst = format.parse("01/01/2025");

    final JobOperation jobOperation = new JobOperation()
            .withS3PutObjectRetention(new S3SetObjectRetentionOperation()
                    .withRetention(new S3Retention()
                            .withMode(S3ObjectLockRetentionMode.COMPLIANCE)
```

```
                            .withRetainUntilDate(janFirst)));

    final String roleArn = "arn:aws:iam::123456789012:role/batch_operations-object-
lock";
    final Boolean requiresConfirmation = true;
    final int priority = 10;

    final CreateJobRequest request = new CreateJobRequest()
            .withAccountId("123456789012")
            .withDescription("Set compliance retain-until to 1 Jan 2025")
            .withManifest(manifestToPublicApi)
            .withOperation(jobOperation)
            .withPriority(priority)
            .withRoleArn(roleArn)
            .withReport(jobReport)
            .withConfirmationRequired(requiresConfirmation);

    final CreateJobResult result = awss3ControlClient.createJob(request);

    return result.getJobId();
}
```

Example — 延长 **COMPLIANCE** 模式的 **retain until date**

以下示例将 COMPLIANCE 模式的 `retain until date` 延长至 2025 年 1 月 15 日。

```
public String createExtendComplianceRetentionJob(final AWSS3ControlClient
 awss3ControlClient) throws ParseException {
    final String manifestObjectArn = "arn:aws:s3:::amzn-s3-demo-manifest-bucket/
compliance-objects-manifest.csv";
    final String manifestObjectVersionId = "15ad5ba069e6bbc465c77bf83d541385";

    final JobManifestLocation manifestLocation = new JobManifestLocation()
            .withObjectArn(manifestObjectArn)
            .withETag(manifestObjectVersionId);

    final JobManifestSpec manifestSpec =
            new JobManifestSpec()
                    .withFormat(JobManifestFormat.S3BatchOperations_CSV_20180820)
                    .withFields("Bucket", "Key");

    final JobManifest manifestToPublicApi = new JobManifest()
            .withLocation(manifestLocation)
            .withSpec(manifestSpec);
```

```
    final String jobReportBucketArn = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
    final String jobReportPrefix = "reports/compliance-objects-batch_operations";

    final JobReport jobReport = new JobReport()
            .withEnabled(true)
            .withReportScope(JobReportScope.AllTasks)
            .withBucket(jobReportBucketArn)
            .withPrefix(jobReportPrefix)
            .withFormat(JobReportFormat.Report_CSV_20180820);

    final SimpleDateFormat format = new SimpleDateFormat("dd/MM/yyyy");
    final Date jan15th = format.parse("15/01/2025");

    final JobOperation jobOperation = new JobOperation()
            .withS3PutObjectRetention(new S3SetObjectRetentionOperation()
                    .withRetention(new S3Retention()
                            .withMode(S3ObjectLockRetentionMode.COMPLIANCE)
                            .withRetainUntilDate(jan15th)));

    final String roleArn = "arn:aws:iam::123456789012:role/batch_operations-object-
lock";
    final Boolean requiresConfirmation = true;
    final int priority = 10;

    final CreateJobRequest request = new CreateJobRequest()
            .withAccountId("123456789012")
            .withDescription("Extend compliance retention to 15 Jan 2025")
            .withManifest(manifestToPublicApi)
            .withOperation(jobOperation)
            .withPriority(priority)
            .withRoleArn(roleArn)
            .withReport(jobReport)
            .withConfirmationRequired(requiresConfirmation);

    final CreateJobResult result = awss3ControlClient.createJob(request);

    return result.getJobId();
}
```

## 将 S3 分批操作与 S3 对象锁定保留监管模式结合使用

以下示例基于上述创建信任策略以及设置 S3 分批操作和 S3 对象锁定配置权限的示例而构建。本示例说明如何跨多个对象应用 S3 对象锁定保留监管，retain until date 为 2025 年 1 月 30 日。它会创建一个分批操作任务，该任务使用清单存储桶，并在报告存储桶中报告结果。

要使用以下示例，请将 *user input placeholders* 替换为您自己的信息。

使用 Amazon CLI

以下 Amazon CLI 示例说明如何使用批量操作跨多个对象应用 S3 对象锁定保留监管模式。

Example — 跨多个对象应用 S3 对象锁定保留监管，“保留到期日”为 2025 年 1 月 30 日

```
export AWS_PROFILE='aws-user'
export AWS_DEFAULT_REGION='us-west-2'
export ACCOUNT_ID=123456789012
export ROLE_ARN='arn:aws:iam::123456789012:role/batch_operations-objectlock'

read -d '' OPERATION <<EOF
{
  "S3PutObjectRetention": {
    "Retention": {
      "RetainUntilDate":"2025-01-30T00:00:00",
      "Mode":"GOVERNANCE"
    }
  }
}
EOF

read -d '' MANIFEST <<EOF
{
  "Spec": {
    "Format": "S3BatchOperations_CSV_20180820",
    "Fields": [
      "Bucket",
      "Key"
    ]
  },
  "Location": {
    "ObjectArn": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/governance-objects-
manifest.csv",
    "ETag": "Your-manifest-ETag"
  }
```

```
}
EOF

read -d '' REPORT <<EOF
{
  "Bucket": "arn:aws:s3:::amzn-s3-demo-completion-report-bucketT",
  "Format": "Report_CSV_20180820",
  "Enabled": true,
  "Prefix": "reports/governance-objects",
  "ReportScope": "AllTasks"
}
EOF

aws \
    s3control create-job \
    --account-id "${ACCOUNT_ID}" \
    --manifest "${MANIFEST//$'\n'}" \
    --operation "${OPERATION//$'\n'/}" \
    --report "${REPORT//$'\n'}" \
    --priority 10 \
    --role-arn "${ROLE_ARN}" \
    --client-request-token "$(uuidgen)" \
    --region "${AWS_DEFAULT_REGION}" \
    --description "Put governance retention";
```

Example — 跨多个对象绕过保留监管

以下示例基于上述创建信任策略以及设置 S3 分批操作和 S3 对象锁定配置权限的示例而构建。它说明如何绕过跨多个对象的保留监管，并创建一个分批操作任务，该任务使用清单存储桶并在报告存储桶中报告结果。

```
export AWS_PROFILE='aws-user'

read -d '' bypass_governance_permissions <<EOF
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:BypassGovernanceRetention"
            ],
            "Resource": [
```

```
                "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
            ]
        }
    ]
}
EOF

aws iam put-role-policy --role-name batch-operations-objectlock --policy-name bypass-
governance-permissions --policy-document "${bypass_governance_permissions}"

export AWS_PROFILE='aws-user'
export AWS_DEFAULT_REGION='us-west-2'
export ACCOUNT_ID=123456789012
export ROLE_ARN='arn:aws:iam::123456789012:role/batch_operations-objectlock'

read -d '' OPERATION <<EOF
{
  "S3PutObjectRetention": {
    "BypassGovernanceRetention": true,
    "Retention": {
    }
  }
}
EOF

read -d '' MANIFEST <<EOF
{
  "Spec": {
    "Format": "S3BatchOperations_CSV_20180820",
    "Fields": [
      "Bucket",
      "Key"
    ]
  },
  "Location": {
    "ObjectArn": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/governance-objects-
manifest.csv",
    "ETag": "Your-manifest-ETag"
  }
}
EOF

read -d '' REPORT <<EOF
{
```

```
  "Bucket": "arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
  "Format": "Report_CSV_20180820",
  "Enabled": true,
  "Prefix": "reports/batch_operations-governance",
  "ReportScope": "AllTasks"
}
EOF

aws \
    s3control create-job \
    --account-id "${ACCOUNT_ID}" \
    --manifest "${MANIFEST//$'\n'}" \
    --operation "${OPERATION//$'\n'/}" \
    --report "${REPORT//$'\n'}" \
    --priority 10 \
    --role-arn "${ROLE_ARN}" \
    --client-request-token "$(uuidgen)" \
    --region "${AWS_DEFAULT_REGION}" \
    --description "Remove governance retention";
```

使用适用于 Java 的 Amazon 开发工具包

以下示例基于上述创建信任策略以及设置 S3 分批操作和 S3 对象锁定配置权限的示例而构建。本示例说明如何跨多个对象应用 S3 对象锁定保留监管，retain until date 设置为 2025 年 1 月 30 日。本示例会创建一个批量操作任务，该任务使用清单存储桶，并在报告存储桶中报告结果。

Example — 跨多个对象应用 S3 对象锁定保留监管，“保留到期日”为 2025 年 1 月 30 日

```
public String createGovernanceRetentionJob(final AWSS3ControlClient awss3ControlClient)
 throws ParseException {
    final String manifestObjectArn = "arn:aws:s3:::amzn-s3-demo-manifest-bucket/
governance-objects-manifest.csv";
    final String manifestObjectVersionId = "15ad5ba069e6bbc465c77bf83d541385";

    final JobManifestLocation manifestLocation = new JobManifestLocation()
            .withObjectArn(manifestObjectArn)
            .withETag(manifestObjectVersionId);

    final JobManifestSpec manifestSpec =
            new JobManifestSpec()
                    .withFormat(JobManifestFormat.S3BatchOperations_CSV_20180820)
                    .withFields("Bucket", "Key");
```

```
    final JobManifest manifestToPublicApi = new JobManifest()
            .withLocation(manifestLocation)
            .withSpec(manifestSpec);

    final String jobReportBucketArn = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
    final String jobReportPrefix = "reports/governance-objects";

    final JobReport jobReport = new JobReport()
            .withEnabled(true)
            .withReportScope(JobReportScope.AllTasks)
            .withBucket(jobReportBucketArn)
            .withPrefix(jobReportPrefix)
            .withFormat(JobReportFormat.Report_CSV_20180820);

    final SimpleDateFormat format = new SimpleDateFormat("dd/MM/yyyy");
    final Date jan30th = format.parse("30/01/2025");

    final JobOperation jobOperation = new JobOperation()
            .withS3PutObjectRetention(new S3SetObjectRetentionOperation()
                    .withRetention(new S3Retention()
                            .withMode(S3ObjectLockRetentionMode.GOVERNANCE)
                            .withRetainUntilDate(jan30th)));

    final String roleArn = "arn:aws:iam::123456789012:role/batch_operations-object-
lock";
    final Boolean requiresConfirmation = true;
    final int priority = 10;

    final CreateJobRequest request = new CreateJobRequest()
            .withAccountId("123456789012")
            .withDescription("Put governance retention")
            .withManifest(manifestToPublicApi)
            .withOperation(jobOperation)
            .withPriority(priority)
            .withRoleArn(roleArn)
            .withReport(jobReport)
            .withConfirmationRequired(requiresConfirmation);

    final CreateJobResult result = awss3ControlClient.createJob(request);

    return result.getJobId();
}
```

### Example — 跨多个对象绕过保留监管

以下示例基于上述创建信任策略以及设置 S3 分批操作和 S3 对象锁定配置权限的示例而构建。本示例说明如何跨多个对象绕过保留监管，并创建一个批量操作任务，该任务使用清单存储桶并在报告存储桶中报告结果。

```
public void allowBypassGovernance() {
    final String roleName = "batch_operations-object-lock";

    final String bypassGovernancePermissions = "{" +
            "    \"Version\": \"2012-10-17\"," +
            "    \"Statement\": [" +
            "        {" +
            "            \"Effect\": \"Allow\"," +
            "            \"Action\": [" +
            "                \"s3:BypassGovernanceRetention\"" +
            "            ]," +
            "            \"Resource\": [" +
            "                \"arn:aws:s3:::amzn-s3-demo-manifest-bucket/*\"" +
            "            ]" +
            "        }" +
            "    ]" +
            "}";

    final AmazonIdentityManagement iam =
            AmazonIdentityManagementClientBuilder.defaultClient();

    final PutRolePolicyRequest putRolePolicyRequest = new PutRolePolicyRequest()
            .withPolicyDocument(bypassGovernancePermissions)
            .withPolicyName("bypass-governance-permissions")
            .withRoleName(roleName);

    final PutRolePolicyResult putRolePolicyResult =
 iam.putRolePolicy(putRolePolicyRequest);
}
public String createRemoveGovernanceRetentionJob(final AWSS3ControlClient
 awss3ControlClient) {
    final String manifestObjectArn = "arn:aws:s3:::amzn-s3-demo-manifest-bucket/
governance-objects-manifest.csv";
    final String manifestObjectVersionId = "15ad5ba069e6bbc465c77bf83d541385";

    final JobManifestLocation manifestLocation = new JobManifestLocation()
            .withObjectArn(manifestObjectArn)
```

```
            .withETag(manifestObjectVersionId);

    final JobManifestSpec manifestSpec =
            new JobManifestSpec()
                    .withFormat(JobManifestFormat.S3BatchOperations_CSV_20180820)
                    .withFields("Bucket", "Key");

    final JobManifest manifestToPublicApi = new JobManifest()
            .withLocation(manifestLocation)
            .withSpec(manifestSpec);

    final String jobReportBucketArn = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
    final String jobReportPrefix = "reports/batch_operations-governance";

    final JobReport jobReport = new JobReport()
            .withEnabled(true)
            .withReportScope(JobReportScope.AllTasks)
            .withBucket(jobReportBucketArn)
            .withPrefix(jobReportPrefix)
            .withFormat(JobReportFormat.Report_CSV_20180820);

    final JobOperation jobOperation = new JobOperation()
            .withS3PutObjectRetention(new S3SetObjectRetentionOperation()
                    .withRetention(new S3Retention()));

    final String roleArn = "arn:aws:iam::123456789012:role/batch_operations-object-
lock";
    final Boolean requiresConfirmation = true;
    final int priority = 10;

    final CreateJobRequest request = new CreateJobRequest()
            .withAccountId("123456789012")
            .withDescription("Remove governance retention")
            .withManifest(manifestToPublicApi)
            .withOperation(jobOperation)
            .withPriority(priority)
            .withRoleArn(roleArn)
            .withReport(jobReport)
            .withConfirmationRequired(requiresConfirmation);

    final CreateJobResult result = awss3ControlClient.createJob(request);

    return result.getJobId();
```

```
}
```

## 使用 S3 批量操作关闭 S3 对象锁定法定保留

以下示例基于上述创建信任策略以及设置 S3 分批操作和 S3 对象锁定配置权限的示例而构建。本示例说明如何使用批量操作在对象上禁用对象锁定法定保留。

在该示例中，首先更新角色以授予 `s3:PutObjectLegalHold` 权限，再创建一个分批操作任务（该任务从清单中标识的对象中禁用（删除）依法保留，然后报告此情况）。

要使用以下示例，请将 *`user input placeholders`* 替换为您自己的信息。

使用 Amazon CLI

以下 Amazon CLI 示例说明如何使用批量操作跨多个对象关闭 S3 对象锁定法定保留。

Example — 更新角色以授予 **`s3:PutObjectLegalHold`** 权限

```
export AWS_PROFILE='aws-user'

read -d '' legal_hold_permissions <<EOF
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObjectLegalHold"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
            ]
        }
    ]

EOF

aws iam put-role-policy --role-name batch_operations-objectlock --policy-name legal-
hold-permissions --policy-document "${legal_hold_permissions}"
```

Example — 关闭法定保留

以下示例禁用了依法保留。

```
export AWS_PROFILE='aws-user'
export AWS_DEFAULT_REGION='us-west-2'
export ACCOUNT_ID=123456789012
export ROLE_ARN='arn:aws:iam::123456789012:role/batch_operations-objectlock'

read -d '' OPERATION <<EOF
{
  "S3PutObjectLegalHold": {
    "LegalHold": {
      "Status":"OFF"
    }
  }
}
EOF

read -d '' MANIFEST <<EOF
{
  "Spec": {
    "Format": "S3BatchOperations_CSV_20180820",
    "Fields": [
      "Bucket",
      "Key"
    ]
  },
  "Location": {
    "ObjectArn": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/legalhold-object-
manifest.csv",
    "ETag": "Your-manifest-ETag"
  }
}
EOF

read -d '' REPORT <<EOF
{
  "Bucket": "arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
  "Format": "Report_CSV_20180820",
  "Enabled": true,
  "Prefix": "reports/legalhold-objects-batch_operations",
  "ReportScope": "AllTasks"
}
EOF

aws \
```

```
    s3control create-job \
    --account-id "${ACCOUNT_ID}" \
    --manifest "${MANIFEST//$'\n'}" \
    --operation "${OPERATION//$'\n'/}" \
    --report "${REPORT//$'\n'}" \
    --priority 10 \
    --role-arn "${ROLE_ARN}" \
    --client-request-token "$(uuidgen)" \
    --region "${AWS_DEFAULT_REGION}" \
    --description "Turn off legal hold";
```

使用适用于 Java 的 Amazon 开发工具包

以下 适用于 Java 的 Amazon SDK 示例说明如何使用批量操作跨多个对象关闭 S3 对象锁定法定保留。

Example — 更新角色以授予 **s3:PutObjectLegalHold** 权限

```
public void allowPutObjectLegalHold() {
    final String roleName = "batch_operations-object-lock";

    final String legalHoldPermissions = "{" +
            "    \"Version\": \"2012-10-17\"," +
            "    \"Statement\": [" +
            "        {" +
            "            \"Effect\": \"Allow\"," +
            "            \"Action\": [" +
            "                \"s3:PutObjectLegalHold\"" +
            "            ]," +
            "            \"Resource\": [" +
            "                \"arn:aws:s3:::amzn-s3-demo-manifest-bucket/*\"" +
            "            ]" +
            "        }" +
            "    ]" +
            "}";

    final AmazonIdentityManagement iam =
            AmazonIdentityManagementClientBuilder.defaultClient();

    final PutRolePolicyRequest putRolePolicyRequest = new PutRolePolicyRequest()
            .withPolicyDocument(legalHoldPermissions)
            .withPolicyName("legal-hold-permissions")
            .withRoleName(roleName);
```

```
    final PutRolePolicyResult putRolePolicyResult =
 iam.putRolePolicy(putRolePolicyRequest);
}
```

### Example — 关闭法定保留

如果要禁用依法保留，请使用以下示例。

```
public String createLegalHoldOffJob(final AWSS3ControlClient awss3ControlClient) {
    final String manifestObjectArn = "arn:aws:s3:::amzn-s3-demo-manifest-bucket/
legalhold-object-manifest.csv";
    final String manifestObjectVersionId = "15ad5ba069e6bbc465c77bf83d541385";

    final JobManifestLocation manifestLocation = new JobManifestLocation()
            .withObjectArn(manifestObjectArn)
            .withETag(manifestObjectVersionId);

    final JobManifestSpec manifestSpec =
            new JobManifestSpec()
                    .withFormat(JobManifestFormat.S3BatchOperations_CSV_20180820)
                    .withFields("Bucket", "Key");

    final JobManifest manifestToPublicApi = new JobManifest()
            .withLocation(manifestLocation)
            .withSpec(manifestSpec);

    final String jobReportBucketArn = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
    final String jobReportPrefix = "reports/legalhold-objects-batch_operations";

    final JobReport jobReport = new JobReport()
            .withEnabled(true)
            .withReportScope(JobReportScope.AllTasks)
            .withBucket(jobReportBucketArn)
            .withPrefix(jobReportPrefix)
            .withFormat(JobReportFormat.Report_CSV_20180820);

    final JobOperation jobOperation = new JobOperation()
            .withS3PutObjectLegalHold(new S3SetObjectLegalHoldOperation()
                    .withLegalHold(new S3ObjectLockLegalHold()
                            .withStatus(S3ObjectLockLegalHoldStatus.OFF)));
```

```
    final String roleArn = "arn:aws:iam::123456789012:role/batch_operations-object-
lock";
    final Boolean requiresConfirmation = true;
    final int priority = 10;

    final CreateJobRequest request = new CreateJobRequest()
            .withAccountId("123456789012")
            .withDescription("Turn off legal hold")
            .withManifest(manifestToPublicApi)
            .withOperation(jobOperation)
            .withPriority(priority)
            .withRoleArn(roleArn)
            .withReport(jobReport)
            .withConfirmationRequired(requiresConfirmation);

    final CreateJobResult result = awss3ControlClient.createJob(request);

    return result.getJobId();
}
```

## 教程：使用 S3 批量操作对视频进行批量转码

视频消费者使用各种形状、尺寸和年份的设备来享受媒体内容。这种广泛的设备类型给内容创作者和转发者带来了挑战。视频不是一刀切的格式，而是必须进行转换，以便涵盖各种尺寸、格式和比特率。如果大量必须转换的视频，这一转换任务就更具挑战性。

Amazon 为您提供了构建可扩展的分布式架构的方法，该架构可执行以下操作：

- 摄取输入视频
- 处理视频以便在各种设备上播放
- 存储转码的媒体文件
- 交付输出媒体文件以满足需求

如果在 Amazon S3 中存储了大量的视频存储库，您可以将这些视频从源格式转换为多种文件类型，按照特定视频播放器或设备所需的大小、分辨率和格式转换为多种文件类型。具体来说，S3 批量操作为您提供了一个可以为 S3 源存储桶中的现有输入视频调用 Amazon Lambda 函数的解决方案。然后，Lambda 函数调用 AWS Elemental MediaConvert 来执行大规模视频转码任务。转换后的输出媒体文件存储在 S3 目标存储桶中。

目标

在本教程中，您将了解如何将 S3 批量操作设置为调用 Lambda 函数对存储在 S3 源存储桶中的视频进行批量转码。Lambda 函数调用 MediaConvert 转码视频。S3 源存储桶中每个视频的输出如下所示：

- HTTP 实时流 (HLS) 自适应比特率流，用于在多个大小的设备和不同的带宽上播放。
- MP4 视频文件
- 按间隔收集的缩略图图像

主题


- 先决条件
- 步骤 1：为输出媒体文件创建 S3 存储桶
- 步骤 2：为 MediaConvert 创建 IAM 角色
- 步骤 3：为您的 Lambda 函数创建 IAM 角色
- 步骤 4：创建 Lambda 函数以进行视频转码
- 步骤 5：为 S3 源存储桶配置 Amazon S3 清单
- 步骤 6：为 S3 批量操作创建 IAM 角色
- 步骤 7：设置并运行 S3 批量操作任务
- 步骤 8：检查 S3 目标存储桶中的输出媒体文件
- 步骤 9：清除
- 后续步骤


## 先决条件

在开始本教程之前，您必须有储存要转码视频的 Amazon S3 源存储桶（例如，*amzn-s3-demo-source-bucket*）。

如果愿意，您可以重新命名存储桶。有关 Amazon S3 存储桶名称的更多信息，请参阅 通用存储桶命名规则。

对于 S3 源存储桶，请保留阻止此存储桶的公有访问设置为默认值（已启用阻止全部公共访问）。有关更多信息，请参阅 创建通用存储桶。

有关将视频上传到 S3 源存储桶的详细信息，请参阅 上传对象。如果将许多大型视频文件上传到 S3 时，您还可以使用 Amazon S3 Transfer Acceleration 配置快速安全的文件传输。Transfer Acceleration 可以加快视频上传到 S3 存储桶的速度，以便远距离传输较大的视频。有关更多信息，请参阅 使用 Amazon S3 Transfer Acceleration 配置快速、安全的文件传输。

## 步骤 1：为输出媒体文件创建 S3 存储桶

在此步骤中，您将创建一个 S3 目标存储桶来存储转换后的输出媒体文件。您还可以创建跨源资源共享（CORS）配置，允许跨源访问存储在 S3 目标存储桶中的转码媒体文件。

分步

- 为输出媒体文件创建存储桶。
- 将 CORS 配置添加到 S3 输出存储桶

为输出媒体文件创建存储桶。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 选择创建存储桶。
4. 对于 Bucket Name（存储桶名称），输入您的存储桶的名称（例如 *amzn-s3-demo-destination-bucket1*）。
5. 对于 Region（区域），选择要放置桶的位置 Amazon Web Services 区域。
6. 要确保公众访问输出媒体文件，请在阻止此存储桶的公有访问设置，清除阻止全部公有访问权限。

   > **Warning**
   >
   > 在完成此步骤之前，请查看 阻止对您的 Amazon S3 存储的公有访问，以确保您了解并接受允许进行公有访问所涉及的风险。当您关闭屏蔽公共访问权限设置以使您的存储桶变为公有时，Internet 上的任何人都可以访问您的存储桶。我们建议您阻止对存储桶的所有公有访问。
   >
   > 如果您不想清除“屏蔽公共访问权限”设置，可以使用 Amazon CloudFront 将转码的媒体文件传送给查看者（最终用户）。有关更多信息，请参阅 教程：使用 Amazon S3、Amazon CloudFront 和 Amazon Route 53 托管点播流视频。

7. 选择旁边的复选框，我确认当前设置可能会导致此存储桶及其中的对象变为公有。
8. 对于其余设置，保留默认值。
9. 选择 Create bucket（创建存储桶）。

### 将 CORS 配置添加到 S3 输出存储桶

JSON CORS 配置定义了在一个域中加载的客户端 Web 应用程序（此处上下文的视频播放器）在另一个域中播放转码后的输出媒体文件的方式。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Buckets（存储桶）。
3. 在 Buckets（存储桶）列表中，选择之前创建的存储桶名称（例如，*amzn-s3-demo-destination-bucket1*）。
4. 选择 Permissions (权限) 选项卡。
5. 在 Cross-origin resource sharing（CORS）（跨源资源共享（CORS））部分中，请选择 Edit（编辑）。
6. 在 CORS 配置文本框中，复制并粘贴如下的 CORS 配置。

   CORS 配置必须采用 JSON 格式。在此示例中，`AllowedOrigins` 属性使用通配符 (*) 来指定所有来源。如果您知道您的特定来源，则可以限制 `AllowedOrigins` 属性添加到您的特定播放器 URL。有关配置此属性和其他属性的更多信息，请参阅 CORS 配置的元素。

   ```
   [
       {
           "AllowedOrigins": [
               "*"
           ],
           "AllowedMethods": [
               "GET"
           ],
           "AllowedHeaders": [
               "*"
           ],
           "ExposeHeaders": []

       }
   ]
   ```

7. 选择 Save changes (保存更改)。

## 步骤 2：为 MediaConvert 创建 IAM 角色

为了使用 AWS Elemental MediaConvert 转码存储在 S3 存储桶中的输入视频，您必须有一个 Amazon Identity and Access Management（IAM）服务角色以授予 MediaConvert 权限，以便从 S3 源存储桶读取视频文件以及向 S3 目标存储桶写入视频文件。当您运行转码任务时，MediaConvert 控制台会使用此角色。

为 MediaConvert 创建 IAM 角色

1. 使用您选择的角色名称创建 IAM 角色（例如，**`tutorial-mediaconvert-role`**）。要创建此角色，请按照《AWS Elemental MediaConvert 用户指南》的在 IAM（控制台）中创建您的 MediaConvert 角色中的步骤操作。
2. 为 MediaConvert 创建 IAM 角色之后，请在 Role (角色)列表中选择您为 MediaConvert 创建的角色的名称（例如，**`tutorial-mediaconvert-role`**）。
3. 在 Summary (摘要) 页面上，复制 Role ARN (角色 ARN) (从 `arn:aws:iam::` 开始) 并保存 ARN 以供稍后使用。

   有关 ARN 的更多信息，请参阅 Amazon 一般参考中的 Amazon Resource Name (ARN)。

## 步骤 3：为您的 Lambda 函数创建 IAM 角色

要使用 MediaConvert 和 S3 Batch 操作批量转码视频，您可使用 Lambda 函数来连接这两个服务来转换视频。此 Lambda 函数必须具有一个 IAM 角色，该角色可授予 Lambda 函数访问 MediaConvert 和 S3 Batch Operations 的权限。

分步

- 为 Lambda 函数创建 IAM 角色
- 为 Lambda 函数的 IAM 角色嵌入内联策略

为 Lambda 函数创建 IAM 角色

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在左侧导航窗格中，选择角色，然后选择创建角色。
3. 选择 Amazon 服务角色类型，然后在 Common use cases (常见用例)中，选择 Lambda。
4. 选择 Next: Permissions (下一步: 权限)。

5. 在 Attach permissions policies (附加权限策略) 页的 Filter policies (筛选策略) 框中输入 **AWSLambdaBasicExecutionRole**。若要附加托管策略 AWSLambdaBasicExecutionRole 至此角色，以向 Amazon CloudWatch Logs 授予写入权限，则应选中 AWSLambdaBasicExecutionRole 旁边的复选框。
6. 选择下一步。
7. 对于角色名称，输入 **tutorial-lambda-transcode-role**。
8. （可选）将标签添加到托管策略。
9. 选择 Create role (创建角色)。

为 Lambda 函数的 IAM 角色嵌入内联策略

您必须使用内联策略，方可向 Lambda 函数执行所需的 MediaConvert 资源授予权限。

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在左侧导航窗格中，选择 Roles（角色）。
3. 在 Roles (角色) 列表中，选择您在前面为 Lambda 函数创建的 IAM 角色的名称（例如，**tutorial-lambda-transcode-role**）。
4. 选择 Permissions (权限) 选项卡。
5. 选择 Add inline policy (添加内联策略)。
6. 选择 JSON 选项卡，然后复制并粘贴以下 JSON 策略。

   将在 JSON 策略中的示例 ARN 值 `Resource` 替换为您在步骤 2中为 MediaConvert 创建的 IAM 角色的角色 ARN（例如，**tutorial-mediaconvert-role**）。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "Logging"
```

```
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "arn:aws:iam::111122223333:role/tutorial-mediaconvert-role"
            ],
            "Effect": "Allow",
            "Sid": "PassRole"
        },
        {
            "Action": [
                "mediaconvert:*"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow",
            "Sid": "MediaConvertService"
        },
        {
            "Action": [
                "s3:*"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow",
            "Sid": "S3Service"
        }
    ]
}
```

7. 选择 Review Policy (查看策略)。
8. 对于 Name (名称)，请输入 **tutorial-lambda-policy**。
9. 选择 Create Policy (创建策略)。

   创建内联策略后，会自动嵌入您的 Lambda 函数 IAM 角色。

## 步骤 4：创建 Lambda 函数以进行视频转码

在本教程的此部分中，您使用适用于 Python 的 SDK 构建 Lambda 函数，以便与 S3 批量操作和 MediaConvert 集成。要开始对存储在 S3 源存储桶中的视频进行转码，您可运行 S3 Batch Operation，该任务直接为 S3 源存储桶中的每个视频调用 Lambda 函数。然后，Lambda 函数将每个视频的转码任务提交给 MediaConvert。

分步

- 编写 Lambda 函数代码并创建部署程序包
- 使用执行角色创建 Lambda 函数（控制台）
- 使用 .zip 文件归档部署 Lambda 函数并配置 Lambda 函数（控制台）

编写 Lambda 函数代码并创建部署程序包

1. 在您的本地计算机上，创建名为 `batch-transcode` 的文件夹。
2. 在 `batch-transcode` 文件夹中，创建具有 JSON 任务设置的文件。例如，您可以使用本部分中提供的设置并为文件指定名称 `job.json`。

   `job.json` 文件指定以下内容：

   - 要转码的文件
   - 您希望如何对输入的视频进行转码
   - 您希望创建何种输出媒体文件
   - 要为转码文件指定的名称
   - 在何处保存转码文件
   - 要应用的高级特征等。

   在本教程中，我们使用如下 `job.json` 文件为 S3 源存储桶中的每个视频创建以下输出：

   - HTTP 实时流 (HLS) 自适应比特率流，用于在多个大小的设备和不同的带宽上播放。
   - MP4 视频文件
   - 按间隔收集的缩略图图像

此示例 job.json 文件使用质量定义的可变比特率 (QVBR) 来优化视频质量。HTTP 实时流 (HLS) 输出符合苹果标准（从视频解除音频，6 秒的段持续时间，并通过自动 QVBR 优化视频质量）。

如果您不想使用此处提供的示例设置，可以基于您的使用案例生成 job.json 规范。要确保输出的一致性，请确保输入文件具有类似的视频和音频配置。对于具有不同视频和音频配置的任何输入文件，可创建单独的自动化（唯一的 job.json 设置）。有关更多信息，请参阅《AWS Elemental MediaConvert 用户指南》中的 JSON 格式的 AWS Elemental MediaConvert 任务设置示例。

```
{
  "OutputGroups": [
    {
      "CustomName": "HLS",
      "Name": "Apple HLS",
      "Outputs": [
        {
          "ContainerSettings": {
            "Container": "M3U8",
            "M3u8Settings": {
              "AudioFramesPerPes": 4,
              "PcrControl": "PCR_EVERY_PES_PACKET",
              "PmtPid": 480,
              "PrivateMetadataPid": 503,
              "ProgramNumber": 1,
              "PatInterval": 0,
              "PmtInterval": 0,
              "TimedMetadata": "NONE",
              "VideoPid": 481,
              "AudioPids": [
                482,
                483,
                484,
                485,
                486,
                487,
                488,
                489,
                490,
                491,
                492
```

```
            ]
          }
        },
        "VideoDescription": {
          "Width": 640,
          "ScalingBehavior": "DEFAULT",
          "Height": 360,
          "TimecodeInsertion": "DISABLED",
          "AntiAlias": "ENABLED",
          "Sharpness": 50,
          "CodecSettings": {
            "Codec": "H_264",
            "H264Settings": {
              "InterlaceMode": "PROGRESSIVE",
              "NumberReferenceFrames": 3,
              "Syntax": "DEFAULT",
              "Softness": 0,
              "GopClosedCadence": 1,
              "GopSize": 2,
              "Slices": 1,
              "GopBReference": "DISABLED",
              "MaxBitrate": 1200000,
              "SlowPal": "DISABLED",
              "SpatialAdaptiveQuantization": "ENABLED",
              "TemporalAdaptiveQuantization": "ENABLED",
              "FlickerAdaptiveQuantization": "DISABLED",
              "EntropyEncoding": "CABAC",
              "FramerateControl": "INITIALIZE_FROM_SOURCE",
              "RateControlMode": "QVBR",
              "CodecProfile": "MAIN",
              "Telecine": "NONE",
              "MinIInterval": 0,
              "AdaptiveQuantization": "HIGH",
              "CodecLevel": "AUTO",
              "FieldEncoding": "PAFF",
              "SceneChangeDetect": "TRANSITION_DETECTION",
              "QualityTuningLevel": "SINGLE_PASS_HQ",
              "FramerateConversionAlgorithm": "DUPLICATE_DROP",
              "UnregisteredSeiTimecode": "DISABLED",
              "GopSizeUnits": "SECONDS",
              "ParControl": "INITIALIZE_FROM_SOURCE",
              "NumberBFramesBetweenReferenceFrames": 2,
              "RepeatPps": "DISABLED"
            }
```

```
            },
            "AfdSignaling": "NONE",
            "DropFrameTimecode": "ENABLED",
            "RespondToAfd": "NONE",
            "ColorMetadata": "INSERT"
          },
          "OutputSettings": {
            "HlsSettings": {
              "AudioGroupId": "program_audio",
              "AudioRenditionSets": "program_audio",
              "SegmentModifier": "$dt$",
              "IFrameOnlyManifest": "EXCLUDE"
            }
          },
          "NameModifier": "_360"
        },
        {
          "ContainerSettings": {
            "Container": "M3U8",
            "M3u8Settings": {
              "AudioFramesPerPes": 4,
              "PcrControl": "PCR_EVERY_PES_PACKET",
              "PmtPid": 480,
              "PrivateMetadataPid": 503,
              "ProgramNumber": 1,
              "PatInterval": 0,
              "PmtInterval": 0,
              "TimedMetadata": "NONE",
              "TimedMetadataPid": 502,
              "VideoPid": 481,
              "AudioPids": [
                482,
                483,
                484,
                485,
                486,
                487,
                488,
                489,
                490,
                491,
                492
              ]
            }
```

```
            },
            "VideoDescription": {
              "Width": 960,
              "ScalingBehavior": "DEFAULT",
              "Height": 540,
              "TimecodeInsertion": "DISABLED",
              "AntiAlias": "ENABLED",
              "Sharpness": 50,
              "CodecSettings": {
                "Codec": "H_264",
                "H264Settings": {
                  "InterlaceMode": "PROGRESSIVE",
                  "NumberReferenceFrames": 3,
                  "Syntax": "DEFAULT",
                  "Softness": 0,
                  "GopClosedCadence": 1,
                  "GopSize": 2,
                  "Slices": 1,
                  "GopBReference": "DISABLED",
                  "MaxBitrate": 3500000,
                  "SlowPal": "DISABLED",
                  "SpatialAdaptiveQuantization": "ENABLED",
                  "TemporalAdaptiveQuantization": "ENABLED",
                  "FlickerAdaptiveQuantization": "DISABLED",
                  "EntropyEncoding": "CABAC",
                  "FramerateControl": "INITIALIZE_FROM_SOURCE",
                  "RateControlMode": "QVBR",
                  "CodecProfile": "MAIN",
                  "Telecine": "NONE",
                  "MinIInterval": 0,
                  "AdaptiveQuantization": "HIGH",
                  "CodecLevel": "AUTO",
                  "FieldEncoding": "PAFF",
                  "SceneChangeDetect": "TRANSITION_DETECTION",
                  "QualityTuningLevel": "SINGLE_PASS_HQ",
                  "FramerateConversionAlgorithm": "DUPLICATE_DROP",
                  "UnregisteredSeiTimecode": "DISABLED",
                  "GopSizeUnits": "SECONDS",
                  "ParControl": "INITIALIZE_FROM_SOURCE",
                  "NumberBFramesBetweenReferenceFrames": 2,
                  "RepeatPps": "DISABLED"
                }
              },
              "AfdSignaling": "NONE",
```

```
            "DropFrameTimecode": "ENABLED",
            "RespondToAfd": "NONE",
            "ColorMetadata": "INSERT"
          },
          "OutputSettings": {
            "HlsSettings": {
              "AudioGroupId": "program_audio",
              "AudioRenditionSets": "program_audio",
              "SegmentModifier": "$dt$",
              "IFrameOnlyManifest": "EXCLUDE"
            }
          },
          "NameModifier": "_540"
        },
        {
          "ContainerSettings": {
            "Container": "M3U8",
            "M3u8Settings": {
              "AudioFramesPerPes": 4,
              "PcrControl": "PCR_EVERY_PES_PACKET",
              "PmtPid": 480,
              "PrivateMetadataPid": 503,
              "ProgramNumber": 1,
              "PatInterval": 0,
              "PmtInterval": 0,
              "TimedMetadata": "NONE",
              "VideoPid": 481,
              "AudioPids": [
                482,
                483,
                484,
                485,
                486,
                487,
                488,
                489,
                490,
                491,
                492
              ]
            }
          },
          "VideoDescription": {
            "Width": 1280,
```

```
            "ScalingBehavior": "DEFAULT",
            "Height": 720,
            "TimecodeInsertion": "DISABLED",
            "AntiAlias": "ENABLED",
            "Sharpness": 50,
            "CodecSettings": {
              "Codec": "H_264",
              "H264Settings": {
                "InterlaceMode": "PROGRESSIVE",
                "NumberReferenceFrames": 3,
                "Syntax": "DEFAULT",
                "Softness": 0,
                "GopClosedCadence": 1,
                "GopSize": 2,
                "Slices": 1,
                "GopBReference": "DISABLED",
                "MaxBitrate": 5000000,
                "SlowPal": "DISABLED",
                "SpatialAdaptiveQuantization": "ENABLED",
                "TemporalAdaptiveQuantization": "ENABLED",
                "FlickerAdaptiveQuantization": "DISABLED",
                "EntropyEncoding": "CABAC",
                "FramerateControl": "INITIALIZE_FROM_SOURCE",
                "RateControlMode": "QVBR",
                "CodecProfile": "MAIN",
                "Telecine": "NONE",
                "MinIInterval": 0,
                "AdaptiveQuantization": "HIGH",
                "CodecLevel": "AUTO",
                "FieldEncoding": "PAFF",
                "SceneChangeDetect": "TRANSITION_DETECTION",
                "QualityTuningLevel": "SINGLE_PASS_HQ",
                "FramerateConversionAlgorithm": "DUPLICATE_DROP",
                "UnregisteredSeiTimecode": "DISABLED",
                "GopSizeUnits": "SECONDS",
                "ParControl": "INITIALIZE_FROM_SOURCE",
                "NumberBFramesBetweenReferenceFrames": 2,
                "RepeatPps": "DISABLED"
              }
            },
            "AfdSignaling": "NONE",
            "DropFrameTimecode": "ENABLED",
            "RespondToAfd": "NONE",
            "ColorMetadata": "INSERT"
```

```
          },
          "OutputSettings": {
            "HlsSettings": {
              "AudioGroupId": "program_audio",
              "AudioRenditionSets": "program_audio",
              "SegmentModifier": "$dt$",
              "IFrameOnlyManifest": "EXCLUDE"
            }
          },
          "NameModifier": "_720"
        },
        {
          "ContainerSettings": {
            "Container": "M3U8",
            "M3u8Settings": {}
          },
          "AudioDescriptions": [
            {
              "AudioSourceName": "Audio Selector 1",
              "CodecSettings": {
                "Codec": "AAC",
                "AacSettings": {
                  "Bitrate": 96000,
                  "CodingMode": "CODING_MODE_2_0",
                  "SampleRate": 48000
                }
              }
            }
          ],
          "OutputSettings": {
            "HlsSettings": {
              "AudioGroupId": "program_audio",
              "AudioTrackType": "ALTERNATE_AUDIO_AUTO_SELECT_DEFAULT"
            }
          },
          "NameModifier": "_audio"
        }
      ],
      "OutputGroupSettings": {
        "Type": "HLS_GROUP_SETTINGS",
        "HlsGroupSettings": {
          "ManifestDurationFormat": "INTEGER",
          "SegmentLength": 6,
          "TimedMetadataId3Period": 10,
```

```
          "CaptionLanguageSetting": "OMIT",
          "Destination": "s3://EXAMPLE-BUCKET/HLS/",
          "DestinationSettings": {
            "S3Settings": {
              "AccessControl": {
                "CannedAcl": "PUBLIC_READ"
              }
            }
          },
          "TimedMetadataId3Frame": "PRIV",
          "CodecSpecification": "RFC_4281",
          "OutputSelection": "MANIFESTS_AND_SEGMENTS",
          "ProgramDateTimePeriod": 600,
          "MinSegmentLength": 0,
          "DirectoryStructure": "SINGLE_DIRECTORY",
          "ProgramDateTime": "EXCLUDE",
          "SegmentControl": "SEGMENTED_FILES",
          "ManifestCompression": "NONE",
          "ClientCache": "ENABLED",
          "StreamInfResolution": "INCLUDE"
        }
      }
    },
    {
      "CustomName": "MP4",
      "Name": "File Group",
      "Outputs": [
        {
          "ContainerSettings": {
            "Container": "MP4",
            "Mp4Settings": {
              "CslgAtom": "INCLUDE",
              "FreeSpaceBox": "EXCLUDE",
              "MoovPlacement": "PROGRESSIVE_DOWNLOAD"
            }
          },
          "VideoDescription": {
            "Width": 1280,
            "ScalingBehavior": "DEFAULT",
            "Height": 720,
            "TimecodeInsertion": "DISABLED",
            "AntiAlias": "ENABLED",
            "Sharpness": 100,
            "CodecSettings": {
```

```
            "Codec": "H_264",
            "H264Settings": {
              "InterlaceMode": "PROGRESSIVE",
              "ParNumerator": 1,
              "NumberReferenceFrames": 3,
              "Syntax": "DEFAULT",
              "Softness": 0,
              "GopClosedCadence": 1,
              "HrdBufferInitialFillPercentage": 90,
              "GopSize": 2,
              "Slices": 2,
              "GopBReference": "ENABLED",
              "HrdBufferSize": 10000000,
              "MaxBitrate": 5000000,
              "ParDenominator": 1,
              "EntropyEncoding": "CABAC",
              "RateControlMode": "QVBR",
              "CodecProfile": "HIGH",
              "MinIInterval": 0,
              "AdaptiveQuantization": "AUTO",
              "CodecLevel": "AUTO",
              "FieldEncoding": "PAFF",
              "SceneChangeDetect": "ENABLED",
              "QualityTuningLevel": "SINGLE_PASS_HQ",
              "UnregisteredSeiTimecode": "DISABLED",
              "GopSizeUnits": "SECONDS",
              "ParControl": "SPECIFIED",
              "NumberBFramesBetweenReferenceFrames": 3,
              "RepeatPps": "DISABLED",
              "DynamicSubGop": "ADAPTIVE"
            }
          },
          "AfdSignaling": "NONE",
          "DropFrameTimecode": "ENABLED",
          "RespondToAfd": "NONE",
          "ColorMetadata": "INSERT"
        },
        "AudioDescriptions": [
          {
            "AudioTypeControl": "FOLLOW_INPUT",
            "AudioSourceName": "Audio Selector 1",
            "CodecSettings": {
              "Codec": "AAC",
              "AacSettings": {
```

```
                "AudioDescriptionBroadcasterMix": "NORMAL",
                "Bitrate": 160000,
                "RateControlMode": "CBR",
                "CodecProfile": "LC",
                "CodingMode": "CODING_MODE_2_0",
                "RawFormat": "NONE",
                "SampleRate": 48000,
                "Specification": "MPEG4"
              }
            },
            "LanguageCodeControl": "FOLLOW_INPUT",
            "AudioType": 0
          }
        ]
      }
    ],
    "OutputGroupSettings": {
      "Type": "FILE_GROUP_SETTINGS",
      "FileGroupSettings": {
        "Destination": "s3://EXAMPLE-BUCKET/MP4/",
        "DestinationSettings": {
          "S3Settings": {
            "AccessControl": {
              "CannedAcl": "PUBLIC_READ"
            }
          }
        }
      }
    }
  },
  {
    "CustomName": "Thumbnails",
    "Name": "File Group",
    "Outputs": [
      {
        "ContainerSettings": {
          "Container": "RAW"
        },
        "VideoDescription": {
          "Width": 1280,
          "ScalingBehavior": "DEFAULT",
          "Height": 720,
          "TimecodeInsertion": "DISABLED",
          "AntiAlias": "ENABLED",
```

```
            "Sharpness": 50,
            "CodecSettings": {
              "Codec": "FRAME_CAPTURE",
              "FrameCaptureSettings": {
                "FramerateNumerator": 1,
                "FramerateDenominator": 5,
                "MaxCaptures": 500,
                "Quality": 80
              }
            },
            "AfdSignaling": "NONE",
            "DropFrameTimecode": "ENABLED",
            "RespondToAfd": "NONE",
            "ColorMetadata": "INSERT"
          }
        }
      ],
      "OutputGroupSettings": {
        "Type": "FILE_GROUP_SETTINGS",
        "FileGroupSettings": {
          "Destination": "s3://EXAMPLE-BUCKET/Thumbnails/",
          "DestinationSettings": {
            "S3Settings": {
              "AccessControl": {
                "CannedAcl": "PUBLIC_READ"
              }
            }
          }
        }
      }
    }
  ],
  "AdAvailOffset": 0,
  "Inputs": [
    {
      "AudioSelectors": {
        "Audio Selector 1": {
          "Offset": 0,
          "DefaultSelection": "DEFAULT",
          "ProgramSelection": 1
        }
      },
      "VideoSelector": {
        "ColorSpace": "FOLLOW"
```

```
      },
      "FilterEnable": "AUTO",
      "PsiControl": "USE_PSI",
      "FilterStrength": 0,
      "DeblockFilter": "DISABLED",
      "DenoiseFilter": "DISABLED",
      "TimecodeSource": "EMBEDDED",
      "FileInput": "s3://EXAMPLE-INPUT-BUCKET/input.mp4"
    }
  ]
}
```

3. 在 batch-transcode 文件夹中，创建 Lambda 函数的文件。您可以使用以下 Python 示例并将文件命名为 convert.py。

   S3 Batch Operation 将特定任务数据发送到 Lambda 函数，并要求返回结果数据。对于 Lambda 函数的请求和响应示例、响应和结果代码的信息以及 S3 Batch Operations 的示例 Lambda 函数的信息，请参阅 调用 Amazon Lambda 函数。

```
import json
import os
from urllib.parse import urlparse
import uuid
import boto3

"""
When you run an S3 Batch Operations job, your job
invokes this Lambda function. Specifically, the Lambda function is
invoked on each video object listed in the manifest that you specify
for the S3 Batch Operations job in Step 5.

Input parameter "event": The S3 Batch Operations event as a request
                         for the Lambda function.

Input parameter "context": Context about the event.

Output: A result structure that Amazon S3 uses to interpret the result
        of the operation. It is a job response returned back to S3 Batch
 Operations.
"""
def handler(event, context):

    invocation_schema_version = event['invocationSchemaVersion']
```

```
    invocation_id = event['invocationId']
    task_id = event['tasks'][0]['taskId']

    source_s3_key = event['tasks'][0]['s3Key']
    source_s3_bucket = event['tasks'][0]['s3BucketArn'].split(':::')[-1]
    source_s3 = 's3://' + source_s3_bucket + '/' + source_s3_key

    result_list = []
    result_code = 'Succeeded'
    result_string = 'The input video object was converted successfully.'

    # The type of output group determines which media players can play
    # the files transcoded by MediaConvert.
    # For more information, see Creating outputs with AWS Elemental MediaConvert.
    output_group_type_dict = {
        'HLS_GROUP_SETTINGS': 'HlsGroupSettings',
        'FILE_GROUP_SETTINGS': 'FileGroupSettings',
        'CMAF_GROUP_SETTINGS': 'CmafGroupSettings',
        'DASH_ISO_GROUP_SETTINGS': 'DashIsoGroupSettings',
        'MS_SMOOTH_GROUP_SETTINGS': 'MsSmoothGroupSettings'
    }

    try:
        job_name = 'Default'
        with open('job.json') as file:
            job_settings = json.load(file)

        job_settings['Inputs'][0]['FileInput'] = source_s3

        # The path of each output video is constructed based on the values of
        # the attributes in each object of OutputGroups in the job.json file.
        destination_s3 = 's3://{0}/{1}/{2}' \
            .format(os.environ['amzn-s3-demo-destination-bucket'],
                    os.path.splitext(os.path.basename(source_s3_key))[0],
                    os.path.splitext(os.path.basename(job_name))[0])

        for output_group in job_settings['OutputGroups']:
            output_group_type = output_group['OutputGroupSettings']['Type']
            if output_group_type in output_group_type_dict.keys():
                output_group_type = output_group_type_dict[output_group_type]
                output_group['OutputGroupSettings'][output_group_type]
['Destination'] = \
                    "{0}{1}".format(destination_s3,
```

```
                                    urlparse(output_group['OutputGroupSettings']
[output_group_type]['Destination']).path)
            else:
                raise ValueError("Exception: Unknown Output Group Type {}."
                                 .format(output_group_type))

        job_metadata_dict = {
            'assetID': str(uuid.uuid4()),
            'application': os.environ['Application'],
            'input': source_s3,
            'settings': job_name
        }

        region = os.environ['AWS_DEFAULT_REGION']
        endpoints = boto3.client('mediaconvert', region_name=region) \
            .describe_endpoints()
        client = boto3.client('mediaconvert', region_name=region,
                              endpoint_url=endpoints['Endpoints'][0]['Url'],
                              verify=False)

        try:
            client.create_job(Role=os.environ['MediaConvertRole'],
                              UserMetadata=job_metadata_dict,
                              Settings=job_settings)
        # You can customize error handling based on different error codes that
        # MediaConvert can return.
        # For more information, see MediaConvert error codes.
        # When the result_code is TemporaryFailure, S3 Batch Operations retries
        # the task before the job is completed. If this is the final retry,
        # the error message is included in the final report.
        except Exception as error:
            result_code = 'TemporaryFailure'
            raise

    except Exception as error:
        if result_code != 'TemporaryFailure':
            result_code = 'PermanentFailure'
        result_string = str(error)

    finally:
        result_list.append({
            'taskId': task_id,
            'resultCode': result_code,
            'resultString': result_string,
```

```
        })

    return {
        'invocationSchemaVersion': invocation_schema_version,
        'treatMissingKeyAs': 'PermanentFailure',
        'invocationId': invocation_id,
        'results': result_list
    }
```

4. 若要在本地终端中使用 `convert.py` 和 `job.json` 创建部署程序包 (作为名为 `lambda.zip` 的 `.zip` 文件)，打开之前创建的 `batch-transcode` 文件夹，并运行以下命令。

   对于 macOS 用户，运行以下命令：

   ```
   zip -r lambda.zip convert.py job.json
   ```

   对于 Windows 用户，运行以下命令：

   ```
   powershell Compress-Archive convert.py lambda.zip
   ```

   ```
   powershell Compress-Archive -update job.json lambda.zip
   ```

使用执行角色创建 Lambda 函数（控制台）

1. 通过 https://console.aws.amazon.com/lambda/ 打开 Amazon Lambda 控制台。
2. 在左侧导航窗格中，选择 Functions (函数)。
3. 选择 Create function (创建函数)。
4. 选择从头开始创作。
5. 在基本信息中，执行以下操作：

   a. 对于 Function name（函数名称），请输入 **`tutorial-lambda-convert`**。

   b. 对于运行时，选择 Python 3.13。

6. 选择 Change default execution role (更改默认执行角色)，在 Execution role (执行角色)中，选择 Use an existing role (使用现有角色)。
7. 在 Existing role (退出角色) 中，选择步骤 3中您为 Lambda 函数创建的 IAM 角色的名称（例如，**`tutorial-lambda-transcode-role`**）。

8. 对于其余设置，保留默认值。
9. 选择 Create function（创建函数）。

使用 .zip 文件归档部署 Lambda 函数并配置 Lambda 函数（控制台）

1. 在您创建的 Lambda 函数代码源部分中（例如，**tutorial-lambda-convert**），请选择上传自，然后选择 .zip 文件。
2. 选择上传以选择本地 `.zip` 文件。
3. 选择您之前创建的 `lambda.zip` 文件，然后选择打开。
4. 选择保存。
5. 在运行时间设置部分，选择编辑。
6. 要告诉 Lambda 运行时要调用 Lambda 函数代码中的哪个处理程序方法，请输入 **convert.handler** 的处理程序字段。

   当您在 Python 中配置函数时，处理程序设置的值是文件名，也是处理程序模块的名称（由点 (.) 分隔）。例如，`convert.handler` 调用在 `convert.py` 文件中定义的 `handler` 方法。
7. 选择保存。
8. 在 Lambda 函数页面上，选择配置选项卡。在左侧导航窗格中的配置选项卡上，选择环境变量，然后选择编辑。
9. 选择添加环境变量。然后，输入以下每个环境变量的指定密钥和值。

   - 密钥：**DestinationBucket** 值：**amzn-s3-demo-destination-bucket1**

     此值是您在步骤 1 中创建的输出媒体文件的 S3 存储桶。
   - 密钥：**MediaConvertRole** 值：**arn:aws:iam::*111122223333*:role/tutorial-mediaconvert-role**

     此值是您在步骤 2 中创建的 MediaConvert IAM 角色 ARN。）确保用 IAM 角色的实际 ARN 替换此 ARN。
   - 密钥：**Application** 值：**Batch-Transcoding**

     此值是您的应用程序的名称。
10. 选择保存。
11. （可选）在配置选项卡上，在左侧导航窗格的常规配置部分中，选择编辑。在超时字段中，输入 **2** 分钟 **0** 秒。然后，选择保存。

超时 –是Lambda允许函数在停止调用之前为调用运行的时长。默认值为 3 秒。定价基于配置的内存量和代码运行的时间量。有关更多信息，请参阅Amazon Lambda定价。

## 步骤 5：为 S3 源存储桶配置 Amazon S3 清单

设置 Lambda 函数转码后，创建 S3 Batch Operation 以转码一组视频。首先，您需要您希望 S3 批量操作对其运行指定转码操作的输入视频对象列表。要获取输入视频对象列表，您可以为 S3 源存储桶生成 S3 清单报告（例如 *amzn-s3-demo-source-bucket*）。

分步

- 为输入视频的 S3 清单报告创建和配置存储桶
- 为 S3 视频源存储桶配置 Amazon S3 清单
- 检查 S3 视频源存储桶清单报告

### 为输入视频的 S3 清单报告创建和配置存储桶

要存储列出 S3 源存储桶对象的 S3 清单报告，请创建 S3 清单目标存储桶，然后为存储桶配置存储桶策略，将清单文件写入 S3 源存储桶。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 选择创建存储桶。
4. 对于 Bucket Name（存储桶名称），输入您的存储桶的名称（例如 *amzn-s3-demo-destination-bucket2*）。
5. 对于 Amazon Web Services 区域，选择要中放置存储桶的 Amazon Web Services 区域。

   目标存储桶必须位于与您为其设置 S3 清单存储桶相同的 Amazon Web Services 区域 中。清单目标存储桶可处于不同的 Amazon Web Services 账户中。
6. 在阻止此存储桶的公有访问设置中，保留默认设置（已启用阻止全部公有访问）。
7. 对于其余设置，保留默认值。
8. 选择 Create bucket（创建存储桶）。
9. 在存储桶列表中，选择刚刚创建的存储桶名称（例如，*amzn-s3-demo-destination-bucket2*）。

10. 要授予 Amazon S3 将清单报告的数据写入 S3 清单目标存储桶的权限，您可选择权限选项卡。
11. 向下滚动到存储桶策略部分，然后选择编辑。存储桶策略页面随即打开。
12. 要授予 S3 清单的权限，请在策略字段中，粘贴以下存储桶策略。

    将三个示例值替换为以下值：

    - 您为存储库存报告创建的存储桶名称（例如，*amzn-s3-demo-destination-bucket2*）。
    - 存储输入视频的源存储桶名称（例如，*amzn-s3-demo-source-bucket*）。
    - 您用于创建 S3 视频源存储桶的 Amazon Web Services 账户 ID（例如，*111122223333*）。

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"InventoryAndAnalyticsExamplePolicy",
      "Effect":"Allow",
      "Principal": {"Service": "s3.amazonaws.com"},
      "Action":"s3:PutObject",
      "Resource":["arn:aws:s3:::amzn-s3-demo-destination-bucket2/*"],
      "Condition": {
          "ArnLike": {
              "aws:SourceArn": "arn:aws:s3:::amzn-s3-demo-source-bucket"
           },
         "StringEquals": {
             "aws:SourceAccount": "111122223333",
             "s3:x-amz-acl": "bucket-owner-full-control"
          }
       }
    }
  ]
}
```

13. 选择 Save changes（保存更改）。

### 为 S3 视频源存储桶配置 Amazon S3 清单

若要生成视频对象和元数据的平面文件列表，您必须为 S3 视频源存储桶配置 S3 清单。这些计划清单可以包括存储桶中的所有对象，或者按共享前缀分组的对象。在本教程中，S3 清单报告包含 S3 源存储桶中的所有视频对象。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 要配置 S3 源存储桶中输入视频的 S3 清单报告，请在存储桶列表中，选择 S3 源存储桶的名称（例如，*amzn-s3-demo-source-bucket*）。
4. 选择管理选项卡。
5. 向下滚动到清单配置部分，然后选择创建清单配置。
6. 对于清单配置名称，输入名称（例如，**tutorial-inventory-config**）。
7. 在清单范围下，为目标版本选择仅当前版本并保留其他清单范围设置为本教程的默认值。
8. 在报告详细信息下，对于目标存储桶，选择此账户。
9. 对于目的地，选择浏览 S3，然后选择您在上面创建的目标存储桶，以将库存报告保存到其中（例如，*amzn-s3-demo-destination-bucket2*）。然后，选择选择路径。

   目标存储桶必须位于与您为其设置 S3 清单存储桶相同的 Amazon Web Services 区域 中。清单目标存储桶可处于不同的 Amazon Web Services 账户中。

   在目标存储桶字段下目标存储桶权限)添加到目标存储桶策略中允许 Amazon S3 在该存储桶中放置数据。有关更多信息，请参阅 创建目标存储桶策略。
10. 在 频率下，选择每天。
11. 为输出格式选择 CSV。
12. 对于状态，选择已启用。
13. 在服务器端加密部分下，对于本教程选择禁用。

    有关更多信息，请参阅 使用 S3 控制台配置清单 和 向 Amazon S3 授予权限以使用客户自主管理型密钥进行加密。
14. 在其他字段 - 可选部分中，选择大小、上次修改和存储类。
15. 选择创建。

有关更多信息，请参阅 使用 S3 控制台配置清单。

检查 S3 视频源存储桶清单报告

在清单列表发布后，清单文件将发送到 S3 清单目标存储桶。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。

2. 在左侧导航窗格中，选择存储桶。
3. 在存储桶列表中，选择视频源存储桶的名称（例如，*amzn-s3-demo-source-bucket*）。
4. 选择管理。
5. 要查看 S3 清单报告是否准备好，以便您在步骤 7 中创建 S3 Batch Operation 任务，则在清单配置下，检查是否启用从清单创建任务按钮。

   > **Note**
   >
   > 交付第一份清单报告可能需要最多 48 小时。如果从清单创建任务按钮处于禁用状态，则第一个清单报告尚未送达。等到第一个清单报告交付，并且从清单创建任务按钮在创建步骤 7中的 S3 Batch Operation 任务之前已启用。

6. 要检查 S3 清单报告（`manifest.json`），在目标列中，选择您在前面创建的用于存储库存报告的库存目标存储桶名称（例如，*amzn-s3-demo-destination-bucket2*）。
7. 在对象选项卡上，选择具有 S3 源存储桶名称的现有文件夹（例如，*amzn-s3-demo-source-bucket*）。然后选择之前创建库存配置时在清单配置名称中输入的名称（例如，**tutorial-inventory-config**）。

   您可以查看以报告生成日期作为其名称的文件夹列表。
8. 要检查某一日期的每日 S3 清单报告，请选择带相应生成日期名称的文件夹，然后选择 `manifest.json`。
9. 要查看特定日期库存报告的详细信息，请在 manifest.json 页面上，选择下载或打开。

## 步骤 6：为 S3 批量操作创建 IAM 角色

要使用 S3 Batch Operation 执行批处理转码，您必须首先创建 IAM 角色，让 Amazon S3 拥有执行 S3 批处理操作的权限。

分步

- 为 S3 批量操作创建 IAM 策略
- 创建 S3 Batch Operations IAM 角色并附加权限策略。

为 S3 批量操作创建 IAM 策略

您必须创建 IAM 策略，为 S3 Batch Operation 授予读取输入清单、调用 Lambda 函数以及编写 S3 Batch Operation 任务完成报告的权限。

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在左侧导航窗格中，选择 Policies（策略）。
3. 选择创建策略。
4. 选择 JSON 选项卡。
5. 在 JSON 文本字段中，粘贴以下 JSON 策略。

   在 JSON 策略中，将四个示例值替换为以下值：

   - 存储输入视频的源存储桶名称（例如，*amzn-s3-demo-source-bucket*）。
   - 您在步骤 5 中创建以存储 `manifest.json` 文件的清单目标存储桶名称（例如，*amzn-s3-demo-destination-bucket2*）。
   - 您在步骤 1 中创建以存储输出媒体文件的存储桶名称（例如，*amzn-s3-demo-destination-bucket1*）。在本教程中，我们将任务完成报告存储在输出媒体文件的目标存储桶中。
   - 您在步骤 4 中创建的 Lambda 函数的角色 ARN。要查找并复制 Lambda 函数的角色 ARN，请执行以下操作：
     - 在新浏览器选项卡中，打开 https://console.amazonaws.cn/lambda/home#/functions 中的 Lambda 控制台上的函数页面。
     - 在函数列表中，选择在步骤 4 中创建的 Lambda 函数（例如，**tutorial-lambda-convert**）。
     - 选择复制 ARN。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3Get",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-source-bucket/*",
                "arn:aws:s3:::amzn-s3-demo-destination-bucket2/*"
            ]
```

```
        },
        {
            "Sid": "S3PutJobCompletionReport",
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket1/*"
        },
        {
            "Sid": "S3BatchOperationsInvokeLambda",
            "Effect": "Allow",
            "Action": [
                "lambda:InvokeFunction"
            ],
            "Resource": [
                "arn:aws:lambda:us-west-2:111122223333:function:tutorial-lambda-
convert"
            ]
        }
    ]
}
```

6. 选择下一步：标签。
7. 选择下一步：审核。
8. 在名称字段中，输入 **tutorial-s3batch-policy**。
9. 选择创建策略。

创建 S3 Batch Operations IAM 角色并附加权限策略。

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在左侧导航窗格中，选择角色，然后选择创建角色。
3. 选择 Amazon Web Services 服务 角色类型，然后选择 S3 服务。
4. 在选择您的用例中，选择 S3 批量操作。
5. 选择下一步。
6. 在附加权限下，在搜索框中输入您以前创建的 IAM 策略的名称（例如 **tutorial-s3batch-policy**），以筛选策略列表。选中策略名称旁边的复选框（例如，**tutorial-s3batch-policy**)。
7. 选择下一步。

8. 对于 Role name（角色名称），输入 **tutorial-s3batch-role**。
9. 选择 Create role（创建角色）。

   创建 S3 批量操作的 IAM 角色后，以下信任策略将自动附加到该角色。此信任策略允许 S3 批量操作服务主体担任 IAM 角色。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"batchoperations.s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

## 步骤 7：设置并运行 S3 批量操作任务

要创建 S3 批量操作任务以处理 S3 源存储桶中的输入视频，您必须为此特定任务指定参数。

> **Note**
>
> 在开始创建 S3 批量操作任务之前，请确保启用从清单创建任务按钮。有关更多信息，请参阅检查 S3 视频源存储桶清单报告。如果从清单创建任务按钮处于禁用状态，则第一个清单报告尚未送达，您必须等到启用该按钮。在步骤 5 中为 S3 源存储桶配置 Amazon S3 清单后，交付第一个清单报告可能需要最长 48 小时。

分步

- 创建 S3 批量操作任务
- 运行 S3 批量操作任务以调用 Lambda 函数
- （可选）检查您的完成报告
- （可选）在 Lambda 控制台中监控每个 Lambda 调用
- （可选）监控 MediaConvert 控制台中的每个 MediaConvert 视频转码任务

创建 S3 批量操作任务

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择批量操作。
3. 选择创建任务。
4. 对于 Amazon Web Services 区域，选择要在其中创建任务的区域。

   在本教程中，要使用 S3 批量操作任务调用 Lambda 函数，您必须在清单中引用的对象所在的 S3 视频源存储桶所在的同一区域中创建任务。
5. 在清单 部分中执行以下操作：

   a. 对于 Manifest format（清单格式），选择 S3 清单报告 (manifest.json)。

   b. 针对清单对象，选择浏览 S3查找您在步骤 5 中创建用于存储清单报告的存储桶（例如，*amzn-s3-demo-destination-bucket2*)。在清单对象页面中，浏览对象名称直到找到特定日期的 `manifest.json` 文件。此文件列出了有关要批量转码的所有视频的信息。当您找到要使用的 `manifest.json` 文件之后，选择旁边的选项按钮。然后，选择选择路径。

   c. （可选）对于清单对象版本 ID - 可选，如果您希望使用其他版本而不是最新版本，则输入清单对象的版本 ID。
6. 选择下一步。
7. 要使用 Lambda 函数来转码选定 `manifest.json` 文件中列出的所有对象，在操作类型中，选择调用 Amazon Lambda 函数。
8. 在调用 Lambda 函数部分中，执行以下操作：

   a. 选择从账户中的函数选择。

   b. 对于 Lambda 函数，选择您在步骤 4 中创建的 Lambda 函数（例如，**`tutorial-lambda-convert`**)。

   c. 对于 Lambda 函数版本，请保留默认值 $LATEST。
9. 选择下一步。配置其他选项页面随即打开。
10. 在其他选项部分下，请保留默认设置。

    有关这些选项的详细信息，请参阅批量操作任务请求元素。
11. 在完成报告部分，对于完成报告目的地的路径，选择浏览 S3。查找您在步骤 1 中创建以存储输出媒体文件的存储桶名称（例如，*amzn-s3-demo-destination-bucket1*)。选择该存储桶名称旁边的选项按钮。然后，选择选择路径。

对于其余的完成报告设置，请保留默认值。有关完成报告设置的更多信息，请参阅 批量操作任务请求元素。完成报告维护任务详细信息和执行的操作的记录。

12. 在权限部分下，选择从现有 IAM 角色中进行选择。对于 IAM 角色，选择您在步骤 6 中创建的 S3 批量操作任务的 IAM 角色（例如，**tutorial-s3batch-role**）。
13. 选择下一步。
14. 在审阅页面上，检查您的设置。然后选择创建任务。

    S3 读取 S3 批量操作任务清单后，它会将任务的状态设为等待确认运行。要查看任务状态的更新，请刷新页面。直到任务状态为等待确认运行，您才可运行任务。

运行 S3 批量操作任务以调用 Lambda 函数

运行批量操作任务以调用 Lambda 函数进行视频转码。如果任务失败，您可以检查完成报告以确定原因。

运行 S3 批量操作任务

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择批量操作。
3. 从任务列表中，在第一行上选择任务的任务 ID，这是之前创建的 S3 批量操作任务。
4. 选择运行任务。
5. 再次复核您的任务参数，并确认清单中列出的对象总数与清单中对象的数量相同。然后选择运行任务。

   您的 S3 批量操作任务页面打开。
6. 任务开始运行后，在任务页面上的状态下，检查 S3 批量操作任务的进度，例如状态、已完成百分比、成功总数（费率）、失败总数（速率）、终止日期和终止原因。

   S3 批量操作任务完成后，查看任务页面上的数据，确认已按预期完成任务。

   如果在尝试超过 1,000 个操作后，超过 50% 的 S3 批量操作任务的对象操作失败，该任务将自动失败。要检查完成报告确定失败的原因，请使用下面的可选步骤。

### （可选）检查您的完成报告

您可以使用完成报告来确定哪些对象失败以及失败的原因。

要检查完成报告以了解有关失败对象的详细信息

1. 在 S3 批量操作任务的页面上，向下滚动至完成报告部分，然后选择完成报告目标下的链接。

   S3 输出目标存储桶页面打开。
2. 在对象选项卡上，选择之前创建的 S3 批量操作务以任务 ID 名称结尾的文件夹。
3. 选择结果/。
4. 选中 `.csv` 文件旁边的复选框。
5. 要查看任务报告，请选择打开或者下载。

### （可选）在 Lambda 控制台中监控每个 Lambda 调用

S3 批量操作任务开始运行后，任务将为每个输入视频对象调用 Lambda 函数。S3 将每次 Lambda 调用的日志写入到 CloudWatch Logs。您可以使用 Lambda 控制台的监控控制面板来监控 Lambda 函数。

1. 通过 https://console.aws.amazon.com/lambda/ 打开 Amazon Lambda 控制台。
2. 在左侧导航窗格中，选择 Functions（函数）。
3. 在函数列表中，选择在步骤 4 中创建的 Lambda 函数（例如，**`tutorial-lambda-convert`**）。
4. 选择监控选项卡。
5. 在指标下，请参阅 Lambda 函数的运行时间指标。
6. 在日志下，通过 CloudWatch Logs Insights 查看每个 Lambda 调用的日志数据。

> **Note**
>
> 将 S3 批量操作与 Lambda 函数结合使用时，会在每个对象上调用 Lambda 函数。如果您的 S3 批量操作任务很大，可以同时调用多个 Lambda 函数，从而导致 Lambda 并发峰值。
>
> 对于每个区域，每个 Amazon Web Services 账户 都有 Lambda 并发配额。有关更多信息，请参阅 Amazon Lambda 开发人员指南中的 Amazon Lambda 函数扩展。将 Lambda 函数与 S3 批量操作结合使用的最佳做法是对 Lambda 函数本身设置并发限制。设置并发

限制会使您的任务不会占用大部分 Lambda 并发，并可能会限制您账户中的其他函数。有关更多信息，请参阅 Amazon Lambda 开发人员指南中的管理 Lambda 预留并发。

（可选）监控 MediaConvert 控制台中的每个 MediaConvert 视频转码任务

MediaConvert 任务执行转换媒体文件的工作。当您的 S3 批量操作任务为每个视频调用 Lambda 函数时，每个 Lambda 函数调用都会为每个输入视频创建一个 MediaConvert 转码任务。

1. 登录到 Amazon Web Services Management Console，然后在 https://console.aws.amazon.com/mediaconvert/ 打开 MediaConvert 控制台。
2. 如果显示 MediaConvert 介绍页面，请选择开始。
3. 从任务列表中，查看每行以监控每个输入视频的转码任务。
4. 确定要检查的任务行，然后选择任务 ID 链接打开任务详细信息页面。
5. 在任务摘要页面，在输出中，根据浏览器支持的内容，选择 HLS、MP4 或缩略图输出的链接，转到输出媒体文件的 S3 目标存储桶。
6. 在 S3 输出目标存储桶的相应文件夹（HLS、MP4 或缩略图）中，选择输出媒体文件对象的名称。

   将打开对象的详细信息页面。
7. 在对象的详细信息页面上，在对象概述中，选择对象 URL 下的链接观看转码输出媒体文件。

## 步骤 8：检查 S3 目标存储桶中的输出媒体文件

若要从 S3 目标存储桶检查输出媒体文件

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 从存储桶列表中，选择您在步骤 1 中创建的输出媒体文件的 S3 目标存储桶名称（例如，*amzn-s3-demo-destination-bucket1*）。
4. 在对象选项卡上，每个输入视频都有一个带输入视频名称的文件夹。每个文件夹都包含输入视频的转码输出媒体文件。

   要检查输出媒体文件中的输入视频，请执行以下操作：

   a. 选择要检查的输入视频名称文件夹。

b. 选择Default/文件夹。

c. 选择转码格式的文件夹（本教程中的 HLS、MP4 或缩略图）。

d. 选择输出媒体文件的名称。

e. 要观看转码后的文件，在对象的详细信息页面上，选择对象 URL 下的链接。

HLS 格式的输出媒体文件被拆分为短段。要播放这些视频，您需要嵌入 `.m3u8` 文件的对象 URL 在兼容的播放器中。

## 步骤 9：清除

如果您只使用 S3 批量操作、Lambda 和 MediaConvert 转码视频作为学习练习，请删除 Amazon 您分配的资源，以免继续产生费用。

分步

- 删除 S3 源存储桶的 S3 清单配置
- 删除 Lambda 函数
- 删除 CloudWatch 日志组
- 删除 IAM 角色以及 IAM 角色的内联策略
- 删除客户管理型 IAM 策略
- 清空 S3 存储桶
- 删除 S3 存储桶

删除 S3 源存储桶的 S3 清单配置

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 在存储桶列表中，选择您的源存储桶名称（例如，*amzn-s3-demo-source-bucket*）。
4. 选择管理选项卡。
5. 在清单配置部分中，选择您在步骤 5 中创建的清单配置旁边的选项按钮（例如，**tutorial-inventory-config**）。
6. 选择删除，然后选择确认。

### 删除 Lambda 函数

1. 通过 https://console.aws.amazon.com/lambda/ 打开 Amazon Lambda 控制台。
2. 在左侧导航窗格中，选择 Functions（函数）。
3. 选择在步骤 4 中创建的函数旁边的复选框（例如，**`tutorial-lambda-convert`**）。
4. 选择操作，然后选择删除。
5. 在删除函数对话框中，选择删除。

### 删除 CloudWatch 日志组

1. 通过 https://console.aws.amazon.com/cloudwatch/ 打开 CloudWatch 控制台。
2. 在左侧导航窗格中，选择日志，然后选择日志组。
3. 选中日志组旁边的复选框，该复选框的名称以在步骤 4 中创建的 Lambda 函数结尾（例如，**`tutorial-lambda-convert`**）。
4. 选择操作，然后选择删除日志组。
5. 在删除日志组对话框中，选择删除。

### 删除 IAM 角色以及 IAM 角色的内联策略

删除您在步骤 2、步骤 3 和步骤 6 中创建的 IAM 角色，执行以下操作：

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在左侧导航窗格中，选择角色，然后选中要删除的角色名称旁的复选框。
3. 在页面的顶部，选择删除。
4. 在确认对话框中，根据提示在文本输入字段中输入所需的响应，然后选择删除。

### 删除客户管理型 IAM 策略

若要删除您在步骤 6 中创建的客户托管 IAM 策略，执行以下操作：

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在左侧导航窗格中，选择 Policies（策略）。

3. 选择您在步骤 6 中创建的策略旁边的选项按钮（例如，**tutorial-s3batch-policy**）。您可以使用搜索框筛选策略列表。
4. 选择 Actions，然后选择 Delete。
5. 在文本字段中输入名称，确认您要删除的策略，然后选择删除。

### 清空 S3 存储桶

若要清空您在先决条件、步骤 1 和步骤 5 中创建的 S3 存储桶，执行以下操作：

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 在存储桶列表中，选择要清空的存储桶名称旁边的选项图标，然后选择清空。
4. 在清空存储桶页面上，通过在文本字段中输入 **permanently delete** 来确认要清空存储桶，然后选择清空。

### 删除 S3 存储桶

若要删除您在先决条件、步骤 1 和步骤 5 中创建的 S3 存储桶，执行以下操作：

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 在存储桶列表中，选择要删除的存储桶名称旁边的选项按钮。
4. 选择删除。
5. 在删除存储桶页面上，通过在文本字段中输入存储桶名称来确认要删除存储桶，然后选择删除存储桶。

## 后续步骤

完成本教程后，您可以进一步探索其他相关使用案例：

- 您可以使用 Amazon CloudFront 将转码后的媒体文件流式传输到全球各地的查看者。有关更多信息，请参阅 教程：使用 Amazon S3、Amazon CloudFront 和 Amazon Route 53 托管点播流视频。

- 将视频上传到 S3 源存储桶时，您可以对视频进行转码。为此，您可以配置 Amazon S3 事件触发器，该触发器自动调用 Lambda 函数以使用 MediaConvert 转码 S3 中的新对象。有关更多信息，请参阅 Amazon Lambda 开发人员指南中的教程：使用 Amazon S3 触发器调用 Lambda函数。

## 排查批量操作问题

以下主题列出了常见错误，有助于您排查在使用 Amazon S3 批量操作时可能遇到的问题。

要排查 S3 批量复制的问题，请参阅the section called “批量复制错误”。

常见错误

- 当存在权限问题或启用了 S3 对象锁定保留模式时，未交付任务报告
- 对于对象的批量操作失败，错误为 400 InvalidRequest：由于缺少 VersionId，任务失败
- 在启用任务标签选项的情况下创建任务失败
- 读取清单的访问被拒绝

### 当存在权限问题或启用了 S3 对象锁定保留模式时，未交付任务报告

在缺少必需权限或者对目标存储桶启用了对象锁定保留模式（监管模式或合规模式）时，会发生以下错误。

错误：失败的原因。无法将任务报告写入您的报告桶。请检查您的权限。

Amazon Identity and Access Management（IAM）角色和信任策略必须配置为支持批量操作具有 `s3:PutObject` 权限，以便将对象 PUT 到要向其中交付报告的存储桶中。如果缺少这些必需的权限，则会出现任务报告交付失败的情况。

启用保留模式后，桶受到“一次写入，多次读取”（WORM）保护。在目标存储桶上，不支持在启用了保留模式时进行对象锁定，因此，任务完成报告交付尝试失败。要解决此问题，请为您的任务完成报告选择一个未启用对象锁定保留模式的目标桶。

### 对于对象的批量操作失败，错误为 400 InvalidRequest：由于缺少 VersionId，任务失败

如果批量操作任务正在对受版本控制的桶中的对象执行操作，并在清单中遇到版本 ID 字段为空的对象，则会出现以下示例错误。

错误：*`bucket_name,prefix/file_name`*,failed,400,InvalidRequest，由于缺少 VersionId，任务失败

之所以出现此错误，是因为清单中的版本 ID 字段是空字符串，而不是文本 null 字符串。

这一特定对象或这些对象的批量操作将失败，但整个任务不会失败。如果在操作期间将清单格式配置为使用版本 ID，则会出现此问题。非版本控制的任务不会遇到此问题，因为它们仅对每个对象的最新版本进行操作，并忽略清单中的版本 ID。

要解决此问题，请将空版本 ID 转换为 null 字符串。有关更多信息，请参阅 the section called “将空版本 ID 字符串转换为空字符串”。

### 在启用任务标签选项的情况下创建任务失败

如果没有 s3:PutJobTagging 权限，在启用了任务标签选项的情况下创建批量操作任务会导致 403 access denied 错误。

要在启用任务标签选项的情况下创建批量操作任务，创建批量操作任务的 Amazon Identity and Access Management（IAM）用户除 s3:CreateJob 权限外还必须具有 s3:PutJobTagging 权限。

有关批量操作所需权限的更多信息，请参阅the section called “授予权限”。

### 读取清单的访问被拒绝

如果您在尝试创建批量操作任务时，批量操作无法读取清单文件，则可能会出现以下错误。

Amazon CLI

禁止读取清单失败的原因：AccessDenied

Amazon S3 控制台

警告：无法获取清单对象的 ETag。指定其他对象以继续。

要解决此问题，请执行下列操作：

- 验证您用于创建批量操作任务的 Amazon Web Services 账户的 IAM 角色是否具有 s3:GetObject 权限。账户的 IAM 角色必须具有 s3:GetObject 权限，以便支持批量操作读取清单文件。

  有关批量操作所需权限的更多信息，请参阅the section called “授予权限”。
- 检查清单对象的元数据中是否存在与 S3 对象所有权不匹配的访问权限。有关 S3 对象所有权的更多信息，请参阅the section called “控制对象所有权”。
- 检查 Amazon Key Management Service（Amazon KMS）密钥是否用于加密清单文件。

  批量操作支持用 Amazon KMS 加密的 CSV 清单报告。但是，批量操作不支持用 Amazon KMS 加密的 CSV 清单文件。有关更多信息，请参阅配置 Amazon S3 清单和指定清单。

# 使用 Amazon S3 Select 就地查询数据

> **Important**
>
> 不再向新客户提供 Amazon S3 Select。Amazon S3 Select 的现有客户可以像往常一样继续使用该功能。了解更多

利用 Amazon S3 Select，您可以使用结构化查询语言（SQL）语句筛选 Amazon S3 对象的内容，并仅检索所需的部分数据。通过使用 Amazon S3 Select 筛选此数据，您可以减少 Amazon S3 传输的数据量，这将减少检索此数据所需的成本和延迟。

Amazon S3 Select 只允许您一次查询一个对象。它适用于以 CSV、JSON 或 Apache Parquet 格式存储的对象。它还使用通过 GZIP 或 BZIP2 压缩的对象（仅对于 CSV 和 JSON 对象）和服务器端加密的对象。可以将结果的格式指定为 CSV 或 JSON，并且可以确定结果中记录的分隔方式。

可以在请求中将 SQL 表达式传递给 Amazon S3。Amazon S3 Select 支持一部分 SQL。有关 Amazon S3 Select 支持的 SQL 元素的更多信息，请参阅 Amazon S3 Select 的 SQL 参考。

您可以使用 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）、`SelectObjectContent` REST API 操作或 Amazon SDK 执行 SQL 查询。

> **Note**
>
> Amazon S3 控制台将返回的数据量限定为 40 MB。要检索更多数据，请使用 Amazon CLI 或 API。

## 要求和限制

以下是使用 Amazon S3 Select 的要求：

- 您必须拥有所查询的对象的 `s3:GetObject` 权限。
- 如果您查询的对象已使用具有客户提供的加密密钥的客户端加密（SSE-C）进行加密，则必须使用 `https`，并且您必须在请求中提供加密密钥。

使用 Amazon S3 Select 时存在以下限制：

- S3 Select 对于每个请求只能查询一个对象。

- SQL 表达式的最大长度为 256 KB。
- 输入或结果中记录的最大长度为 1 MB。
- Amazon S3 Select 只能使用 JSON 输出格式发出嵌套数据。
- 您无法查询存储在 S3 Glacier Flexible Retrieval、S3 Glacier Deep Archive 或低冗余存储（RRS）存储类中的对象。您无法查询存储在 S3 Intelligent-Tiering 存档访问层或 S3 Intelligent-Tiering 深度存档访问层中的对象。有关存储类的更多信息，请参阅 了解和管理 Amazon S3 存储类。

在将 Amazon S3 Select 用于 Parquet 对象时，以下额外限制适用：

- Amazon S3 Select 仅支持使用 GZIP 或 Snappy 的列式压缩。Amazon S3 Select 对于 Parquet 对象不支持整个对象压缩。
- Amazon S3 Select 不支持 Parquet 输出。您必须将输出格式指定为 CSV 或 JSON。
- 未压缩的最大行组大小为 512MB。
- 您必须使用在对象的模式中指定的数据类型。
- 选择重复字段将只返回最后一个值。

## 构建请求

在构造请求时，您提供通过使用 `InputSerialization` 对象查询的对象的详细信息。您提供要使用 `OutputSerialization` 对象返回结果的方式的详细信息。您还包含 Amazon S3 用于筛选请求的 SQL 表达式。

有关构造 Amazon S3 Select 请求的更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 SelectObjectContent。您也可以参阅以下部分中的某个开发工具包代码示例。

### 使用扫描范围的请求

借助 Amazon S3 Select，您可以通过指定要查询的字节范围来扫描对象的子集。利用此功能，您可以将工作分为一系列非重叠扫描范围的独立 Amazon S3 Select 请求，从而并行扫描整个对象。

扫描范围不需要与记录边界对齐。Amazon S3 Select 扫描范围请求在您指定的字节范围内运行。查询将处理在指定的扫描范围内开始但延伸到该扫描范围之外的记录。例如，下面显示了包含一系列记录（采用以行分隔的 CSV 格式）的 Amazon S3 对象：

```
A,B
C,D
D,E
```

```
E,F
G,H
I,J
```

假设您使用 Amazon S3 Select ScanRange 参数，并从（字节）1 开始，在（字节）4 结束。因此，扫描范围将从“,”开始，并扫描直到记录结尾 C。您的扫描范围请求将返回结果 C， D，因为这是记录的结尾。

Amazon S3 Select 扫描范围请求支持 Parquet、CSV（不带引号的分隔符）或 JSON 对象（仅在 LINES 模式下）。CSV 和 JSON 对象必须未压缩。对于基于行的 CSV 和 JSON 对象，当将扫描范围指定为 Amazon S3 Select 请求的一部分时，将处理在该扫描范围内开始的所有记录。对于 Parquet 对象，将处理在请求的扫描范围内开始的所有行组。

Amazon S3 Select 扫描范围请求可在 Amazon CLI、Amazon S3 API 和 Amazon SDK 中使用。您可以在 Amazon S3 Select 请求中使用 ScanRange 参数来实现此功能。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 SelectObjectContent。

### 错误

如果在尝试运行查询时遇到问题，Amazon S3 Select 将返回错误代码和关联的错误消息。有关错误代码和描述的列表，请参阅 Amazon Simple Storage Service API 参考中的错误响应页面的 SELECT 对象内容错误代码列表部分。

有关 Amazon S3 Select 的更多信息，请参阅以下主题。

主题

- 在对象上使用 Amazon S3 Select 的示例
- Amazon S3 Select 的 SQL 参考

## 在对象上使用 Amazon S3 Select 的示例

> **Important**
>
> 不再向新客户提供 Amazon S3 Select。Amazon S3 Select 的现有客户可以像往常一样继续使用该功能。了解更多

您可以使用 S3 Select，通过 Amazon S3 控制台、REST API 和 Amazon SDK 从一个对象中选择内容。

有关 S3 Select 支持的 SQL 函数的更多信息，请参阅SQL 函数。

使用 S3 控制台

在 Amazon S3 控制台中选择对象中的内容

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 选择包含您想要从中选择内容的对象的桶，然后选择对象的名称。
4. 选择对象操作，然后选择使用 S3 Select 进行查询。
5. 根据输入数据的格式配置输入设置。
6. 根据要接收的输出的格式配置输出设置。
7. 要从所选对象中提取记录，请在 SQL 查询下输入 SELECT SQL 命令。有关如何编写 SQL 命令的更多信息，请参阅Amazon S3 Select 的 SQL 参考。
8. 输入 SQL 查询后，选择运行 SQL 查询。然后，在查询结果下，您可以看到 SQL 查询的结果。

使用 REST API

您可以使用 Amazon SDK 从对象中选择内容。然而，如果您的应用程序需要它，则可以直接发送 REST 请求。有关请求和响应格式的更多信息，请参阅 SelectObjectContent。

使用 Amazon SDK

您可以使用 Amazon S3 Select 通过 `selectObjectContent` 方法选择对象的一些内容。如果此方法成功，它将返回 SQL 表达式的结果。

Java

以下 Java 代码返回对象 (包含以 CSV 格式存储的数据) 中存储的每条记录的第一列的值。它还请求返回 `Progress` 和 `Stats` 消息。必须提供有效的存储桶名称和包含 CSV 格式的数据的对象。

有关创建和测试有效示例的说明，请参阅《适用于 Java 的 Amazon SDK 开发人员指南》中的入门。

```
package com.amazonaws;

import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
```

```
import com.amazonaws.services.s3.model.CSVInput;
import com.amazonaws.services.s3.model.CSVOutput;
import com.amazonaws.services.s3.model.CompressionType;
import com.amazonaws.services.s3.model.ExpressionType;
import com.amazonaws.services.s3.model.InputSerialization;
import com.amazonaws.services.s3.model.OutputSerialization;
import com.amazonaws.services.s3.model.SelectObjectContentEvent;
import com.amazonaws.services.s3.model.SelectObjectContentEventVisitor;
import com.amazonaws.services.s3.model.SelectObjectContentRequest;
import com.amazonaws.services.s3.model.SelectObjectContentResult;

import java.io.File;
import java.io.FileOutputStream;
import java.io.InputStream;
import java.io.OutputStream;
import java.util.concurrent.atomic.AtomicBoolean;

import static com.amazonaws.util.IOUtils.copy;

/**
 * This example shows how to query data from S3Select and consume the response in
 the form of an
 * InputStream of records and write it to a file.
 */

public class RecordInputStreamExample {

    private static final String BUCKET_NAME = "${my-s3-bucket}";
    private static final String CSV_OBJECT_KEY = "${my-csv-object-key}";
    private static final String S3_SELECT_RESULTS_PATH = "${my-s3-select-results-
path}";
    private static final String QUERY = "select s._1 from S3Object s";

    public static void main(String[] args) throws Exception {
        final AmazonS3 s3Client = AmazonS3ClientBuilder.defaultClient();

        SelectObjectContentRequest request = generateBaseCSVRequest(BUCKET_NAME,
 CSV_OBJECT_KEY, QUERY);
        final AtomicBoolean isResultComplete = new AtomicBoolean(false);

        try (OutputStream fileOutputStream = new FileOutputStream(new File
 (S3_SELECT_RESULTS_PATH));
             SelectObjectContentResult result =
 s3Client.selectObjectContent(request)) {
```

```
            InputStream resultInputStream =
result.getPayload().getRecordsInputStream(
                    new SelectObjectContentEventVisitor() {
                        @Override
                        public void visit(SelectObjectContentEvent.StatsEvent event)
                        {
                            System.out.println(
                                    "Received Stats, Bytes Scanned: " +
event.getDetails().getBytesScanned()
                                            +  " Bytes Processed: " +
event.getDetails().getBytesProcessed());
                        }

                        /*
                         * An End Event informs that the request has finished
successfully.
                         */
                        @Override
                        public void visit(SelectObjectContentEvent.EndEvent event)
                        {
                            isResultComplete.set(true);
                            System.out.println("Received End Event. Result is
complete.");
                        }
                    }
            );

            copy(resultInputStream, fileOutputStream);
        }

        /*
         * The End Event indicates all matching records have been transmitted.
         * If the End Event is not received, the results may be incomplete.
         */
        if (!isResultComplete.get()) {
            throw new Exception("S3 Select request was incomplete as End Event was
not received.");
        }
    }

    private static SelectObjectContentRequest generateBaseCSVRequest(String bucket,
String key, String query) {
        SelectObjectContentRequest request = new SelectObjectContentRequest();
        request.setBucketName(bucket);
```

```
        request.setKey(key);
        request.setExpression(query);
        request.setExpressionType(ExpressionType.SQL);

        InputSerialization inputSerialization = new InputSerialization();
        inputSerialization.setCsv(new CSVInput());
        inputSerialization.setCompressionType(CompressionType.NONE);
        request.setInputSerialization(inputSerialization);

        OutputSerialization outputSerialization = new OutputSerialization();
        outputSerialization.setCsv(new CSVOutput());
        request.setOutputSerialization(outputSerialization);

        return request;
    }
}
```

JavaScript

有关将 适用于 JavaScript 的 Amazon SDK 与 S3 `SelectObjectContent` API 操作一起使用从 Amazon S3 中存储的 JSON 和 CSV 文件中选择记录的 JavaScript 示例，请参阅博客文章在 适用于 JavaScript 的 Amazon SDK 中引入对 Amazon S3 Select 的支持。

Python

有关使用 SQL 查询来搜索通过使用 S3 Select 以逗号分隔值（CSV）文件形式加载到 Amazon S3 中的数据的 Python 示例，请参阅博客文章使用 Amazon S3 Select 在没有服务器或数据库的情况下查询数据。

## Amazon S3 Select 的 SQL 参考

> **Important**
>
> 不再向新客户提供 Amazon S3 Select。Amazon S3 Select 的现有客户可以像往常一样继续使用该功能。了解更多

此参考包含 Amazon S3 Select 支持的结构化查询语言（SQL）元素的描述。

主题

- SELECT 命令

- 数据类型
- 运算符
- 保留关键字
- SQL 函数

## SELECT 命令

> **Important**
>
> 不再向新客户提供 Amazon S3 Select。Amazon S3 Select 的现有客户可以像往常一样继续使用该功能。了解更多

Amazon S3 Select 仅支持 SELECT SQL 命令。SELECT 支持以下 ANSI 标准子句：

- SELECT list
- FROM 子句
- WHERE 子句
- LIMIT 子句

> **Note**
>
> Amazon S3 Select 查询目前不支持子查询或联接。

### SELECT list

SELECT 列表指定希望查询返回的列、函数和表达式。列表表示查询的输出。

```
SELECT *
SELECT projection1 AS column_alias_1, projection2 AS column_alias_2
```

第一个带 *（星号）的 SELECT 形式按原样返回每个传递 WHERE 子句的行。第二个 SELECT 形式使用用户定义的输出标量表达式 ***projection1*** 和 ***projection2*** 为每列创建一行。

### FROM 子句

Amazon S3 Select 支持以下形式的 FROM 子句：

```
FROM table_name
FROM table_name alias
FROM table_name AS alias
```

在 FROM 子句的每种形式中，table_name 都是被查询的 S3Object。对于来自传统关系数据库的用户，可以将其视为一个数据库架构，其中包含一个表的多个视图。

按照标准 SQL，FROM 子句将会创建在 WHERE 子句中筛选并在 SELECT 列表中投影的行。

对于在 Amazon S3 Select 中存储的 JSON 对象，您也可以使用以下形式的 FROM 子句：

```
FROM S3Object[*].path
FROM S3Object[*].path alias
FROM S3Object[*].path AS alias
```

使用这种形式的 FROM 子句，您可以从 JSON 对象内的数组或对象中进行选择。您可以使用以下形式之一指定 path：

- 通过名称（在对象中）：.*name* 或 ['*name*']
- 通过索引（在数组中）：[*index*]
- 通过通配符（在对象中）：.*
- 通过通配符（在数组中）：[*]

> **Note**
>
> - 这种形式的 FROM 子句只适用于 JSON 对象。
> - 通配符始终至少发出一条记录。如果没有匹配的记录，Amazon S3 Select 将发射值 MISSING。在输出序列化期间（在查询完成运行后），Amazon S3 Select 会将 MISSING 值替换为空记录。
> - 聚合函数（AVG、COUNT、MAX、MIN 和 SUM）会跳过 MISSING 值。
> - 如果您在使用通配符时未提供别名，则可使用路径中的最后一个元素引用行。例如，可以使用查询 SELECT price FROM S3Object[*].books[*].price 从书籍列表中选择

所有价格。如果路径以通配符而不是名称结束，则可使用值 _1 来引用行。例如，您可以使用查询 SELECT price FROM S3Object[*].books[*].price，而不是 SELECT _1.price FROM S3Object[*].books[*]。

- Amazon S3 Select 始终将 JSON 文档视为根级值组成的数组。因此，即使您查询的 JSON 对象只有一个根元素，FROM 子句也必须以 S3Object[*] 开头。但为了确保兼容性，Amazon S3 Select 允许您在不包含路径时省略通配符。因此，完整的子句 FROM S3Object 等效于 FROM S3Object[*] as S3Object。如果包含路径，则还必须使用通配符。因此，FROM S3Object 和 FROM S3Object[*].*path* 都是有效子句，但 FROM S3Object.*path* 不是。

Example

示例：

示例 1

此示例显示使用以下数据集和查询时的结果：

```
{ "Rules": [ {"id": "1"}, {"expr": "y > x"}, {"id": "2", "expr": "z = DEBUG"} ]}
{ "created": "June 27", "modified": "July 6" }
```

```
SELECT id FROM S3Object[*].Rules[*].id
```

```
{"id":"1"}
{}
{"id":"2"}
{}
```

Amazon S3 Select 因以下原因生成每个结果：

- {"id":"id-1"} – S3Object[0].Rules[0].id 产生了匹配。
- {} – S3Object[0].Rules[1].id 与记录不匹配，因此 Amazon S3 Select 发出 MISSING，后者随后在输出序列化期间变为空记录并返回。
- {"id":"id-2"} – S3Object[0].Rules[2].id 产生了匹配。
- {} – S3Object[1] 对于 Rules 不匹配，因此 Amazon S3 Select 发出 MISSING，后者随后在输出序列化期间变为空记录并返回。

如果您不希望 Amazon S3 Select 在找不到匹配项时返回空记录，则可测试值 MISSING。以下查询将返回与上一查询相同的结果，但会省略空值：

```
SELECT id FROM S3Object[*].Rules[*].id WHERE id IS NOT MISSING
```

```
{"id":"1"}
{"id":"2"}
```

示例 2

此示例显示使用以下数据集和查询时的结果：

```
{ "created": "936864000", "dir_name": "important_docs", "files": [ { "name": "." },
 { "name": ".." }, { "name": ".aws" }, { "name": "downloads" } ], "owner": "Amazon
 S3" }
{ "created": "936864000", "dir_name": "other_docs", "files": [ { "name": "." },
 { "name": ".." }, { "name": "my stuff" }, { "name": "backup" } ], "owner": "User" }
```

```
SELECT d.dir_name, d.files FROM S3Object[*] d
```

```
{"dir_name":"important_docs","files":[{"name":"."},{"name":".."},{"name":".aws"},
{"name":"downloads"}]}
{"dir_name":"other_docs","files":[{"name":"."},{"name":".."},{"name":"my stuff"},
{"name":"backup"}]}
```

```
SELECT _1.dir_name, _1.owner FROM S3Object[*]
```

```
{"dir_name":"important_docs","owner":"Amazon S3"}
{"dir_name":"other_docs","owner":"User"}
```

WHERE 子句

WHERE 子句遵循以下语法：

```
WHERE condition
```

WHERE 子句根据 *condition* 筛选行。condition 是具有布尔结果的表达式。只有 condition 计算结果为 TRUE 的行才会在结果中返回。

### LIMIT 子句

LIMIT 子句遵循以下语法：

```
LIMIT number
```

LIMIT 子句根据 *number* 限制您希望查询返回的记录数。

### 属性访问

SELECT 和 WHERE 子句可以使用以下部分的任一方法引用记录数据，具体取决于将查询的文件是采用 CSV 还是 JSON 格式。

#### CSV

- 列编号 – 您可以引用列名为 *_N* 的行的第 N 列，其中 *N* 是列位置。位置计数从 1 开始。例如，第一列名为 _1，第二列名为 _2。

  您可以通过 *_N* 或 *alias*.*_N* 引用列。例如，_2 和 myAlias._2 都是有效的，都可用于引用 SELECT 列表中的列和 WHERE 子句。
- Column Headers (列标头) – 对于具有标头行的 CSV 格式的对象，可在 SELECT 列表和 WHERE 子句中使用这些标头。尤其在传统 SQL 的 SELECT 和 WHERE 子句表达式中，可以通过 *alias*.*column_name* 或 *column_name* 引用列。

#### JSON

- Document (文档) – 可将 JSON 文档字段作为 *alias*.*name* 进行访问。还可以访问嵌套字段，例如 *alias*.*name1*.*name2*.*name3*。
- 列表 – 可以将零基索引与 [] 运算符结合使用以访问 JSON 列表中的元素。例如，可以通过 *alias*[1] 访问列表中第二个元素。例如，您可以将访问列表元素与字段结合起来，例如 *alias*.*name1*.*name2*[1].*name3*。
- 示例：将此 JSON 对象视为示例数据集：

```
{"name": "Susan Smith",
"org": "engineering",
"projects":
    [
     {"project_name":"project1", "completed":false},
```

```
     {"project_name":"project2", "completed":true}
    ]
}
```

示例 1

以下查询返回以下结果：

```
Select s.name from S3Object s
```

```
{"name":"Susan Smith"}
```

示例 2

以下查询返回以下结果：

```
Select s.projects[0].project_name from S3Object s
```

```
{"project_name":"project1"}
```

标头和属性名称的区分大小写

借助 Amazon S3 Select，您可以使用双引号指示区分大小写的列标头（对于 CSV 对象）和属性（对于 JSON 对象）。如果没有双引号，则对象标头和属性不区分大小写。如果出现歧义，则会抛出错误。

以下示例是：1) 带有指定列标头并对于查询请求将 `FileHeaderInfo` 设置为 `"Use"` 的 CSV 格式的 Amazon S3 对象；或 2) 带有指定属性的 JSON 格式的 Amazon S3 对象。

示例 1：所查询的对象具有标头或属性 `NAME`。

- 以下表达式从对象成功返回值。因为没有引号，所以查询不区分大小写。

```
SELECT s.name from S3Object s
```

- 以下表达式导致出现 400 错误 `MissingHeaderName`。因为有引号，所以查询区分大小写。

```
SELECT s."name" from S3Object s
```

示例 2：所查询的 Amazon S3 对象具有一个包含 NAME 的标头或属性和另一个包含 name 的标头或属性。

- 以下表达式导致出现 400 错误 AmbiguousFieldName。由于无引号，所以查询不区分大小写，但有两个匹配项，因此引发错误。

```
SELECT s.name from S3Object s
```

- 以下表达式从对象成功返回值。因为有引号，所以查询区分大小写，因此没有歧义。

```
SELECT s."NAME" from S3Object s
```

将保留关键字用作用户定义的术语

Amazon S3 Select 具有一组保留关键字，在运行用于查询对象内容的 SQL 表达式时需要使用这组关键字。保留关键字包含函数名称、数据类型、运算符等。在某些情况下，诸如列标头（用于 CSV 文件）或属性（用于 JSON 对象）之类的用户定义的术语可能与保留关键字发生冲突。发生这种情况时，必须使用双引号指示您特意使用与保留关键字冲突的用户定义的术语。否则将会导致出现 400 解析错误。

有关保留关键字的完整列表，请参阅保留关键字。

以下示例是：1) 带有指定列标头和对于查询请求将 FileHeaderInfo 设置为 "Use" 的 CSV 格式的 Amazon S3 对象；或 2) 带有指定属性的 JSON 格式的 Amazon S3 对象。

示例：所查询的对象具有名为 CAST 的标头和属性，但这是保留关键字。

- 以下表达式从对象成功返回值。由于查询中使用了引号，因此 S3 Select 使用用户定义的标题或属性。

```
SELECT s."CAST" from S3Object s
```

- 以下表达式导致出现 400 解析错误。由于查询中不使用引号，因此 CAST 与保留关键字发生冲突。

```
SELECT s.CAST from S3Object s
```

标量表达式

在 WHERE 子句和 SELECT 列表中，您可以使用 SQL 标量表达式 (返回标量值的表达式)。它们具有以下形式：

- ***literal***

  SQL 文本。
- ***column_reference***

  对采用 *column_name* 或 *alias*.*column_name* 形式的列的引用。
- ***unary_op expression***

  在这种情况下，***unary_op*** 是一个 SQL 一元运算符。
- ***expression binary_op expression***

  在这种情况下，***binary_op*** 是一个 SQL 二进制运算符。
- ***func_name***

  在这种情况下，***func_name*** 是要调用的标量函数的名称。
- ***expression*** [ NOT ] BETWEEN ***expression*** AND ***expression***
- ***expression*** LIKE ***expression*** [ ESCAPE ***expression*** ]

## 数据类型

> **Important**
>
> 不再向新客户提供 Amazon S3 Select。Amazon S3 Select 的现有客户可以像往常一样继续使用该功能。了解更多

Amazon S3 Select 支持多个基元数据类型。

数据类型转换

一般规则是遵循 CAST 函数（如果已定义）。如果未定义 CAST，则将所有输入数据视为字符串。在这种情况下，必要时，您必须将输入数据强制转换为相关的数据类型。

有关 CAST 函数的更多信息，请参阅CAST。

## 支持的数据类型

Amazon S3 Select 支持以下这组基元数据类型。

| 名称 | 说明 | 示例 |
| --- | --- | --- |
| `bool` | 一个布尔值，可以是 TRUE 或 FALSE。 | `FALSE` |
| `int`, `integer` | 范围为 -9,223,372,036,854,775,808 到 9,223,372,036,854,775,807 的 8 字节有符号整数。 | `100000` |
| `string` | UTF8 编码的长度可变的字符串。原定设置限制为 1 个字符。最大字符限制为 2,147,483,647。 | `'xyz'` |
| `float` | 8 字节浮点数。 | `CAST(0.456 AS FLOAT)` |
| `decimal`, `numeric` | Base-10 数字，最大精度为 38（即最大有效位数），取值范围在 $-2^{31}$ 到 $2^{31}-1$ 之间（即以 10 为底的指数）。<br><br>**Note**<br>如果您同时提供数值范围和精度，则 Amazon S3 Select 会全部忽略。 | `123.456` |
| `timestamp` | 时间戳表示特定的时刻，始终包括本地偏移，并且能够支持任意精度。<br><br>在文本格式中，时间戳遵循关于日期和时间格式的 W3C 注释，但它们必须以文本 T 结尾（如果时间戳不是最低限度全天精度）。允许使用小数秒，具有至少一位精度，以及无限的最大值。本地时间偏移可以表示为与 UTC 相比的小时:分钟偏移量，或表示为文本 Z 以指示 UTC 的本地时间。本地时间偏移对于具有时间的时间戳是必需的，但对于日期值是不允许的。 | `CAST('2007-04-05T14:30Z' AS TIMESTAMP)` |

### 支持的 Parquet 类型

Amazon S3 Select 支持以下 Parquet 类型。

- DATE
- DECIMAL
- ENUM
- INT(8)
- INT(16)
- INT(32)
- INT(64)
- LIST

> **Note**
>
> 对于 LIST Parquet 类型输出，Amazon S3 Select 仅支持 JSON 格式。但是，如果查询将数据限定为简单值，还可以用 CSV 格式查询 LIST Parquet 类型。

- STRING
- TIMESTAMP 支持的精度（MILLIS/MICROS/NANOS）

> **Note**
>
> 不支持保存为 INT(96) 的时间戳。
> 由于 INT(64) 类型的范围，使用 NANOS 单位的时间戳只能表示介于 1677-09-21 00:12:43 和 2262-04-11 23:47:16 之间的值。超出此范围的值不能用 NANOS 单位表示。

### 将 Parquet 类型映射到 Amazon S3 Select 中支持的数据类型

| Parquet 类型 | 支持的数据类型 |
| --- | --- |
| DATE | timestamp |

| Parquet 类型 | 支持的数据类型 |
| --- | --- |
| DECIMAL | decimal, numeric |
| ENUM | string |
| INT(8) | int, integer |
| INT(16) | int, integer |
| INT(32) | int, integer |
| INT(64) | decimal, numeric |
| LIST | 列表中的每个 Parquet 类型都映射到相应的数据类型。 |
| STRING | string |
| TIMESTAMP | timestamp |

## 运算符

> **Important**
>
> 不再向新客户提供 Amazon S3 Select。Amazon S3 Select 的现有客户可以像往常一样继续使用该功能。了解更多

Amazon S3 Select 支持以下运算符。

### 逻辑运算符

- AND
- NOT
- OR

### 比较运算符

- <
- >
- <=
- >=
- =
- <>
- !=
- BETWEEN
- IN - 例如：IN ('a', 'b', 'c')

### 模式匹配运算符

- LIKE
- _（匹配任何字符）
- %（匹配任何字符序列）

### 一元运算符

- IS NULL
- IS NOT NULL

### 数学运算符

支持加法、减法、乘法、除法和取模，如下所示：

- +
- -
- *
- /
- %

### 运算符优先顺序

下表按降序显示运算符的优先顺序。

| 运算符或元素 | 关联性 | 必需 |
| --- | --- | --- |
| - | 右 | 一元减法 |
| *, /, % | 左 | 乘法、除法和取模 |
| +, - | 左 | 加法、减法 |
| IN | | 设置成员资格 |
| BETWEEN | | 范围包含 |
| LIKE | | 字符串模式匹配 |
| <> | | 小于、大于 |
| = | 右 | 等于、分配 |
| NOT | 右 | 逻辑非 |
| AND | 左 | 逻辑和 |
| OR | 左 | 逻辑或 |

## 保留关键字

> **Important**
>
> 不再向新客户提供 Amazon S3 Select。Amazon S3 Select 的现有客户可以像往常一样继续使用该功能。了解更多

以下是适用于 Amazon S3 Select 的保留关键字列表。这些关键字包括函数名称、数据类型、运算符等，在运行用于查询对象内容的 SQL 表达式时需要使用它们。

```
absolute
action
add
all
allocate
alter
and
any
are
as
asc
assertion
at
authorization
avg
bag
begin
between
bit
bit_length
blob
bool
boolean
both
by
cascade
cascaded
case
cast
catalog
char
char_length
character
character_length
check
clob
close
coalesce
collate
collation
column
commit
connect
```

```
connection
constraint
constraints
continue
convert
corresponding
count
create
cross
current
current_date
current_time
current_timestamp
current_user
cursor
date
day
deallocate
dec
decimal
declare
default
deferrable
deferred
delete
desc
describe
descriptor
diagnostics
disconnect
distinct
domain
double
drop
else
end
end-exec
escape
except
exception
exec
execute
exists
external
```

```
extract
false
fetch
first
float
for
foreign
found
from
full
get
global
go
goto
grant
group
having
hour
identity
immediate
in
indicator
initially
inner
input
insensitive
insert
int
integer
intersect
interval
into
is
isolation
join
key
language
last
leading
left
level
like
limit
list
```

```
local
lower
match
max
min
minute
missing
module
month
names
national
natural
nchar
next
no
not
null
nullif
numeric
octet_length
of
on
only
open
option
or
order
outer
output
overlaps
pad
partial
pivot
position
precision
prepare
preserve
primary
prior
privileges
procedure
public
read
real
```

```
references
relative
restrict
revoke
right
rollback
rows
schema
scroll
second
section
select
session
session_user
set
sexp
size
smallint
some
space
sql
sqlcode
sqlerror
sqlstate
string
struct
substring
sum
symbol
system_user
table
temporary
then
time
timestamp
timezone_hour
timezone_minute
to
trailing
transaction
translate
translation
trim
true
```

```
tuple
union
unique
unknown
unpivot
update
upper
usage
user
using
value
values
varchar
varying
view
when
whenever
where
with
work
write
year
zone
```

## SQL 函数

> **Important**
>
> 不再向新客户提供 Amazon S3 Select。Amazon S3 Select 的现有客户可以像往常一样继续使用该功能。了解更多

Amazon S3 Select 支持以下 SQL 函数。

主题

- 聚合函数
- 条件函数
- 转换函数
- 日期函数
- 字符串函数

## 聚合函数

> **Important**
>
> 不再向新客户提供 Amazon S3 Select。Amazon S3 Select 的现有客户可以像往常一样继续使用该功能。了解更多

Amazon S3 Select 支持以下聚合函数。

| 函数 | 参数类型 | 返回类型 |
| --- | --- | --- |
| AVG(*expression* ) | INT, FLOAT, DECIMAL | DECIMAL 适用于 INT 参数，FLOAT 适用于浮点型参数；否则与参数数据类型相同。 |
| COUNT | - | INT |
| MAX(*expression* ) | INT, DECIMAL | 和参数类型相同。 |
| MIN(*expression* ) | INT, DECIMAL | 和参数类型相同。 |
| SUM(*expression* ) | INT, FLOAT, DOUBLE, DECIMAL | INT 适用于 INT 参数，FLOAT 适用于浮点型参数；否则与参数数据类型相同。 |

SUM 示例

要聚合 S3 清单报告中某个文件夹的对象总大小，请使用 SUM 表达式。

以下 S3 清单报告是使用 GZIP 压缩的 CSV 文件。共有三列。

- 第一列是 S3 清单报告所用于的 S3 桶（*DOC-EXAMPLE-BUCKET*）的名称。
- 第二列是唯一标识桶中对象的对象键名称。

  第一行中的 *example-folder/* 值表示文件夹 *example-folder*。在 Amazon S3 中，当您在桶中创建文件夹时，S3 使用设置为您提供的文件夹名称的键创建一个 0 字节对象。

  第二行中的 *example-folder/object1* 值表示文件夹 *example-folder* 中的对象 *object1*。

  第三行中的 *example-folder/object2* 值表示文件夹 *example-folder* 中的对象 *object2*。

  有关 S3 文件夹的更多信息，请参阅使用文件夹在 Amazon S3 控制台中整理对象。
- 第三列是对象大小（以字节为单位）。

```
"DOC-EXAMPLE-BUCKET","example-folder/","0"
"DOC-EXAMPLE-BUCKET","example-folder/object1","2011267"
"DOC-EXAMPLE-BUCKET","example-folder/object2","1570024"
```

要使用 SUM 表达式计算文件夹 *example-folder* 的总大小，请使用 Amazon S3 Select 运行 SQL 查询。

```
SELECT SUM(CAST(_3 as INT)) FROM s3object s WHERE _2 LIKE 'example-folder/%' AND _2 !=
 'example-folder/';
```

查询结果：

```
3581291
```

条件函数

> **Important**
>
> 不再向新客户提供 Amazon S3 Select。Amazon S3 Select 的现有客户可以像往常一样继续使用该功能。了解更多

Amazon S3 Select 支持以下条件函数。

主题

- CASE
- COALESCE
- NULLIF

## CASE

CASE 表达式是一种条件表达式，类似于其他语言中的 if/then/else 语句。CASE 用于指定存在多个条件时的结果。有两种类型的 CASE 表达式：简单和搜索。

在简单 CASE 表达式中，将一个表达式与一个值比较。在找到匹配项时，将应用 THEN 子句中的指定操作。如果未找到匹配项，则应用 ELSE 子句中的操作。

在搜索 CASE 表达式中，基于布尔表达式计算每个 CASE，而且 CASE 语句会返回第一个匹配的 CASE。如果在 WHEN 子句中未找到匹配的 CASE，则返回 ELSE 子句中的操作。

语法

> **Note**
>
> 目前，Amazon S3 Select 不支持 ORDER BY 或包含新行的查询。请确保使用不带换行符的查询。

以下是用于匹配条件的简单 CASE 语句：

```
CASE expression WHEN value THEN result [WHEN...] [ELSE result] END
```

以下是用于计算每个条件的搜索 CASE 语句：

```
CASE WHEN boolean condition THEN result [WHEN ...] [ELSE result] END
```

示例

> **Note**
>
> 如果您使用 Amazon S3 控制台运行以下示例，并且 CSV 文件包含标题行，请选择排除第一行 CSV 数据。

示例 1：使用简单 CASE 表达式以在查询中将 New York City 替换为 Big Apple。将所有其他城市名称替换为 other。

```
SELECT venuecity, CASE venuecity WHEN 'New York City' THEN 'Big Apple' ELSE 'other' END
 FROM S3Object;
```

查询结果：

```
venuecity        |   case
-----------------+-----------
Los Angeles      | other
New York City    | Big Apple
San Francisco    | other
Baltimore        | other
...
```

示例 2：使用搜索 CASE 表达式来基于单个门票销售的 pricepaid 值分配组编号：

```
SELECT pricepaid, CASE WHEN CAST(pricepaid as FLOAT) < 10000 THEN 'group 1' WHEN
 CAST(pricepaid as FLOAT) > 10000 THEN 'group 2' ELSE 'group 3' END FROM S3Object;
```

查询结果：

```
pricepaid |  case
-----------+---------
12624.00 | group 2
10000.00 | group 3
10000.00 | group 3
9996.00 | group 1
9988.00 | group 1
...
```

### COALESCE

COALESCE 按顺序评估参数并返回第一个非未知值，即第一个非空或非缺失值。此函数无法传播空值和缺失值。

#### 语法

```
COALESCE ( expression, expression, ... )
```

#### 参数

*expression*

对其执行函数的目标表达式。

#### 示例

```
COALESCE(1)                -- 1
COALESCE(null)             -- null
COALESCE(null, null)       -- null
COALESCE(missing)          -- null
COALESCE(missing, missing) -- null
COALESCE(1, null)          -- 1
COALESCE(null, null, 1)    -- 1
COALESCE(null, 'string')   -- 'string'
COALESCE(missing, 1)       -- 1
```

### NULLIF

给定两个表达式，如果两个表达式的计算结果为相同值，则 NULLIF 返回 NULL；否则 NULLIF 返回第一个表达式的计算结果。

#### 语法

```
NULLIF ( expression1, expression2 )
```

#### 参数

*expression1*, *expression2*

对其执行函数的目标表达式。

示例

```
NULLIF(1, 1)             -- null
NULLIF(1, 2)             -- 1
NULLIF(1.0, 1)           -- null
NULLIF(1, '1')           -- 1
NULLIF([1], [1])         -- null
NULLIF(1, NULL)          -- 1
NULLIF(NULL, 1)          -- null
NULLIF(null, null)       -- null
NULLIF(missing, null)    -- null
NULLIF(missing, missing) -- null
```

转换函数

> **Important**
>
> 不再向新客户提供 Amazon S3 Select。Amazon S3 Select 的现有客户可以像往常一样继续使用该功能。了解更多

Amazon S3 Select 支持以下转换函数。

主题

- CAST

CAST

CAST 函数将一种类型的实体 (如计算结果为单个值的表达式) 转换为另一种类型。

语法

```
CAST ( expression AS data_type )
```

参数

*expression*

一个或多个值、运算符和计算结果为值的 SQL 函数的组合。

*data_type*

要将表达式转换到的目标数据类型，如 INT。有关支持的数据类型的列表，请参阅 数据类型。

示例

```
CAST('2007-04-05T14:30Z' AS TIMESTAMP)
CAST(0.456 AS FLOAT)
```

日期函数

> **Important**
>
> 不再向新客户提供 Amazon S3 Select。Amazon S3 Select 的现有客户可以像往常一样继续使用该功能。了解更多

Amazon S3 Select 支持以下日期函数。

主题

- DATE_ADD
- DATE_DIFF
- EXTRACT
- TO_STRING
- TO_TIMESTAMP
- UTCNOW

DATE_ADD

给定日期部分、数量和时间戳，DATE_ADD 返回通过修改由数量的日期部分而更新的时间戳。

语法

```
DATE_ADD( date_part, quantity, timestamp )
```

参数

*date_part*

指定要修改的日期部分。这可能是以下值之一：

- 年
- 个月
- day
- 小时
- minute
- 秒

*quantity*

应用到已更新的时间戳的值。*quantity* 的正值添加到时间戳的 date_part，并减去负值。

*timestamp*

对其执行函数的目标时间戳。

示例

```
DATE_ADD(year, 5, `2010-01-01T`)                -- 2015-01-01 (equivalent to
 2015-01-01T)
DATE_ADD(month, 1, `2010T`)                     -- 2010-02T (result will add precision
 as necessary)
DATE_ADD(month, 13, `2010T`)                    -- 2011-02T
DATE_ADD(day, -1, `2017-01-10T`)                -- 2017-01-09 (equivalent to
 2017-01-09T)
DATE_ADD(hour, 1, `2017T`)                      -- 2017-01-01T01:00-00:00
DATE_ADD(hour, 1, `2017-01-02T03:04Z`)          -- 2017-01-02T04:04Z
DATE_ADD(minute, 1, `2017-01-02T03:04:05.006Z`) -- 2017-01-02T03:05:05.006Z
DATE_ADD(second, 1, `2017-01-02T03:04:05.006Z`) -- 2017-01-02T03:04:06.006Z
```

DATE_DIFF

给定日期部分和两个有效的时间戳，DATE_DIFF 返回日期部分的不同之处。当 *date_part* 的 *timestamp1* 值大于 *date_part* 的 *timestamp2* 值时，返回值为负整数。当 *date_part* 的 *timestamp1* 值小于 *date_part* 的 *timestamp2* 值时，返回值为正整数。

语法

```
DATE_DIFF( date_part, timestamp1, timestamp2 )
```

参数

*date_part*

指定要比较的时间戳部分。有关 date_part 的定义，请参阅DATE_ADD。

*timestamp1*

要比较的第一个时间戳。

*timestamp2*

要比较的第二个时间戳。

示例

```
DATE_DIFF(year, `2010-01-01T`, `2011-01-01T`)            -- 1
DATE_DIFF(year, `2010T`, `2010-05T`)                     -- 4 (2010T is equivalent to
 2010-01-01T00:00:00.000Z)
DATE_DIFF(month, `2010T`, `2011T`)                       -- 12
DATE_DIFF(month, `2011T`, `2010T`)                       -- -12
DATE_DIFF(day, `2010-01-01T23:00`, `2010-01-02T01:00`) -- 0 (need to be at least 24h
 apart to be 1 day apart)
```

## EXTRACT

给定日期部分和时间戳，EXTRACT 返回时间戳的日期部分的值。

语法

```
EXTRACT( date_part FROM timestamp )
```

参数

*date_part*

指定时间戳中要提取的部分。这可能是以下值之一：

- YEAR

- MONTH
- DAY
- HOUR
- MINUTE
- SECOND
- TIMEZONE_HOUR
- TIMEZONE_MINUTE

*timestamp*

对其执行函数的目标时间戳。

示例

```
EXTRACT(YEAR FROM `2010-01-01T`)                              -- 2010
EXTRACT(MONTH FROM `2010T`)                                   -- 1 (equivalent to
 2010-01-01T00:00:00.000Z)
EXTRACT(MONTH FROM `2010-10T`)                                -- 10
EXTRACT(HOUR FROM `2017-01-02T03:04:05+07:08`)                -- 3
EXTRACT(MINUTE FROM `2017-01-02T03:04:05+07:08`)              -- 4
EXTRACT(TIMEZONE_HOUR FROM `2017-01-02T03:04:05+07:08`)       -- 7
EXTRACT(TIMEZONE_MINUTE FROM `2017-01-02T03:04:05+07:08`)     -- 8
```

### TO_STRING

给定时间戳和格式模式，TO_STRING 以指定格式返回时间戳的字符串表示形式。

语法

```
TO_STRING ( timestamp time_format_pattern )
```

参数

*timestamp*

对其执行函数的目标时间戳。

*time_format_pattern*

具有以下特殊字符解释的字符串：

| 格式 | 示例 | 说明 |
| --- | --- | --- |
| yy | 69 | 2 位年份 |
| y | 1969 | 4 位年份 |
| yyyy | 1969 | 以零填充的 4 位年份 |
| M | 1 | 一年中的月 |
| MM | 01 | 以零填充的一年中的月份 |
| MMM | Jan | 一年中的月的缩写名称 |
| MMMM | January | 一年中的月的完整名称 |
| MMMMM | J | 一年中的月的首字母（注释：此格式与 TO_TIMESTAMP 函数结合使用时无效） |
| d | 2 | 一个月中的日 (1-31) |
| dd | 02 | 以零填充的一个月中的日 (01-31) |
| a | AM | 一天的 AM 或 PM |

| 格式 | 示例 | 说明 |
| --- | --- | --- |
| h | 3 | 一天中的小时 (1-12) |
| hh | 03 | 以零填充的一天中的小时 (01-12) |
| H | 3 | 一天中的小时 (0-23) |
| HH | 03 | 以零填充的一天中的小时 (00-23) |
| m | 4 | 一小时中的分钟 (0-59) |
| mm | 04 | 以零填充的一小时中的分钟 (00-59) |
| s | 5 | 一分钟中的秒 (0-59) |
| ss | 05 | 以零填充的一分钟中的秒 (00-59) |
| S | 0 | 一秒钟的若干分之几（精度：0.1，范围：0.0-0.9） |

| 格式 | 示例 | 说明 |
| --- | --- | --- |
| SS | 6 | 一秒钟的若干分之几（精度：0.01，范围：0.0-0.99） |
| SSS | 60 | 一秒钟的若干分之几（精度：0.001，范围：0.0-0.999） |
| … | … | … |
| SSSSSSSSS | 60000000 | 一秒钟的若干分之几（最大精度：1 纳秒，范围：0.0-0.999999999） |
| n | 60000000 | 纳秒级 |
| X | +07 或 Z | 小时数偏移，如果偏移为 0，则为 Z |
| XX 或 XXXX | +0700 或 Z | 小时和分钟数偏移，如果偏移为 0，则为 Z |
| XXX 或 XXXXX | +07:00 或 Z | 小时和分钟数偏移，如果偏移为 0，则为 Z |

| 格式 | 示例 | 说明 |
| --- | --- | --- |
| x | 7 | 小时数偏移 |
| xx 或 xxxx | 700 | 小时和分钟数偏移 |
| xxx 或 xxxxx | +07:00 | 小时和分钟数偏移 |

示例

```
TO_STRING(`1969-07-20T20:18Z`,  'MMMM d, y')                    -- "July 20, 1969"
TO_STRING(`1969-07-20T20:18Z`, 'MMM d, yyyy')                   -- "Jul 20, 1969"
TO_STRING(`1969-07-20T20:18Z`, 'M-d-yy')                        -- "7-20-69"
TO_STRING(`1969-07-20T20:18Z`, 'MM-d-y')                        -- "07-20-1969"
TO_STRING(`1969-07-20T20:18Z`, 'MMMM d, y h:m a')               -- "July 20, 1969 8:18
 PM"
TO_STRING(`1969-07-20T20:18Z`, 'y-MM-dd''T''H:m:ssX')           --
 "1969-07-20T20:18:00Z"
TO_STRING(`1969-07-20T20:18+08:00Z`, 'y-MM-dd''T''H:m:ssX')     --
 "1969-07-20T20:18:00Z"
TO_STRING(`1969-07-20T20:18+08:00`, 'y-MM-dd''T''H:m:ssXXXX')   --
 "1969-07-20T20:18:00+0800"
TO_STRING(`1969-07-20T20:18+08:00`, 'y-MM-dd''T''H:m:ssXXXXX')  --
 "1969-07-20T20:18:00+08:00"
```

### TO_TIMESTAMP

给定字符串，TO_TIMESTAMP 将其转换为时间戳。TO_TIMESTAMP 是 TO_STRING 的逆运算。

语法

```
TO_TIMESTAMP ( string )
```

参数

*string*

对其执行函数的目标字符串。

示例

```
TO_TIMESTAMP('2007T')                          -- `2007T`
TO_TIMESTAMP('2007-02-23T12:14:33.079-08:00') -- `2007-02-23T12:14:33.079-08:00`
```

### UTCNOW

UTCNOW 以时间戳的形式返回当前时间（UTC）。

语法

```
UTCNOW()
```

参数

UTCNOW 不带任何参数。

示例

```
UTCNOW() -- 2017-10-13T16:02:11.123Z
```

### 字符串函数

> **Important**
>
> 不再向新客户提供 Amazon S3 Select。Amazon S3 Select 的现有客户可以像往常一样继续使用该功能。了解更多

Amazon S3 Select 支持以下字符串函数。

主题

- CHAR_LENGTH, CHARACTER_LENGTH
- LOWER
- SUBSTRING
- TRIM
- UPPER

### CHAR_LENGTH, CHARACTER_LENGTH

CHAR_LENGTH（或 CHARACTER_LENGTH）计算指定字符串中的字符数。

> **Note**
>
> CHAR_LENGTH 和 CHARACTER_LENGTH 是同义词。

#### 语法

```
CHAR_LENGTH ( string )
```

#### 参数

*string*

对其执行函数的目标字符串。

#### 示例

```
CHAR_LENGTH('')          -- 0
CHAR_LENGTH('abcdefg')   -- 7
```

### LOWER

给定字符串，LOWER 将所有大写字符转换为小写字符。所有非大写字符保持不变。

#### 语法

```
LOWER ( string )
```

#### 参数

*string*

对其执行函数的目标字符串。

示例

```
LOWER('AbCdEfG!@#$') -- 'abcdefg!@#$'
```

### SUBSTRING

指定字符串、起始索引和长度（可选），SUBSTRING 返回从起始索引直至字符串结尾处的子字符串，或最大长度为输入的字符串长度的子字符串。

> **Note**
>
> 输入字符串的首字符的索引位置为 1。
>
> - 如果 `start < 1`，且未指定长度，则索引位置设置为 1。
> - 如果 `start < 1`，且指定了长度，则索引位置设置为 `start + length -1`。
> - 如果 `start + length -1 < 0`，则返回一个空字符串。
> - 如果 `start + length -1 > = 0`，则返回从索引位置 1 开始的长度为 `start + length - 1` 的子字符串。

语法

```
SUBSTRING( string FROM start [ FOR length ] )
```

参数

*string*

对其执行函数的目标字符串。

*start*

字符串的开始位置。

*length*

要返回的子字符串的长度。如果不存在，则执行到字符串的结尾。

示例

```
SUBSTRING("123456789", 0)      -- "123456789"
```

```
SUBSTRING("123456789", 1)      -- "123456789"
SUBSTRING("123456789", 2)      -- "23456789"
SUBSTRING("123456789", -4)     -- "123456789"
SUBSTRING("123456789", 0, 999) -- "123456789"
SUBSTRING("123456789", 1, 5)   -- "12345"
```

### TRIM

从字符串中剪裁前导或尾随字符。要删除的原定设置字符为空格 ( ' ' ) 。

#### 语法

```
TRIM ( [[LEADING | TRAILING | BOTH remove_chars] FROM] string )
```

#### 参数

*string*

对其执行函数的目标字符串。

LEADING | TRAILING | BOTH

此参数指示是否剪裁前导和/或尾随字符。

*remove_chars*

要删除的一组字符。*remove_chars* 可能是长度 > 1 的字符串。此函数返回包含在已删除字符串开头或结尾发现的 *remove_chars* 中任何字符的字符串。

#### 示例

```
TRIM('       foobar         ')               -- 'foobar'
TRIM('      \tfoobar\t         ')            -- '\tfoobar\t'
TRIM(LEADING FROM '       foobar         ')  -- 'foobar         '
TRIM(TRAILING FROM '       foobar         ') -- '       foobar'
TRIM(BOTH FROM '       foobar         ')     -- 'foobar'
TRIM(BOTH '12' FROM '1112211foobar22211122') -- 'foobar'
```

### UPPER

给定字符串，UPPER 将所有小写字符转换为大写字符。所有非小写字符保持不变。

### 语法

```
UPPER ( string )
```

### 参数

*string*

对其执行函数的目标字符串。

### 示例

```
UPPER('AbCdEfG!@#$') -- 'ABCDEFG!@#$'
```

# 使用目录存储桶

目录桶将数据按层次结构组织到目录中，而不是通用桶的扁平存储结构。目录存储桶没有前缀限制，单个目录可以横向扩展。

每个 Amazon Web Services 账户中最多可以创建 100 个目录存储桶，并且对存储桶中可以存储的对象数量没有限制。您的存储桶限额适用于您的 Amazon Web Services 账户中的每个区域。如果您的应用程序需要提高此限制，请联系 Amazon Web Services 支持。

> **Important**
>
> 可用区中在至少 90 天期间内没有请求活动的目录存储桶将转换为非活动状态。处于非活动状态时，目录存储桶暂时无法进行读取和写入。非活动存储桶会保留所有存储、对象元数据和存储桶元数据。现有的存储费用适用于非活动桶。如果您向非活动桶发出访问请求，该桶通常会在几分钟内转换为活动状态。在此转换期间，读取和写入操作会返回 HTTP 503 (Service Unavailable) 错误代码。这不适用于本地区域中的存储桶。

Amazon S3 存储桶有几种类型。在创建存储桶之前，请确保选择最适合应用程序和性能要求的存储桶类型。有关各种存储桶类型以及每种类型的相应用例的更多信息，请参阅存储桶。

以下主题提供有关目录存储桶的信息。有关通用存储桶的更多信息，请参阅通用存储桶概述。

有关目录存储桶的更多信息，请参阅以下主题。

- 目录存储桶名称
- 目录
- 键名称
- 访问权限管理

## 目录存储桶名称

目录存储桶名称由您提供的基本名称和包含存储桶所在区域（可用区或本地区域）ID 的后缀组成。目录存储桶名称必须使用以下格式并遵循目录存储桶的命名规则：

```
bucket-base-name--zone-id--x-s3
```

例如，以下目录存储桶名称包含可用区 ID usw2-az1：

```
bucket-base-name--usw2-az1--x-s3
```

有关更多信息，请参阅 目录存储桶命名规则。

## 目录

目录桶将数据按层次结构组织到目录中，而不是通用桶的扁平存储结构。

对于分层命名空间，对象键中的分隔符很重要。唯一支持的分隔符是正斜杠（/）。目录由分隔符边界确定。例如，对象键 dir1/dir2/file1.txt 会自动创建目录 dir1/ 和 dir2/，并将对象 file1.txt 添加到路径 dir1/dir2/file1.txt 中的 /dir2 目录。

目录存储桶索引模型会为 ListObjectsV2 API 操作返回未排序的结果。如果您需要将结果限制在存储桶的某个子部分，则可以在 prefix 参数中指定子目录路径，例如 prefix=dir1/。

## 键名称

对于目录存储桶，多个对象键共用的子目录将使用第一个对象键创建。同一子目录的其它对象键使用之前创建的子目录。此模型使您可以灵活地选择最适合应用程序的对象键，同时同样支持稀疏目录和密集目录。

## 访问权限管理

目录存储桶默认在存储桶级别启用了所有 S3 屏蔽公共访问权限设置。S3 对象所有权设置为强制存储桶拥有者，并禁用访问控制列表（ACL）。无法修改这些设置。

默认情况下，用户没有目录存储桶的权限。要授予对目录存储桶的访问权限，您可以使用 IAM 创建用户、组或角色，然后将权限附加到这些身份。有关更多信息，请参阅 使用 IAM 对区域端点 API 操作进行授权。

还可以通过接入点控制对目录存储桶的访问权限。访问点可简化对 Amazon S3 中的共享数据集的大规模数据访问管理。接入点是您创建的具有唯一性的主机名，用于对通过接入点发出的所有请求强制实施不同的权限和网络控制。有关更多信息，请参阅 通过接入点管理对目录存储桶中共享数据集的访问权限。

# 目录存储桶配额

配额（也称为限制）是 Amazon Web Services 账户的服务资源或操作的最大数量。以下是目录存储桶的配额。有关 Amazon S3 中配额的更多信息，请参阅 Amazon S3 quotas。

| 名称 | 默认值 | 可调整 | 描述 |
| --- | --- | --- | --- |
| 目录存储桶 | 每个账户：100 | 是 | 您可以在一个账户中创建的 Amazon S3 目录存储桶的数量。 |
| 每个目录存储桶的读取 TPS | 每个目录存储桶：读取 TPS 多达 200000 | 要请求提高配额，请联系 Support。 | 每个目录存储桶每秒的 GET/HEAD 请求数。 |
| 每个目录存储桶的写入 TPS | 每个目录存储桶：写入 TPS 多达 100000 | 要请求提高配额，请联系 Support。 | 每个目录存储桶每秒的 PUT/DELETE 请求数。 |

# 创建和使用目录存储桶

有关使用目录存储桶的更多信息，请参阅以下主题。

- 目录存储桶的应用场景
- 目录存储桶的差异
- 目录存储桶的联网
- 目录存储桶命名规则
- 查看目录存储桶属性
- 管理目录存储桶策略
- 清空目录存储桶
- 删除目录存储桶
- 列出目录存储桶
- 确定您是否可以访问目录存储桶
- 使用目录桶中的对象
- 目录存储桶的安全性

- 通过接入点管理对目录存储桶中共享数据集的访问权限
- 优化目录存储桶性能
- 使用目录存储桶进行开发

# 目录存储桶的应用场景

目录存储桶支持在以下存储桶位置类型中创建存储桶：可用区或本地区域。

对于低延迟应用场景，您可以在单个可用区中创建目录存储桶来存储数据。可用区中的目录存储桶支持 S3 Express One Zone 存储类。如果您的应用程序注重性能，并且受益于个位数毫秒的 PUT 和 GET 延迟，则建议使用 S3 Express One Zone 存储类。要了解有关在可用区中创建目录存储桶的更多信息，请参阅高性能工作负载。

对于数据驻留应用场景，您可以在单个 Amazon 专用本地区域（DLZ）中创建目录存储桶来存储数据。Local Zones 中的目录存储桶支持 S3 One Zone-Infrequent Access（S3 One Zone-IA；Z-IA）存储类。要了解有关在 Local Zones 中创建目录存储桶的更多信息，请参阅数据驻留工作负载。

主题

- 高性能工作负载
- 数据驻留工作负载

## 高性能工作负载

### S3 Express One Zone

您可以将 Amazon S3 Express One Zone 存储类用于高性能工作负载。S3 Express One Zone 是第一种可以在其中选择单个可用区的 S3 存储类，您可以选择将您的对象存储与计算资源联合托管在一个位置，从而提供尽可能高的访问速度。S3 Express One Zone 中的对象存储在可用区内的目录存储桶中。有关目录存储桶的更多信息，请参阅目录存储桶。

Amazon S3 Express One Zone 是高性能的单区 Amazon S3 存储类，专门用于为延迟要求极高的应用程序提供稳定的毫秒级数据访问。S3 Express One Zone 是目前具有极低延迟的云对象存储类，相比 S3 Standard，其数据访问速度要快 10 倍，且请求成本低 50%。请求的完成速度实现了数量级的提升，应用程序可以直接从中获益。S3 Express One Zone 提供与其它 S3 存储类相似的性能弹性。S3 Express One Zone 适用于需要一致的个位数毫秒级延迟的工作负载或性能关键型应用程序。

与 Amazon S3 存储类一样，您无需事先规划或预调配容量或吞吐量需求。您可以根据需要纵向扩展或缩减，并通过 Amazon S3 API 访问数据。

Amazon S3 Express One Zone 存储类设计为在单个可用区内提供 99.95% 的可用性，并由 Amazon S3 服务等级协议提供保障。使用 S3 Express One Zone，您的数据将冗余地存储在单个可用区中的多个设备上。S3 Express One Zone 设计为通过快速检测和修复任何丢失的冗余来处理并发设备故障。在现有设备出现故障时，S3 Express One Zone 会自动将请求转移到相同可用区内的新设备。这种冗余有助于确保不间断地访问可用区中的数据。

S3 Express One Zone 非常适合任何需要尽可能减少访问对象所需延迟的应用程序。此类应用程序可以是人机交互式工作流，例如视频编辑，在这种情况下，创意专业人士需要在通过用户界面访问内容时获得快速的响应。对数据响应能力具有类似要求的分析和机器学习工作负载也可以从 S3 Express One Zone 中获益，尤其是大量访问小文件或者有大量随机访问情况时。S3 Express One Zone 可以与其它 Amazon Web Services 服务一起使用来支持分析和人工智能与机器学习（AI/ML）工作负载，例如 Amazon EMR、Amazon SageMaker AI 和 Amazon Athena。

对于使用 S3 Express One Zone 存储类的目录存储桶，数据会存储在单个可用区内的多个设备上，但不会跨多个可用区进行冗余存储。当创建目录存储桶以使用 S3 Express One Zone 时，我们建议您指定 Amazon EC2、Amazon Elastic Kubernetes Service 或 Amazon Elastic Container Service（Amazon ECS）计算实例的本地 Amazon Web Services 区域和可用区，以优化性能。

使用 S3 Express One Zone 时，您可以使用网关 VPC 端点，与虚拟私有云（VPC）中的目录桶进行交互。借助网关端点，您可以从 VPC 访问 S3 Express One Zone 目录桶，而无需为 VPC 配备互联网网关或 NAT 设备，也无需任何额外费用。

对于目录桶，您可以使用您用于通用桶和其它存储类的相同 Amazon S3 API 操作和特征。这些包括适用于 Amazon S3 的 Mountpoint、具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）、S3 批量操作和 S3 屏蔽公共访问权限。您可以通过 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）、Amazon SDK 和 Amazon S3 REST API 访问 S3 Express One Zone。

有关 S3 Express One Zone 的更多信息，请参阅以下主题。

- 概览
- S3 Express One Zone 的功能
- 相关服务
- 后续步骤

## 概览

为了优化性能和减少延迟，S3 Express One Zone 引入了以下新概念。

可用区

Amazon S3 Express One Zone 存储类设计为在单个可用区内提供 99.95% 的可用性，并由 Amazon S3 服务等级协议提供保障。使用 S3 Express One Zone，您的数据将冗余地存储在单个可用区中的多个设备上。S3 Express One Zone 设计为通过快速检测和修复任何丢失的冗余来处理并发设备故障。在现有设备出现故障时，S3 Express One Zone 会自动将请求转移到相同可用区内的新设备。这种冗余有助于确保不间断地访问可用区中的数据。

可用区是 Amazon Web Services 区域 中一个或多个具有冗余电源、网络和连接的离散数据中心。创建目录存储桶时，您可以选择存储桶所在的可用区以及 Amazon Web Services 区域。

单可用区

创建目录存储桶时，您可以选择可用区和 Amazon Web Services 区域。

目录存储桶使用 S3 Express One Zone 存储类，该存储类专用于注重性能的应用程序。S3 Express One Zone 是第一种可以在其中选择单个可用区的 S3 存储类，您可以选择将您的对象存储与计算资源联合托管在一个位置，从而提供尽可能高的访问速度。

使用 S3 Express One Zone，您的数据将冗余地存储在单个可用区中的多个设备上。S3 Express One Zone 设计为在单个可用区内提供 99.95% 的可用性，并由 Amazon S3 服务等级协议提供支持。有关更多信息，请参阅 可用区。

端点和网关 VPC 端点

目录桶的桶管理 API 操作可通过区域端点使用，称为区域端点 API 操作。区域端点 API 操作的示例包括 `CreateBucket` 和 `DeleteBucket`。创建目录存储桶后，您可以使用可用区端点 API 操作来上传和管理目录存储桶中的对象。可用区端点 API 操作可通过可用区端点执行。可用区端点 API 操作的示例包括 `PutObject` 和 `CopyObject`。

您可以使用网关 VPC 端点从 VPC 访问 S3 Express One Zone。创建网关端点后，您可以将其添加作为路由表中的目标，用于从您的 VPC 流向 S3 Express One Zone 的流量。与 Amazon S3 一样，使用网关端点不会产生任何额外费用。有关如何配置网关 VPC 端点的更多信息，请参阅 目录存储桶的联网

基于会话的授权

借助 S3 Express One Zone，您可以通过基于会话的新机制，对请求进行身份验证和授权，该机制经过优化，可提供极低的延迟。您可以使用 `CreateSession` 来请求临时凭证，以便提供对存储桶的低延迟访问。这些临时凭证的作用范围限制为特定的 S3 目录存储桶。会话令牌仅用于可用区（对象级）操作（CopyObject 除外）。有关更多信息，请参阅 使用 `CreateSession` 对可用区端点 API 操作进行授权。

S3 Express One Zone 支持的 Amazon SDK 代表您处理会话的建立和刷新。为了保护您的会话，临时安全凭证在 5 分钟后过期。您在下载和安装 Amazon SDK 并配置必要的 Amazon Identity and Access Management（IAM）权限后，便可立即开始使用 API 操作。

S3 Express One Zone 的功能

以下 S3 功能可用于 S3 Express One Zone。有关支持的 API 操作和不支持的特征的完整列表，请参阅目录存储桶的差异。

访问管理和安全性

您可以使用以下功能来审计和管理访问权限。默认情况下，目录存储桶为私有，只有被明确授予访问权限的用户才可以访问。与可以在存储桶、前缀或对象标签级设置访问控制边界的通用存储桶不同，目录存储桶只能在存储桶级设置访问控制边界。有关更多信息，请参阅 使用 IAM 对区域端点 API 操作进行授权。

- S3 屏蔽公共访问权限 – 默认情况下，所有 S3 屏蔽公共访问权限设置均在桶级启用。无法修改此默认设置。
- S3 对象所有权（默认情况下为强制桶拥有者）– 目录桶不支持访问控制列表（ACL）。目录桶对于 S3 对象所有权自动使用强制桶拥有者设置。强制桶拥有者意味着 ACL 被禁用，桶拥有者自动拥有并完全控制桶中的每个对象。无法修改此默认设置。
- Amazon Identity and Access Management（IAM） – IAM 有助于您安全地控制对目录存储桶的访问权限。您可以使用 IAM，通过 `s3express:CreateSession` 操作授予对桶管理（区域）API 操作和对象管理（可用区）API 操作的访问权限。有关更多信息，请参阅 使用 IAM 对区域端点 API 操作进行授权。与对象管理操作不同，存储桶管理操作不能跨账户。只有存储桶拥有者可以执行这些操作。
- 存储桶策略 – 使用基于 IAM 的策略语言，为目录存储桶配置基于资源的权限。您还可以使用 IAM 来控制对 `CreateSession` API 的访问权限，这允许您使用可用区或对象管理 API 操作。您可以向可用区 API 操作授予同账户或跨账户访问权限。有关 S3 Express One Zone 权限和策略的更多信息，请参阅使用 IAM 对区域端点 API 操作进行授权。
- 适用于 S3 的 IAM Access Analyzer – 评估和监控您的访问策略，确保这些策略仅提供对 S3 资源的预期访问权限。

日志记录和监控

S3 Express One Zone 使用以下 S3 日志记录和监控工具，您可以使用这些工具来监控和控制资源的使用方式：

- Amazon CloudWatch 指标 – 通过使用 CloudWatch 收集和跟踪指标，监控您的 Amazon 资源和应用程序。S3 Express One Zone 使用与其他 Amazon S3 存储类相同的 CloudWatch 命名空间（`AWS/S3`），并支持目录存储桶的日常存储指标：`BucketSizeBytes` 和 `NumberOfObjects`。有关更多信息，请参阅 使用 Amazon CloudWatch 监控指标。
- Amazon CloudTrail 日志 – Amazon CloudTrail 是一项 Amazon Web Services 服务，通过记录用户、角色或 Amazon Web Services 服务执行的操作，协助您实现运营和风险审计、治理以及 Amazon Web Services 账户合规性。对于 S3 Express One Zone，CloudTrail 将区域端点 API 操作（例如 `CreateBucket` 和 `PutBucketPolicy`）捕获为管理事件，并将可用区 API 操作（例如 `GetObject` 和 `PutObject`）捕获为数据事件。这些事件包括了在 Amazon Web Services Management Console、Amazon Command Line Interface（Amazon CLI）、Amazon SDK 和 Amazon API 操作中执行的操作。有关更多信息，请参阅使用 Amazon CloudTrail 为 S3 Express One Zone 记录日志。

> **Note**
>
> S3 Express One Zone 不支持 Amazon S3 服务器访问日志。

对象管理

您可以使用 Amazon S3 控制台、Amazon SDK 和 Amazon CLI 管理对象存储。以下特征可用于 S3 Express One Zone 的对象管理：

- S3 批量操作 – 使用批量操作对目录存储桶中的对象执行批量操作，例如复制和调用 Amazon Lambda 函数。例如，您可以使用批量操作在目录存储桶和通用存储桶之间复制对象。通过批量操作，您可以使用 Amazon SDK 或 Amazon CLI，或者只需在 Amazon S3 控制台中单击几次，即可通过单个 S3 请求大规模管理数十亿个对象。
- 导入 – 创建目录存储桶后，您可以使用 Amazon S3 控制台中的导入功能在存储桶中填充对象。导入是一种创建批量操作作业的简化方法，用于将对象从通用存储桶复制到目录存储桶。

Amazon SDK 和客户端库

您可以使用 Amazon SDK 和客户端库来管理对象存储。

- 适用于 Amazon S3 的 Mountpoint – 适用于 Amazon S3 的 Mountpoint 是一种开源文件客户端，可提供高吞吐量的访问，从而降低 Amazon S3 上数据湖的计算成本。适用于 Amazon S3 的 Mountpoint 将本地文件系统 API 调用转换为 S3 对象 API 调用，如 `GET` 和 `LIST`。它非常适合有大

量读取操作的数据湖工作负载，在这种情况下需要处理数 PB 的数据，且需要 Amazon S3 提供的高弹性吞吐量来跨数千个实例进行纵向扩展和缩减。

- S3A – S3A 是推荐使用的 Hadoop 兼容接口，用于访问 Amazon S3 中的数据存储。S3A 取代了 S3N Hadoop 文件系统客户端。
- Amazon 上的 PyTorch – Amazon 上的 PyTorch 是一个开源深度学习框架，它简化了机器学习模型开发以及将其部署到生产环境的过程。
- Amazon SDK – 为 Amazon S3 开发应用程序时，您可以使用 Amazon SDK。Amazon SDK 包装了底层 Amazon S3 REST API，可以简化您的编程任务。有关将 Amazon SDK 与 S3 Express One Zone 结合使用的更多信息，请参阅the section called “Amazon SDK”。

### 数据保护和加密

S3 Express One Zone 中的对象自动通过采用 Amazon S3 托管式密钥的服务器端加密（SSE-S3）进行加密。S3 Express One Zone 还支持使用 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）。S3 Express One Zone 不支持使用客户提供的加密密钥的服务器端加密（SSE-C），也不支持使用 Amazon KMS keys 的双层服务器端加密（DSSE-KMS）。有关更多信息，请参阅 数据保护和加密。

S3 Express One Zone 可让您选择用于在上传或下载过程中验证数据的校验和算法。您可以选择以下安全哈希算法（SHA）或循环冗余校验（CRC）数据完整性检查算法之一：CRC32、CRC32C、SHA-1 和 SHA-256。S3 Express One Zone 存储类不支持基于 MD5 的校验和。

有关更多信息，请参阅 其他 S3 校验和最佳实践。

### Amazon 签名版本 4（SigV4）

S3 Express One Zone 使用 Amazon 签名版本 4（SigV4）。SigV4 是一种签名协议，用于对通过 HTTPS 发送到 Amazon S3 的请求进行身份验证。S3 Express One Zone 使用 Amazon Sigv4 对请求签名。有关更多信息，请参阅《Amazon Simple Storage Service API》参考中的验证请求 (Amazon Signature Version 4)。

### 强一致性

在所有 Amazon Web Services 区域中，S3 Express One Zone 为针对目录桶中对象的 PUT 和 DELETE 请求，提供了可靠的先写后读一致性。有关更多信息，请参阅 Amazon S3 数据一致性模型。

### 相关服务

您可以将以下 Amazon Web Services 服务与 S3 Express One Zone 存储类配合使用，以支持您的特定低延迟使用场景。

- Amazon Elastic Compute Cloud（Amazon EC2）– Amazon EC2 在 Amazon Web Services 云 中提供安全可扩展的计算容量。使用 Amazon EC2 可减少前期的硬件投入，因此您能够快速开发和部署应用程序。您可以使用 Amazon EC2 启动所需数量的虚拟服务器，配置安全性和联网以及管理存储。
- Amazon Lambda – Lambda 是一项计算服务，可使您无需预置或管理服务器即可运行代码。您在存储桶上配置通知设置，并向 Amazon S3 授予权限来根据函数的基于资源的权限策略调用函数。
- Amazon Elastic Kubernetes Service（Amazon EKS）– Amazon EKS 是一项托管式服务，无需在 Amazon 上安装、操作和维护自己的 Kubernetes 控制面板。Kubernetes 是一个开源系统，用于自动管理、扩展和部署容器化应用程序。
- Amazon Elastic Container Service（Amazon ECS）– Amazon ECS 是完全托管的容器编排服务，可协助您轻松地部署、管理和扩展容器化应用程序。
- Amazon Key Management Service（Amazon KMS）– Amazon Key Management Service（Amazon KMS）是一项 Amazon 托管式服务，可让您轻松创建和控制加密您的数据所用的加密密钥。您在 Amazon KMS 中创建的 Amazon KMS 密钥受 FIPS 140-2 经验证硬件安全模块（HSM）的保护。要使用或管理 KMS 密钥，您需要与 Amazon KMS 交互。
- Amazon Athena – Athena 是一种交互式查询服务，方便通过使用标准 SQL 直接分析 Amazon S3 中的数据。还可以使用 Athena，通过 Apache Spark 以交互方式运行数据分析，而无需规划、配置或管理资源。在 Athena 上运行 Apache Spark 应用程序时，您需要提交 Spark 代码以供处理并直接接收结果。
- Amazon SageMaker 培训 – 查看使用 Amazon SageMaker 训练模型的选项，包括内置算法、自定义算法、库和 Amazon Marketplace 中的模型。
- Amazon Glue – Amazon Glue 是一项无服务器数据集成服务，可让使用分析功能的用户轻松发现、准备、移动和集成来自多个来源的数据。您可以使用 Amazon Glue 进行分析、机器学习和应用程序开发。Amazon Glue 还包括用于编写、运行任务和实施业务工作流程的额外生产率和数据操作工具。
- Amazon EMR – Amazon EMR 是一个托管式集群平台，可简化在 Amazon 上运行大数据框架（如 Apache Hadoop 和 Apache Spark）来处理和分析海量数据的过程。
- Amazon CloudTrail – Amazon CloudTrail 是一项 Amazon 服务，可协助您对 Amazon 账户进行运营和风险审计、监管及合规性管理。用户、角色或 Amazon 服务执行的操作将以事件的形式记录在 CloudTrail 中。事件包括在 Amazon 管理控制台、Amazon 命令行界面、Amazon SDK 和 API 中所执行的操作。
- Amazon CloudFormation – 这是一项服务，有助于您对 Amazon 资源进行建模和设置，以便能花较少的时间管理这些资源，而将更多的时间花在运行于 Amazon 中的应用程序上。您创建一个描述您所需的所有 Amazon 资源（如 Amazon EC2 实例或 Amazon RDS 数据库实例）的模板，并

且 CloudFormation 将负责为您预置和配置这些资源。您无需单独创建和配置 Amazon 资源并了解 what; CloudFormation 句柄处理该工作时所依赖的内容。

后续步骤

有关使用 S3 Express One Zone 存储类和目录存储桶的更多信息，请参阅以下主题：

- 教程：开始使用 S3 Express One Zone
- S3 Express One Zone 可用区和区域
- 可用区内目录存储桶的联网
- 在可用区中创建目录存储桶
- 可用区中适用于目录存储桶的区域和可用区端点
- 优化 S3 Express One Zone 性能

## 教程：开始使用 S3 Express One Zone

Amazon S3 Express One Zone 存储类是第一种可以在其中选择单个可用区的 S3 存储类，您可以选择将您的对象存储与计算资源联合托管在一个位置，从而提供尽可能高的访问速度。S3 Express One Zone 中的数据存储在可用区内的目录存储桶中。有关目录存储桶的更多信息，请参阅目录存储桶。

S3 Express One Zone 非常适合任何务必尽可能减少请求延迟的应用程序。此类应用程序可以是人机交互式工作流，例如视频编辑，在这种情况下，创意专业人士需要在通过用户界面访问内容时获得快速的响应。对数据响应能力具有类似要求的分析和机器学习工作负载也可以从 S3 Express One Zone 中获益，尤其是对于有大量访问小文件或大量随机访问的工作负载。S3 Express One Zone 可以与其它 Amazon 服务一起使用来支持分析以及人工智能与机器学习（AI/ML）工作负载，例如 Amazon EMR、Amazon Athena、Amazon Glue Data Catalog 和 Amazon SageMaker Model Training。可以通过 Amazon S3 控制台、Amazon SDK、Amazon 命令行界面（Amazon CLI）和 Amazon S3 REST API 使用 S3 Express One Zone 存储类和目录存储桶。有关更多信息，请参阅什么是 S3 Express One Zone？和 S3 Express One Zone 有哪些不同？

目标

在本教程中，您将学习如何创建网关端点、创建和附加 IAM 策略、创建目录存储桶，然后使用“导入”操作用当前存储在通用存储桶中的对象填充目录存储桶。或者，您可以手动将对象上传到目录存储桶。

主题

- 先决条件

- 步骤 1：配置网关 VPC 端点以访问 S3 Express One Zone 目录存储桶
- 步骤 2：创建 S3 Express One Zone 目录存储桶
- 步骤 3：将数据导入到 S3 Express One Zone 目录存储桶
- 步骤 4：手动将对象上传到 S3 Express One Zone 目录存储桶
- 步骤 5：清空 S3 Express One Zone 目录存储桶
- 步骤 6：删除 S3 Express One Zone 目录存储桶
- 后续步骤


先决条件

在开始本教程之前，您必须具有 Amazon Web Services 账户，您可使用具有正确权限的 Amazon Identity and Access Management（IAM）用户登录此账户。

分步


- 创建 Amazon Web Services 账户
- 在 Amazon Web Services 账户中创建 IAM 用户（控制台）
- 创建 IAM 策略并将其附加到 IAM 用户或角色（控制台）


创建 Amazon Web Services 账户

要完成此教程，您需要一个Amazon Web Services 账户。在注册 Amazon 时，将在 Amazon 中为您的 Amazon Web Services 账户 自动注册所有服务，包括 Amazon S3。您只需为使用的服务付费。有关定价的更多信息，请参阅 S3 定价。

在 Amazon Web Services 账户中创建 IAM 用户（控制台）

Amazon Identity and Access Management（IAM）是一项 Amazon Web Services 服务，有助于管理员安全地控制对 Amazon 资源的访问。IAM 管理员可控制哪些用户能够通过身份验证（登录）和获得授权（拥有权限），来在 S3 Express One Zone 中访问对象和使用目录存储桶。使用 IAM 不会产生额外的费用。

默认情况下，用户没有访问目录存储桶和执行 S3 Express One Zone 操作的权限。要授予对目录存储桶和 S3 Express One Zone 操作的访问权限，您可以使用 IAM 创建用户或角色，然后将权限附加到这些身份。有关如何创建 IAM 用户的更多信息，请参阅 《IAM 用户指南》中的创建 IAM 用户（控制台）。有关如何创建 IAM 角色的更多信息，请参阅《IAM 用户指南》中的创建向 IAM 用户委派权限的角色。

为简单起见，本教程创建并使用 IAM 用户。完成本教程后，请记住 删除 IAM 用户。对于生产用途，我们建议您遵循《IAM 用户指南》中的 IAM 中的安全最佳实践。最佳实践要求人类用户将联合身份验证与身份提供商结合使用，以使用临时凭证访问 Amazon。另一项最佳实践是要求工作负载使用带有 IAM 角色的临时凭证访问 Amazon。要详细了解如何使用 Amazon IAM Identity Center 创建具有临时凭证的用户，请参阅《Amazon IAM Identity Center 用户指南》中的 Getting started。

> **Warning**
>
> IAM 用户具有长期凭证，这会带来安全风险。为帮助减轻这种风险，我们建议仅向这些用户提供执行任务所需的权限，并在不再需要这些用户时将其移除。

创建 IAM 策略并将其附加到 IAM 用户或角色（控制台）

默认情况下，用户没有目录存储桶和 S3 Express One Zone 操作的权限。要授予对目录存储桶的访问权限，您可以使用 IAM 创建用户、组或角色，然后将权限附加到这些身份。对于 S3 Express One Zone 访问权限，目录存储桶是唯一可以包括在存储桶策略或 IAM 身份策略中的资源。

要在 S3 Express One Zone 中使用区域端点 API 操作（存储桶级或控制面板操作），请使用 IAM 授权模型，该模型不涉及会话管理。对于操作，将单独授予权限。要使用可用区端点 API 操作（对象级或数据面板操作），可以使用 `CreateSession` 来创建和管理会话，这些会话经过优化，可为数据请求提供低延迟授权。要检索和使用会话令牌，您必须在基于身份的策略或存储桶策略中，允许对目录存储桶执行 `s3express:CreateSession` 操作。如果您在 Amazon S3 控制台中通过 Amazon 命令行界面（Amazon CLI）或使用 Amazon SDK 访问 S3 Express One Zone，S3 Express One Zone 会代表您创建会话。有关更多信息，请参阅 `CreateSession` 授权和适用于 S3 Express One Zone 的 Amazon Identity and Access Management（IAM）。

创建 IAM 策略并将该策略附加到 IAM 用户（或角色）

1. 登录 Amazon 管理控制台，并打开 IAM 管理控制台。
2. 在导航窗格中，选择策略。
3. 选择创建策略。
4. 选择 JSON。
5. 将以下策略复制到策略编辑器窗口。在创建目录存储桶或使用 S3 Express One Zone 之前，您必须向 Amazon Identity and Access Management（IAM）角色或用户授予必要的权限。此示例策略支持访问 `CreateSession` API 操作（与其它可用区或对象级 API 操作结合使用）和所有区域端点（存储桶级）API 操作。此策略允许将 `CreateSession` API 操作用于所有目录存储桶，

但仅允许将区域端点 API 操作用于指定的目录存储桶。要使用此示例策略，请将 *user input placeholders* 替换为您自己的信息。

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Sid": "AllowAccessRegionalEndpointAPIs",
             "Effect": "Allow",
             "Action": [
                 "s3express:DeleteBucket",
                 "s3express:DeleteBucketPolicy",
                 "s3express:CreateBucket",
                 "s3express:PutBucketPolicy",
                 "s3express:GetBucketPolicy",
                 "s3express:ListAllMyDirectoryBuckets"
             ],

             "Resource": "arn:aws:s3express:region:account_id:bucket/bucket-base-name--zone-id--x-s3/*"
         },
         {
             "Sid": "AllowCreateSession",
             "Effect": "Allow",
             "Action": "s3express:CreateSession",
             "Resource": "*"
         }
     ]
 }
```

6. 选择下一步。
7. 为该策略命名。

> **Note**
>
> S3 Express One Zone 不支持存储桶标签。

8. 选择创建策略。
9. 创建 IAM 策略后，可以将其附加到 IAM 用户。在导航窗格中，选择策略。
10. 在搜索栏中，输入策略的名称。
11. 从操作菜单中，选择附加。

12. 在按实体类型筛选下，选择 IAM 用户或角色。
13. 在搜索字段中，键入您要使用的用户或角色的名称。
14. 选择附加策略。

### 步骤 1：配置网关 VPC 端点以访问 S3 Express One Zone 目录存储桶

您可以通过网关虚拟私有云（VPC）端点访问可用区和区域 API 操作。网关端点可让流量在不通过 NAT 网关的情况下到达 S3 Express One Zone。我们强烈建议使用网关端点，因为在使用 S3 Express One Zone 时，此类端点可提供最佳的联网路径。您可以从 VPC 访问 S3 Express One Zone 目录存储桶，而无需为 VPC 配备互联网网关或 NAT 设备，也无需任何额外费用。使用以下过程可配置连接到 S3 Express One Zone 存储类对象和目录存储桶的网关端点。

要访问 S3 Express One Zone，您需要使用不同于标准 Amazon S3 端点的区域和可用区端点。根据您使用的 Amazon S3 API 操作，需要区域端点或可用区端点。有关各端点类型支持的 API 操作的完整列表，请参阅 S3 Express One Zone 支持的 API 操作。您必须通过网关虚拟私有云（VPC）端点访问可用区端点和区域端点。

使用以下过程创建连接到 S3 Express One Zone 存储类对象和目录存储桶的网关端点。

配置网关 VPC 端点

1. 打开位于 https://console.amazonaws.cn/vpc/ 的 Amazon VPC 控制台。
2. 在侧导航窗格中的虚拟私有云下，选择端点。
3. 选择创建端点。
4. 为端点创建名称。
5. 对于 Service category（服务类别），选择 Amazon Web Services 服务。
6. 在服务下，使用筛选条件 Type=Gateway 进行搜索，然后选择 com.amazonaws.***region***.s3express 旁边的选项按钮。
7. 对于 VPC，选择要在其中创建端点的 VPC。
8. 对于 Route tables（路由表），选择端点要使用的路由表。Amazon VPC 自动添加路由，将流向服务的流量指向端点网络接口。
9. 对于策略，请选择完整访问权限以允许所有主体通过 VPC 端点对所有资源执行所有操作。否则，选择自定义以附加 VPC 端点策略，该策略控制主体通过 VPC 端点对资源执行操作的权限。
10. 选择创建端点。

创建网关端点后，您可以使用区域 API 端点和可用区 API 端点来访问 Amazon S3 Express One Zone 存储类对象和目录存储桶。

步骤 2：创建 S3 Express One Zone 目录存储桶

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在页面顶部的导航栏中，选择当前所显示 Amazon Web Services 区域的名称。接下来，选择要在其中创建存储桶的区域。

   > **Note**
   >
   > 要最大程度地减少延迟和成本以及满足法规要求，请选择一个靠近您的区域。在某一区域存储的对象将一直留在该区域，除非您特意将其转移到其他区域。有关 Amazon S3 Amazon Web Services 区域的列表，请参阅《Amazon Web Services 一般参考》中的 Amazon Web Services 服务 端点。

3. 在左侧导航窗格中，选择目录存储桶。
4. 选择创建存储桶。此时将打开创建存储桶页面。
5. 在常规配置下，查看将在其中创建存储桶的 Amazon Web Services 区域。

   在存储桶类型下，请选择目录。

   > **Note**
   >
   > - 如果您选择的区域不支持目录桶，则桶类型选项将消失，桶类型默认为通用桶。要创建目录桶，您必须选择受支持的区域。有关支持目录桶和 Amazon S3 Express One Zone 存储类的区域列表，请参阅the section called “S3 Express One Zone 可用区和区域”。
   > - 在创建存储桶后，便无法更改存储桶类型。

   > **Note**
   >
   > 创建存储桶后无法更改可用区。

6. 对于可用区，请选择计算服务本地的可用区。有关支持目录桶和 S3 Express One Zone 存储类的可用区列表，请参阅the section called “S3 Express One Zone 可用区和区域”。

在可用区下，选中复选框以确认在可用区中断时，您的数据可能不可用或丢失。

> **Important**
>
> 尽管目录桶存储在单个可用区中的多个设备上，但目录桶不会跨可用区冗余存储数据。

7. 对于存储桶名称，请输入目录存储桶的名称。

   以下命名规则适用于目录存储桶。

   - 在选定的区域（Amazon 可用区或 Amazon 本地区域）内是唯一的。
   - 名称的长度必须介于 3（最小）到 63（最大）个字符之间，包括后缀。
   - 仅包含小写字母、数字和连字符（-）。
   - 以字母或数字开头和结尾。
   - 必须包含以下后缀：`--`*`zone-id`*`--x-s3`。
   - 存储桶名称不得以前缀 `xn--` 开头。
   - 存储桶名称不得以前缀 `sthree-` 开头。
   - 存储桶名称不得以前缀 `sthree-configurator` 开头。
   - 存储桶名称不得以前缀 `amzn-s3-demo-` 开头。
   - 存储桶名称不得以后缀 `-s3alias` 结尾。此后缀是为接入点别名预留的。有关更多信息，请参阅 通用存储桶的接入点别名。
   - 存储桶名称不得以后缀 `--ol-s3` 结尾。此后缀是为对象 Lambda 接入点别名预留的。有关更多信息，请参阅 如何为您的 S3 存储桶对象 Lambda 接入点使用存储桶式别名。
   - 存储桶名称不得以后缀 `.mrap` 结尾。此后缀预留用于多区域接入点名称。有关更多信息，请参阅 命名 Amazon S3 多区域接入点的规则。

   后缀将自动添加到您使用控制台创建目录存储桶时提供的基本名称中。此后缀包括您选择的可用区的可用区 ID。

   创建存储桶后，便无法更改其名称。有关给存储桶命名的更多信息，请参阅通用存储桶命名规则。

> **Important**
>
> 请勿在桶名称中包含敏感信息，如账号。存储桶名称会显示在指向存储桶中的对象的 URL 中。

8. 在对象所有权下，将自动启用强制桶拥有者设置，并禁用所有访问控制列表（ACL）。对于目录存储桶，无法启用 ACL。

   强制存储桶拥有者（默认）：ACL 已禁用，存储桶拥有者自动拥有并完全控制通用存储桶中的每个对象。ACL 不再影响对 S3 通用存储桶中数据的访问权限。存储桶专门使用策略来定义访问控制。

9. 在此桶的屏蔽公共访问权限设置下，目录桶的所有屏蔽公共访问权限设置已自动启用。无法修改目录桶的这些设置。有关阻止公共访问的更多信息，请参阅阻止对您的 Amazon S3 存储的公有访问。

10. 要配置默认加密，请在加密类型下，选择以下选项之一：

    - 具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）
    - 具有 Amazon Key Management Service 密钥的服务器端加密（SSE-KMS）

    有关使用 Amazon S3 服务器端加密对数据进行加密的更多信息，请参阅数据保护和加密。

    > **Important**
    >
    > 如果您将 SSE-KMS 选项用于默认加密配置，则您将受到 Amazon KMS 的每秒请求数（RPS）限额限制。有关 Amazon KMS 限额以及如何请求增加限额的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的限额。
    > 当您启用默认加密时，您可能需要更新存储桶策略。有关更多信息，请参阅 使用 SSE-KMS 加密进行跨账户操作。

11. 如果您选择具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3），则在存储桶密钥下方将显示已启用。当您将目录存储桶配置为使用 SSE-S3 进行默认加密时，始终启用 S3 存储桶密钥。始终为目录存储桶中的 `GET` 和 `PUT` 操作启用 S3 存储桶密钥，并且不能禁用。当您通过 CopyObject、UploadPartCopy、批量操作中的 Copy 操作或 import 任务，将 SSE-KMS 加密的对象从通用存储桶复制到目录存储桶、从目录存储桶复制到通用存储桶，或在目录存储桶之间复制时，不支持 S3 存储桶密钥。在这种情况下，每次对 KMS 加密的对象发出复制请求时，Amazon S3 都会调用 Amazon KMS。

S3 存储桶密钥可通过减少从 Amazon S3 到 Amazon KMS 的请求流量，降低加密成本。有关更多信息，请参阅 使用 Amazon S3 存储桶密钥降低 SSE-KMS 的成本。

12. 如果您选择具有 Amazon Key Management Service 密钥的服务器端加密（SSE-KMS），则在 Amazon KMS 密钥下方，通过以下方式之一指定您的 Amazon Key Management Service 密钥或创建新密钥。

    - 要从可用 KMS 密钥列表中进行选择，选择从您的 Amazon KMS keys中进行选择，并从可用的 Amazon KMS keys中选择您的 KMS 密钥。

      只有您的客户自主管理型密钥显示在此列表中。目录存储桶不支持 Amazon 托管式密钥 (aws/s3)。有关客户自主管理型密钥的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的客户密钥和 Amazon 密钥。
    - 要输入 KMS 密钥 ARN 或别名，选择输入 Amazon KMS key ARN，然后在 Amazon KMS key ARN 中输入您的 KMS 密钥 ARN 或别名。
    - 要在 Amazon KMS 控制台中创建新的客户自主管理型密钥，请选择创建 KMS 密钥。

      有关创建 Amazon KMS key 的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的创建密钥。

    > **Important**
    >
    > - 在存储桶的生命周期内，SSE-KMS 配置只能支持每个目录存储桶 1 个 customer managed key。Amazon 托管式密钥 (aws/s3) 不受支持。此外，在为 SSE-KMS 指定客户自主管理型密钥后，无法覆盖存储桶的 SSE-KMS 配置的客户自主管理型密钥。
    >
    >   可以通过以下方式，确定您为存储桶的 SSE-KMS 配置指定的客户自主管理型密钥：
    >
    >   - 您发出 `HeadObject` API 操作请求以查找响应中 `x-amz-server-side-encryption-aws-kms-key-id` 的值。
    >
    >   要对数据使用新的客户自主管理型密钥，我们建议使用新的客户自主管理型密钥将现有对象复制到新的目录存储桶中。
    > - 您只能使用与存储桶所在相同的 Amazon Web Services 区域中可用的 KMS 密钥。Amazon S3 控制台仅列出与存储桶位于同一区域中的前 100 个 KMS 密钥。要使用未列出的 KMS 密钥，您必须输入 KMS 密钥 ARN。如果您希望使用其他账户拥有的 KMS 密钥，则必须首先有权使用该密钥，然后必须输入相应的 KMS 密钥 ARN。有关 KMS 密钥的跨账户权限的更多信息，请参阅《Amazon Key Management Service 开

发人员指南》中的创建其他账户可以使用的 KMS 密钥。有关 SSE-KMS 的更多信息，请参阅为目录存储桶中的新对象上传指定具有 Amazon KMS 的服务器端加密（SSE-KMS）。

- 在目录存储桶中使用 Amazon KMS key进行服务器端加密时，您必须选择对称加密 KMS 密钥。Amazon S3 仅支持对称加密 KMS 密钥，而不支持非对称 KMS 密钥。有关更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的确定对称和非对称 KMS 密钥。

有关将 Amazon KMS 与 Amazon S3 结合使用的更多信息，请参阅在目录存储桶中使用具有 Amazon KMS 密钥的服务器端加密（SSE-KMS）。

13. 选择 创建存储桶 。创建存储桶后，您可以向存储桶中添加文件和文件夹。有关更多信息，请参阅 the section called “使用目录桶中的对象”。

步骤 3：将数据导入到 S3 Express One Zone 目录存储桶

要完成此步骤，您必须有一个包含对象的通用存储桶，并且它与目录存储桶位于同一个 Amazon Web Services 区域中。

在 Amazon S3 中创建目录存储桶后，可以使用 Amazon S3 控制台中的“导入”操作在新的存储桶中填充数据。导入过程可让您选择要从中导入数据的前缀或通用存储桶，而无需单独指定要复制的所有对象，从而简化了将数据复制到目录存储桶的过程。导入过程使用 S3 批量操作，这会复制所选前缀或通用存储桶中的对象。可以通过 S3 批量操作任务详细信息页面监控“导入”复制任务的进度。

使用“导入”操作

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在页面顶部的导航栏中，选择当前所显示 Amazon Web Services 区域的名称。接下来，选择与目录存储桶所在的可用区关联的区域。
3. 在左侧导航窗格中，选择目录存储桶。
4. 选择要将对象导入到的存储桶名称旁边的选项按钮。
5. 选择导入。
6. 对于源，输入包含要导入的对象的通用存储桶（或包含前缀的存储桶路径）。要从列表中选择现有的通用存储桶，请选择浏览 S3。

7. 在权限部分，可以选择自动生成 IAM 角色。或者，可以从列表中选择 IAM 角色，或直接输入 IAM 角色 ARN。

   - 要允许 Amazon S3 代表您创建新的 IAM 角色，请选择创建新的 IAM 角色。

     > **Note**
     >
     > 如果您的源对象使用具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）进行加密，请不要选择创建新的 IAM 角色选项。而是指定具有 `kms:Decrypt` 权限的现有 IAM 角色。
     > Amazon S3 将使用此权限来解密您的对象。在导入过程中，Amazon S3 将使用具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）对这些对象进行重新加密。

   - 要从列表中选择现有 IAM 角色，请选择从现有 IAM 角色中选择。
   - 要通过输入 Amazon 资源名称（ARN）指定现有 IAM 角色，请选择输入 IAM 角色 ARN，然后在相应字段中输入 ARN。

8. 查看目标和复制的对象设置部分中显示的信息。如果目标部分中的信息正确，请选择导入以启动复制作业。

   Amazon S3 控制台在批量操作页面上显示新作业的状态。有关作业的更多信息，请选择作业名称旁边的选项按钮，然后在操作菜单上选择查看详细信息。要打开要导入对象的目录存储桶，请选择查看导入目标。

步骤 4：手动将对象上传到 S3 Express One Zone 目录存储桶

也可以手动将对象上传到目录存储桶。

手动上传对象

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在页面右上角的导航栏中，选择当前所显示的 Amazon Web Services 区域的名称。接下来，选择与目录存储桶所在的可用区关联的区域。
3. 在左侧导航窗格中，选择目录存储桶。
4. 选择要将文件夹或文件上传到的桶的名称。

> **Note**
>
> 如果您选择的目录存储桶与本教程前面的步骤中使用的目录存储桶相同，则目录存储桶将包含从“导入”工具上传的对象。请注意，这些对象现在存储在 S3 Express One Zone 存储类中。

5. 在对象列表中，选择上传。
6. 在上传页面上，执行以下操作之一：
   - 将文件和文件夹拖放到虚线上传区域。
   - 选择添加文件或添加文件夹，选择要上传的文件或文件夹，然后选择打开或上传。
7. 在校验和下，选择要使用的校验和函数。

> **Note**
>
> 我们建议使用 CRC32 和 CRC32C，以便在 S3 Express One Zone 存储类上获得最佳性能。有关更多信息，请参阅其它 S3 校验和最佳实践。

（可选）如果您要上传大小不到 16 MB 的单个对象，也可以指定预先计算的校验和值。当您提供预先计算的值时，Amazon S3 会将该值与它使用所选校验和函数计算的值进行比较。如果值不匹配，则上传不会开始。

8. 权限和属性部分中的选项会自动设置为默认设置，无法修改。将自动启用“屏蔽公共访问权限”，而无法为目录桶启用 S3 版本控制和 S3 对象锁定。

   （可选）如果要以键值对的形式向对象添加元数据，请展开属性部分，然后在元数据部分中选择添加元数据。
9. 要上传列出的文件和文件夹，请选择上传。

   Amazon S3 会上传您的对象和文件夹。上传完成后，您可以在上传：状态页面上看到成功消息。

   您已成功创建了目录存储桶并将对象上传到存储桶。

### 步骤 5：清空 S3 Express One Zone 目录存储桶

可以使用 Amazon S3 控制台来清空 Amazon S3 目录存储桶。

清空目录桶

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在页面右上角的导航栏中，选择当前所显示的 Amazon Web Services 区域的名称。接下来，选择与目录存储桶所在的可用区关联的区域。
3. 在左侧导航窗格中，选择目录存储桶。
4. 选择您要清空的桶名称旁边的选项按钮，然后选择清空。
5. 在清空存储桶页面上，通过在文本字段中输入 **`permanently delete`** 来确认要清空存储桶，然后选择清空。
6. 在清空桶：状态页面上监控桶清空过程的进度。

### 步骤 6：删除 S3 Express One Zone 目录存储桶

清空目录存储桶并中止所有正在进行的分段上传后，可以使用 Amazon S3 控制台删除存储桶。

删除目录存储桶

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在页面右上角的导航栏中，选择当前所显示的 Amazon Web Services 区域的名称。接下来，选择与目录存储桶所在的可用区关联的区域。
3. 在左侧导航窗格中，选择目录存储桶。
4. 在目录桶列表中，选择要删除的桶旁边的选项按钮。
5. 选择删除。
6. 在删除桶页面上，在文本字段中输入桶的名称以确认删除您的桶。

> **Important**
>
> 无法撤消删除目录存储桶的操作。

7. 要删除您的目录存储桶，请选择删除存储桶。

## 后续步骤

在本教程中，您学习了如何创建目录存储桶和使用 S3 Express One Zone 存储类。完成本教程后，您可以探索要与 S3 Express One Zone 存储类一起使用的相关 Amazon 服务。

您可以将以下 Amazon Web Services 服务与 S3 Express One Zone 存储类配合使用，以支持您的特定低延迟使用场景。

- Amazon Elastic Compute Cloud（Amazon EC2）– Amazon EC2 在 Amazon Web Services 云 中提供安全可扩展的计算容量。使用 Amazon EC2 可减少前期的硬件投入，因此您能够快速开发和部署应用程序。您可以使用 Amazon EC2 启动所需数量的虚拟服务器，配置安全性和联网以及管理存储。
- Amazon Lambda – Lambda 是一项计算服务，可使您无需预置或管理服务器即可运行代码。您在存储桶上配置通知设置，并向 Amazon S3 授予权限来根据函数的基于资源的权限策略调用函数。
- Amazon Elastic Kubernetes Service（Amazon EKS）– Amazon EKS 是一项托管式服务，无需在 Amazon 上安装、操作和维护自己的 Kubernetes 控制面板。Kubernetes 是一个开源系统，用于自动管理、扩展和部署容器化应用程序。
- Amazon Elastic Container Service（Amazon ECS）– Amazon ECS 是完全托管的容器编排服务，可协助您轻松地部署、管理和扩展容器化应用程序。
- Amazon EMR – Amazon EMR 是一个托管式集群平台，可简化在 Amazon 上运行大数据框架（如 Apache Hadoop 和 Apache Spark）来处理和分析海量数据的过程。
- Amazon Athena – Athena 是一种交互式查询服务，方便通过使用标准 SQL 直接分析 Amazon S3 中的数据。还可以使用 Athena，通过 Apache Spark 以交互方式运行数据分析，而无需规划、配置或管理资源。在 Athena 上运行 Apache Spark 应用程序时，您需要提交 Spark 代码以供处理并直接接收结果。
- Amazon Glue Data Catalog – Amazon Glue 是一项无服务器数据集成服务，可让使用分析功能的用户轻松发现、准备、移动和集成来自多个来源的数据。您可以使用 Amazon Glue 进行分析、机器学习和应用程序开发。AmazonGlue Data Catalog 是一个集中式存储库，用于存储有关贵组织数据集的元数据。它充当数据来源的位置、架构和运行时指标的索引。
- Amazon SageMaker Runtime 模型训练 – Amazon SageMaker Runtime 是一项完全托管式机器学习服务。借助 SageMaker Runtime，数据科学家和开发人员可以快速、轻松地构建和训练机器学习模型，然后直接将模型部署到生产就绪托管环境中。

有关 S3 Express One Zone 的更多信息，请参阅什么是 S3 Express One Zone？和 S3 Express One Zone 有哪些不同？

## S3 Express One Zone 可用区和区域

可用区是 Amazon Web Services 区域 中一个或多个具有冗余电源、网络和连接的离散数据中心。为了实现优化的低延迟检索，Amazon S3 Express One Zone 存储类中的对象以冗余方式存储在 S3 目录存储桶中，这种存储桶位于计算工作负载所在的单个可用区。创建目录存储桶时，您可以选择存储桶所在的可用区以及 Amazon Web Services 区域。

Amazon 将物理可用区随机映射到每个 Amazon Web Services 账户的可用区名称。这种方法有助于在 Amazon Web Services 区域的可用区之间分配资源，而不是将资源集中在每个区域的第一个可用区中。因此，您的 Amazon Web Services 账户的可用区 `us-east-1a` 可能与其他 Amazon Web Services 账户的 `us-east-1a` 表示的物理位置不同。有关更多信息，请参阅《Amazon EC2 用户指南》中的区域和可用区。

要跨账户协调可用区，您必须使用 AZ ID（可用区的唯一、一致的标识符）。例如，`use1-az1` 是 `us-east-1` 区域的可用区 ID，它在每个 Amazon Web Services 账户 中的实际位置均相同。下图显示了每个账户的 AZ ID 是相同的，尽管每个账户的可用区名称映射可能不同。

使用 S3 Express One Zone，您的数据将冗余地存储在单个可用区中的多个设备上。S3 Express One Zone 设计为在单个可用区内提供 99.95% 的可用性，并由 Amazon S3 服务等级协议提供支持。有关更多信息，请参阅 可用区。

下表显示了 S3 Express One Zone 支持的区域和可用区。

| 区域名称 | 区域代码 | 可用区 ID |
| --- | --- | --- |
| 美国东部（弗吉尼亚州北部） | `us-east-1` | `use1-az4` |
| | | `use1-az5` |
| | | `use1-az6` |
| 美国东部（俄亥俄州） | `us-east-2` | `use2-az1` |
| | | `use2-az2` |
| 美国西部（俄勒冈州） | `us-west-2` | `usw2-az1` |
| | | `usw2-az3` |
| | | `usw2-az4` |

| 区域名称 | 区域代码 | 可用区 ID |
| --- | --- | --- |
| 亚太地区（孟买） | ap-south-1 | aps1-az1 |
| | | aps1-az3 |
| 亚太地区（东京） | ap-northeast-1 | apne1-az1 |
| | | apne1-az4 |
| 欧洲地区（爱尔兰） | eu-west-1 | euw1-az1 |
| | | euw1-az3 |
| 欧洲地区（斯德哥尔摩） | eu-north-1 | eun1-az1 |
| | | eun1-az2 |
| | | eun1-az3 |

## 可用区内目录存储桶的联网

以下主题介绍使用网关 VPC 端点访问 S3 Express One Zone 时的联网要求。

主题

- 可用区中目录存储桶的端点
- 配置 VPC 网关端点

### 可用区中目录存储桶的端点

下表显示了在各个区域和可用区中可以使用的区域和可用区 API 端点。

### 配置 VPC 网关端点

使用以下过程创建连接到 Amazon S3 Express One Zone 存储类对象和目录存储桶的网关端点。

配置网关 VPC 端点

1. 打开 Amazon VPC 控制台。
2. 在导航窗格中，选择端点。

3. 选择 创建端点。
4. 为端点创建名称。
5. 对于 Service category（服务类别），选择 Amazon Web Services 服务。
6. 对于服务，添加筛选条件 Type=Gateway，然后选择 com.amazonaws.***region***.s3express 旁边的选项按钮。
7. 对于 VPC，选择要在其中创建端点的 VPC。
8. 对于 Route tables（路由表），选择端点要使用的路由表。Amazon VPC 自动添加路由，将流向服务的流量指向端点网络接口。
9. 对于策略，请选择完整访问权限以允许所有主体通过 VPC 端点对所有资源执行所有操作。否则，选择自定义以附加 VPC 端点策略，该策略控制主体通过 VPC 端点对资源执行操作的权限。
10. （可选）要添加标签，请选择添加新标签，然后输入标签键和标签值。
11. 选择创建端点。

创建网关端点后，您可以使用区域 API 端点和可用区 API 端点来访问 Amazon S3 Express One Zone 存储类对象和目录存储桶。

## 在可用区中创建目录存储桶

要开始使用 Amazon S3 Express One Zone 存储类，您需要创建一个目录存储桶。S3 Express One Zone 存储类只能用于目录存储桶。S3 Express One Zone 存储类支持低延迟使用案例，并在单个可用区内提供更快的数据处理速度。如果您的应用程序注重性能，并且受益于个位数毫秒的 PUT 和 GET 延迟，我们建议您创建一个目录存储桶，以便可以使用 S3 Express One Zone 存储类。

Amazon S3 存储桶有两种类型：通用存储桶和目录存储桶。您应该选择适合您应用程序和性能要求的存储桶类型。通用存储桶是最初的 S3 存储桶类型。对于大多数使用案例和访问模式，建议使用通用桶，通用桶允许在除 S3 Express One Zone 之外的所有存储类中存储对象。有关通用存储桶的更多信息，请参阅通用存储桶概述。

目录存储桶使用 S3 Express One Zone 存储类，该存储类专用于需要一致的个位数毫秒延迟的工作负载或性能关键型应用程序。S3 Express One Zone 是第一种可以在其中选择单个可用区的 S3 存储类，您可以选择将您的对象存储与计算资源联合托管在一个位置，从而提供尽可能高的访问速度。创建目录存储桶时，您可以选择指定 Amazon EC2、Amazon Elastic Kubernetes Service 或 Amazon Elastic Container Service（Amazon ECS）计算实例的本地 Amazon Web Services 区域和可用区，以优化性能。

使用 S3 Express One Zone，您的数据将冗余地存储在单个可用区中的多个设备上。S3 Express One Zone 设计为在单个可用区内提供 99.95% 的可用性，并由 Amazon S3 服务等级协议提供支持。有关更多信息，请参阅 可用区。

目录桶将数据按层次结构组织到目录中，而不是通用桶的扁平存储结构。目录存储桶没有前缀限制，单个目录可以横向扩展。

有关目录存储桶的更多信息，请参阅使用目录存储桶。

目录存储桶名称

目录存储桶名称必须遵循以下格式并遵守目录存储桶命名规则：

```
bucket-base-name--zone-id--x-s3
```

例如，以下目录存储桶名称包含可用区 ID `usw2-az1`：

```
bucket-base-name--usw2-az1--x-s3
```

有关目录存储桶命名规则的更多信息，请参阅目录存储桶命名规则。

使用 S3 控制台

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在页面顶部的导航栏中，选择当前所显示 Amazon Web Services 区域的名称。接下来，选择要在其中创建存储桶的区域。

   > **Note**
   >
   > 要最大程度地减少延迟和成本以及满足法规要求，请选择一个靠近您的区域。在某一区域存储的对象将一直留在该区域，除非您特意将其转移到其他区域。有关 Amazon S3 Amazon Web Services 区域的列表，请参阅《Amazon Web Services 一般参考》中的 Amazon Web Services 服务 端点。

3. 在左侧导航窗格中，选择目录存储桶。
4. 选择创建存储桶。此时将打开创建存储桶页面。
5. 在常规配置下，查看将在其中创建存储桶的 Amazon Web Services 区域。

在存储桶类型下，请选择目录。

> **Note**
>
> - 如果您选择的区域不支持目录桶，则桶类型选项将消失，桶类型默认为通用桶。要创建目录桶，您必须选择受支持的区域。有关支持目录桶和 Amazon S3 Express One Zone 存储类的区域列表，请参阅the section called “S3 Express One Zone 可用区和区域”。
> - 在创建存储桶后，便无法更改存储桶类型。

> **Note**
>
> 创建存储桶后无法更改可用区。

6. 对于可用区，请选择计算服务本地的可用区。有关支持目录桶和 S3 Express One Zone 存储类的可用区列表，请参阅the section called “S3 Express One Zone 可用区和区域”。

   在可用区下，选中复选框以确认在可用区中断时，您的数据可能不可用或丢失。

> **Important**
>
> 尽管目录桶存储在单个可用区中的多个设备上，但目录桶不会跨可用区冗余存储数据。

7. 对于存储桶名称，请输入目录存储桶的名称。

   以下命名规则适用于目录存储桶。

   - 在选定的区域（Amazon 可用区或 Amazon 本地区域）内是唯一的。
   - 名称的长度必须介于 3（最小）到 63（最大）个字符之间，包括后缀。
   - 仅包含小写字母、数字和连字符（-）。
   - 以字母或数字开头和结尾。
   - 必须包含以下后缀：`--`*`zone-id`*`--x-s3`。
   - 存储桶名称不得以前缀 `xn--` 开头。
   - 存储桶名称不得以前缀 `sthree-` 开头。
   - 存储桶名称不得以前缀 `sthree-configurator` 开头。

- 存储桶名称不得以前缀 `amzn-s3-demo-` 开头。
- 存储桶名称不得以后缀 `-s3alias` 结尾。此后缀是为接入点别名预留的。有关更多信息，请参阅 通用存储桶的接入点别名。
- 存储桶名称不得以后缀 `--ol-s3` 结尾。此后缀是为对象 Lambda 接入点别名预留的。有关更多信息，请参阅 如何为您的 S3 存储桶对象 Lambda 接入点使用存储桶式别名。
- 存储桶名称不得以后缀 `.mrap` 结尾。此后缀预留用于多区域接入点名称。有关更多信息，请参阅 命名 Amazon S3 多区域接入点的规则。

后缀将自动添加到您使用控制台创建目录存储桶时提供的基本名称中。此后缀包括您选择的可用区的可用区 ID。

创建存储桶后，便无法更改其名称。有关给存储桶命名的更多信息，请参阅通用存储桶命名规则。

> **Important**
>
> 请勿在桶名称中包含敏感信息，如账号。存储桶名称会显示在指向存储桶中的对象的 URL 中。

8. 在对象所有权下，将自动启用强制桶拥有者设置，并禁用所有访问控制列表（ACL）。对于目录存储桶，无法启用 ACL。

   强制存储桶拥有者（默认）：ACL 已禁用，存储桶拥有者自动拥有并完全控制通用存储桶中的每个对象。ACL 不再影响对 S3 通用存储桶中数据的访问权限。存储桶专门使用策略来定义访问控制。

9. 在此桶的屏蔽公共访问权限设置下，目录桶的所有屏蔽公共访问权限设置已自动启用。无法修改目录桶的这些设置。有关阻止公共访问的更多信息，请参阅阻止对您的 Amazon S3 存储的公有访问。

10. 要配置默认加密，请在加密类型下，选择以下选项之一：

    - 具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）
    - 具有 Amazon Key Management Service 密钥的服务器端加密（SSE-KMS）

    有关使用 Amazon S3 服务器端加密对数据进行加密的更多信息，请参阅数据保护和加密。

> **Important**
>
> 如果您将 SSE-KMS 选项用于默认加密配置，则您将受到 Amazon KMS 的每秒请求数（RPS）限额限制。有关 Amazon KMS 限额以及如何请求增加限额的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的限额。
> 当您启用默认加密时，您可能需要更新存储桶策略。有关更多信息，请参阅 使用 SSE-KMS 加密进行跨账户操作。

11. 如果您选择具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3），则在存储桶密钥下方将显示已启用。当您将目录存储桶配置为使用 SSE-S3 进行默认加密时，始终启用 S3 存储桶密钥。始终为目录存储桶中的 GET 和 PUT 操作启用 S3 存储桶密钥，并且不能禁用。当您通过 CopyObject、UploadPartCopy、批量操作中的 Copy 操作或 import 任务，将 SSE-KMS 加密的对象从通用存储桶复制到目录存储桶、从目录存储桶复制到通用存储桶，或在目录存储桶之间复制时，不支持 S3 存储桶密钥。在这种情况下，每次对 KMS 加密的对象发出复制请求时，Amazon S3 都会调用 Amazon KMS。

    S3 存储桶密钥可通过减少从 Amazon S3 到 Amazon KMS 的请求流量，降低加密成本。有关更多信息，请参阅 使用 Amazon S3 存储桶密钥降低 SSE-KMS 的成本。

12. 如果您选择具有 Amazon Key Management Service 密钥的服务器端加密（SSE-KMS），则在 Amazon KMS 密钥下方，通过以下方式之一指定您的 Amazon Key Management Service 密钥或创建新密钥。

    - 要从可用 KMS 密钥列表中进行选择，选择从您的 Amazon KMS keys中进行选择，并从可用的 Amazon KMS keys中选择您的 KMS 密钥。

      只有您的客户自主管理型密钥显示在此列表中。目录存储桶不支持 Amazon 托管式密钥 (aws/s3)。有关客户自主管理型密钥的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的客户密钥和 Amazon 密钥。

    - 要输入 KMS 密钥 ARN 或别名，选择输入 Amazon KMS key ARN，然后在 Amazon KMS key ARN 中输入您的 KMS 密钥 ARN 或别名。

    - 要在 Amazon KMS 控制台中创建新的客户自主管理型密钥，请选择创建 KMS 密钥。

      有关创建 Amazon KMS key 的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的创建密钥。

**Important**

- 在存储桶的生命周期内，SSE-KMS 配置只能支持每个目录存储桶 1 个 customer managed key。Amazon 托管式密钥 (aws/s3) 不受支持。此外，在为 SSE-KMS 指定客户自主管理型密钥后，无法覆盖存储桶的 SSE-KMS 配置的客户自主管理型密钥。

  可以通过以下方式，确定您为存储桶的 SSE-KMS 配置指定的客户自主管理型密钥：

  - 您发出 HeadObject API 操作请求以查找响应中 x-amz-server-side-encryption-aws-kms-key-id 的值。

  要对数据使用新的客户自主管理型密钥，我们建议使用新的客户自主管理型密钥将现有对象复制到新的目录存储桶中。

- 您只能使用与存储桶所在相同的 Amazon Web Services 区域中可用的 KMS 密钥。Amazon S3 控制台仅列出与存储桶位于同一区域中的前 100 个 KMS 密钥。要使用未列出的 KMS 密钥，您必须输入 KMS 密钥 ARN。如果您希望使用其他账户拥有的 KMS 密钥，则必须首先有权使用该密钥，然后必须输入相应的 KMS 密钥 ARN。有关 KMS 密钥的跨账户权限的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的创建其他账户可以使用的 KMS 密钥。有关 SSE-KMS 的更多信息，请参阅为目录存储桶中的新对象上传指定具有 Amazon KMS 的服务器端加密（SSE-KMS）。
- 在目录存储桶中使用 Amazon KMS key进行服务器端加密时，您必须选择对称加密 KMS 密钥。Amazon S3 仅支持对称加密 KMS 密钥，而不支持非对称 KMS 密钥。有关更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的确定对称和非对称 KMS 密钥。

有关将 Amazon KMS 与 Amazon S3 结合使用的更多信息，请参阅在目录存储桶中使用具有 Amazon KMS 密钥的服务器端加密（SSE-KMS）。

13. 选择 创建存储桶 。创建存储桶后，您可以向存储桶中添加文件和文件夹。有关更多信息，请参阅 the section called “使用目录桶中的对象”。

使用 Amazon SDK

SDK for Go

此示例说明如何使用 适用于 Go 的 Amazon SDK 创建目录桶。

Example

```
var bucket = "..."

func runCreateBucket(c *s3.Client) {
    resp, err := c.CreateBucket(context.Background(), &s3.CreateBucketInput{
        Bucket: &bucket,
        CreateBucketConfiguration: &types.CreateBucketConfiguration{
            Location: &types.LocationInfo{
                Name: aws.String("usw2-az1"),
                Type: types.LocationTypeAvailabilityZone,
            },
            Bucket: &types.BucketInfo{
                DataRedundancy: types.DataRedundancySingleAvailabilityZone,
                Type:           types.BucketTypeDirectory,
            },
        },
    })
    var terr *types.BucketAlreadyOwnedByYou
    if errors.As(err, &terr) {
        fmt.Printf("BucketAlreadyOwnedByYou: %s\n", aws.ToString(terr.Message))
        fmt.Printf("noop...\n")
        return
    }
    if err != nil {
        log.Fatal(err)
    }

    fmt.Printf("bucket created at %s\n", aws.ToString(resp.Location))
}
```

SDK for Java 2.x

此示例说明如何使用 Amazon SDK for Java 2.x 创建目录桶。

Example

```
public static void createBucket(S3Client s3Client, String bucketName) {
```

```
   //Bucket name format is {base-bucket-name}--{az-id}--x-s3
   //example: doc-example-bucket--usw2-az1--x-s3 is a valid name for a directory
bucket created in
   //Region us-west-2, Availability Zone 2

   CreateBucketConfiguration bucketConfiguration =
CreateBucketConfiguration.builder()
            .location(LocationInfo.builder()
                    .type(LocationType.AVAILABILITY_ZONE)
                    .name("usw2-az1").build()) //this must match the Region and
Availability Zone in your bucket name
            .bucket(BucketInfo.builder()
                   .type(BucketType.DIRECTORY)
                   .dataRedundancy(DataRedundancy.SINGLE_AVAILABILITY_ZONE)
                   .build()).build();
   try {

            CreateBucketRequest bucketRequest =
CreateBucketRequest.builder().bucket(bucketName).createBucketConfiguration(bucketConfigurat
            CreateBucketResponse response = s3Client.createBucket(bucketRequest);
            System.out.println(response);
   }

   catch (S3Exception e) {
           System.err.println(e.awsErrorDetails().errorMessage());
           System.exit(1);
        }
   }
```

### 适用于 JavaScript 的 Amazon SDK

此示例说明如何使用 适用于 JavaScript 的 Amazon SDK 创建目录桶。

Example

```
// file.mjs, run with Node.js v16 or higher
// To use with the preview build, place this in a folder
// inside the preview build directory, such as /aws-sdk-js-v3/workspace/

import { S3 } from "@aws-sdk/client-s3";
```

```
const region = "us-east-1";
const zone = "use1-az4";
const suffix = `${zone}--x-s3`;

const s3 = new S3({ region });

const bucketName = `...--${suffix}`;

const createResponse = await s3.createBucket(
    { Bucket: bucketName,
      CreateBucketConfiguration: {Location: {Type: "AvailabilityZone", Name: zone},
      Bucket: { Type: "Directory", DataRedundancy: "SingleAvailabilityZone" }}
    }
   );
```

适用于 .NET 的 Amazon SDK

此示例说明如何使用 适用于 .NET 的 Amazon SDK 创建目录桶。

Example

```
using (var amazonS3Client = new AmazonS3Client())
{
    var putBucketResponse = await amazonS3Client.PutBucketAsync(new PutBucketRequest
    {

       BucketName = "DOC-EXAMPLE-BUCKET--usw2-az1--x-s3",
       PutBucketConfiguration = new PutBucketConfiguration
       {
         BucketInfo = new BucketInfo { DataRedundancy =
 DataRedundancy.SingleAvailabilityZone, Type = BucketType.Directory },
         Location = new LocationInfo { Name = "usw2-az1", Type =
 LocationType.AvailabilityZone }
       }
     }).ConfigureAwait(false);
}
```

SDK for PHP

此示例说明如何使用 Amazon SDK for PHP 创建目录桶。

Example

```
require 'vendor/autoload.php';
```

```
$s3Client = new S3Client([

    'region'      => 'us-east-1',
]);


$result = $s3Client->createBucket([
    'Bucket' => 'doc-example-bucket--use1-az4--x-s3',
    'CreateBucketConfiguration' => [
        'Location' => ['Name'=> 'use1-az4', 'Type'=> 'AvailabilityZone'],
        'Bucket' => ["DataRedundancy" => "SingleAvailabilityZone" ,"Type" =>
 "Directory"]   ],
]);
```

SDK for Python

此示例说明如何使用 适用于 Python (Boto3) 的 Amazon SDK 创建目录桶。

Example

```
import logging
import boto3
from botocore.exceptions import ClientError

def create_bucket(s3_client, bucket_name, availability_zone):
    '''
    Create a directory bucket in a specified Availability Zone

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket to create; for example, 'doc-example-bucket--usw2-
az1--x-s3'
    :param availability_zone: String; Availability Zone ID to create the bucket in,
 for example, 'usw2-az1'
    :return: True if bucket is created, else False
    '''

    try:
        bucket_config = {
                'Location': {
                    'Type': 'AvailabilityZone',
                    'Name': availability_zone
                },
                'Bucket': {
```

```
                    'Type': 'Directory',
                    'DataRedundancy': 'SingleAvailabilityZone'
                }
            }
        s3_client.create_bucket(
            Bucket = bucket_name,
            CreateBucketConfiguration = bucket_config
        )
    except ClientError as e:
        logging.error(e)
        return False
    return True


if __name__ == '__main__':
    bucket_name = 'BUCKET_NAME'
    region = 'us-west-2'
    availability_zone = 'usw2-az1'
    s3_client = boto3.client('s3', region_name = region)
    create_bucket(s3_client, bucket_name, availability_zone)
```

SDK for Ruby

此示例说明如何使用 适用于 Ruby 的 Amazon SDK 创建目录桶。

Example

```
s3 = Aws::S3::Client.new(region:'us-west-2')
s3.create_bucket(
  bucket: "bucket_base_name--az_id--x-s3",
  create_bucket_configuration: {
    location: { name: 'usw2-az1', type: 'AvailabilityZone' },
    bucket: { data_redundancy: 'SingleAvailabilityZone', type: 'Directory' }
  }
)
```

使用 Amazon CLI

此示例说明如何使用 Amazon CLI 创建目录桶。要使用该命令，请将*#######* 替换为您自己的信息。

创建目录存储桶时，必须提供配置详细信息并使用以下命名约定：*bucket-base-name*--*zone-id*--x-s3

```
aws s3api create-bucket
--bucket bucket-base-name--zone-id--x-s3
--create-bucket-configuration 'Location={Type=AvailabilityZone,Name=usw2-
az1},Bucket={DataRedundancy=SingleAvailabilityZone,Type=Directory}'
--region us-west-2
```

有关更多信息，请参阅 Amazon Command Line Interface 中的 create-bucket。

## 可用区中适用于目录存储桶的区域和可用区端点

要访问 S3 Express One Zone 中存储的对象和目录存储桶，您可以使用网关 VPC 端点。目录存储桶使用区域和可用区 API 端点。根据您使用的 Amazon S3 API 操作，需要区域端点或可用区端点。使用网关端点不会发生任何额外费用。

存储桶级（或控制面板）API 操作可通过区域端点使用，称为区域端点 API 操作。区域端点 API 操作的示例包括 `CreateBucket` 和 `DeleteBucket`。

当您创建存储在 S3 Express One Zone 中的目录存储桶时，您可以选择存储桶所在的可用区。您可以使用可用区端点 API 操作来上传和管理目录存储桶中的对象。

对象级（或数据面板）API 操作可通过可用区端点使用，称为可用区端点 API 操作。可用区端点 API 操作的示例包括 `CreateSession` 和 `PutObject`。

## 优化 S3 Express One Zone 性能

Amazon S3 Express One Zone 是高性能的单可用区（AZ）S3 存储类，专门用于为注重延迟的应用程序提供稳定的毫秒级数据访问。S3 Express One Zone 是第一种允许您选择将高性能对象存储和 Amazon 计算资源（例如 Amazon Elastic Compute Cloud、Amazon Elastic Kubernetes Service 和 Amazon Elastic Container Service）联合托管在单个可用区内的 S3 存储类。将存储和计算资源联合托管在一起，可以优化计算性能和成本，并提高数据处理速度。

S3 Express One Zone 提供了与其他 S3 存储类相似的性能弹性，但首字节读取和写入请求延迟能够稳定地保持在毫秒级，比 S3 Standard 存储快 10 倍。S3 Express One Zone 采用了全新设计，可支持非常高聚合水平的突发吞吐量。S3 Express One Zone 存储类使用定制架构来优化性能，并通过将数据存储在高性能硬件中，提供稳定的低请求延迟。S3 Express One Zone 的对象协议进行了增强，用于简化身份验证和元数据开销。

为了进一步缩短延迟并支持每秒多达 200 万次读取和多达 200000 次写入，S3 Express One Zone 将数据存储在新的存储桶类型中：Amazon S3 目录存储桶。默认情况下，每个目录存储桶支持每秒多达

200000 次读取和多达 100000 次写入。如果工作负载要求高于默认 TPS 限制，则可以通过 Amazon Support 来申请增加。

S3 Express One Zone 将提供数据访问速度达毫秒级的高性能专用硬件和软件，与可进行扩展以便每秒处理大量事务的目录存储桶相结合，使其成为非常适合请求密集型操作或注重性能的应用程序的 Amazon S3 存储类。

以下主题针对使用 S3 Express One Zone 存储类的应用程序，介绍了用于优化性能的最佳实践准则和设计模式。

主题

- S3 Express One Zone 的性能准则和设计模式

## S3 Express One Zone 的性能准则和设计模式

构建从 Amazon S3 Express One Zone 上传和检索对象的应用程序时，请遵循最佳实践准则以优化性能。要使用 S3 Express One Zone 存储类，您必须创建 S3 目录存储桶。S3 Express One Zone 存储类不支持与 S3 通用存储桶一起使用。

有关其他所有 Amazon S3 存储类和 S3 通用存储桶的性能准则，请参阅最佳实践设计模式：优化 Amazon S3 性能。

应用程序在使用 S3 Express One Zone 存储类和目录存储桶时，要想获得最佳性能，我们建议遵循以下准则和设计模式。

主题

- 将 S3 Express One Zone 存储与您的 Amazon 计算资源联合托管在一个位置
- 目录存储桶
- 目录存储桶横向扩展请求并行化
- 性能故障排除

### 将 S3 Express One Zone 存储与您的 Amazon 计算资源联合托管在一个位置

每个目录存储桶存储在创建存储桶时选择的单个可用区中。首先，在计算工作负载或资源所在的可用区中，可以创建一个新的目录存储桶。然后就可以立即开始享受到延迟非常低的读取和写入。目录存储桶是第一种可以选择 Amazon Web Services 区域中可用区的 S3 存储桶，可以减少计算和存储之间的延迟。

如果您跨可用区访问目录存储桶，则延迟会增加。为了优化性能，我们建议您尽可能从位于同一可用区的 Amazon Elastic Container Service、Amazon Elastic Kubernetes Service 和 Amazon Elastic Compute Cloud 实例访问目录存储桶。

目录存储桶

每个目录存储桶支持每秒多达 200 万个事务（TPS）。与通用存储桶不同，目录存储桶将键分层组织到目录中，而不是前缀中。前缀是对象键名称开头的一串字符串。您可以把前缀视为一种以类似于目录的方式组织数据的方式。但是，前缀不是目录。

前缀在通用存储桶的平面命名空间中组织数据，通用存储桶中的前缀数量没有限制。每个前缀每秒可以实现每秒至少 3500 个 PUT/POST/DELETE 或 5500 个 GET/HEAD 请求。您还可以并行处理多个前缀的请求以扩展性能。但是，无论是读取操作还是写入操作，此扩展都是逐渐发生的，而不是瞬间发生。当通用存储桶扩展到新的更高请求速率时，您可能会收到一些 HTTP 状态码 503（服务不可用）错误。

对于分层命名空间，对象键中的分隔符很重要。唯一支持的分隔符是正斜杠（/）。目录由分隔符边界确定。例如，对象键 `dir1/dir2/file1.txt` 会自动创建目录 `dir1/` 和 `dir2/`，并将对象 `file1.txt` 添加到路径 `dir1/dir2/file1.txt` 中的 `/dir2` 目录。

当对象上传到目录存储桶时创建的目录没有每前缀 TPS 限制。相反，每个存储桶可以支持每个 S3 目录存储桶多达 200 万 TPS。由于这种灵活性，应用程序可以根据需要并行处理目录内和跨目录的读取和写入请求。

目录存储桶横向扩展请求并行化

您可以将多个并行请求发送到目录存储桶，以便在不同的连接上分布请求，尽可能充分利用可用带宽，从而实现出色的性能。S3 Express One Zone 对与目录存储桶建立的连接数没有任何限制。在对同一目录进行大量并发写入操作时，这一目录可以横向自动扩展性能。

在最初创建对象键并且其键名包含目录时，将自动为该对象创建该目录。后续对象上传到相同目录时不需要创建目录，这样可以减少将对象上传到现有目录的延迟。

虽然目录存储桶中支持以浅层目录结构和深层目录结构存储对象，但目录存储桶可以自动横向扩展，同时上传到相同目录或并行同级目录的延迟更低。

性能故障排除

延迟敏感型应用程序的重试请求

S3 Express One Zone 专为提供稳定的高性能而设计，无需额外调整。但是，设置更主动的超时值和重试次数可以进一步推动实现稳定的延迟和性能。Amazon SDK 具有可配置的超时和重试值，您可以进行调整以符合特定应用程序的容限。

Amazon Common Runtime（CRT）库和 Amazon EC2 实例类型搭配

执行大量读取和写入操作的应用程序，相比不执行这些操作的应用程序会需要更多的内存或计算容量。在为具有高性能要求的工作负载启动 Amazon Elastic Compute Cloud（Amazon EC2）实例时，应选择具有您的应用程序需要的这些资源量的实例类型。S3 Express One Zone 高性能存储非常适合与更大、更新的实例类型搭配使用，这些实例类型具有更大的系统内存以及计算能力更强的 CPU 和 GPU，可以利用性能更高的存储。我们还建议使用启用了 CRT 的 Amazon SDK 的最新版本，这样可以更好地加速并行读取和写入请求。

在 Amazon SDK 而不是 HTTP REST API 中使用基于会话的身份验证

借助 Amazon S3，在使用 HTTP REST API 请求时，您还可以遵循 Amazon SDK 中相同的最佳实践，以此来优化性能。但是，对于 S3 Express One Zone 使用的基于会话的授权和身份验证机制，我们强烈建议您使用 Amazon SDK 管理 `CreateSession` 及其托管会话令牌。Amazon SDK 使用 `CreateSession` API 操作，自动代表您创建和刷新令牌。使用 `CreateSession` 可减少 Amazon Identity and Access Management（IAM）授权各个请求的请求往返延迟。

## 数据驻留工作负载

本地区域是一种类型的 Amazon Web Services 基础设施部署，它将精选的计算、存储和其它 Amazon Web Services 服务放在人口密集区和工业中心附近。要了解有关本地区域的更多信息，请参阅 Amazon 本地区域。

在本地区域中，您可以创建 S3 目录存储桶来将数据存储在特定的数据边界或大都市区中，这有助于支持数据驻留应用场景。Amazon Web Services 北京本地区域由 Sinnet 运营和提供，该公司还运营和提供 Amazon Web Services 中国（北京）区域的服务。目录存储桶目前在其它 Amazon Local Zones 站点不可用。

可以在本地区域中使用 Amazon Web Services Management Console、REST API、Amazon Command Line Interface（Amazon CLI）和 Amazon SDK。

有关在 Local Zones 中使用目录存储桶的更多信息，请参阅以下主题：

主题

- Local Zones 中目录存储桶的概念
- 为本地区域启用账户
- 来自 VPC 的私有连接
- 在本地区域中创建目录存储桶
- 对 Local Zones 中的目录存储桶进行身份验证和授权

## Local Zones 中目录存储桶的概念

在本地区域中创建目录存储桶之前，您必须拥有要在其中创建存储桶的本地区域 ID。可以使用 DescribeAvailabilityZones API 操作查找所有本地区域信息。此 API 操作列出有关本地区域的信息，包括本地区域 ID、父区域名称、网络边界组和选择加入状态。获得本地区域 ID 并且您选择加入后，您可以在本地区域中创建目录存储桶。目录存储桶名称由您提供的基本名称和包含存储桶位置的可用区 ID 的后缀组成，后跟 `--x-s3`。

本地区域使用私有网络连接到父区域。父可用区 ID 是处理本地区域控制面板操作的可用区的 ID。网络边界组是 Amazon 从中通告公有 IP 地址的唯一组。有关 Local Zones、父区域和父可用区 ID 的更多信息，请参阅《Amazon Local Zones User Guide》中的 Amazon Local Zones concepts。

所有目录存储桶都使用 `s3express` 命名空间，该命名空间不同于通用存储桶的 `s3` 命名空间。对于目录存储桶，请求会被路由到区域端点或可用区端点。如果您使用 Amazon Web Services Management Console、Amazon CLI 或 Amazon SDK，则会自动为您处理路由。

大多数存储桶级 API 操作（如 `CreateBucket` 和 `DeleteBucket`）路由到区域端点，称为区域端点 API 操作。区域端点的格式为 `s3express-control.ParentRegionCode.amazonaws.com.cn`。所有对象级 API 操作（例如 `PutObject`）和两个存储桶级 API 操作（`CreateSession` 和 `HeadBucket`）都路由到可用区端点，称为可用区端点 API 操作。可用区端点的格式为 `s3express-LocalZoneID.ParentRegionCode.amazonaws.com.cn`。有关按端点类型划分的 API 操作的完整列表，请参阅目录存储桶 API 操作。

S3 在北京本地区域中可用：

本地区域 ID：`cnn1-pkx1-az1`

- 父区域名称：`China (Beijing)`
- 父地区代码：`cn-north-1`
- 父区域 ID：`cnn1-az1`
- 本地区域名称：`China (Beijing)`
- 本地区域代码：`cnn1-pkx1-az1`
- 网络边界组：`cn-north-1-pkx-1`
- 示例存储桶 ARN：`arn:aws-cn:s3express:cn-north-1:`*`123456789012`*`:bucket/`*`amzn-s3-demo-bucket`*`--cnn1-pkx1-az1--x-s3`

区域端点：`s3express-control.cn-north-1.amazonaws.com.cn`

可用区端点：`s3express-cnn1-pkx1-az1.cn-north-1.amazonaws.com.cn`

存储类：`S3 One Zone-Infrequent Access (S3 One Zone-IA; Z-IA)`

要从虚拟私有云（VPC）中访问 Local Zones 中的目录存储桶，可以使用网关 VPC 端点。使用网关端点不会发生任何额外费用。要配置网关 VPC 端点来访问 Local Zones 中的目录存储桶和对象，请参阅来自 VPC 的私有连接。

## 为本地区域启用账户

以下主题介绍了如何为北京本地区域启用账户。

对于北京本地区域中的所有服务，包括 Amazon S3，管理员必须先启用您的 Amazon Web Services 账户，然后您才能在 Amazon Web Services 北京本地区域中创建或访问任何资源。可以使用 DescribeAvailabilityZones API 操作来确认您的账户 ID 对本地区域的访问权限。

为了进一步保护您在 Amazon S3 中的数据，默认情况下，您只能访问自己创建的 S3 资源。Local Zones 中的存储桶默认启用了所有 S3 屏蔽公共访问权限设置，并且 S3 对象所有权设置为强制存储桶拥有者。无法修改这些设置。有关更多信息，请参阅 对 Local Zones 中的目录存储桶进行身份验证和授权。

## 来自 VPC 的私有连接

您可以使用网关端点，从虚拟私有云（VPC）访问 Amazon Local Zones（即 Local Zones）中的目录存储桶，而无需为 VPC 配备互联网网关或 NAT 设备，也无需任何额外费用。以下主题介绍在 VPC 和 Local Zones 中的目录存储桶之间配置网关 VPC 端点。

### 配置网关 VPC 端点

1. 打开 Amazon VPC 控制台。
2. 在导航窗格中，选择端点。
3. 选择 创建端点。
4. 为端点创建名称。
5. 对于 Service category（服务类别），选择 Amazon Web Services 服务。
6. 对于服务，添加筛选条件 Type=Gateway，然后选择 com.amazonaws.cn-north-1.s3express 旁边的选项按钮。
7. 对于 VPC，选择要在其中创建端点的 VPC。

8. 对于路由表，选择本地区域上端点要使用的路由表。创建端点后，将在此步骤中选择的路由表中添加一条路径记录。
9. 对于策略，请选择完整访问权限以允许所有主体通过 VPC 端点对所有资源执行所有操作。否则，选择自定义以附加 VPC 端点策略，该策略控制主体通过 VPC 端点对资源执行操作的权限。
10. （可选）要添加标签，请选择添加新标签，然后输入标签键和标签值。
11. 选择创建端点。

有关网关 VPC 端点的更多信息，请参阅《Amazon PrivateLink Guide》中的 Gateway endpoints。对于数据驻留应用场景，我们建议使用网关 VPC 端点仅从 VPC 访问存储桶。当访问权限限于 VPC 或 VPC 端点时，可以通过 Amazon Web Services Management Console、REST API、Amazon CLI 和 Amazon SDK 访问对象。

> **Note**
>
> 要使用 Amazon Web Services Management Console将访问权限限于 VPC 或 VPC 端点，必须使用 Amazon Web Services Management Console私有访问权限。有关更多信息，请参阅《Amazon Web Services Management Console Guide》中的 Amazon Web Services Management Console Private Access。

## 在本地区域中创建目录存储桶

在专用本地区域中，您可以创建目录存储桶来存储和检索特定数据边界中的对象，以有助于满足数据驻留和数据隔离应用场景的要求。S3 目录存储桶是 Local Zones 中唯一支持的存储桶类型，并且包含名为 `LocalZone` 的存储桶位置类型。目录存储桶名称由您提供的基本名称以及包含存储桶位置的可用区 ID 和 `--x-s3` 的后缀组成。可以使用 DescribeAvailabilityZones API 操作获取本地区域 ID 的列表。有关更多信息，请参阅 目录存储桶命名规则。

> **Note**
>
> - 对于 Amazon 专用本地区域（专用本地区域）中的所有服务，包括 S3，管理员必须先启用您的 Amazon Web Services 账户，然后您才能在专用本地区域中创建或访问任何资源。有关更多信息，请参阅 为本地区域启用账户。
> - 对于数据驻留要求，我们建议仅允许从网关 VPC 端点访问您的存储桶。有关更多信息，请参阅 来自 VPC 的私有连接。

下面介绍使用 Amazon Web Services Management Console、Amazon CLI 和 Amazon SDK 在单个本地区域中创建目录存储桶的方法。

使用 S3 控制台

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在页面顶部的导航栏中，选择当前所显示 Amazon Web Services 区域的名称。接下来，选择要在其中创建目录存储桶的本地区域的父区域。

   > **Note**
   >
   > 有关父区域的更多信息，请参阅Local Zones 中目录存储桶的概念。

3. 在左侧导航窗格中，选择存储桶。
4. 选择创建存储桶。

   此时将打开创建存储桶页面。
5. 在常规配置下，查看将在其中创建存储桶的 Amazon Web Services 区域。
6. 在存储桶类型下，请选择目录。

   > **Note**
   >
   > - 如果您选择的区域不支持目录存储桶，则存储桶类型默认为通用存储桶。要创建目录桶，您必须选择受支持的区域。有关支持目录存储桶的区域列表，请参阅the section called “目录存储桶的区域和可用区端点”。
   > - 在创建存储桶后，便无法更改存储桶类型。

7. 在存储桶位置下，选择要使用的本地区域。

   > **Note**
   >
   > 创建存储桶后无法更改本地区域。

8. 在存储桶位置下，选中复选框以确认在本地区域中断的情况下，您的数据可能不可用或丢失。

> **Important**
>
> 尽管目录存储桶存储在单个 Local Zones 中的多个设备上，但目录存储桶不会跨 Local Zones 冗余存储数据。

9. 对于存储桶名称，请输入目录存储桶的名称。

   有关目录存储桶的命名规则的更多信息，请参阅通用存储桶命名规则。后缀将自动添加到您使用控制台创建目录存储桶时提供的基本名称中。此后缀包括您选择的本地区域的可用区 ID。

   创建存储桶后，便无法更改其名称。

   > **Important**
   >
   > 请勿在存储桶名称中包含敏感信息，如账号。存储桶名称会显示在指向存储桶中的对象的 URL 中。

10. 在对象所有权下，将自动启用强制桶拥有者设置，并禁用所有访问控制列表（ACL）。对于目录存储桶，ACL 已禁用且无法启用。

    在启用强制存储桶拥有者设置的情况下，存储桶拥有者会自动拥有并完全控制存储桶中的每个对象。ACL 不再影响对 S3 存储桶中数据的访问权限。存储桶专门使用策略来定义访问控制。Amazon S3 中的大多数现代使用案例不再需要使用 ACL。有关更多信息，请参阅 为您的存储桶控制对象所有权和禁用 ACL。。

11. 在此桶的屏蔽公共访问权限设置下，目录桶的所有屏蔽公共访问权限设置已自动启用。无法修改目录桶的这些设置。有关阻止公共访问的更多信息，请参阅阻止对您的 Amazon S3 存储的公有访问。

12. 默认情况下，在默认加密下，目录存储桶使用具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）来加密数据。还可以选择使用具有 Amazon Key Management Service 密钥的服务器端加密（SSE-KMS）对目录存储桶中的数据进行加密。

13. 选择 创建存储桶 。

    创建存储桶后，您可以向存储桶中添加文件和文件夹。有关更多信息，请参阅 the section called “使用目录桶中的对象”。

使用 Amazon CLI

此示例说明如何在本地区域中使用 Amazon CLI 创建目录存储桶。要使用该命令，请将####### 替换为您自己的信息。

创建目录存储桶时，必须提供配置详细信息并使用以下命名约定：*bucket-base-name*--*zone-id*--x-s3。

```
aws s3api create-bucket
--bucket bucket-base-name--zone-id--x-s3
--create-bucket-configuration 'Location={Type=LocalZone,Name=local-zone-
id},Bucket={DataRedundancy=SingleLocalZone,Type=Directory}'
--region parent-region-code
```

有关本地区域 ID 和父区域代码的更多信息，请参阅Local Zones 中目录存储桶的概念。有关 Amazon CLI 命令的更多信息，请参阅《Amazon CLI Command Reference》中的 create-bucket。

使用 Amazon SDK

SDK for Go

此示例说明如何在本地区域中使用适用于 Go 的 Amazon SDK 创建目录存储桶。

Example

```
var bucket = "bucket-base-name--zone-id--x-s3" // The full directory bucket name

func runCreateBucket(c *s3.Client) {
    resp, err := c.CreateBucket(context.Background(), &s3.CreateBucketInput{
        Bucket: &bucket,
        CreateBucketConfiguration: &types.CreateBucketConfiguration{
            Location: &types.LocationInfo{
                Name: aws.String("local-zone-id"),
                Type: types.LocationTypeLocalZone,
            },
            Bucket: &types.BucketInfo{
                DataRedundancy: types.DataRedundancySingleLocalZone,
                Type:           types.BucketTypeDirectory,
            },
        },
    })
    var terr *types.BucketAlreadyOwnedByYou
    if errors.As(err, &terr) {
```

```
        fmt.Printf("BucketAlreadyOwnedByYou: %s\n", aws.ToString(terr.Message))
        fmt.Printf("noop...\n") // No operation performed, just printing a message
        return
    }
    if err != nil {
        log.Fatal(err)
    }

    fmt.Printf("bucket created at %s\n", aws.ToString(resp.Location))
}
```

SDK for Java 2.x

此示例说明如何在本地区域中使用Amazon SDK for Java 2.x 创建目录存储桶。

Example

```
public static void createBucket(S3Client s3Client, String bucketName) {

    //Bucket name format is {base-bucket-name}--{local-zone-id}--x-s3
    //example: doc-example-bucket--local-zone-id--x-s3 is a valid name for a
 directory bucket created in a Local Zone.

    CreateBucketConfiguration bucketConfiguration =
 CreateBucketConfiguration.builder()
             .location(LocationInfo.builder()
                     .type(LocationType.LOCAL_ZONE)
                     .name("local-zone-id").build()) //this must match the Local
 Zone ID in your bucket name
             .bucket(BucketInfo.builder()
                    .type(BucketType.DIRECTORY)
                    .dataRedundancy(DataRedundancy.SINGLE_LOCAL_ZONE)
                    .build()).build();
    try {

             CreateBucketRequest bucketRequest =
 CreateBucketRequest.builder().bucket(bucketName).createBucketConfiguration(bucketConfigurat
             CreateBucketResponse response = s3Client.createBucket(bucketRequest);
             System.out.println(response);
    }

    catch (S3Exception e) {
            System.err.println(e.awsErrorDetails().errorMessage());
```

```
            System.exit(1);
        }
    }
```

适用于 JavaScript 的 Amazon SDK

此示例说明如何在本地区域中使用适用于 JavaScript 的 Amazon SDK 创建目录存储桶。

Example

```
// file.mjs, run with Node.js v16 or higher
// To use with the preview build, place this in a folder
// inside the preview build directory, such as /aws-sdk-js-v3/workspace/

import { S3 } from "@aws-sdk/client-s3";

const region = "parent-region-code";
const zone = "local-zone-id";
const suffix = `${zone}--x-s3`;

const s3 = new S3({ region });

const bucketName = `bucket-base-name--${suffix}`; // Full directory bucket name

const createResponse = await s3.createBucket(
    { Bucket: bucketName,
      CreateBucketConfiguration: {Location: {Type: "LocalZone", Name: "local-zone-
id"},
      Bucket: { Type: "Directory", DataRedundancy: "SingleLocalZone" }}
    }
   );
```

适用于 .NET 的 Amazon SDK

此示例说明如何在本地区域中使用适用于 .NET 的 Amazon SDK 创建目录存储桶。

Example

```
using (var amazonS3Client = new AmazonS3Client())
{
    var putBucketResponse = await amazonS3Client.PutBucketAsync(new PutBucketRequest
```

```
    {

       BucketName = "bucket-base-name--local-zone-id--x-s3",
       PutBucketConfiguration = new PutBucketConfiguration
       {
         BucketInfo = new BucketInfo { DataRedundancy =
 DataRedundancy.SingleLocalZone, Type = BucketType.Directory },
         Location = new LocationInfo { Name = "local-zone-id", Type =
 LocationType.LocalZone }
       }
     }).ConfigureAwait(false);
}
```

SDK for PHP

此示例说明如何在本地区域中使用Amazon SDK for PHP 创建目录存储桶。

Example

```
require 'vendor/autoload.php';

$s3Client = new S3Client([

    'region'      => 'parent-region-code',
]);


$result = $s3Client->createBucket([
    'Bucket' => 'bucket-base-name--local-zone-id--x-s3',
    'CreateBucketConfiguration' => [
        'Location' => ['Name'=> 'local-zone-id', 'Type'=> 'LocalZone'],
        'Bucket' => ["DataRedundancy" => "SingleLocalZone" ,"Type" => "Directory"]
  ],
]);
```

SDK for Python

此示例说明如何在本地区域中使用适用于 Python (Boto3) 的 Amazon SDK 创建目录存储桶。

Example

```
import logging
import boto3
```

```
from botocore.exceptions import ClientError

def create_bucket(s3_client, bucket_name, local_zone):
    '''
    Create a directory bucket in a specified Local Zone

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket to create; for example, 'bucket-base-name--local-
zone-id--x-s3'
    :param local_zone: String; Local Zone ID to create the bucket in
    :return: True if bucket is created, else False
    '''

    try:
        bucket_config = {
                'Location': {
                    'Type': 'LocalZone',
                    'Name': local_zone
                },
                'Bucket': {
                    'Type': 'Directory',
                    'DataRedundancy': 'SingleLocalZone'
                }
            }
        s3_client.create_bucket(
            Bucket = bucket_name,
            CreateBucketConfiguration = bucket_config
        )
    except ClientError as e:
        logging.error(e)
        return False
    return True


if __name__ == '__main__':
    bucket_name = 'BUCKET_NAME'
    region = 'parent-region-code'
    local_zone = 'local-zone-id'
    s3_client = boto3.client('s3', region_name = region)
    create_bucket(s3_client, bucket_name, local_zone)
```

### SDK for Ruby

此示例说明如何在本地区域中使用适用于 Ruby 的 Amazon SDK 创建目录存储桶。

Example

```
s3 = Aws::S3::Client.new(region:'parent-region-code')
s3.create_bucket(
  bucket: "bucket-base-name--local-zone-id--x-s3",
  create_bucket_configuration: {
    location: { name: 'local-zone-id', type: 'LocalZone' },
    bucket: { data_redundancy: 'SingleLocalZone', type: 'Directory' }
  }
)
```

### 对 Local Zones 中的目录存储桶进行身份验证和授权

Local Zones 中的目录存储桶同时支持 Amazon Identity and Access Management（IAM）授权和基于会话的授权。有关目录存储桶的身份验证和授权的更多信息，请参阅对请求进行身份验证和授权。

资源

目录存储桶的 Amazon 资源名称（ARN）包含 `s3express` 命名空间、Amazon 父区域、Amazon Web Services 账户 ID 和目录存储桶名称（包括可用区 ID）。要访问目录存储桶并对其执行操作，您必须使用以下 ARN 格式：

```
arn:aws:s3express:region-code:account-id:bucket/bucket-base-name--ZoneID--x-s3
```

对于本地区域中的目录存储桶，可用区 ID 是本地区域的 ID。有关 Local Zones 中的目录存储桶的更多信息，请参阅Local Zones 中目录存储桶的概念。有关 ARN 的更多信息，请参阅《IAM 用户指南》中的 Amazon 资源名称（ARN）。有关资源的更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：Resource。

> **Note**
>
> 北京本地区域不支持条件键 `s3express:AllAccessRestrictedToLocalZoneGroup`。

## 目录存储桶的差异

使用 Amazon S3 时，您可以选择最适合您应用程序和性能要求的存储桶类型。目录存储桶是一种最适合低延迟或数据驻留应用场景的存储桶。要了解有关目录存储桶的更多信息，请参阅使用目录存储桶。

有关目录存储桶差异的更多信息，请参阅以下主题。

主题


- 目录存储桶的差异
- 目录存储桶支持的 API 操作
- 目录存储桶不支持的 Amazon S3 功能


# 目录存储桶的差异

- 目录存储桶名称
  - 目录存储桶名称由您提供的基本名称和包含存储桶所在区域（可用区）ID 的后缀组成。目录存储桶名称必须使用特定格式并遵循目录存储桶的命名规则。有关规则列表和目录存储桶名称的示例，请参阅目录存储桶命名规则。
- **`ListObjectsV2`** 行为
  - 对于目录存储桶，`ListObjectsV2` 不按字母表顺序返回对象。此外，前缀必须以分隔符结尾，并且只能将“/”指定为分隔符。
  - 对于目录存储桶，`ListObjectsV2` 响应包含仅与正在进行的分段上传相关的前缀。
- 删除行为 – 当您删除目录存储桶中的对象时，Amazon S3 会递归删除对象路径中的所有空目录。例如，如果您删除对象键 `dir1/dir2/file1.txt`，Amazon S3 会删除 `file1.txt`。如果 `dir1/` 和 `dir2/` 目录为空且不包含其他对象，Amazon S3 还会删除这些目录。
- ETag 与校验和：目录存储桶的实体标签（ETag）是对象独有的随机字母数字字符串，而不是 MD5 校验和。有关在目录存储桶中使用附加校验和的更多信息，请参阅 其他 S3 校验和最佳实践。
- **`DeleteObjects`** 请求中的对象键
  - `DeleteObjects` 请求中的对象键必须至少包含一个非空格字符。`DeleteObjects` 请求中不支持完全由空格组成的字符串。
  - `DeleteObjects` 请求中的对象键不能包含 Unicode 控制字符，但换行符（`\n`）、制表符（`\t`）和回车符（`\r`）字符除外。
- 区域和可用区端点 – 目录存储桶的存储桶管理 API 操作可通过区域端点使用，称为区域端点 API 操作。区域端点 API 操作的示例包括 CreateBucket 和 DeleteBucket。创建目录存储桶后，您可以使用可用区端点 API 操作来上传和管理目录存储桶中的对象。可用区端点 API 操作可通过可用区端点执行。可用区端点 API 操作的示例包括 `PutObject` 和 `CopyObject`。使用目录存储桶时，您必须在所有请求中指定区域。对于区域端点，您可以指定区域，例如 `s3express-control.us-west-2.amazonaws.com`。对于可用区端点，您需要同时指定区域和可用区，例如 `s3express-usw2-az1.us-west-2.amazonaws.com`。有关更多信息，请参阅 目录存储桶的区域和可用区端点。

- 分段上传 – 您可以使用分段上传流程，上传和复制目录存储桶中存储的大型对象。但是，对存储在目录存储桶中的对象使用分段上传流程时，会有以下一些区别。有关更多信息，请参阅 the section called “对目录桶使用分段上传”。
  - 对象的创建日期是分段上传完成的日期。
  - 分段上传的分段编号必须连续。如果您尝试使用非连续分段编号完成分段上传请求，Amazon S3 会生成 HTTP `400 (Bad Request)` 错误。
  - 只有在通过 `s3express:CreateSession` 权限明确向分段上传的发起者授予了对 `AbortMultipartUpload` 的访问权限时，才能中止分段上传请求。有关更多信息，请参阅 使用 IAM 对区域端点 API 操作进行授权。
- 清空目录存储桶：通过 Amazon Command Line Interface（CLI）执行的 `s3 rm` 命令、通过 Mountpoint 执行的 `delete` 操作以及通过 Amazon Web Services Management Console执行的清空存储桶选项按钮无法删除目录存储桶中正在进行的分段上传。要删除这些正在进行的分段上传，请使用 `ListMultipartUploads` 操作列出存储桶中正在进行的分段上传，然后使用 `AbortMultipartUpload` 操作中止所有正在进行的分段上传。
- Amazon Local Zones：仅目录存储桶支持 Local Zones，通用存储桶不支持 Local Zones。
  - 位于 Local Zones 中的目录存储桶不支持向现有对象追加数据。您只能向位于可用区内的目录存储桶中的现有对象追加数据。
  - Local Zones 中的目录存储桶不支持 S3 生命周期。

## 目录存储桶支持的 API 操作

目录存储桶同时支持区域（存储桶级或控制面板）和可用区（对象级或数据面板）端点 API 操作。有关更多信息，请参阅目录存储桶的联网和端点和网关 VPC 端点。

区域端点 API 操作

目录存储桶支持以下区域端点 API 操作：

- CreateBucket
- DeleteBucket
- DeleteBucketLifecycle
- DeleteBucketPolicy
- GetBucketPolicy
- GetBucketLifecycleConfiguration
- ListDirectoryBuckets

- PutBucketLifecycleConfiguration
- PutBucketPolicy

可用区端点 API 操作

目录存储桶支持使用以下可用区端点 API 操作：

- CreateSession
- CopyObject
- DeleteObject
- DeleteObjects
- GetObject
- GetObjectAttributes
- HeadBucket
- HeadObject
- ListObjectsV2
- PutObject
- AbortMultipartUpload
- CompleteMultiPartUpload
- CreateMultipartUpload
- ListMultipartUploads
- ListParts
- UploadPart
- UploadPartCopy
- UploadPartCopy
- PutBucketEncryption
- GetBucketEncryption
- DeleteBucketEncryption

## 目录存储桶不支持的 Amazon S3 功能

目录存储桶不支持以下 Amazon S3 功能：

- Amazon 托管式策略
- 适用于 S3 的 Amazon PrivateLink
- MD5 校验和
- 多重验证 (MFA) 删除
- S3 对象锁定
- 申请方付款
- S3 访问授权
- 存储桶标签
- Amazon CloudWatch 请求指标
- S3 事件通知
- S3 生命周期转换操作
- S3 多区域接入点
- S3 对象 Lambda 接入点
- S3 版本控制
- S3 清单
- S3 复制
- 对象标签
- S3 Select
- 服务器访问日志
- 静态网站托管
- S3 Storage Lens 存储统计管理工具
- S3 Storage Lens 组
- S3 Transfer Acceleration
- 具有 Amazon Key Management Service（Amazon KMS）密钥的双层服务器端加密（DSSE-KMS）
- 具有客户提供密钥的服务器端加密（SSE-C）
- 在 Amazon S3 控制台中创建新存储桶时复制现有存储桶的设置的选项
- 增强拒绝访问（HTTP `403 Forbidden`）错误消息

# 目录存储桶的联网

要访问目录存储桶及其内部的对象，您需要使用不同于标准 Amazon S3 端点的区域和可用区 API 端点。根据您使用的 S3 API 操作，需要区域端点或可用区端点。有关按端点类型统计的 API 操作的完整列表，请参阅 目录存储桶的差异。

您可以通过网关虚拟私有云（VPC）端点访问可用区和区域 API 操作。

以下主题介绍使用网关 VPC 端点访问 S3 Express One Zone 时的联网要求。

主题


- 了解如何查看、监控和管理 SageMaker 端点。
- 配置 VPC 网关端点


## 了解如何查看、监控和管理 SageMaker 端点。

您可以通过使用网关 VPC 端点，从 VPC 访问目录存储桶及其内部的对象。目录存储桶使用区域和可用区 API 端点。根据您使用的 Amazon S3 API 操作，需要区域端点或可用区端点。使用网关端点不会发生任何额外费用。

存储桶级（或控制面板）API 操作可通过区域端点使用，称为区域端点 API 操作。区域端点 API 操作的示例包括 `CreateBucket` 和 `DeleteBucket`。在创建目录存储桶时，您需要选择单个用于创建目录存储桶的区域（可用区或本地区域）。创建目录存储桶后，您可以使用可用区端点 API 操作来上传和管理目录存储桶中的对象。

对象级（或数据面板）API 操作可通过可用区端点使用，称为可用区端点 API 操作。可用区端点 API 操作的示例包括 `CreateSession` 和 `PutObject`。

有关支持可用区中目录存储桶的端点和位置的更多信息，请参阅可用区中目录存储桶的端点。

有关支持 Local Zones 中目录存储桶的端点和位置的更多信息，请参阅为本地区域启用账户。

## 配置 VPC 网关端点

要为可用区中的访问目录存储桶配置网关 VPC 端点，请参阅the section called “配置 VPC 网关端点”。

要为 Local Zones 中的访问目录存储桶配置网关 VPC 端点，请参阅来自 VPC 的私有连接。

# 目录存储桶命名规则

在 Amazon S3 中创建目录存储桶时，以下存储桶命名规则适用。有关通用存储桶命名规则，请参阅通用存储桶命名规则。

目录存储桶名称由您提供的基本名称和后缀组成，该后缀包含您的存储桶所在 Amazon 区域（可用区或本地区域）的 ID 以及 `--x-s3`。*`zone-id`* 可以是可用区或本地区域的 ID。

```
base-name--zoneid--x-s3
```

例如，以下目录存储桶名称包含可用区 ID `usw2-az1`：

```
bucket-base-name--usw2-az1--x-s3
```

> **Note**
>
> 当您使用控制台创建目录存储桶时，系统会自动将后缀添加到您提供的基本名称。此后缀包括您所选可用区（可用区或本地区域）的可用区 ID。
> 当您使用 API 创建目录存储桶时，必须在请求中提供包括区域 ID 在内的完整后缀。有关区域 ID 的列表，请访问了解如何查看、监控和管理 SageMaker 端点。。

以下命名规则适用于目录存储桶。

- 在选定的区域（Amazon 可用区或 Amazon 本地区域）内是唯一的。
- 名称的长度必须介于 3（最小）到 63（最大）个字符之间，包括后缀。
- 仅包含小写字母、数字和连字符（-）。
- 以字母或数字开头和结尾。
- 必须包含以下后缀：`--`*`zone-id`*`--x-s3`。
- 存储桶名称不得以前缀 `xn--` 开头。
- 存储桶名称不得以前缀 `sthree-` 开头。
- 存储桶名称不得以前缀 `sthree-configurator` 开头。
- 存储桶名称不得以前缀 `amzn-s3-demo-` 开头。
- 存储桶名称不得以后缀 `-s3alias` 结尾。此后缀是为接入点别名预留的。有关更多信息，请参阅 通用存储桶的接入点别名。

- 存储桶名称不得以后缀 `--ol-s3` 结尾。此后缀是为对象 Lambda 接入点别名预留的。有关更多信息，请参阅 如何为您的 S3 存储桶对象 Lambda 接入点使用存储桶式别名。
- 存储桶名称不得以后缀 `.mrap` 结尾。此后缀预留用于多区域接入点名称。有关更多信息，请参阅 命名 Amazon S3 多区域接入点的规则。

# 查看目录存储桶属性

您可以使用 Amazon S3 控制台查看和配置 Amazon S3 目录桶的属性。有关更多信息，请参阅 使用目录存储桶。

## 使用 S3 控制台

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择目录存储桶。
3. 在目录存储桶列表中，选择要查看其属性的存储桶的名称。
4. 选择属性选项卡。
5. 在属性选项卡上，您可以查看桶的以下属性：

   - 目录存储桶概述：您可以查看存储桶的 Amazon Web Services 区域、可用区（可用区或本地区域）、Amazon 资源名称（ARN）和创建日期。
   - 服务器端加密设置：Amazon S3 应用具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3），作为对所有 Amazon S3 存储桶的基本加密级别。Amazon S3 会在将对象保存到磁盘之前对其进行加密，并在下载对象时对其进行解密。有关更多信息，请参阅 设置和监控目录存储桶的默认加密。

     有关目录存储桶支持的功能的更多信息，请参阅创建和使用目录存储桶。

# 管理目录存储桶策略

可以使用 Amazon S3 控制台、Amazon SDK 和 Amazon CLI 来添加、删除、更新和查看 Amazon S3 目录存储桶的存储桶策略。有关更多信息，请参阅以下主题。有关受支持的 Amazon Identity and Access Management（IAM）操作的更多信息，请参阅 使用 IAM 对区域端点 API 操作进行授权。有关目录存储桶的存储桶策略示例，请参阅目录存储桶的存储桶策略示例。

主题

- 添加存储桶策略
- 查看存储桶策略
- 删除存储桶策略


# 添加存储桶策略

要向目录存储桶添加存储桶策略，您可以使用 Amazon S3 控制台、Amazon SDK 或 Amazon CLI。

使用 S3 控制台

创建或编辑存储桶策略

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择目录存储桶。
3. 在目录存储桶列表中，选择要向其添加策略的存储桶的名称。
4. 选择 Permissions（权限）选项卡。
5. 在 Bucket policy（存储桶策略）下，请选择 Edit（编辑）。将出现 Edit bucket policy（编辑存储桶策略）页面。
6. 要自动生成策略，请选择策略生成器。

   如果选择 Policy generator（策略生成器），Amazon 策略生成器将在新窗口中打开。

   如果您不想使用 Amazon 策略生成器，则可以在策略部分添加或编辑 JSON 语句。

   a. 在 Amazon 策略生成器页面上，对于选择策略类型，选择 S3 存储桶策略。
   b. 通过在提供的字段中输入信息来添加语句，然后选择添加语句。对您要添加的所需数量的语句重复此步骤。有关这些字段的更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素参考。

      > **Note**
      >
      > 为方便起见，编辑桶策略页面会在策略文本字段上方显示当前桶的桶 ARN（Amazon 资源名称）。您可以复制此 ARN，以便在 Amazon 策略生成器页面上的语句中使用。

   c. 添加完语句后，请选择生成策略。

d. 复制生成的策略文本，请选择 Close（关闭），然后返回到 Amazon S3 控制台中的 Edit bucket policy（编辑存储桶策略）页面。

7. 在 Policy（策略）框中，编辑现有策略或从 Amazon 策略生成器粘贴存储桶策略。确保在保存策略之前解决安全警告、错误、一般警告和建议。

> **Note**
>
> 存储桶策略的大小限制为 20 KB。

8. 选择保存更改，此操作将让您返回到权限选项卡。

使用 Amazon SDK

SDK for Java 2.x

Example

PutBucketPolicy Amazon SDK for Java 2.x

```
public static void setBucketPolicy(S3Client s3Client, String bucketName, String
 policyText) {

      //sample policy text
      /**
       * policy_statement = {
        *         'Version': '2012-10-17',
        *         'Statement': [
        *             {
        *                 'Sid': 'AdminPolicy',
        *                 'Effect': 'Allow',
        *                 'Principal': {
        *                     "AWS": "111122223333"
        *                 },
        *                 'Action': 's3express:*',
        *                 'Resource':
 'arn:aws:s3express:region:111122223333:bucket/bucket-base-name--zone-id--x-s3'
        *             }
        *         ]
        *     }
        */
        System.out.println("Setting policy:");
```

```
        System.out.println("----");
        System.out.println(policyText);
        System.out.println("----");
        System.out.format("On Amazon S3 bucket: \"%s\"\n", bucketName);

        try {
            PutBucketPolicyRequest policyReq = PutBucketPolicyRequest.builder()
                    .bucket(bucketName)
                    .policy(policyText)
                    .build();
            s3Client.putBucketPolicy(policyReq);
            System.out.println("Done!");
        }

        catch (S3Exception e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }
```

使用 Amazon CLI

此示例显示如何使用 Amazon CLI 将存储桶策略添加到目录存储桶。要使用该命令，请将####### 替换为您自己的信息。

```
aws s3api put-bucket-policy --bucket bucket-base-name--zone-id--x-s3 --policy file://
bucket_policy.json
```

bucket_policy.json：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AdminPolicy",
            "Effect": "Allow",
            "Principal": {
                "AWS": "111122223333"
            },
            "Action": "s3express*",
```

```
            "Resource": "arn:aws:s3express:us-west-2:111122223333:bucket/amzn-s3-demo-
bucket--usw2-az1--x-s3"
        }
    ]
}
```

有关更多信息，请参阅 Amazon Command Line Interface 中的 put-bucket-policy。

## 查看存储桶策略

要查看目录存储桶的存储桶策略，请使用以下示例。

使用 Amazon CLI

此示例说明如何使用 Amazon CLI 查看附加到目录存储桶的存储桶策略。要使用该命令，请将###### 替换为您自己的信息。

```
aws s3api get-bucket-policy --bucket bucket-base-name--zone-id--x-s3
```

有关更多信息，请参阅 Amazon Command Line Interface 中的 get-bucket-policy。

## 删除存储桶策略

要删除目录存储桶的存储桶策略，请使用以下示例。

使用 Amazon SDK

SDK for Java 2.x

Example

DeleteBucketPolicy Amazon SDK for Java 2.x

```
public static void deleteBucketPolicy(S3Client s3Client, String bucketName) {
      try {
          DeleteBucketPolicyRequest deleteBucketPolicyRequest =
 DeleteBucketPolicyRequest
                  .builder()
                  .bucket(bucketName)
                  .build()
```

```
            s3Client.deleteBucketPolicy(deleteBucketPolicyRequest);
            System.out.println("Successfully deleted bucket policy");
        }

        catch (S3Exception e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
```

使用 Amazon CLI

此示例显示如何使用 Amazon CLI 删除目录存储桶的存储桶策略。要使用该命令，请将*#######* 替换为您自己的信息。

```
aws s3api delete-bucket-policy --bucket bucket-base-name--zone-id--x-s3
```

有关更多信息，请参阅 Amazon Command Line Interface 中的 delete-bucket-policy。

# 清空目录存储桶

您可以使用 Amazon S3 控制台清空 Amazon S3 目录桶。有关目录存储桶的更多信息，请参阅使用目录存储桶。

清空目录存储桶之前，请注意以下几点：

- 清空目录存储桶时，您将删除所有对象，但会保留目录存储桶。
- 清空目录桶后，清空操作无法撤销。
- 当正在执行清空桶操作时添加到目录桶的对象可能被删除。

如果您还要删除桶，请注意以下几点：

- 必须先删除目录存储桶中的所有对象，然后才能删除目录存储桶本身。
- 必须先中止目录存储桶中正在进行的分段上传，然后才能删除存储桶本身。

> **Note**
>
> 通过 Amazon Command Line Interface（CLI）执行的 `s3 rm` 命令、通过 Mountpoint 执行的 `delete` 操作以及通过 Amazon Web Services Management Console执行的清空存

储桶选项按钮无法删除目录存储桶中正在进行的分段上传。要删除这些正在进行的分段上传，请使用 ListMultipartUploads 操作列出存储桶中正在进行的分段上传，然后使用 AbortMultipartUpload 操作中止所有正在进行的分段上传。

要删除目录存储桶，请参阅删除目录存储桶。要中止正在进行的分段上传，请参阅the section called “中止分段上传”。

要清空通用存储桶，请参阅清空通用存储桶。

### 使用 S3 控制台

清空目录桶

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择目录存储桶。
3. 选择您要清空的桶名称旁边的选项按钮，然后选择清空。
4. 在清空存储桶页面上，通过在文本字段中输入 **permanently delete** 来确认要清空存储桶，然后选择清空。
5. 在清空桶：状态页面上监控桶清空过程的进度。

## 删除目录存储桶

您只能删除空的 Amazon S3 目录桶。在删除目录桶之前，必须删除桶中的所有对象并中止所有正在进行的分段上传。

如果目录存储桶已附加到接入点，则必须先删除该接入点。有关更多信息，请参阅 删除目录存储桶的接入点。

要清空目录存储桶，请参阅清空目录存储桶。要中止正在进行的分段上传，请参阅the section called “中止分段上传”。

要删除通用存储桶，请参阅删除通用存储桶。

### 使用 S3 控制台

清空目录桶并中止所有正在进行的分段上传后，您可以删除桶。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择目录存储桶。
3. 在目录桶列表中，选择要删除的桶旁边的选项按钮。
4. 选择删除。
5. 在删除桶页面上，在文本字段中输入桶的名称以确认删除您的桶。

> **Important**
>
> 无法撤消删除目录存储桶的操作。

6. 要删除您的目录存储桶，请选择删除存储桶。

## 使用 Amazon SDK

以下示例使用 Amazon SDK for Java 2.x 和 适用于 Python (Boto3) 的 Amazon SDK 删除目录桶。

SDK for Java 2.x

Example

```
public static void deleteBucket(S3Client s3Client, String bucketName) {

    try {
        DeleteBucketRequest del = DeleteBucketRequest.builder()
                .bucket(bucketName)
                .build();
        s3Client.deleteBucket(del);
        System.out.println("Bucket " + bucketName + " has been deleted");
    }
    catch (S3Exception e) {
        System.err.println(e.awsErrorDetails().errorMessage());
        System.exit(1);
    }
}
```

SDK for Python

Example

```
import logging
import boto3
from botocore.exceptions import ClientError

def delete_bucket(s3_client, bucket_name):
    '''
    Delete a directory bucket in a specified Region

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket to delete; for example, 'doc-example-bucket--usw2-
az1--x-s3'
    :return: True if bucket is deleted, else False
    '''

    try:
        s3_client.delete_bucket(Bucket = bucket_name)
    except ClientError as e:
        logging.error(e)
        return False
    return True

if __name__ == '__main__':
    bucket_name = 'BUCKET_NAME'
    region = 'us-west-2'
    s3_client = boto3.client('s3', region_name = region)
```

## 使用 Amazon CLI

此示例说明如何使用 Amazon CLI 删除目录存储桶。要使用该命令，请将####### 替换为您自己的信息。

```
aws s3api delete-bucket --bucket bucket-base-name--zone-id--x-s3 --region us-west-2
```

有关更多信息，请参阅 Amazon Command Line Interface 中的 delete-bucket。

# 列出目录存储桶

以下示例显示如何使用 Amazon SDK 和 Amazon CLI 列出目录存储桶。

## 使用 Amazon SDK

### SDK for Java 2.x

#### Example

下面的示例通过使用 Amazon SDK for Java 2.x 列出目录桶。

```
public static void listBuckets(S3Client s3Client) {
       try {
           ListDirectoryBucketsRequest listDirectoryBucketsRequest =
ListDirectoryBucketsRequest.builder().build();
           ListDirectoryBucketsResponse response =
s3Client.listDirectoryBuckets(listDirectoryBucketsRequest);
           if (response.hasBuckets()) {
               for (Bucket bucket: response.buckets()) {
                   System.out.println(bucket.name());
                   System.out.println(bucket.creationDate());
               }
           }
       }

       catch (S3Exception e) {
           System.err.println(e.awsErrorDetails().errorMessage());
           System.exit(1);
       }
   }
```

### SDK for Python

#### Example

下面的示例通过使用 适用于 Python (Boto3) 的 Amazon SDK 列出目录桶。

```
import logging
import boto3
from botocore.exceptions import ClientError
```

```
def list_directory_buckets(s3_client):
'''
Prints a list of all directory buckets in a Region

:param s3_client: boto3 S3 client
:return: True if there are buckets in the Region, else False
'''
try:
    response = s3_client.list_directory_buckets()
    for bucket in response['Buckets']:
        print (bucket['Name'])
except ClientError as e:
    logging.error(e)
    return False
return True


if __name__ == '__main__':
    region = 'us-east-1'
    s3_client = boto3.client('s3', region_name = region)
    list_directory_buckets(s3_client)
```

适用于 .NET 的 Amazon SDK

Example

下面的示例通过使用 适用于 .NET 的 Amazon SDK 列出目录桶。

```
var listDirectoryBuckets = await amazonS3Client.ListDirectoryBucketsAsync(new
 ListDirectoryBucketsRequest
{
  MaxDirectoryBuckets = 10
  }).ConfigureAwait(false);
```

SDK for PHP

Example

下面的示例通过使用 适用于 PHP 的 Amazon SDK 列出目录桶。

```
require 'vendor/autoload.php';

$s3Client = new S3Client([
    'region'      => 'us-east-1',
]);
$result = $s3Client->listDirectoryBuckets();
```

SDK for Ruby

Example

下面的示例通过使用 适用于 Ruby 的 Amazon SDK 列出目录桶。

```
s3 = Aws::S3::Client.new(region:'us-west-1')
s3.list_directory_buckets
```

### 使用 Amazon CLI

以下 `list-directory-buckets` 示例命令显示如何使用 Amazon CLI 列出 *us-east-1* 区域中的目录存储桶。要运行此命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3api list-directory-buckets --region us-east-1
```

有关更多信息，请参阅 Amazon CLI 命令参考 中的 list-directory-buckets。

## 确定您是否可以访问目录存储桶

以下 Amazon SDK 示例显示如何使用 `HeadBucket` API 操作来确定 Amazon S3 目录桶是否存在以及您是否有权访问它。

### 使用 Amazon SDK

以下 Amazon SDK for Java 2.x 示例说明如何确定桶是否存在以及您是否有权访问该桶。

SDK for Java 2.x

Example

Amazon SDK for Java 2.x

```
public static void headBucket(S3Client s3Client, String bucketName) {
   try {
        HeadBucketRequest headBucketRequest = HeadBucketRequest
                .builder()
                .bucket(bucketName)
                .build();
        s3Client.headBucket(headBucketRequest);
        System.out.format("Amazon S3 bucket: \"%s\" found.", bucketName);
   }

   catch (S3Exception e) {
       System.err.println(e.awsErrorDetails().errorMessage());
       System.exit(1);
   }
}
```

### 使用 Amazon CLI

以下 head-bucket 示例命令显示了如何使用 Amazon CLI 来确定目录存储桶是否存在以及您是否有权访问该存储桶。要运行此命令，请将用户输入占位符替换为您自己的信息。

```
aws s3api head-bucket --bucket bucket-base-name--zone-id--x-s3
```

有关更多信息，请参阅 Amazon CLI 命令参考 中的 head-bucket。

## 使用目录桶中的对象

创建 Amazon S3 目录桶后，您可以使用 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）和 Amazon SDK 处理对象。

有关在目录存储桶中执行批量操作、导入、上传、复制、删除和下载对象的更多信息，请参阅下面的主题。

主题

- 将对象导入到目录存储桶
- 使用针对目录存储桶的 S3 生命周期

- 对目录存储桶使用批量操作
- 向目录存储桶中的对象追加数据
- 将对象上传到目录存储桶
- 从目录存储桶复制对象或向目录存储桶复制对象
- 删除目录存储桶中的对象
- 下载目录存储桶中的对象
- 生成预签名 URL 以共享对象目录存储桶
- 检索目录存储桶的对象元数据
- 列出目录存储桶中的对象

## 将对象导入到目录存储桶

在 Amazon S3 中创建目录存储桶后，您可以使用导入操作在新的存储桶中填充数据。导入是一种创建 S3 批量操作作业的简化方法，用于将对象从通用存储桶复制到目录存储桶。

> **Note**
>
> 以下限制适用于导入作业：
>
> - 源存储桶和目标存储桶必须位于相同的 Amazon Web Services 区域和账户中。
> - 源存储桶不能是目录存储桶。
> - 不支持大于 5 GB 的对象，复制操作中将省略这些对象。
> - Glacier Flexible Retrieval、Glacier Deep Archive、Intelligent-Tiering 归档访问层和 Intelligent-Tiering 深度归档层存储类中的对象必须先恢复，然后才能导入。
> - 使用 MD5 校验和算法导入的对象将转换为使用 CRC32 校验和。
> - 导入的对象使用 Express One Zone 存储类，其定价结构与通用桶使用的存储类不同。在导入大量对象时，请考虑这种成本差异。

配置导入作业时，您需要指定从中复制现有对象的源存储桶或前缀。您还可以提供一个 Amazon Identity and Access Management（IAM）角色，该角色拥有访问源对象的权限。然后，Amazon S3 会启动批量操作作业，复制对象并自动应用适当的存储类和校验和设置。

要配置导入作业，您可以使用 Amazon S3 控制台。

### 使用 Amazon S3 控制台

将对象导入到目录存储桶

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶，然后选择目录存储桶选项卡。选择要将对象导入到的目录存储桶旁边的选项按钮。
3. 选择导入。
4. 对于源，输入包含要导入的对象的通用存储桶（或包含前缀的存储桶路径）。要从列表中选择现有的通用存储桶，请选择浏览 S3。
5. 要获得访问和复制源对象的权限，请执行以下任一操作来指定具有导入源对象所需权限的 IAM 角色：

   - 要允许 Amazon S3 代表您创建新的 IAM 角色，请选择创建新的 IAM 角色。
   - 要从列表中选择现有 IAM 角色，请选择从现有 IAM 角色中选择。
   - 要通过输入 Amazon 资源名称（ARN）指定现有 IAM 角色，请选择输入 IAM 角色 ARN，然后在相应字段中输入 ARN。
6. 查看目标和复制的对象设置部分中显示的信息。如果目标部分中的信息正确，请选择导入以启动复制作业。

   Amazon S3 控制台在批量操作页面上显示新作业的状态。有关作业的更多信息，请选择作业名称旁边的选项按钮，然后在操作菜单上选择查看详细信息。要打开要导入对象的目录存储桶，请选择查看导入目标。

## 使用针对目录存储桶的 S3 生命周期

S3 生命周期通过代表您删除已过期对象，助力您以更具成本效益的方式在目录存储桶中的 S3 Express One Zone 内存储对象。要管理对象的生命周期，请为目录存储桶创建 S3 生命周期配置。S3 生命周期配置 是一组规则，用于定义 Amazon S3 对一组对象应用的操作。您可以使用 Amazon 命令行界面（Amazon CLI）、Amazon SDK、Amazon S3 REST API 和 Amazon CloudFormation，在目录存储桶上设置 Amazon S3 生命周期配置。

在生命周期配置中，您可以使用规则来定义希望 Amazon S3 在对象上执行的操作。对于存储在目录存储桶中的对象，您可以创建生命周期规则，以便随着对象存在时间的增长而使其过期。您还可以创建生命周期规则，以每天一次的频率删除目录存储桶中未完成的分段上传。

当您向存储桶添加生命周期配置时，配置规则将应用到现有对象以及您在以后添加的对象。例如，如果您在今天添加带有过期操作的生命周期配置规则，而该规则使带有特定前缀的对象在创建 30 天后过期，S3 会将任何超过 30 天且具有指定前缀的现有对象加入移除队列。

## 目录存储桶的 S3 生命周期有何不同

对于目录存储桶中的对象，您可以创建生命周期规则，使对象过期并删除未完成的分段上传。但是，目录存储桶的 S3 生命周期不支持存储类之间的转换操作。

CreateSession

生命周期使用公共 `DeleteObject` 和 `DeleteObjects` API 操作来使目录存储桶中的对象过期。要使用这些 API 操作，S3 生命周期将使用 `CreateSession` API 建立临时安全凭证，以访问目录存储桶中的对象。有关更多信息，请参阅《Amazon S3 API Reference》中的 `CreateSession`。

如果您具有拒绝向生命周期主体授予删除权限的有效策略，这将阻止您允许 S3 生命周期代表您删除对象。

使用存储桶策略向 S3 生命周期服务主体授予权限

以下存储桶策略授予允许使用默认 `ReadWrite` 会话进行 CreateSession 调用的权限，并允许生命周期服务主体。

Example – 允许通过默认 **`ReadWrite`** 会话执行 **`CreateSession`** 调用的存储桶策略

```
{
  "Version":"2008-10-17",
  "Statement":[
     {
        "Effect":"Allow",
        "Principal": {
           "Service":"lifecycle.s3.amazonaws.com"
         },
         "Action":"s3express:CreateSession",
         "Condition": {
            "StringEquals": {
               "s3express:SessionMode": "ReadWrite"
             }
          },
          "Resource":"arn:aws:s3express:us-east-2:412345678921:bucket/amzn-s3-demo-
bucket--use2-az2--x-s3"
       }
```

```
    ]
}
```

监控生命周期规则

对于存储在目录存储桶中的对象，S3 生命周期会生成 Amazon CloudTrail 管理和数据事件日志。有关更多信息，请参阅 S3 Express One Zone 的 CloudTrail 日志文件示例。

有关创建生命周期配置以及排查 S3 生命周期相关问题的更多信息，请参阅以下主题：

主题

- 为目录存储桶创建和管理生命周期配置
- 目录存储桶的 S3 生命周期问题排查

## 为目录存储桶创建和管理生命周期配置

您可以通过使用 Amazon Command Line Interface（Amazon CLI）、Amazon SDK 和 REST API，为目录存储桶创建生命周期配置。

使用 Amazon CLI

您可以使用以下 Amazon CLI 命令管理 S3 生命周期配置：

- `put-bucket-lifecycle-configuration`
- `get-bucket-lifecycle-configuration`
- `delete-bucket-lifecycle`

有关设置 Amazon CLI 的说明，请参阅《Amazon S3 API 参考》中的 Developing with Amazon S3 using the Amazon CLI。

Amazon S3 生命周期配置是一个 XML 文件。但在使用 Amazon CLI 时，您不能指定 XML 格式。您必须改为指定 JSON 格式。以下是您可在 Amazon CLI 命令中指定的示例 XML 生命周期配置和等效 JSON 配置。

以下 Amazon CLI 示例在目录存储桶上放置生命周期配置策略。此策略指定，所有带有标记前缀（myprefix）且符合规定对象大小的对象，将在 7 天后过期。要使用此示例，请将每个*******替换为您自己的信息。

将生命周期配置策略保存到 JSON 文件中。在本示例中，文件命名为 lifecycle1.json。

Example

JSON

```
{
    "Rules": [
        {
        "Expiration": {
            "Days": 7
        },
        "ID": "Lifecycle expiration rule",
        "Filter": {
            "And": {
                "Prefix": "myprefix/",
                "ObjectSizeGreaterThan": 500,
                "ObjectSizeLessThan": 64000
            }
        },
        "Status": "Enabled"
    }
    ]
}
```

将 JSON 文件作为put-bucket-lifecycle-configuration CLI 命令的一部分提交。要使用此命令，请将每个*#######*替换为您自己的信息。

```
aws s3api put-bucket-lifecycle-configuration --region us-west-2 --profile default
 --bucket amzn-s3-demo-bucket--usw2-az1--x-s3 --lifecycle-configuration file://lc-
policy.json --checksum-algorithm crc32c
```

Example

XML

```
<LifecycleConfiguration>
    <Rule>
        <ID>Lifecycle expiration rule</ID>
        <Filter>
            <And>
                <Prefix>myprefix/</Prefix>
                <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
```

```
                <ObjectSizeLessThan>64000</ObjectSizeLessThan>
            </And>
        </Filter>
        <Status>Enabled</Status>
        <Expiration>
             <Days>7</Days>
        </Expiration>
    </Rule>
</LifecycleConfiguration>
```

## 使用 Amazon SDK

### SDK for Java

#### Example

```
import
 software.amazon.awssdk.services.s3.model.PutBucketLifecycleConfigurationRequest;
import
 software.amazon.awssdk.services.s3.model.PutBucketLifecycleConfigurationResponse;
import software.amazon.awssdk.services.s3.model.ChecksumAlgorithm;
import software.amazon.awssdk.services.s3.model.BucketLifecycleConfiguration;
import software.amazon.awssdk.services.s3.model.LifecycleRule;
import software.amazon.awssdk.services.s3.model.LifecycleRuleFilter;
import software.amazon.awssdk.services.s3.model.LifecycleExpiration;
import software.amazon.awssdk.services.s3.model.LifecycleRuleAndOperator;
import
 software.amazon.awssdk.services.s3.model.GetBucketLifecycleConfigurationResponse;
import
 software.amazon.awssdk.services.s3.model.GetBucketLifecycleConfigurationRequest;
import software.amazon.awssdk.services.s3.model.DeleteBucketLifecycleRequest;
import software.amazon.awssdk.services.s3.model.DeleteBucketLifecycleResponse;
import software.amazon.awssdk.services.s3.model.AbortIncompleteMultipartUpload;

// PUT a Lifecycle policy
LifecycleRuleFilter objectExpirationFilter =
 LifecycleRuleFilter.builder().and(LifecycleRuleAndOperator.builder().prefix("dir1/").object
LifecycleRuleFilter mpuExpirationFilter =
 LifecycleRuleFilter.builder().prefix("dir2/").build();

LifecycleRule objectExpirationRule =
 LifecycleRule.builder().id("lc").filter(objectExpirationFilter).status("Enabled").expiratio
                    .days(10)
```

```
                    .build())
                .build();
LifecycleRule mpuExpirationRule = LifecycleRule.builder().id("lc-
mpu").filter(mpuExpirationFilter).status("Enabled").abortIncompleteMultipartUpload(AbortInco
                        .daysAfterInitiation(10)
                        .build())
                .build();

PutBucketLifecycleConfigurationRequest putLifecycleRequest =
 PutBucketLifecycleConfigurationRequest.builder()
                .bucket("amzn-s3-demo-bucket--usw2-az1--x-s3")
                .checksumAlgorithm(ChecksumAlgorithm.CRC32)
                .lifecycleConfiguration(
                        BucketLifecycleConfiguration.builder()
                                .rules(objectExpirationRule, mpuExpirationRule)
                                .build()
                ).build();

PutBucketLifecycleConfigurationResponse resp =
 client.putBucketLifecycleConfiguration(putLifecycleRequest);

// GET the Lifecycle policy
GetBucketLifecycleConfigurationResponse getResp =
 client.getBucketLifecycleConfiguration(GetBucketLifecycleConfigurationRequest.builder().buc
s3-demo-bucket--usw2-az1--x-s3").build());

// DELETE the Lifecycle policy
DeleteBucketLifecycleResponse delResp =
 client.deleteBucketLifecycle(DeleteBucketLifecycleRequest.builder().bucket("amzn-
s3-demo-bucket--usw2-az1--x-s3").build());
```

### SDK for Go

#### Example

```
package main

import (
    "context"
    "log"

    "github.com/aws/aws-sdk-go-v2/aws"
    "github.com/aws/aws-sdk-go-v2/config"
    "github.com/aws/aws-sdk-go-v2/service/s3"
```

```
    "github.com/aws/aws-sdk-go-v2/service/s3/types"
)
// PUT a Lifecycle policy
func putBucketLifecycleConfiguration(client *s3.Client, bucketName string ) error {
    lifecycleConfig := &s3.PutBucketLifecycleConfigurationInput{
        Bucket: aws.String(bucketName),
        LifecycleConfiguration: &types.BucketLifecycleConfiguration{
            Rules: []types.LifecycleRule{
                {
                    ID:     aws.String("lc"),
                    Filter: &types.LifecycleRuleFilter{
                        And: &types.LifecycleRuleAndOperator{
                            Prefix: aws.String("foo/"),
                            ObjectSizeGreaterThan: aws.Int64(1000000),
                            ObjectSizeLessThan:    aws.Int64(100000000),
                            },
                        },

                    Status: types.ExpirationStatusEnabled,
                    Expiration: &types.LifecycleExpiration{
                        Days: aws.Int32(int32(1)),
                    },
                },
                {
                    ID:     aws.String("abortmpu"),
                    Filter: &types.LifecycleRuleFilter{
                        Prefix: aws.String("bar/"),
                    },
                    Status: types.ExpirationStatusEnabled,
                    AbortIncompleteMultipartUpload:
 &types.AbortIncompleteMultipartUpload{
                        DaysAfterInitiation: aws.Int32(int32(5)),
                    },
                },
            },
        },
    }
    _, err := client.PutBucketLifecycleConfiguration(context.Background(),
 lifecycleConfig)
    return err
}
// Get the Lifecycle policy
func getBucketLifecycleConfiguration(client *s3.Client, bucketName string) error {
    getLifecycleConfig := &s3.GetBucketLifecycleConfigurationInput{
```

```
        Bucket: aws.String(bucketName),
    }

    resp, err := client.GetBucketLifecycleConfiguration(context.Background(),
 getLifecycleConfig)
    if err != nil {
        return err
    }
    return nil
}
// Delete the Lifecycle policy
func deleteBucketLifecycleConfiguration(client *s3.Client, bucketName string) error
 {
    deleteLifecycleConfig := &s3.DeleteBucketLifecycleInput{
        Bucket: aws.String(bucketName),
    }
    _, err := client.DeleteBucketLifecycle(context.Background(),
 deleteLifecycleConfig)
    return err
}
func main() {
    cfg, err := config.LoadDefaultConfig(context.Background(),
 config.WithRegion("us-west-2")) // Specify your region here
    if err != nil {
        log.Fatalf("unable to load SDK config, %v", err)
    }
    s3Client := s3.NewFromConfig(cfg)
    bucketName := "amzn-s3-demo-bucket--usw2-az1--x-s3"
    putBucketLifecycleConfiguration(s3Client, bucketName)
    getBucketLifecycleConfiguration(s3Client, bucketName)
    deleteBucketLifecycleConfiguration(s3Client, bucketName)
    getBucketLifecycleConfiguration(s3Client, bucketName)
}
```

SDK for .NET

Example

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.Threading.Tasks;
```

```
namespace Amazon.DocSamples.S3
{
    class LifecycleTest
    {
        private const string bucketName = "amzn-s3-demo-bucket--usw2-az1--x-s3";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;
        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            AddUpdateDeleteLifecycleConfigAsync().Wait();
        }

        private static async Task AddUpdateDeleteLifecycleConfigAsync()
        {
            try
            {
                var lifeCycleConfiguration = new LifecycleConfiguration()
                {
                    Rules = new List <LifecycleRule>
                        {
                            new LifecycleRule
                            {
                                 Id = "delete rule",
                                  Filter = new LifecycleFilter()
                                 {
                                     LifecycleFilterPredicate = new
 LifecyclePrefixPredicate()
                                     {
                                         Prefix = "projectdocs/"
                                     }
                                 },
                                 Status = LifecycleRuleStatus.Enabled,
                                 Expiration = new LifecycleRuleExpiration()
                                 {
                                       Days = 10
                                 }
                            }
                        }
                };
```

```
                // Add the configuration to the bucket.
                await AddExampleLifecycleConfigAsync(client,
lifeCycleConfiguration);

                // Retrieve an existing configuration.
                lifeCycleConfiguration = await RetrieveLifecycleConfigAsync(client);

                // Add a new rule.
                lifeCycleConfiguration.Rules.Add(new LifecycleRule
                {
                    Id = "mpu abort rule",
                    Filter = new LifecycleFilter()
                    {
                        LifecycleFilterPredicate = new LifecyclePrefixPredicate()
                        {
                            Prefix = "YearlyDocuments/"
                        }
                    },
                    Expiration = new LifecycleRuleExpiration()
                    {
                        Days = 10
                    },
                    AbortIncompleteMultipartUpload = new
LifecycleRuleAbortIncompleteMultipartUpload()
                    {
                        DaysAfterInitiation = 10
                    }
                });

                // Add the configuration to the bucket.
                await AddExampleLifecycleConfigAsync(client,
lifeCycleConfiguration);

                // Verify that there are now two rules.
                lifeCycleConfiguration = await RetrieveLifecycleConfigAsync(client);
                Console.WriteLine("Expected # of rulest=2; found:{0}",
lifeCycleConfiguration.Rules.Count);

                // Delete the configuration.
                await RemoveLifecycleConfigAsync(client);

                // Retrieve a nonexistent configuration.
                lifeCycleConfiguration = await RetrieveLifecycleConfigAsync(client);
```

```
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered ***. Message:'{0}' when writing
an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
        }

        static async Task AddExampleLifecycleConfigAsync(IAmazonS3 client,
LifecycleConfiguration configuration)
        {

            PutLifecycleConfigurationRequest request = new
PutLifecycleConfigurationRequest
            {
                BucketName = bucketName,
                Configuration = configuration
            };
            var response = await client.PutLifecycleConfigurationAsync(request);
        }

        static async Task <LifecycleConfiguration>
RetrieveLifecycleConfigAsync(IAmazonS3 client)
        {
            GetLifecycleConfigurationRequest request = new
GetLifecycleConfigurationRequest
            {
                BucketName = bucketName
            };
            var response = await client.GetLifecycleConfigurationAsync(request);
            var configuration = response.Configuration;
            return configuration;
        }

        static async Task RemoveLifecycleConfigAsync(IAmazonS3 client)
        {
            DeleteLifecycleConfigurationRequest request = new
DeleteLifecycleConfigurationRequest
            {
```

```
                BucketName = bucketName
            };
            await client.DeleteLifecycleConfigurationAsync(request);
        }
    }
}
```

SDK for Python

Example

```
import boto3

client = boto3.client("s3", region_name="us-west-2")
bucket_name = 'amzn-s3-demo-bucket--usw2-az1--x-s3'

client.put_bucket_lifecycle_configuration(
    Bucket=bucket_name,
    ChecksumAlgorithm='CRC32',
    LifecycleConfiguration={
        'Rules': [
            {
                'ID': 'lc',
                'Filter': {
                    'And': {
                        'Prefix': 'foo/',
                        'ObjectSizeGreaterThan': 1000000,
                        'ObjectSizeLessThan': 100000000,
                    }
                },
                'Status': 'Enabled',
                'Expiration': {
                    'Days': 1
                }
            },
            {
                'ID': 'abortmpu',
                'Filter': {
                    'Prefix': 'bar/'
                },
                'Status': 'Enabled',
                'AbortIncompleteMultipartUpload': {
                    'DaysAfterInitiation': 5
```

```
                }
            }
        ]
    }
)

result = client.get_bucket_lifecycle_configuration(
    Bucket=bucket_name
)

client.delete_bucket_lifecycle(
    Bucket=bucket_name
)
```

## 目录存储桶的 S3 生命周期问题排查

主题

- 我设置了生命周期配置，但是我的目录存储桶中的对象没有过期
- 如何监控生命周期规则执行的操作？

我设置了生命周期配置，但是我的目录存储桶中的对象没有过期

针对目录存储桶的 S3 生命周期利用公共 API 来删除 S3 Express One Zone 中的对象。要使用对象级公共 API，您必须授予 `CreateSession` 权限并允许 S3 生命周期删除您的对象。如果您具有拒绝执行删除的有效策略，这将阻止您允许 S3 生命周期代表您删除对象。

请务必正确配置存储桶策略，以确保要删除的对象符合过期条件。您可以在 Amazon CloudTrail 日志中查看 CloudTrail 中是否针对 `CreateSession` API 调用的 `AccessDenied` 跟踪，以验证访问是否被拒绝。查看 CloudTrail 日志有助于您排查访问问题，并确定访问遭拒绝错误的根本原因。然后，您可以通过更新相关策略来修复错误的访问控制。

如果您确认存储桶策略设置正确，但仍遇到问题，我们建议您查看生命周期规则，确保它们适用于正确的对象子集。

如何监控生命周期规则执行的操作？

您可以使用 Amazon CloudTrail 数据事件日志，来监控 S3 生命周期在目录存储桶中执行的操作。有关更多信息，请参阅 CloudTrail 日志文件示例。

# 对目录存储桶使用批量操作

您可以使用 Amazon S3 批量操作对存储在 S3 存储桶中的对象执行操作。要了解有关 S3 批量操作的更多信息，请参阅对 Amazon S3 对象执行大规模批量操作。

以下主题讨论对存储在目录桶的 S3 Express One Zone 存储类中的对象执行批量操作。

主题


- 对目录存储桶使用批量操作
- 主要区别


## 对目录存储桶使用批量操作

您可以对存储在目录桶中的对象执行复制操作和调用 Amazon Lambda 函数操作。通过复制，您可以在相同类型的桶之间复制对象（例如，从目录桶复制到目录桶）。您也可以在通用存储桶和目录存储桶之间进行复制。通过调用 Amazon Lambda 函数操作，您可以通过 Lambda 函数使用您定义的代码对目录存储桶中的对象执行操作。

复制对象

您可以在相同的存储桶类型之间进行复制，也可以在目录存储桶和通用存储桶之间进行复制。当您复制到目录桶时，必须为此桶类型使用正确的 Amazon 资源名称（ARN）格式。目录存储桶的 ARN 格式为 `arn:aws:s3express:region:account-id:bucket/bucket-base-name--x-s3`。

> **Note**
>
> 当源存储桶或目标存储桶位于 Amazon 本地区域时，不支持跨不同 Amazon Web Services 区域复制对象。源存储桶和目标存储桶必须具有相同的父 Amazon Web Services 区域。源存储桶和目标存储桶可以是不同的存储桶位置类型（可用区或本地区域）。

您也可以使用 S3 控制台中的导入操作在目录存储桶中填充数据。导入是一种创建批量操作作业的简化方法，用于将对象从通用存储桶复制到目录存储桶。对于从通用存储桶到目录存储桶的导入复制作业，S3 会自动生成清单。有关更多信息，请参阅将对象导入到目录桶和指定清单。

调用 Lambda 函数（**`LambdaInvoke`**）

使用批量操作来调用处理目录存储桶的 Lambda 函数有特殊要求。例如，您必须使用 v2 JSON 调用架构来构建 Lambda 请求，并在创建任务时指定 InvocationSchemaVersion 2.0。有关更多信息，请参阅调用 Amazon Lambda 函数。

## 主要区别

下面列出了使用批量操作对存储在目录桶（使用 S3 Express One Zone 存储类）中的对象执行批量操作时的主要区别：

- 对于目录存储桶，支持 SSE-S3 和具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）。如果您发出 `CopyObject` 请求来指定在目录存储桶（源或目标）上使用具有客户提供的密钥的服务器端加密（SSE-C），则响应将返回 HTTP `400 (Bad Request)` 错误。

  我们建议存储桶的默认加密使用所需的加密配置，并且不要在 `CreateSession` 请求或 PUT 对象请求中覆盖存储桶默认加密。然后，使用所需的加密设置自动对新对象进行加密。有关目录存储桶中的加密覆盖行为以及如何使用 SSE-KMS 加密目录存储桶中的新对象副本的更多信息，请参阅 Specifying server-side encryption with Amazon KMS for new object uploads。

  当您通过批量操作中的 Copy 操作将 SSE-KMS 加密的对象从通用存储桶复制到目录存储桶、从目录存储桶复制到通用存储桶，或在目录存储桶之间复制时，不支持 S3 存储桶密钥。在这种情况下，每次对 KMS 加密的对象发出复制请求时，Amazon S3 都会调用 Amazon KMS。有关在目录存储桶上使用 SSE-KMS 的更多信息，请参阅设置和监控目录存储桶的默认加密和在目录存储桶中使用具有 Amazon KMS 密钥的服务器端加密（SSE-KMS）。
- 无法标记目录存储桶中的对象。您只能指定一个空标签集。默认情况下，批量操作会复制标签。如果您在通用桶和目录桶之间复制带有标签的对象，则将收到 `501 (Not Implemented)` 响应。
- S3 Express One Zone 可让您选择用于在上传或下载过程中验证数据的校验和算法。您可以选择以下安全哈希算法（SHA）或循环冗余校验（CRC）数据完整性检查算法之一：CRC32、CRC32、SHA-1 和 SHA-256。S3 Express One Zone 存储类不支持基于 MD5 的校验和。
- 默认情况下，所有 Amazon S3 桶都将 S3 对象所有权设置设为强制桶拥有者，并禁用访问控制列表（ACL）。对于目录存储桶，无法修改此设置。您可以将对象从通用存储桶复制到目录存储桶。然而，当您复制到目录桶或从目录桶复制时，无法覆盖默认 ACL。
- 无论您如何指定清单，列表本身都必须存储在通用存储桶中。批量操作无法从目录桶中导入现有清单，也无法将生成的清单保存到目录桶。但是，清单中描述的对象可以存储在目录存储桶中。
- 批量操作无法将目录桶指定为 S3 清单报告中的位置。清单报告不支持目录桶。您可以使用 `ListObjectsV2` API 操作列出对象，为目录桶中的对象创建清单文件。然后，您可以在 CSV 文件中插入该列表。

授予访问权限

要执行复制作业，您必须拥有以下权限：

- 要将对象从一个目录存储桶复制到另一个目录存储桶，您必须拥有 `s3express:CreateSession` 权限。
- 要将对象从目录存储桶复制到通用存储桶，您必须拥有将对象副本写入目标存储桶的 `s3express:CreateSession` 权限和 `s3:PutObject` 权限。
- 要将对象从通用桶复制到目录桶，您必须拥有读取正在复制的源对象的 `s3express:CreateSession` 权限和 `s3:GetObject` 权限。

  有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 CopyObject。
- 要调用 Lambda 函数，您必须根据 Lambda 函数授予对资源的权限。要确定需要哪些权限，请检查相应的 API 操作。

## 向目录存储桶中的对象追加数据

您可以将数据添加到存储在目录存储桶内 S3 Express One Zone 存储类中的现有对象的末尾。如果数据是在一段时间内连续写入的，或者如果您需要在写入对象的同时读取该对象，我们建议您使用向对象追加数据的功能。向对象追加数据对于一些应用场景很常见，例如，向日志文件添加新的日志条目，或在视频文件转码并流式传输时向其中添加新的视频片段等。通过向对象追加数据，您可以简化之前需要先在本地存储中合并数据然后再将最终对象复制到 Amazon S3 的应用程序。

可以追加到对象的数据没有最小大小要求。但是，您可以在单个请求中追加到对象的最大数据大小为 5 GB。这与使用任何 Amazon S3 API 上传数据时的最大请求大小限制相同。

每次成功的追加操作都将创建对象的一部分，每个对象最多可以有 10000 个部分。这意味着您最多可以向对象追加数据 10000 次。如果使用 S3 分段上传创建对象，那么每个上传的部分都会计入总计最多 10000 个部分的限制中。例如，对于通过分段上传创建的包含 1000 个部分的对象，您最多可以追加 9000 次。

> **Note**
>
> 如果达到部分的限制数，您将收到 TooManyParts 错误。您可以使用 `CopyObject` API 来重置计数。

如果您想将分段并行上传至对象，并且无需在上传分段时读取分段，我们建议您使用 Amazon S3 分段上传。有关更多信息，请参阅使用分段上传。

仅支持向存储在 S3 Express One Zone 存储类中的目录存储桶内的对象追加数据。有关 S3 Express One Zone 的更多信息，请参阅开始使用 S3 Express One Zone。

要开始向目录存储桶中的对象追加数据，您可以使用 Amazon SDK、Amazon CLI 和 `PutObject` API。当您发出 `PutObject` 请求时，您可以将 `x-amz-write-offset-bytes` 标头设置为要追加到的对象的大小。要使用 `PutObject` API 操作，您必须使用 `CreateSession` API 建立临时安全凭证，才能访问目录存储桶中的对象。有关更多信息，请参阅《Amazon S3 API Reference》中的 `PutObject` 和 `CreateSession`。

每次成功的追加操作都会按 `PutObject` 请求计费。要了解有关定价的更多信息，请参阅 `Amazon S3 pricing`。

> **Note**
>
> 从 1.12 版起，适用于 Amazon S3 的 Mountpoint 支持向存储在 S3 Express One Zone 中的对象追加数据。要开始使用，您必须通过设置 `--incremental-upload` 标志来选择启用该功能。有关 Mountpoint 的更多信息，请参阅使用 Mountpoint。

如果您在上传追加的数据时使用 CRC（循环冗余校验）算法，则可以使用 `HeadObject` 或 `GetObject` 请求来检索基于 CRC 的完整对象校验和。如果您在上传追加的数据时使用 SHA-1 或 SHA-256 算法，则可以检索追加部分的校验和，并使用之前的 PutObject 响应中返回的 SHA 校验和来验证其完整性。有关更多信息，请参阅数据保护和加密。

## 使用 Amazon CLI、Amazon SDK 和 REST API 向对象追加数据

您可以使用 Amazon Command Line Interface（Amazon CLI）、Amazon SDK 和 REST API 将数据追加到您的对象中。

使用 Amazon CLI

以下 `put-object` 示例命令演示了如何使用 Amazon CLI 将数据追加到对象。要运行此命令，请将*########*替换为您自己的信息。

```
aws s3api put-object --bucket amzn-s3-demo-bucket--azid--x-s3 --key sampleinput/
file001.bin --body bucket-seed/file001.bin --write-offset-bytes size-of-sampleinput/
file001.bin
```

使用 Amazon SDK

SDK for Java

您可以使用 适用于 Java 的 Amazon SDK 将数据追加到您的对象。

```
var putObjectRequestBuilder = PutObjectRequest.builder()
                                              .key(key)
                                              .bucket(bucketName)
                                              .writeOffsetBytes(9);
var response = s3Client.putObject(putObjectRequestBuilder.build());
```

SDK for Python

```
s3.put_object(Bucket='amzn-s3-demo-bucket--use2-az2--x-s3', Key='2024-11-05-sdk-
test', Body=b'123456789', WriteOffsetBytes=9)
```

使用 REST API

您可以发送 REST 请求来将数据追加到对象。有关更多信息，请参阅 PutObject。

## 将对象上传到目录存储桶

创建 Amazon S3 目录桶后，可以将对象上传到该桶。以下示例显示如何使用 S3 控制台和 Amazon SDK 将对象上传到目录桶。有关使用 S3 Express One Zone 进行批量上传对象操作的信息，请参阅对象管理。

使用 S3 控制台

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择目录存储桶。
3. 选择要将文件夹或文件上传到的桶的名称。
4. 在对象列表中，选择上传。
5. 在上传页面上，执行以下操作之一：
   - 将文件和文件夹拖放到虚线上传区域。
   - 选择添加文件或添加文件夹，选择要上传的文件或文件夹，然后选择打开或上传。

6. 在校验和下，选择要使用的校验和函数。

   （可选）如果您要上传大小不到 16MB 的单个对象，也可以指定预先计算的校验和值。当您提供预先计算的值时，Amazon S3 会将该值与它使用所选校验和函数计算的值进行比较。如果值不匹配，则上传不会开始。

7. 权限和属性部分中的选项会自动设置为默认设置，无法修改。将自动启用“屏蔽公共访问权限”，而无法为目录桶启用 S3 版本控制和 S3 对象锁定。

   （可选）如果要以键值对的形式向对象添加元数据，请展开属性部分，然后在元数据部分中选择添加元数据。

8. 要上传列出的文件和文件夹，请选择上传。

   Amazon S3 会上传您的对象和文件夹。上传完成后，您可以在上传：状态页面上看到成功消息。

使用 Amazon SDK

SDK for Java 2.x

Example

```
public static void putObject(S3Client s3Client, String bucketName, String objectKey,
 Path filePath) {
       //Using File Path to avoid loading the whole file into memory
       try {
           PutObjectRequest putObj = PutObjectRequest.builder()
                   .bucket(bucketName)
                   .key(objectKey)
                   //.metadata(metadata)
                   .build();
           s3Client.putObject(putObj, filePath);
           System.out.println("Successfully placed " + objectKey +" into bucket
 "+bucketName);

       }

       catch (S3Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
       }
}
```

SDK for Python

Example

```
import boto3
import botocore
from botocore.exceptions import ClientError


def put_object(s3_client, bucket_name, key_name, object_bytes):
    """
    Upload data to a directory bucket.
    :param s3_client: The boto3 S3 client
    :param bucket_name: The bucket that will contain the object
    :param key_name: The key of the object to be uploaded
    :param object_bytes: The data to upload
    """
    try:
        response = s3_client.put_object(Bucket=bucket_name, Key=key_name,
                                Body=object_bytes)
        print(f"Upload object '{key_name}' to bucket '{bucket_name}'.")
        return response
    except ClientError:
        print(f"Couldn't upload object '{key_name}' to bucket '{bucket_name}'.")
        raise

def main():
    # Share the client session with functions and objects to benefit from S3 Express
 One Zone auth key
    s3_client = boto3.client('s3')
    # Directory bucket name must end with --zone-id--x-s3
    resp = put_object(s3_client, 'doc-bucket-example--use1-az5--x-s3', 'sample.txt',
 b'Hello, World!')
    print(resp)

if __name__ == "__main__":
    main()
```

使用 Amazon CLI

以下 put-object 示例命令显示如何使用 Amazon CLI 从 Amazon S3 上传对象。要运行此命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3api put-object --bucket bucket-base-name--zone-id--x-s3 --key sampleinut/
file001.bin --body bucket-seed/file001.bin
```

有关更多信息，请参阅 Amazon CLI 命令参考 中的 put-object。

主题

- 对目录桶使用分段上传

## 对目录桶使用分段上传

您可以使用分段上传过程将单个对象作为一组分段上传。每个分段都是对象数据的连续部分。您可以独立上传以及按任意顺序上传这些对象分段。如果任意分段传输失败，可以重新传输该分段且不会影响其他分段。上传完所有的对象分段后，Amazon S3 将汇集这些分段并创建对象。一般而言，如果您的对象大小达到了 100 MB，您应该考虑使用分段上传，而不是在单个操作中上传对象。

使用分段上传可提供以下优势：

- 提高吞吐量 – 您可以并行上传分段以提高吞吐量。
- 从任何网络问题中快速恢复 – 较小的分段大小可以将由于网络错误而重启失败的上传所产生的影响降至最低。
- 暂停和恢复对象上传 – 您可以在一段时间内逐步上传对象分段。启动分段上传后，没有过期日期。您必须显式完成或中止分段上传。
- 在您知道对象的最终大小前开始上传 – 您可以在创建对象时将其上传。

我们建议您按以下方式使用分段上传：

- 如果您在稳定的高带宽网络上传大型对象，请通过并行分段上传对象实现多线程性能，从而使用分段上传来充分利用您的可用带宽。
- 如果您在不稳定的网络中上传对象，请使用分段上传来提高应对网络错误的弹性，避免重启上传。在使用分段上传时，您只需重新尝试上传在上传期间中断的分段即可。而无需从头重新开始上传对象。

当您使用分段上传将对象上传到目录桶中的 Amazon S3 Express One Zone 存储类时，分段上传过程与使用分段上传将对象上传到通用桶的过程类似。但是，二者之间仍存在一些显著区别。

有关使用分段上传将对象上传到 S3 Express One Zone 的更多信息，请参阅以下主题。

主题

- 分段上传过程
- 使用分段上传操作的校验和
- 并发分段上传操作
- 分段上传和定价
- 分段上传 API 操作和权限
- 示例


### 分段上传过程

分段上传的过程包括三个步骤：

- 启动上传。
- 上传对象分段。
- 上传完所有分段后，即完成分段上传。

在收到完成分段上传请求后，Amazon S3 会利用上传的分段构造对象，然后您可以像在您的桶中访问任何其它对象一样访问该对象。

#### 分段上传开始

当您发送请求以开始分段上传时，Amazon S3 将返回具有上传 ID 的响应，此 ID 是分段上传的唯一标识符。无论您何时上传分段、列出分段、完成上传或中止上传，您都必须包括此上传 ID。

#### 分段上传

上传分段时，除了指定上传 ID，还必须指定分段编号。在 S3 Express One Zone 中使用分段上传时，分段编号必须是连续的编号。如果您尝试使用非连续分段编号完成分段上传请求，则会生成 HTTP `400 Bad Request`（分段顺序无效）错误。

分段编号在您正在上传的对象中唯一地识别分段及其位置。如果您使用之前上传的分段的同一分段编号上传新分段，则之前上传的分段将被覆盖。

无论您何时上传分段，Amazon S3 都将在其响应中返回实体标签 (ETag) 标头。对于每个分段上传，您必须记录分段编号和 ETag 值。所有对象分段上传的 ETag 值将保持不变，但将为每个分段分配不同的分段编号。您必须在随后的请求中包括这些值以完成分段上传。

Amazon S3 会自动加密上传到 S3 存储桶的所有新对象。在进行分段上传时，如果您未在请求中指定加密信息，则已上传分段的加密设置将设为目标存储桶的默认加密配置。Amazon S3 存储桶的默认加

密配置始终处于启用状态，并至少设置为使用 Amazon S3 托管密钥的服务器端加密（SSE-S3）。对于目录存储桶，支持 SSE-S3 和具有 Amazon KMS 密钥的服务器端加密（SSE-KMS）。有关更多信息，请参阅 数据保护和加密。

分段上传完成

完成分段上传时，Amazon S3 会按分段编号的升序将各个分段连接起来，从而创建对象。成功完成请求后，分段将不再存在。

完成分段上传请求必须包括上传 ID 以及分段编号及其相应的 ETag 值的列表。Amazon S3 响应包括可唯一地识别组合对象数据的 ETag。此 ETag 并非对象数据的 MD5 哈希。

分段上传列表

您可以列出特定分段上传或所有正在进行的分段上传的分段。列出分段操作将返回您已为特定分段上传而上传的分段信息。对于每个列出分段请求，Amazon S3 将返回有关特定分段上传的分段信息，最多为 1000 个分段。如果分段上传中的分段超过 1000 个，则必须使用分页来检索所有分段。

返回的分段列表不包括未完成上传的分段。使用列出分段上传操作，您可以获得正在进行的分段上传的列表。

正在进行的分段上传是已开始但还未完成或中止的上传。每个请求将返回最多 1000 个分段上传。如果正在进行的分段上传超过 1000 个，您必须发送其他请求才能检索剩余的分段上传。仅使用返回的列表进行验证。发送完成分段上传 请求时，请勿使用此列表的结果。相反，当上传分段和 Amazon S3 返回的相应 ETag 值时，请保留您自己的指定分段编号的列表。

有关分段上传列表的更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 ListParts。

使用分段上传操作的校验和

上传对象时，可指定校验和算法来检查对象的完整性。目录存储桶不支持 MD5。您可以指定以下安全哈希算法（SHA）或循环冗余校验（CRC）数据完整性检查算法之一：

- CRC32
- CRC32C
- SHA-1
- SHA-256

您可以使用 Amazon S3 REST API 或 Amazon SDK，通过 `GetObject` 或 `HeadObject` 来检索个别分段的校验和值。如果您想检索仍在进行的分段上传的各个分段的校验和值，可以使用 `ListParts`。

> **Important**
>
> 在使用前面的校验和算法时，分段编号必须是连续的编号。如果您尝试使用非连续分段编号完成分段上传请求，Amazon S3 会生成 `HTTP 400 Bad Request`（分段顺序无效）错误。

有关校验和如何处理分段上传对象的更多信息，请参阅在 Amazon S3 中检查对象完整性。

### 并发分段上传操作

在分布式开发环境中，您的应用程序可以同时在同一对象上启动多个更新。例如，您的应用程序可能会使用同一对象键启动多个分段上传。然后，对于其中每个上传，您的应用程序可以上传分段并将完成上传请求发送到 Amazon S3，以创建对象。对于 S3 Express One Zone，对象创建时间是分段上传的完成日期。

> **Important**
>
> 对于存储在目录桶中的对象，不支持版本控制。

### 分段上传和定价

开始分段上传后，Amazon S3 将保留所有分段，直到您完成或中止上传。在整个其生命周期内，您将支付有关此分段上传及其关联分段的所有存储、带宽和请求的费用。如果您中止分段上传，Amazon S3 将删除上传构件和已上传的任何分段，您将不再为它们支付费用。无论指定的存储类如何，删除未完成的分段上传均不收取提前删除费用。有关定价的更多信息，请参阅 Amazon S3 定价。

> **Important**
>
> 如果未成功发送完成分段上传请求，则不会汇集对象分段且不会创建对象。您需要为与上传的分段关联的所有存储付费。完成分段上传来创建对象，或者中止分段上传来移除任何已上传的分段非常重要。
>
> 在可删除目录桶之前，必须完成或中止所有正在进行的分段上传。目录桶不支持 S3 生命周期配置。如果需要，您可以列出正在进行的分段上传，然后中止上传并删除桶。

### 分段上传 API 操作和权限

要允许访问目录桶上的对象管理 API 操作，您需要在桶策略或基于 Amazon Identity and Access Management（IAM）身份的策略中授予 `s3express:CreateSession` 权限。

您必须具有使用分段上传操作的所需权限。您可以使用桶策略或基于 IAM 身份的策略向 IAM 主体授予执行这些操作的权限。下表列出了各种分段上传操作所需的权限。

您可以通过 `Initiator` 元素识别分段上传的发起者。如果发起者是 Amazon Web Services 账户，此元素将提供与 `Owner` 元素相同的信息。如果发起者是 IAM 用户，此元素将提供用户 ARN 和显示名称。

| 操作 | 所需的权限 |
| --- | --- |
| 创建分段上传 | 要创建分段上传，您必须得到可以对目录桶执行 `s3express:CreateSession` 操作的许可。 |
| 启动分段上传 | 要启动分段上传，您必须得到可以对目录桶执行 `s3express:CreateSession` 操作的许可。 |
| 上传分段 | 要上传分段，您必须得到可以对目录桶执行 `s3express:CreateSession` 操作的许可。<br><br>要使发起者能够上传分段，桶拥有者必须允许发起者对目录桶执行 `s3express:CreateSession` 操作。 |
| 上传分段（复制） | 要上传分段，您必须得到可以对目录桶执行 `s3express:CreateSession` 操作的许可。<br><br>存储桶拥有者必须允许发起者对对象执行 `s3express:CreateSession` 操作，发起者才能上传该对象的分段。 |
| 完成分段上传 | 要完成分段上传，您必须得到可以对目录桶执行 `s3express:CreateSession` 操作的许可。<br><br>要使发起者能够完成分段上传，桶拥有者必须允许发起者对于对象执行 `s3express:CreateSession` 操作。 |
| 中止分段上传 | 要中止分段上传，您必须得到可以执行 `s3express:CreateSession` 操作的许可。<br><br>要使发起者能够中止分段上传，必须向发起者授予执行 `s3express:CreateSession` 操作的显式允许访问权限。 |

| 操作 | 所需的权限 |
| --- | --- |
| 列出分段 | 要列出分段上传中的分段，您必须得到可以对目录桶执行 `s3express:CreateSession` 操作的许可。 |
| 列出正在进行的分段上传 | 要列出正在上传到桶的分段上传，您必须得到可以对桶执行 `s3:ListBucketMultipartUploads` 操作的许可。 |

分段上传的 API 操作支持

《Amazon Simple Storage Service API 参考》的下面几节描述了适用于分段上传的 Amazon S3 REST API 操作。

- CreateMultipartUpload
- UploadPart
- UploadPartCopy
- CompleteMultipartUpload
- AbortMultipartUpload
- ListParts
- ListMultipartUploads

示例

要使用分段上传将对象上传到目录桶中的 S3 Express One Zone，请参阅以下示例。

主题

- 创建分段上传
- 上传分段上传的分段
- 完成分段上传
- 中止分段上传
- 创建分段上传复制操作
- 列出正在进行的分段上传
- 列出分段上传的分段

创建分段上传

> **Note**
>
> 对于目录存储桶，当您执行 CreateMultipartUpload 操作和 UploadPartCopy 操作时，存储桶的默认加密必须使用所需的加密配置，并且您在 CreateMultipartUpload 请求中提供的请求标头必须与目标存储桶的默认加密配置相匹配。

以下示例显示如何创建分段上传。

使用 Amazon SDK

SDK for Java 2.x

Example

```
/**
 * This method creates a multipart upload request that generates a unique upload ID
 that is used to track
 * all the upload parts
 *
 * @param s3
 * @param bucketName - for example, 'doc-example-bucket--use1-az4--x-s3'
 * @param key
 * @return
 */
 private static String createMultipartUpload(S3Client s3, String bucketName, String
 key) {

     CreateMultipartUploadRequest createMultipartUploadRequest =
 CreateMultipartUploadRequest.builder()
             .bucket(bucketName)
             .key(key)
             .build();

     String uploadId = null;

     try {
         CreateMultipartUploadResponse response =
 s3.createMultipartUpload(createMultipartUploadRequest);
         uploadId = response.uploadId();
     }
```

```
    catch (S3Exception e) {
        System.err.println(e.awsErrorDetails().errorMessage());
        System.exit(1);
    }
    return uploadId;
```

SDK for Python

Example

```
def create_multipart_upload(s3_client, bucket_name, key_name):
    '''
   Create a multipart upload to a directory bucket

   :param s3_client: boto3 S3 client
   :param bucket_name: The destination bucket for the multipart upload
   :param key_name: The key name for the object to be uploaded
   :return: The UploadId for the multipart upload if created successfully, else None
   '''

   try:
        mpu = s3_client.create_multipart_upload(Bucket = bucket_name, Key =
 key_name)
        return mpu['UploadId']
    except ClientError as e:
        logging.error(e)
        return None
```

使用 Amazon CLI

此示例说明如何使用 Amazon CLI 创建到目录存储桶的分段上传。此命令启动一个对目录存储桶 *bucket-base-name*--*zone-id*--x-s3 中对象 *KEY_NAME* 的分段上传。要使用该命令，请将*#######* 替换为您自己的信息。

```
aws s3api create-multipart-upload --bucket bucket-base-name--zone-id--x-s3 --
key KEY_NAME
```

有关更多信息，请参阅 Amazon Command Line Interface 中的 create-multipart-upload。

上传分段上传的分段

以下示例显示了如何上传分段上传的各分段。

使用 Amazon SDK

SDK for Java 2.x

以下示例显示了如何使用 SDK for Java 2.x 将单个对象分段，然后将这些分段上传到目录存储桶。

Example

```
/**
 * This method creates part requests and uploads individual parts to S3 and then
 returns all the completed parts
 *
 * @param s3
 * @param bucketName
 * @param key
 * @param uploadId
 * @throws IOException
 */
 private static ListCompletedPartmultipartUpload(S3Client s3, String bucketName,
 String key, String uploadId, String filePath) throws IOException {

        int partNumber = 1;
        ListCompletedPart completedParts = new ArrayList<>();
        ByteBuffer bb = ByteBuffer.allocate(1024 * 1024 * 5); // 5 MB byte buffer

        // read the local file, breakdown into chunks and process
        try (RandomAccessFile file = new RandomAccessFile(filePath, "r")) {
            long fileSize = file.length();
            int position = 0;
            while (position < fileSize) {
                file.seek(position);
                int read = file.getChannel().read(bb);

                bb.flip(); // Swap position and limit before reading from the
 buffer.
                UploadPartRequest uploadPartRequest = UploadPartRequest.builder()
                        .bucket(bucketName)
                        .key(key)
                        .uploadId(uploadId)
                        .partNumber(partNumber)
                        .build();

                UploadPartResponse partResponse = s3.uploadPart(
                        uploadPartRequest,
```

```
                        RequestBody.fromByteBuffer(bb));

                CompletedPart part = CompletedPart.builder()
                        .partNumber(partNumber)
                        .eTag(partResponse.eTag())
                        .build();
                completedParts.add(part);

                bb.clear();
                position += read;
                partNumber++;
            }
        }

        catch (IOException e) {
            throw e;
        }
        return completedParts;
    }
```

SDK for Python

以下示例显示了如何使用 SDK for Python 将单个对象分段，然后将这些分段上传到目录存储桶。

Example

```
def multipart_upload(s3_client, bucket_name, key_name, mpu_id, part_size):
    '''
    Break up a file into multiple parts and upload those parts to a directory bucket

    :param s3_client: boto3 S3 client
    :param bucket_name: Destination bucket for the multipart upload
    :param key_name: Key name for object to be uploaded and for the local file
 that's being uploaded
    :param mpu_id: The UploadId returned from the create_multipart_upload call
    :param part_size: The size parts that the object will be broken into, in bytes.
                      Minimum 5 MiB, Maximum 5 GiB. There is no minimum size for the
 last part of your multipart upload.
    :return: part_list for the multipart upload if all parts are uploaded
 successfully, else None
    '''

    part_list = []
```

```
    try:
        with open(key_name, 'rb') as file:
            part_counter = 1
            while True:
                file_part = file.read(part_size)
                if not len(file_part):
                    break
                upload_part = s3_client.upload_part(
                    Bucket = bucket_name,
                    Key = key_name,
                    UploadId = mpu_id,
                    Body = file_part,
                    PartNumber = part_counter
                )
                part_list.append({'PartNumber': part_counter, 'ETag':
upload_part['ETag']})
                part_counter += 1
    except ClientError as e:
        logging.error(e)
        return None
    return part_list
```

使用 Amazon CLI

此示例显示了如何使用 Amazon CLI 将单个对象分段，然后将这些分段上传到目录存储桶。要使用该命令，请将*#######* 替换为您自己的信息。

```
aws s3api upload-part --bucket bucket-base-name--zone-id--x-s3 --
key KEY_NAME --part-number 1 --body LOCAL_FILE_NAME --upload-id
 "AS_mgt9RaQE9GEaifATue15dAAAAAAAAAAEMAAAAAAAAADQwNzI4MDU0MjUyMBYAAAAAAAAAAA0AAAAAAAAAAH2AfYAA
```

有关更多信息，请参阅 Amazon Command Line Interface 中的 upload-part。

完成分段上传

以下示例显示了如何完成分段上传。

使用 Amazon SDK

SDK for Java 2.x

以下示例显示了如何使用 SDK for Java 2.x 完成分段上传。

### Example

```
/**
 * This method completes the multipart upload request by collating all the upload
 parts
 * @param s3
 * @param bucketName - for example, 'doc-example-bucket--usw2-az1--x-s3'
 * @param key
 * @param uploadId
 * @param uploadParts
 */
 private static void completeMultipartUpload(S3Client s3, String bucketName, String
 key, String uploadId, ListCompletedPart uploadParts) {
        CompletedMultipartUpload completedMultipartUpload =
 CompletedMultipartUpload.builder()
                .parts(uploadParts)
                .build();

        CompleteMultipartUploadRequest completeMultipartUploadRequest =
                CompleteMultipartUploadRequest.builder()
                        .bucket(bucketName)
                        .key(key)
                        .uploadId(uploadId)
                        .multipartUpload(completedMultipartUpload)
                        .build();

        s3.completeMultipartUpload(completeMultipartUploadRequest);
    }

    public static void multipartUploadTest(S3Client s3, String bucketName, String
 key, String localFilePath)  {
        System.out.println("Starting multipart upload for: " + key);
        try {
            String uploadId = createMultipartUpload(s3, bucketName, key);
            System.out.println(uploadId);
            ListCompletedPart parts = multipartUpload(s3, bucketName, key, uploadId,
 localFilePath);
            completeMultipartUpload(s3, bucketName, key, uploadId, parts);
            System.out.println("Multipart upload completed for: " + key);
        }

        catch (Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
```

```
        }
    }
```

SDK for Python

以下示例显示了如何使用 SDK for Python 完成分段上传。

Example

```
def complete_multipart_upload(s3_client, bucket_name, key_name, mpu_id, part_list):
    '''
    Completes a multipart upload to a directory bucket

    :param s3_client: boto3 S3 client
    :param bucket_name: The destination bucket for the multipart upload
    :param key_name: The key name for the object to be uploaded
    :param mpu_id: The UploadId returned from the create_multipart_upload call
    :param part_list: The list of uploaded part numbers with their associated ETags
    :return: True if the multipart upload was completed successfully, else False
    '''

    try:
        s3_client.complete_multipart_upload(
            Bucket = bucket_name,
            Key = key_name,
            UploadId = mpu_id,
            MultipartUpload = {
                'Parts': part_list
            }
        )
    except ClientError as e:
        logging.error(e)
        return False
    return True

if __name__ == '__main__':
    MB = 1024 ** 2
    region = 'us-west-2'
    bucket_name = 'BUCKET_NAME'
    key_name = 'OBJECT_NAME'
    part_size = 10 * MB
    s3_client = boto3.client('s3', region_name = region)
    mpu_id = create_multipart_upload(s3_client, bucket_name, key_name)
    if mpu_id is not None:
```

```
        part_list = multipart_upload(s3_client, bucket_name, key_name, mpu_id,
part_size)
        if part_list is not None:
            if complete_multipart_upload(s3_client, bucket_name, key_name, mpu_id,
part_list):
                print (f'{key_name} successfully uploaded through a ultipart upload
to {bucket_name}')
            else:
                print (f'Could not upload {key_name} hrough a multipart upload to
{bucket_name}')
```

使用 Amazon CLI

此示例说明如何使用 Amazon CLI 完成目录存储桶的分段上传。要使用该命令，请将*#######* 替换为您自己的信息。

```
aws s3api complete-multipart-upload --bucket bucket-base-name--zone-id--x-s3 --
key KEY_NAME --upload-id
 "AS_mgt9RaQE9GEaifATue15dAAAAAAAAAAEMAAAAAAAAADQwNzI4MDU0MjUyMBYAAAAAAAAAAA0AAAAAAAAAAH2AfYAA
 --multipart-upload file://parts.json
```

此示例采用 JSON 结构，用于描述分段上传中应重新组合成完整文件的各个分段。在此示例中，`file://` 前缀用于从名为 `parts` 的本地文件夹中的文件加载 JSON 结构。

parts.json：

```
parts.json
{
  "Parts": [
    {
      "ETag": "6b78c4a64dd641a58dac8d9258b88147",
      "PartNumber": 1
    }
  ]
}
```

有关更多信息，请参阅 Amazon Command Line Interface 中的 complete-multipart-upload。

中止分段上传

以下示例显示了如何中止分段上传。

使用 Amazon SDK

SDK for Java 2.x

以下示例显示了如何使用 SDK for Java 2.x 中止分段上传。

Example

```
public static void abortMultiPartUploads( S3Client s3, String bucketName ) {

        try {
            ListMultipartUploadsRequest listMultipartUploadsRequest =
 ListMultipartUploadsRequest.builder()
                    .bucket(bucketName)
                    .build();

            ListMultipartUploadsResponse response =
 s3.listMultipartUploads(listMultipartUploadsRequest);
            ListMultipartUpload uploads = response.uploads();

            AbortMultipartUploadRequest abortMultipartUploadRequest;
            for (MultipartUpload upload: uploads) {
                abortMultipartUploadRequest = AbortMultipartUploadRequest.builder()
                        .bucket(bucketName)
                        .key(upload.key())
                        .uploadId(upload.uploadId())
                        .build();

                s3.abortMultipartUpload(abortMultipartUploadRequest);
            }

        }

        catch (S3Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

SDK for Python

以下示例显示了如何使用 SDK for Python 中止分段上传。

### Example

```
import logging
import boto3
from botocore.exceptions import ClientError


def abort_multipart_upload(s3_client, bucket_name, key_name, upload_id):
    '''
    Aborts a partial multipart upload in a directory bucket.

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket where the multipart upload was initiated - for
 example, 'doc-example-bucket--usw2-az1--x-s3'
    :param key_name: Name of the object for which the multipart upload needs to be
 aborted
    :param upload_id: Multipart upload ID for the multipart upload to be aborted
    :return: True if the multipart upload was successfully aborted, False if not
    '''
    try:
        s3_client.abort_multipart_upload(
            Bucket = bucket_name,
            Key = key_name,
            UploadId = upload_id
        )
    except ClientError as e:
        logging.error(e)
        return False
    return True


if __name__ == '__main__':
    region = 'us-west-2'
    bucket_name = 'BUCKET_NAME'
    key_name = 'KEY_NAME'
        upload_id = 'UPLOAD_ID'
    s3_client = boto3.client('s3', region_name = region)
    if abort_multipart_upload(s3_client, bucket_name, key_name, upload_id):
        print (f'Multipart upload for object {key_name} in {bucket_name} bucket has
 been aborted')
    else:
        print (f'Unable to abort multipart upload for object {key_name} in
 {bucket_name} bucket')
```

使用 Amazon CLI

以下示例显示了如何使用 Amazon CLI 中止分段上传。要使用该命令，请将####### 替换为您自己的信息。

```
aws s3api abort-multipart-upload --bucket bucket-base-name--zone-id--x-s3 --
key KEY_NAME --upload-id
 "AS_mgt9RaQE9GEaifATue15dAAAAAAAAAAEMAAAAAAAAADQwNzI4MDU0MjUyMBYAAAAAAAAAAA0AAAAAAAAAAH2AfYAA
MAQAAAAB0OxUFeA7LTbWWFS8WYwhrxDxTIDN-pdEEq_agIHqsbg"
```

有关更多信息，请参阅 Amazon Command Line Interface 中的 abort-multipart-upload。

创建分段上传复制操作

> **Note**
>
> - 要使用 SSE-KMS 加密目录存储桶中新的对象分段副本，必须将具有 KMS 密钥（特别是 customer managed key）的 SSE-KMS 指定为目录存储桶的默认加密配置。Amazon 托管式密钥 (aws/s3) 不受支持。在存储桶的生命周期内，SSE-KMS 配置只能支持每个目录存储桶 1 个 customer managed key。在为 SSE-KMS 指定客户自主管理型密钥后，无法覆盖存储桶的 SSE-KMS 配置的客户自主管理型密钥。无法在 UploadPartCopy 请求标头中使用 SSE-KMS 为新的对象分段副本指定服务器端加密设置。此外，在 `CreateMultipartUpload` 请求中提供的请求标头必须与目标存储桶的默认加密配置相匹配。
> - 当您通过 UploadPartCopy 将 SSE-KMS 加密的对象从通用存储桶复制到目录存储桶、从目录存储桶复制到通用存储桶，或在目录存储桶之间复制时，不支持 S3 存储桶密钥。在这种情况下，每次对 KMS 加密的对象发出复制请求时，Amazon S3 都会调用 Amazon KMS。

以下示例显示了如何使用分段上传将对象从一个存储桶复制到另一个存储桶。

使用 Amazon SDK

SDK for Java 2.x

以下示例显示了如何使用 SDK for Java 2.x，通过分段上传以编程方式将对象从一个存储桶复制到另一个存储桶。

### Example

```
/**
 * This method creates a multipart upload request that generates a unique upload ID
 that is used to track
 * all the upload parts.
 *
 * @param s3
 * @param bucketName
 * @param key
 * @return
 */
 private static String createMultipartUpload(S3Client s3, String bucketName, String
 key) {
        CreateMultipartUploadRequest createMultipartUploadRequest =
 CreateMultipartUploadRequest.builder()
                .bucket(bucketName)
                .key(key)
                .build();
        String uploadId = null;
        try {
            CreateMultipartUploadResponse response =
 s3.createMultipartUpload(createMultipartUploadRequest);
            uploadId = response.uploadId();
        } catch (S3Exception e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
        return uploadId;
  }

  /**
   * Creates copy parts based on source object size and copies over individual parts
   *
   * @param s3
   * @param sourceBucket
   * @param sourceKey
   * @param destnBucket
   * @param destnKey
   * @param uploadId
   * @return
   * @throws IOException
   */
```

```
   public static ListCompletedPart multipartUploadCopy(S3Client s3, String
sourceBucket, String sourceKey, String destnBucket, String destnKey, String
uploadId) throws IOException {

        // Get the object size to track the end of the copy operation.
        HeadObjectRequest headObjectRequest = HeadObjectRequest
                .builder()
                .bucket(sourceBucket)
                .key(sourceKey)
                .build();
        HeadObjectResponse response = s3.headObject(headObjectRequest);
        Long objectSize = response.contentLength();

        System.out.println("Source Object size: " + objectSize);

        // Copy the object using 20 MB parts.
        long partSize = 20 * 1024 * 1024;
        long bytePosition = 0;
        int partNum = 1;
        ListCompletedPart completedParts = new ArrayList<>();
        while (bytePosition < objectSize) {
            // The last part might be smaller than partSize, so check to make sure
            // that lastByte isn't beyond the end of the object.
            long lastByte = Math.min(bytePosition + partSize - 1, objectSize - 1);

            System.out.println("part no: " + partNum + ", bytePosition: " +
bytePosition + ", lastByte: " + lastByte);

            // Copy this part.
            UploadPartCopyRequest req = UploadPartCopyRequest.builder()
                    .uploadId(uploadId)
                    .sourceBucket(sourceBucket)
                    .sourceKey(sourceKey)
                    .destinationBucket(destnBucket)
                    .destinationKey(destnKey)
                    .copySourceRange("bytes="+bytePosition+"-"+lastByte)
                    .partNumber(partNum)
                    .build();
            UploadPartCopyResponse res = s3.uploadPartCopy(req);
            CompletedPart part = CompletedPart.builder()
                    .partNumber(partNum)
                    .eTag(res.copyPartResult().eTag())
                    .build();
            completedParts.add(part);
```

```
            partNum++;
            bytePosition += partSize;
        }
        return completedParts;
    }


    public static void multipartCopyUploadTest(S3Client s3, String srcBucket, String
 srcKey, String destnBucket, String destnKey)  {
        System.out.println("Starting multipart copy for: " + srcKey);
        try {
            String uploadId = createMultipartUpload(s3, destnBucket, destnKey);
            System.out.println(uploadId);
            ListCompletedPart parts = multipartUploadCopy(s3, srcBucket,
 srcKey,destnBucket,  destnKey, uploadId);
            completeMultipartUpload(s3, destnBucket, destnKey, uploadId, parts);
            System.out.println("Multipart copy completed for: " + srcKey);
        } catch (Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

SDK for Python

以下示例显示了如何使用 SDK for Python，通过分段上传以编程方式将对象从一个存储桶复制到另一个存储桶。

Example

```
import logging
import boto3
from botocore.exceptions import ClientError

def head_object(s3_client, bucket_name, key_name):
    '''
    Returns metadata for an object in a directory bucket

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket that contains the object to query for metadata
    :param key_name: Key name to query for metadata
    :return: Metadata for the specified object if successful, else None
    '''
```

```
    try:
        response = s3_client.head_object(
            Bucket = bucket_name,
            Key = key_name
        )
        return response
    except ClientError as e:
        logging.error(e)
        return None

def create_multipart_upload(s3_client, bucket_name, key_name):
    '''
    Create a multipart upload to a directory bucket

    :param s3_client: boto3 S3 client
    :param bucket_name: Destination bucket for the multipart upload
    :param key_name: Key name of the object to be uploaded
    :return: UploadId for the multipart upload if created successfully, else None
    '''

    try:
        mpu = s3_client.create_multipart_upload(Bucket = bucket_name, Key =
 key_name)
        return mpu['UploadId']
    except ClientError as e:
        logging.error(e)
        return None

def multipart_copy_upload(s3_client, source_bucket_name, key_name,
 target_bucket_name, mpu_id, part_size):
    '''
    Copy an object in a directory bucket to another bucket in multiple parts of a
 specified size

    :param s3_client: boto3 S3 client
    :param source_bucket_name: Bucket where the source object exists
    :param key_name: Key name of the object to be copied
    :param target_bucket_name: Destination bucket for copied object
    :param mpu_id: The UploadId returned from the create_multipart_upload call
    :param part_size: The size parts that the object will be broken into, in bytes.
                      Minimum 5 MiB, Maximum 5 GiB. There is no minimum size for the
 last part of your multipart upload.
    :return: part_list for the multipart copy if all parts are copied successfully,
 else None
```

```
    '''

    part_list = []
    copy_source = {
        'Bucket': source_bucket_name,
        'Key': key_name
    }
    try:
        part_counter = 1
        object_size = head_object(s3_client, source_bucket_name, key_name)
        if object_size is not None:
            object_size = object_size['ContentLength']
        while (part_counter - 1) * part_size <object_size:
            bytes_start = (part_counter - 1) * part_size
            bytes_end = (part_counter * part_size) - 1
            upload_copy_part = s3_client.upload_part_copy (
                Bucket = target_bucket_name,
                CopySource = copy_source,
                CopySourceRange = f'bytes={bytes_start}-{bytes_end}',
                Key = key_name,
                PartNumber = part_counter,
                UploadId = mpu_id
            )
            part_list.append({'PartNumber': part_counter, 'ETag':
 upload_copy_part['CopyPartResult']['ETag']})
            part_counter += 1
    except ClientError as e:
        logging.error(e)
        return None
    return part_list

def complete_multipart_upload(s3_client, bucket_name, key_name, mpu_id, part_list):
    '''
    Completes a multipart upload to a directory bucket

    :param s3_client: boto3 S3 client
    :param bucket_name: Destination bucket for the multipart upload
    :param key_name: Key name of the object to be uploaded
    :param mpu_id: The UploadId returned from the create_multipart_upload call
    :param part_list: List of uploaded part numbers with associated ETags
    :return: True if the multipart upload was completed successfully, else False
    '''

    try:
```

```
        s3_client.complete_multipart_upload(
            Bucket = bucket_name,
            Key = key_name,
            UploadId = mpu_id,
            MultipartUpload = {
                'Parts': part_list
            }
        )
    except ClientError as e:
        logging.error(e)
        return False
    return True

if __name__ == '__main__':
    MB = 1024 ** 2
    region = 'us-west-2'
    source_bucket_name = 'SOURCE_BUCKET_NAME'
    target_bucket_name = 'TARGET_BUCKET_NAME'
    key_name = 'KEY_NAME'
    part_size = 10 * MB
    s3_client = boto3.client('s3', region_name = region)
    mpu_id = create_multipart_upload(s3_client, target_bucket_name, key_name)
    if mpu_id is not None:
        part_list = multipart_copy_upload(s3_client, source_bucket_name, key_name,
 target_bucket_name, mpu_id, part_size)
        if part_list is not None:
            if complete_multipart_upload(s3_client, target_bucket_name, key_name,
 mpu_id, part_list):
                print (f'{key_name} successfully copied through multipart copy from
 {source_bucket_name} to {target_bucket_name}')
            else:
                print (f'Could not copy {key_name} through multipart copy from
 {source_bucket_name} to {target_bucket_name}')
```

### 使用 Amazon CLI

以下示例显示了如何使用 Amazon CLI，通过分段上传以编程方式将对象从一个存储桶复制到目录存储桶。要使用该命令，请将*#######* 替换为您自己的信息。

```
aws s3api upload-part-copy --bucket bucket-base-name--zone-id--x-s3 --
key TARGET_KEY_NAME --copy-source SOURCE_BUCKET_NAME/SOURCE_KEY_NAME --part-number 1 --
```

```
upload-id
 "AS_mgt9RaQE9GEaifATue15dAAAAAAAAAAEMAAAAAAAAADQwNzI4MDU0MjUyMBYAAAAAAAAAAA0AAAAAAAAAAH2AfYAA
```

有关更多信息，请参阅 Amazon Command Line Interface 中的 upload-part-copy。

列出正在进行的分段上传

要列出正在进行的到目录存储桶的分段上传，可以使用 Amazon SDK 或 Amazon CLI。

使用 Amazon SDK

SDK for Java 2.x

以下示例显示了如何使用 SDK for Java 2.x 列出正在进行（未完成）的分段上传。

Example

```
public static void listMultiPartUploads( S3Client s3, String bucketName) {
       try {
           ListMultipartUploadsRequest listMultipartUploadsRequest =
ListMultipartUploadsRequest.builder()
                .bucket(bucketName)
                .build();

           ListMultipartUploadsResponse response =
s3.listMultipartUploads(listMultipartUploadsRequest);
           List MultipartUpload uploads = response.uploads();
           for (MultipartUpload upload: uploads) {
               System.out.println("Upload in progress: Key = \"" + upload.key() +
"\", id = " + upload.uploadId());
           }
     }
     catch (S3Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
     }
 }
```

SDK for Python

以下示例显示了如何使用 SDK for Python 列出正在进行（未完成）的分段上传。

Example

```
import logging
import boto3
from botocore.exceptions import ClientError

def list_multipart_uploads(s3_client, bucket_name):
    '''
    List any incomplete multipart uploads in a directory bucket in e specified gion

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket to check for incomplete multipart uploads
    :return: List of incomplete multipart uploads if there are any, None if not
    '''

    try:
        response = s3_client.list_multipart_uploads(Bucket = bucket_name)
        if 'Uploads' in response.keys():
            return response['Uploads']
        else:
            return None
    except ClientError as e:
        logging.error(e)

if __name__ == '__main__':
    bucket_name = 'BUCKET_NAME'
    region = 'us-west-2'
    s3_client = boto3.client('s3', region_name = region)
    multipart_uploads = list_multipart_uploads(s3_client, bucket_name)
    if multipart_uploads is not None:
        print (f'There are {len(multipart_uploads)} ncomplete multipart uploads for
 {bucket_name}')
    else:
        print (f'There are no incomplete multipart uploads for {bucket_name}')
```

使用 Amazon CLI

以下示例显示了如何使用 Amazon CLI 列出正在进行（未完成）的分段上传。要使用该命令，请将*### ####* 替换为您自己的信息。

```
aws s3api list-multipart-uploads --bucket bucket-base-name--zone-id--x-s3
```

有关更多信息，请参阅 Amazon Command Line Interface 中的 list-multipart-uploads。

列出分段上传的分段

以下示例显示了如何列出到目录存储桶的分段上传的各个分段。

使用 Amazon SDK

SDK for Java 2.x

以下示例显示了如何使用 SDK for Java 2.x 列出到目录存储桶的分段上传的各个分段。

```
public static void listMultiPartUploadsParts( S3Client s3, String bucketName, String
 objKey, String uploadID) {

        try {
            ListPartsRequest listPartsRequest = ListPartsRequest.builder()
                .bucket(bucketName)
                .uploadId(uploadID)
                .key(objKey)
                .build();

            ListPartsResponse response = s3.listParts(listPartsRequest);
            ListPart parts = response.parts();
            for (Part part: parts) {
                System.out.println("Upload in progress: Part number = \"" +
 part.partNumber() + "\", etag = " + part.eTag());
            }

        }

        catch (S3Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }


    }
```

SDK for Python

以下示例显示了如何使用 SDK for Python 列出到目录存储桶的分段上传的各个分段。

```
import logging
```

```
import boto3
from botocore.exceptions import ClientError

def list_parts(s3_client, bucket_name, key_name, upload_id):
    '''
    Lists the parts that have been uploaded for a specific multipart upload to a
 directory bucket.

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket that multipart uploads parts have been uploaded to
    :param key_name: Name of the object that has parts uploaded
    :param upload_id: Multipart upload ID that the parts are associated with
    :return: List of parts associated with the specified multipart upload, None if
 there are no parts
    '''
    parts_list = []
    next_part_marker = ''
    continuation_flag = True
    try:
        while continuation_flag:
            if next_part_marker == '':
                response = s3_client.list_parts(
                    Bucket = bucket_name,
                    Key = key_name,
                    UploadId = upload_id
                )
            else:
                response = s3_client.list_parts(
                    Bucket = bucket_name,
                    Key = key_name,
                    UploadId = upload_id,
                    NextPartMarker = next_part_marker
                )
            if 'Parts' in response:
                for part in response['Parts']:
                    parts_list.append(part)
                if response['IsTruncated']:
                    next_part_marker = response['NextPartNumberMarker']
                else:
                    continuation_flag = False
            else:
                continuation_flag = False
        return parts_list
    except ClientError as e:
```

```
        logging.error(e)
        return None

if __name__ == '__main__':
    region = 'us-west-2'
    bucket_name = 'BUCKET_NAME'
    key_name = 'KEY_NAME'
    upload_id = 'UPLOAD_ID'
    s3_client = boto3.client('s3', region_name = region)
    parts_list = list_parts(s3_client, bucket_name, key_name, upload_id)
    if parts_list is not None:
        print (f'{key_name} has {len(parts_list)} parts uploaded to {bucket_name}')
    else:
        print (f'There are no multipart uploads with that upload ID for
 {bucket_name} bucket')
```

使用 Amazon CLI

以下示例显示了如何使用 Amazon CLI 列出到目录存储桶的分段上传的各个分段。要使用该命令，请将*#######* 替换为您自己的信息。

```
aws s3api list-parts --bucket bucket-base-name--zone-id--x-s3 --key KEY_NAME --upload-
id
 "AS_mgt9RaQE9GEaifATue15dAAAAAAAAAAAEMAAAAAAAAADQwNzI4MDU0MjUyMBYAAAAAAAAAAA0AAAAAAAAAAH2AfYAA
```

有关更多信息，请参阅 Amazon Command Line Interface 中的 list-parts。

## 从目录存储桶复制对象或向目录存储桶复制对象

复制操作将创建已存储在 Amazon S3 中的对象的副本。您可以在目录存储桶和通用存储桶之间复制对象。您还可以在一个存储桶内复制对象，也可以在同一类型的存储桶之间复制对象，例如，从目录存储桶复制到目录存储桶。

> **Note**
>
> 当源存储桶或目标存储桶位于 Amazon 本地区域时，不支持跨不同 Amazon Web Services 区域复制对象。源存储桶和目标存储桶必须具有相同的父 Amazon Web Services 区域。源存储桶和目标存储桶可以是不同的存储桶位置类型（可用区或本地区域）。

在单个原子操作中，您可以创建最大 5GB 的对象副本。但是，要复制大于 5GB 的对象，您必须使用分段上传 API 操作。有关更多信息，请参阅 对目录桶使用分段上传。

权限

要复制对象，您必须拥有以下权限：

- 要将对象从一个目录存储桶复制到另一个目录存储桶，您必须拥有 `s3express:CreateSession` 权限。
- 要将对象从目录存储桶复制到通用存储桶，您必须拥有将对象副本写入目标存储桶的 `s3express:CreateSession` 权限和 `s3:PutObject` 权限。
- 要将对象从通用桶复制到目录桶，您必须拥有读取正在复制的源对象的 `s3express:CreateSession` 权限和 `s3:GetObject` 权限。

  有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 CopyObject。

加密

Amazon S3 会自动加密上传到 S3 存储桶的所有新对象。S3 存储桶的默认加密配置始终处于启用状态，并至少设置为具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）。

对于目录存储桶，支持 SSE-S3 和具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）。当目标存储桶是目录存储桶时，我们建议，目标存储桶的默认加密使用所需的加密配置，并且不要覆盖存储桶的默认加密。然后，使用所需的加密设置自动对新对象进行加密。此外，当您通过 CopyObject 将 SSE-KMS 加密的对象从通用存储桶复制到目录存储桶、从目录存储桶复制到通用存储桶，或在目录存储桶之间复制时，不支持 S3 存储桶密钥。在这种情况下，每次对 KMS 加密的对象发出复制请求时，Amazon S3 都会调用 Amazon KMS。有关目录存储桶中加密覆盖行为的更多信息，请参阅 Specifying server-side encryption with Amazon KMS for new object uploads。

对于通用桶，您可以使用 SSE-S3（默认）、采用 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）、采用 Amazon KMS 密钥的双层服务器端加密（DSSE-KMS），或采用客户提供密钥的服务器端加密（SSE-C）。

如果您发出复制请求来指定对目录存储桶（源存储桶或目标存储桶）使用 DSSE-KMS 或 SSE-C，则响应将返回错误。

标签

目录存储桶不支持标签。如果您将带有标签的对象从通用桶复制到目录桶，您会收到 HTTP 501 (Not Implemented) 响应。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 CopyObject。

ETag

S3 Express One Zone 的实体标签（ETag）是随机的字母数字字符串，而不是 MD5 校验和。为协助确保对象完整性，请使用额外的校验和。

其他校验和

S3 Express One Zone 可让您选择用于在上传或下载过程中验证数据的校验和算法。您可以选择以下安全哈希算法（SHA）或循环冗余校验（CRC）数据完整性检查算法之一：CRC32、CRC32C、SHA-1 和 SHA-256。S3 Express One Zone 存储类不支持基于 MD5 的校验和。

有关更多信息，请参阅 其他 S3 校验和最佳实践。

支持的特征

有关 S3 Express One Zone 支持哪些 Amazon S3 特征的更多信息，请参阅目录存储桶的差异。

使用 S3 控制台（复制到目录存储桶）

> **Note**
>
> 使用控制台将对象复制到目录存储桶时的限制和局限性如下所示：
>
> - Copy 操作适用于指定文件夹（前缀）中的所有对象。当正在执行操作时添加到这些文件夹的对象可能受到影响。
> - 无法使用 S3 控制台复制使用客户提供的加密密钥（SSE-C）加密的对象。要复制使用 SSE-C 加密的对象，请使用 Amazon CLI、Amazon SDK 或 Amazon S3 REST API。
> - 复制的对象将不会保留原始对象的对象锁定设置。
> - 如果要从中复制对象的存储桶对于 S3 对象所有权使用“强制存储桶拥有者”设置，则对象 ACL 将不会复制到指定的目标。
> - 如果要将对象复制到对于 S3 对象所有权使用“强制存储桶拥有者”设置的存储桶，请确保源存储桶也使用“强制存储桶拥有者”设置，或移除对其它 Amazon 账户和组的任何对象 ACL 授权。
> - 从通用存储桶复制到目录存储桶的对象将不会保留对象标签、ACL 或 Etag 值。可以复制校验和值，但它们并不等同于 Etag。与添加时相比，校验和值可能会发生变化。

- 复制到目录存储桶的所有对象都将对 S3 对象所有权使用“强制存储桶拥有者”设置。

将对象从通用桶或目录桶复制到目录桶

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择您要从中复制对象的存储桶：
   - 要从通用桶进行复制，请选择通用桶选项卡。
   - 要从目录桶进行复制，请选择目录桶选项卡。
3. 选择包含要复制的对象的通用桶或目录桶。
4. 请选择对象选项卡。在对象页面上，选中要复制的对象名称左侧的复选框。
5. 在 Actions (操作) 菜单中，选择 Copy (复制)。

   将出现复制页面。
6. 在目标下，为您的目标类型选择目录桶。要指定目标路径，请选择浏览 S3，导航到目标，然后选中目标左侧的选项按钮。选择右下角的选择目标。

   或者，输入目标路径。
7. 在其它复制设置下，选择是要复制源设置、请勿指定设置还是指定设置。复制源设置是默认选项。如果您只想复制不带源设置属性的对象，请选择请勿指定设置。选择指定设置来指定服务器端加密、校验和以及元数据的设置。
8. 选择右下角的复制。Amazon S3 会将对象复制到目标。

使用 S3 控制台（复制到通用存储桶）

> **Note**
>
> 使用控制台将对象复制到通用存储桶时的限制和局限性如下所示：
>
> - Copy 操作适用于指定文件夹（前缀）中的所有对象。当正在执行操作时添加到这些文件夹的对象可能受到影响。
> - 无法使用 S3 控制台复制使用客户提供的加密密钥（SSE-C）加密的对象。要复制使用 SSE-C 加密的对象，请使用 Amazon CLI、Amazon SDK 或 Amazon S3 REST API。
> - 复制的对象将不会保留原始对象的对象锁定设置。

- 如果要从中复制对象的存储桶对于 S3 对象所有权使用“强制存储桶拥有者”设置，则对象 ACL 将不会复制到指定的目标。
- 如果要将对象复制到对于 S3 对象所有权使用“强制存储桶拥有者”设置的存储桶，请确保源存储桶也使用“强制存储桶拥有者”设置，或移除对其它 Amazon 账户和组的任何对象 ACL 授权。

将对象从目录存储桶复制到通用存储桶

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 选择目录桶选项卡。
4. 选择包含您要复制的对象的目录桶。
5. 请选择对象选项卡。在对象页面上，选中要复制的对象名称左侧的复选框。
6. 在 Actions (操作) 菜单中，选择 Copy (复制)。
7. 在目标下，为您的目标类型选择通用桶。要指定目标路径，请选择浏览 S3，导航到目标，然后选中目标左侧的选项按钮。选择右下角的选择目标。

   或者，输入目标路径。
8. 在其它复制设置下，选择是要复制源设置、请勿指定设置还是指定设置。复制源设置是默认选项。如果您只想复制不带源设置属性的对象，请选择请勿指定设置。选择指定设置，来指定存储类、ACL、对象标签、元数据、服务器端加密和其它校验和的设置。
9. 选择右下角的复制。Amazon S3 会将对象复制到目标。

使用 Amazon SDK

SDK for Java 2.x

Example

```
public static void copyBucketObject (S3Client s3, String sourceBucket, String
objectKey, String targetBucket) {
     CopyObjectRequest copyReq = CopyObjectRequest.builder()
         .sourceBucket(sourceBucket)
```

```
            .sourceKey(objectKey)
            .destinationBucket(targetBucket)
            .destinationKey(objectKey)
            .build();
        String temp = "";

        try {
            CopyObjectResponse copyRes = s3.copyObject(copyReq);
            System.out.println("Successfully copied " + objectKey +" from bucket " +
sourceBucket +" into bucket "+targetBucket);
        }

        catch (S3Exception e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
}
```

使用 Amazon CLI

以下 copy-object 示例命令显示了如何使用 Amazon CLI 将对象从一个存储桶复制到另一个存储库。您可以在存储桶类型之间复制对象。要运行此命令，请将用户输入占位符替换为您自己的信息。

```
aws s3api copy-object --copy-source SOURCE_BUCKET/SOURCE_KEY_NAME --key TARGET_KEY_NAME
 --bucket TARGET_BUCKET_NAME
```

有关更多信息，请参阅 Amazon CLI 命令参考 中的 copy-object。

## 删除目录存储桶中的对象

您可以使用 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）或 Amazon SDK 从 Amazon S3 目录桶中删除对象。有关更多信息，请参阅使用目录存储桶和S3 Express One Zone。

**Warning**

- 删除对象的操作无法撤销。
- 此操作将删除所有指定的对象。删除文件夹时，请等待删除操作完成，然后再将新对象添加到文件夹。否则，新对象也可能会被删除。

> **Note**
>
> 当以编程方式从目录桶中删除多个对象时，请注意以下事项：
>
> - `DeleteObjects` 请求中的对象键必须至少包含一个非空格字符。不支持完全由空格字符组成的字符串。
> - `DeleteObjects` 请求中的对象键不能包含 Unicode 控制字符，但换行符（`\n`）、制表符（`\t`）和回车符（`\r`）除外。

使用 S3 控制台

删除对象

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择目录存储桶。
3. 选择包含您要删除的对象的目录桶。
4. 请选择对象选项卡。在对象列表中，选中要删除的一个或多个对象左侧的复选框。
5. 选择删除。
6. 在删除对象页面上，在文本框中输入 **`permanently delete`**。
7. 选择删除对象。

使用 Amazon SDK

SDK for Java 2.x

Example

下面的示例通过使用 Amazon SDK for Java 2.x 删除目录桶中的对象。

```
static void deleteObject(S3Client s3Client, String bucketName, String objectKey) {


        try {
```

```
            DeleteObjectRequest del = DeleteObjectRequest.builder()
                    .bucket(bucketName)
                    .key(objectKey)
                    .build();

            s3Client.deleteObject(del);

            System.out.println("Object " + objectKey + " has been deleted");


        } catch (S3Exception e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }

    }
```

SDK for Python

Example

下面的示例通过使用 适用于 Python (Boto3) 的 Amazon SDK 删除目录桶中的对象。

```
import logging
import boto3
from botocore.exceptions import ClientError

def delete_objects(s3_client, bucket_name, objects):
    '''
    Delete a list of objects in a directory bucket

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket that contains objects to be deleted; for example,
 'doc-example-bucket--usw2-az1--x-s3'
    :param objects: List of dictionaries that specify the key names to delete
    :return: Response output, else False
    '''

    try:
        response = s3_client.delete_objects(
            Bucket = bucket_name,
            Delete = {
                'Objects': objects
```

```
            }
        )
        return response
    except ClientError as e:
        logging.error(e)
        return False


if __name__ == '__main__':
    region = 'us-west-2'
    bucket_name = 'BUCKET_NAME'
    objects = [
        {
            'Key': '0.txt'
        },
        {
            'Key': '1.txt'
        },
        {
            'Key': '2.txt'
        },
        {
            'Key': '3.txt'
        },
        {
            'Key': '4.txt'
        }
    ]

    s3_client = boto3.client('s3', region_name = region)
    results = delete_objects(s3_client, bucket_name, objects)
    if results is not None:
        if 'Deleted' in results:
            print (f'Deleted {len(results["Deleted"])} objects from {bucket_name}')
        if 'Errors' in results:
            print (f'Failed to delete {len(results["Errors"])} objects from
 {bucket_name}')
```

### 使用 Amazon CLI

以下 `delete-object` 示例命令显示如何使用 Amazon CLI 从目录存储桶中删除对象。要运行此命令，请将 *`user input placeholders`* 替换为您自己的信息。

```
aws s3api delete-object --bucket bucket-base-name--zone-id--x-s3 --key KEY_NAME
```

有关更多信息，请参阅 Amazon CLI 命令参考 中的 delete-object。

以下 delete-objects 示例命令显示如何使用 Amazon CLI 从目录存储桶中删除对象。要运行此命令，请将 *user input placeholders* 替换为您自己的信息。

delete.json 文件如下所示：

```
{
    "Objects": [
        {
            "Key": "0.txt"
        },
        {
            "Key": "1.txt"
        },
        {
            "Key": "2.txt"
        },
        {
            "Key": "3.txt"
        }
    ]
}
```

delete-objects 示例命令如下所示：

```
aws s3api delete-objects --bucket bucket-base-name--zone-id--x-s3 --delete
 file://delete.json
```

有关更多信息，请参阅 Amazon CLI 命令参考 中的 delete-objects。

## 下载目录存储桶中的对象

下面的代码示例显示了如何使用 GetObject API 操作从 Amazon S3 目录桶中的对象读取（下载）数据。

使用 Amazon SDK

SDK for Java 2.x

Example

下面的代码示例显示了如何使用 Amazon SDK for Java 2.x 从目录桶中的对象读取数据。

```
public static void getObject(S3Client s3Client, String bucketName, String objectKey)
 {
     try {
         GetObjectRequest objectRequest = GetObjectRequest
            .builder()
            .key(objectKey)
            .bucket(bucketName)
            .build();

         ResponseBytes GetObjectResponse objectBytes =
 s3Client.getObjectAsBytes(objectRequest);
         byte[] data = objectBytes.asByteArray();

         //Print object contents to console
         String s = new String(data, StandardCharsets.UTF_8);
         System.out.println(s);
    }

    catch (S3Exception e) {
        System.err.println(e.awsErrorDetails().errorMessage());
        System.exit(1);
    }
}
```

SDK for Python

Example

下面的代码示例显示了如何使用 适用于 Python (Boto3) 的 Amazon SDK 从目录桶中的对象读取数据。

```
import boto3
from botocore.exceptions import ClientError
from botocore.response import StreamingBody
```

```
def get_object(s3_client: boto3.client, bucket_name: str, key_name: str) ->
 StreamingBody:
    """
    Gets the object.
    :param s3_client:
    :param bucket_name: The bucket that contains the object.
    :param key_name: The key of the object to be downloaded.
    :return: The object data in bytes.
    """
    try:
        response = s3_client.get_object(Bucket=bucket_name, Key=key_name)
        body = response['Body'].read()
        print(f"Got object '{key_name}' from bucket '{bucket_name}'.")
    except ClientError:
        print(f"Couldn't get object '{key_name}' from bucket '{bucket_name}'.")
        raise
    else:
        return body

def main():
    s3_client = boto3.client('s3')
    resp = get_object(s3_client, 'doc-example-bucket--use1-az4--x-s3', 'sample.txt')
    print(resp)

if __name__ == "__main__":
     main()
```

使用 Amazon CLI

以下 `get-object` 示例将向您展示如何使用 Amazon CLI 从 Amazon S3 下载对象。此命令从目录存储桶 *bucket-base-name--zone-id--x-s3* 获取对象 *KEY_NAME*。该对象将下载到名为 *LOCAL_FILE_NAME* 的文件中。要运行此命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3api get-object --bucket bucket-base-name--zone-id--x-s3 --
key KEY_NAME LOCAL_FILE_NAME
```

有关更多信息，请参阅 Amazon CLI 命令参考 中的 get-object。

## 生成预签名 URL 以共享对象目录存储桶

以下代码示例显示如何生成预签名 URL 以共享 Amazon S3 目录存储桶中的对象。

使用 Amazon CLI

以下示例命令显示如何使用 Amazon CLI 为来自 Amazon S3 的对象生成预签名 URL。此命令从目录存储桶 *bucket-base-name*--*zone-id*--x-s3 为对象 *KEY_NAME* 生成预签名 URL。要运行此命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3 presign s3://bucket-base-name--zone-id--x-s3/KEY_NAME --expires-in 7200
```

有关更多信息，请参阅 Amazon CLI 命令参考 中的 presign。

## 检索目录存储桶的对象元数据

以下 Amazon SDK 和 Amazon CLI 示例显示如何使用 HeadObject 和 GetObjectAttributes API 操作从 Amazon S3 目录存储桶中的对象检索元数据，而不返回对象本身。

使用 Amazon SDK

SDK for Java 2.x

Example

```
public static void headObject(S3Client s3Client, String bucketName, String
 objectKey) {
    try {
        HeadObjectRequest headObjectRequest = HeadObjectRequest
                .builder()
                .bucket(bucketName)
                .key(objectKey)
                .build();
        HeadObjectResponse response = s3Client.headObject(headObjectRequest);
        System.out.format("Amazon S3 object: \"%s\" found in bucket: \"%s\" with
 ETag: \"%s\"", objectKey, bucketName, response.eTag());
    }
    catch (S3Exception e) {
        System.err.println(e.awsErrorDetails().errorMessage());
```

使用 Amazon CLI

以下 `head-object` 示例命令显示您如何使用 Amazon CLI 从对象检索元数据。要运行此命令，请将 *`user input placeholders`* 替换为您自己的信息。

```
aws s3api head-object --bucket bucket-base-name--zone-id--x-s3 --key KEY_NAME
```

有关更多信息，请参阅 Amazon CLI 命令参考 中的 head-object。

以下 `get-object-attributes` 示例命令显示您如何使用 Amazon CLI 从对象检索元数据。要运行此命令，请将 *`user input placeholders`* 替换为您自己的信息。

```
aws s3api get-object-attributes --bucket bucket-base-name--zone-id--x-s3 --key KEY_NAME
 --object-attributes "StorageClass" "ETag" "ObjectSize"
```

有关更多信息，请参阅 Amazon CLI 命令参考 中的 get-object-attributes。

## 列出目录存储桶中的对象

下面的代码示例显示了如何使用 `ListObjectsV2` API 操作列出 Amazon S3 目录存储桶中的对象。

使用 Amazon CLI

以下 `list-objects-v2` 示例命令显示如何使用 Amazon CLI 列出 Amazon S3 中的对象。此命令列出目录存储桶 *`bucket-base-name--zone-id`*`--x-s3` 中的对象。要运行此命令，请将 *`user input placeholders`* 替换为您自己的信息。

```
aws s3api list-objects-v2 --bucket bucket-base-name--zone-id--x-s3
```

有关更多信息，请参阅 Amazon CLI 命令参考 中的 list-objects-v2。

# 目录存储桶的安全性

Amazon 的云安全性的优先级最高。为了满足对安全性最敏感的组织的需求，我们打造了具有超高安全性的数据中心和网络架构。作为 Amazon 的客户，您也可以从这些数据中心和网络架构受益。安全性是 Amazon 和您的共同责任。责任共担模式将其描述为云本身的安全性和云中的安全性：

- 云的安全性 – Amazon 负责保护在 Amazon Web Services 云 中运行 Amazon Web Services 服务的基础设施。Amazon 还向您提供可安全使用的服务。作为 Amazon Compliance Programs的一部分，第三方审计人员将定期测试和验证我们安全措施的有效性。

要了解合规性计划，请参阅Amazon Web Services 服务 in Scope by Compliance Program。

- 云中的安全性：您的责任由您使用的 Amazon Web Services 服务 决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

此文档将协助您了解如何在使用目录存储桶时应用责任共担模式。以下主题说明如何配置目录存储桶以实现您的安全性和合规性目标。您还将了解如何使用其他 Amazon Web Services 服务来帮助您监控和保护目录存储桶中的对象。

## 数据保护和加密

有关如何为目录存储桶配置加密的更多信息，请参阅以下主题。

主题

- 服务器端加密
- 设置和监控目录存储桶的默认加密
- 在目录存储桶中使用具有 Amazon KMS 密钥的服务器端加密（SSE-KMS）
- 传输中加密
- 数据删除

### 服务器端加密

默认情况下，所有目录存储桶都配置了加密，所有上传到目录存储桶的新对象都会自动静态加密。具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）是每个目录存储桶的默认加密配置。如果要指定不同的加密类型，则可以通过设置存储桶的默认加密配置，来使用具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）。有关目录存储桶中的 SSE-KMS 的更多信息，请参阅在目录存储桶中使用具有 Amazon KMS 密钥的服务器端加密（SSE-KMS）。

我们建议存储桶的默认加密使用所需的加密配置，并且不要在 `CreateSession` 请求或 PUT 对象请求中覆盖存储桶默认加密。然后，使用所需的加密设置自动对新对象进行加密。有关目录存储桶中加密覆盖行为的更多信息，请参阅 Specifying server-side encryption with Amazon KMS for new object uploads。

目录存储桶中的 SSE-KMS 与通用存储桶中的 SSE-KMS 在以下几个方面有所不同。

- 在存储桶的生命周期内，SSE-KMS 配置只能支持每个目录存储桶 1 个 customer managed key。Amazon 托管式密钥 (aws/s3) 不受支持。此外，在为 SSE-KMS 指定客户自主管理型密钥后，无法覆盖存储桶的 SSE-KMS 配置的客户自主管理型密钥。

  可以通过以下方式，确定您为存储桶的 SSE-KMS 配置指定的客户自主管理型密钥：

  - 您发出 HeadObject API 操作请求以查找响应中 x-amz-server-side-encryption-aws-kms-key-id 的值。

  要对数据使用新的客户自主管理型密钥，我们建议使用新的客户自主管理型密钥将现有对象复制到新的目录存储桶中。

- 对于除 CopyObject 和 UploadPartCopy 之外的可用区端点（对象级）API 操作，可以通过 CreateSession 验证请求和为请求授权，以实现低延迟。我们建议存储桶的默认加密使用所需的加密配置，并且不要在 CreateSession 请求或 PUT 对象请求中覆盖存储桶默认加密。然后，使用所需的加密设置自动对新对象进行加密。要使用 SSE-KMS 加密目录存储桶中的新对象，必须将具有 KMS 密钥（特别是 customer managed key）的 SSE-KMS 指定为目录存储桶的默认加密配置。然后，在为可用区端点 API 操作创建会话时，将在会话期间使用 SSE-KMS 和 S3 存储桶密钥自动加密和解密新对象。有关目录存储桶中加密覆盖行为的更多信息，请参阅 Specifying server-side encryption with Amazon KMS for new object uploads。

  在可用区端点 API 调用（CopyObject 和 UploadPartCopy 除外）中，无法覆盖 CreateSession 请求中加密设置（x-amz-server-side-encryption、x-amz-server-side-encryption-aws-kms-key-id、x-amz-server-side-encryption-context 和 x-amz-server-side-encryption-bucket-key-enabled）的值。无需在可用区端点 API 调用中显式指定这些加密设置值，Amazon S3 将使用 CreateSession 请求中的加密设置值来保护目录存储桶中的新对象。

  > **Note**
  >
  > 当您使用 Amazon CLI 或 Amazon SDK 时，对于 CreateSession，会话令牌会自动刷新，以避免在会话到期时服务中断。Amazon CLI 或 Amazon SDK 将存储桶的默认加密配置用于 CreateSession 请求。不支持覆盖 CreateSession 请求中的加密设置值。此外，在可用区端点 API 调用（CopyObject 和 UploadPartCopy 除外）中，不支持覆盖 CreateSession 请求中加密设置的值。

- 对于 CopyObject，要使用 SSE-KMS 加密目录存储桶中新的对象副本，必须将具有 KMS 密钥（特别是 customer managed key）的 SSE-KMS 指定为目录存储桶的默认加密配置。然后，当您使用 SSE-KMS 为新的对象副本指定服务器端加密设置时，必须确保加密密钥与您为目录存储桶的默认加密配置指定的客户自主管理型密钥相同。对于 UploadPartCopy，要使用 SSE-KMS 加密目录存储桶

中新的对象分段副本，必须将具有 KMS 密钥（特别是 customer managed key）的 SSE-KMS 指定为目录存储桶的默认加密配置。无法在 UploadPartCopy 请求标头中使用 SSE-KMS 为新的对象分段副本指定服务器端加密设置。此外，您在 CreateMultipartUpload 请求中提供的加密设置必须与目标存储桶的默认加密配置相匹配。

- 始终为目录存储桶中的 GET 和 PUT 操作启用 S3 存储桶密钥，并且不能禁用。当您通过 CopyObject、UploadPartCopy、批量操作中的 Copy 操作或 import 任务，将 SSE-KMS 加密的对象从通用存储桶复制到目录存储桶、从目录存储桶复制到通用存储桶，或在目录存储桶之间复制时，不支持 S3 存储桶密钥。在这种情况下，每次对 KMS 加密的对象发出复制请求时，Amazon S3 都会调用 Amazon KMS。
- 当您在目录存储桶中指定用于加密的 Amazon KMS customer managed key 时，请仅使用密钥 ID 或密钥 ARN。不支持 KMS 密钥的密钥别名格式。

目录存储桶不支持具有 Amazon Key Management Service（Amazon KMS）密钥的双层服务器端加密（DSSE-KMS），也不支持具有客户提供的加密密钥的服务器端加密（SSE-C）。

## 设置和监控目录存储桶的默认加密

默认设置情况下，Amazon S3 存储桶启用了存储桶加密，并且通过具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）来自动加密新对象。这种加密适用于您的 Amazon S3 存储桶中的所有新对象，并且不收取任何费用。

如果您需要对加密密钥进行更多控制，例如管理密钥轮换和访问策略授予，则可以选择使用具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）。

> **Note**
>
> - 我们建议存储桶的默认加密使用所需的加密配置，并且不要在 CreateSession 请求或 PUT 对象请求中覆盖存储桶默认加密。然后，使用所需的加密设置自动对新对象进行加密。有关目录存储桶中加密覆盖行为的更多信息，请参阅 Specifying server-side encryption with Amazon KMS for new object uploads。
> - 要使用 SSE-KMS 加密目录存储桶中的新对象，必须将具有 KMS 密钥（特别是客户自主管理型密钥）的 SSE-KMS 指定为目录存储桶的默认加密配置。然后，在为可用区端点 API 操作创建会话时，将在会话期间使用 SSE-KMS 和 S3 存储桶密钥自动加密和解密新对象。
> - 当您将默认存储桶加密设置为 SSE-KMS 时，将始终为目录存储桶中的 GET 和 PUT 操作启用 S3 存储桶密钥，并且不能禁用。当您通过 CopyObject、UploadPartCopy、批量操作中的 Copy 操作或 import 任务，将 SSE-KMS 加密的对象从通用存储桶复制到目录存

储桶、从目录存储桶复制到通用存储桶，或在目录存储桶之间复制时，不支持 S3 存储桶密钥。在这种情况下，每次对 KMS 加密的对象发出复制请求时，Amazon S3 都会调用 Amazon KMS。有关 S3 存储桶密钥如何降低 Amazon KMS 请求成本的更多信息，请参阅使用 Amazon S3 存储桶密钥降低 SSE-KMS 的成本。

- 当您在目录存储桶中指定用于加密的 Amazon KMS customer managed key 时，请仅使用密钥 ID 或密钥 ARN。不支持 KMS 密钥的密钥别名格式。
- 对于目录存储桶中的默认加密，不支持具有 Amazon KMS 密钥的双层服务器端加密（DSSE-KMS）和具有客户提供的密钥的服务器端加密（SSE-C）。

有关配置默认加密的更多信息，请参阅配置默认加密。

有关默认加密所需的权限的更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 PutBucketEncryption。

您可以使用 Amazon S3 控制台、Amazon SDK、Amazon S3 REST API 和 Amazon Command Line Interface（Amazon CLI）为 S3 存储桶配置 Amazon S3 默认加密。

使用 S3 控制台

在 Amazon S3 存储桶上配置默认加密

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 在 Buckets（存储桶）列表中，请选择您想要的存储桶的名称。
4. 选择属性选项卡。
5. 在服务器端加密设置下，目录存储桶使用具有 Amazon S3 托管式密钥（SSE-S3）的服务器端加密。
6. 选择保存更改。

使用 Amazon CLI

这些示例说明如何使用 SSE-S3 或将 SSE-KMS 与 S3 存储桶密钥结合使用来配置默认加密。

有关默认加密的更多信息，请参阅为 Amazon S3 存储桶设置默认服务器端加密行为。有关使用 Amazon CLI 配置默认加密的更多信息，请参阅 put-bucket-encryption。

Example – 使用 SSE-S3 进行默认加密

此示例使用 Amazon S3 托管密钥来配置默认存储桶加密。要使用该命令，请将####### 替换为您自己的信息。

```
aws s3api put-bucket-encryption --bucket bucket-base-name--zone-id--x-s3 --server-side-encryption-configuration '{
    "Rules": [
        {
            "ApplyServerSideEncryptionByDefault": {
                "SSEAlgorithm": "AES256"
            }
        }
    ]
}'
```

Example – 使用 S3 存储桶密钥通过 SSE-KMS 进行默认加密

此示例使用 S3 存储桶密钥通过 SSE-KMS 配置默认存储桶加密。要使用该命令，请将####### 替换为您自己的信息。

```
aws s3api put-bucket-encryption --bucket bucket-base-name--zone-id--x-s3 --server-side-encryption-configuration '{
    "Rules": [
            {
                "ApplyServerSideEncryptionByDefault": {
                    "SSEAlgorithm": "aws:kms",
                    "KMSMasterKeyID": "KMS-Key-ARN"
                },
                "BucketKeyEnabled": true
            }
        ]
    }'
```

使用 REST API

使用 REST API PutBucketEncryption 操作可设置默认加密，要使用的服务器端加密类型为 SSE-S3 或 SSE-KMS。

有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 PutBucketEncryption。

使用 Amazon SDK

使用 Amazon SDK 时，您可以请求 Amazon S3 使用 Amazon KMS keys 进行服务器端加密。以下适用于 Java 和 .NET 的 Amazon SDK 示例使用 SSE-KMS 和 S3 存储桶密钥为目录存储桶配置默认加密配置。有关其它 SDK 的信息，请参阅 Amazon 开发人员中心上的示例代码和库。

> **Important**
>
> 在 Amazon S3 中使用 Amazon KMS key 进行服务器端加密时，您必须选择对称加密 KMS 密钥。Amazon S3 仅支持对称加密 KMS 密钥。有关这些密钥的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的对称加密 KMS 密钥。

Java

使用Amazon SDK for Java 2.x，可以通过 `applyServerSideEncryptionByDefault` 方法来指定目录存储桶的默认加密配置（也即使用 SSE-KMS 进行数据加密），从而请求 Amazon S3 使用 Amazon KMS key。可以创建对称加密 KMS 密钥并在请求中指定该密钥。

```
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.PutBucketEncryptionRequest;
import software.amazon.awssdk.services.s3.model.ServerSideEncryption;
import software.amazon.awssdk.services.s3.model.ServerSideEncryptionByDefault;
import software.amazon.awssdk.services.s3.model.ServerSideEncryptionConfiguration;
import software.amazon.awssdk.services.s3.model.ServerSideEncryptionRule;

public class Main {
    public static void main(String[] args) {
        S3Client s3 = S3Client.create();
        String bucketName = "bucket-base-name--zoneid--x-s3";
        String kmsKeyId = "your-kms-customer-managed-key-id";

        // AWS managed KMS keys aren't supported. Only customer-managed keys are
 supported.
        ServerSideEncryptionByDefault serverSideEncryptionByDefault =
 ServerSideEncryptionByDefault.builder()
                .sseAlgorithm(ServerSideEncryption.AWS_KMS)
                .kmsMasterKeyID(kmsKeyId)
                .build();

        // The bucketKeyEnabled field is enforced to be true.
```

```
        ServerSideEncryptionRule rule = ServerSideEncryptionRule.builder()
                .bucketKeyEnabled(true)
                .applyServerSideEncryptionByDefault(serverSideEncryptionByDefault)
                .build();

        ServerSideEncryptionConfiguration serverSideEncryptionConfiguration =
 ServerSideEncryptionConfiguration.builder()
                .rules(rule)
                .build();

        PutBucketEncryptionRequest putRequest = PutBucketEncryptionRequest.builder()
                .bucket(bucketName)

 .serverSideEncryptionConfiguration(serverSideEncryptionConfiguration)
                .build();

        s3.putBucketEncryption(putRequest);

    }
}
```

有关创建客户托管密钥的更多信息，请参阅 Amazon Key Management Service 开发人员指南中的对 Amazon KMS API 进行编程。

有关上传对象的工作代码示例，请参阅以下主题。要使用这些示例，您必须更新这些代码示例并提供加密信息，如上述代码片段所示。

- 有关在单个操作中上传对象，请参阅 将对象上传到目录存储桶。
- 有关分段上传 API 操作，请参阅对目录桶使用分段上传。

.NET

使用适用于 .NET 的 Amazon SDK，可以通过 `ServerSideEncryptionByDefault` 属性来指定目录存储桶的默认加密配置（也即使用 SSE-KMS 进行数据加密），从而请求 Amazon S3 使用 Amazon KMS key。可以创建对称加密客户自主管理型密钥并在请求中指定该密钥。

```
    // Set the bucket server side encryption to use AWSKMS with a customer-managed
 key id.
    // bucketName: Name of the directory bucket. "bucket-base-name--zonsid--x-s3"
```

```
    // kmsKeyId: The Id of the customer managed KMS Key. "your-kms-customer-managed-
key-id"
    // Returns True if successful.
    public static async Task<bool> SetBucketServerSideEncryption(string bucketName,
 string kmsKeyId)
    {
        var serverSideEncryptionByDefault = new ServerSideEncryptionConfiguration
        {
            ServerSideEncryptionRules = new List<ServerSideEncryptionRule>
            {
                new ServerSideEncryptionRule
                {
                    ServerSideEncryptionByDefault = new
 ServerSideEncryptionByDefault
                    {
                        ServerSideEncryptionAlgorithm =
 ServerSideEncryptionMethod.AWSKMS,
                        ServerSideEncryptionKeyManagementServiceKeyId = kmsKeyId
                    }
                }
            }
        };
        try
        {
            var encryptionResponse =await _s3Client.PutBucketEncryptionAsync(new
 PutBucketEncryptionRequest
            {
                BucketName = bucketName,
                ServerSideEncryptionConfiguration = serverSideEncryptionByDefault,
            });

            return encryptionResponse.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (AmazonS3Exception ex)
        {
            Console.WriteLine(ex.ErrorCode == "AccessDenied"
                ? $"This account does not have permission to set encryption on
 {bucketName}, please try again."
                : $"Unable to set bucket encryption for bucket {bucketName},
 {ex.Message}");
        }
        return false;
    }
```

有关创建客户托管密钥的更多信息，请参阅 Amazon Key Management Service 开发人员指南中的对 Amazon KMS API 进行编程。

有关上传对象的工作代码示例，请参阅以下主题。要使用这些示例，您必须更新这些代码示例并提供加密信息，如上述代码片段所示。

- 有关在单个操作中上传对象，请参阅 将对象上传到目录存储桶。
- 有关分段上传 API 操作，请参阅对目录桶使用分段上传。

使用 Amazon CloudTrail 监控目录存储桶的默认加密

可以使用 Amazon CloudTrail 事件跟踪 Amazon S3 目录存储桶的默认加密配置请求。CloudTrail 日志中使用以下 API 事件名称：

- `PutBucketEncryption`
- `GetBucketEncryption`
- `DeleteBucketEncryption`

> **Note**
>
> - 目录存储桶不支持 EventBridge。
> - 目录存储桶不支持具有 Amazon Key Management Service（Amazon KMS）密钥的双层服务器端加密（DSSE-KMS），也不支持具有客户提供的加密密钥的服务器端加密（SSE-C）。

有关使用 Amazon CloudTrail 监控默认加密的更多信息，请参阅使用 Amazon CloudTrail 和 Amazon EventBridge 监控默认加密。

## 在目录存储桶中使用具有 Amazon KMS 密钥的服务器端加密（SSE-KMS）

Amazon KMS 中的安全控制可帮助您满足与加密相关的合规性要求。可以选择将目录存储桶配置为使用具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS），并

使用这些 KMS 密钥保护您在 Amazon S3 目录存储桶中的数据。有关 SSE-KMS 的更多信息，请参阅使用具有 Amazon KMS 密钥的服务器端加密（SSE-KMS）。

权限

要将使用 Amazon KMS key加密的对象上传到 Amazon S3 或从 Amazon S3 中下载该对象，您需要对密钥具有 `kms:GenerateDataKey` 和 `kms:Decrypt` 权限。有关更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的允许密钥用户使用 KMS 密钥进行加密操作。有关分段上传所需的 Amazon KMS 权限的信息，请参阅分段上传 API 和权限。

有关用于 SSE-KMS 的 KMS 密钥的更多信息，请参阅使用 Amazon KMS (SSE-KMS) 指定服务器端加密。

主题

- Amazon KMS keys
- 对跨账户操作使用 SSE-KMS
- Amazon S3 存储桶密钥
- 需要 SSE-KMS
- 加密上下文
- 发送对 Amazon KMS 加密对象的请求
- 审计目录存储桶中的 SSE-KMS 加密
- 为目录存储桶中的新对象上传指定具有 Amazon KMS 的服务器端加密（SSE-KMS）

Amazon KMS keys

在存储桶的生命周期内，SSE-KMS 配置只能支持每个目录存储桶 1 个 customer managed key。Amazon 托管式密钥 (`aws/s3`) 不受支持。此外，在为 SSE-KMS 指定客户自主管理型密钥后，无法覆盖存储桶的 SSE-KMS 配置的客户自主管理型密钥。

可以通过以下方式，确定您为存储桶的 SSE-KMS 配置指定的客户自主管理型密钥：

- 您发出 `HeadObject` API 操作请求以查找响应中 `x-amz-server-side-encryption-aws-kms-key-id` 的值。

要对数据使用新的客户自主管理型密钥，我们建议使用新的客户自主管理型密钥将现有对象复制到新的目录存储桶中。

当您在目录存储桶中指定用于加密的 Amazon KMS customer managed key 时，请仅使用密钥 ID 或密钥 ARN。不支持 KMS 密钥的密钥别名格式。

有关用于 SSE-KMS 的 KMS 密钥的更多信息，请参阅Amazon KMS keys。

对跨账户操作使用 SSE-KMS

在对目录存储桶中的跨账户操作使用加密时，请注意以下事项：

- 如果您希望授予对 S3 对象的跨账户访问权限，请配置客户自主管理型密钥的策略，以支持从其它账户进行访问。
- 要指定客户自主管理型密钥，必须使用完全限定的 KMS 密钥 ARN。

Amazon S3 存储桶密钥

始终为目录存储桶中的 GET 和 PUT 操作启用 S3 存储桶密钥，并且不能禁用。当您通过 CopyObject、UploadPartCopy、批量操作中的 Copy 操作或 import 任务，将 SSE-KMS 加密的对象从通用存储桶复制到目录存储桶、从目录存储桶复制到通用存储桶，或在目录存储桶之间复制时，不支持 S3 存储桶密钥。在这种情况下，每次对 KMS 加密的对象发出复制请求时，Amazon S3 都会调用 Amazon KMS。

对于除 CopyObject 和 UploadPartCopy 之外的可用区端点（对象级）API 操作，可以通过 CreateSession 验证请求和为请求授权，以实现低延迟。我们建议存储桶的默认加密使用所需的加密配置，并且不要在 CreateSession 请求或 PUT 对象请求中覆盖存储桶默认加密。然后，使用所需的加密设置自动对新对象进行加密。要使用 SSE-KMS 加密目录存储桶中的新对象，必须将具有 KMS 密钥（特别是 customer managed key）的 SSE-KMS 指定为目录存储桶的默认加密配置。然后，在为可用区端点 API 操作创建会话时，将在会话期间使用 SSE-KMS 和 S3 存储桶密钥自动加密和解密新对象。有关目录存储桶中加密覆盖行为的更多信息，请参阅 Specifying server-side encryption with Amazon KMS for new object uploads。

S3 存储桶密钥在 Amazon S3 内限时使用，从而进一步减少了 Amazon S3 向 Amazon KMS 发出请求以完成加密操作的需求。有关使用 S3 存储桶密钥的更多信息，请参阅 Amazon S3 存储桶密钥和使用 Amazon S3 存储桶密钥降低 SSE-KMS 的成本。

需要 SSE-KMS

如果要求对特定目录存储桶中的所有对象使用 SSE-KMS，可以使用存储桶策略。例如，当您使用 CreateSession API 操作授予上传新对象的权限（PutObject、CopyObject 和 CreateMultipartUpload）时，如果 CreateSession 请求不包括用于请求 SSE-KMS 的 x-amz-

server-side-encryption-aws-kms-key-id 标头，则以下存储桶策略将拒绝向任何人授予上传对象权限 (s3express:CreateSession)。

```
{
   "Version":"2012-10-17",
   "Id":"UploadObjectPolicy",
   "Statement":[{
         "Sid":"DenyObjectsThatAreNotSSEKMS",
         "Effect":"Deny",
         "Principal":"*",
         "Action":"s3express:CreateSession",
         "Resource":"arn:aws:s3express:region:account-id:bucket/bucket-base-name--zone-id--x-s3/*",
         "Condition":{
            "Null":{
               "s3express:x-amz-server-side-encryption-aws-kms-key-id":"true"
            }
         }
      }
   ]
}
```

如要求使用特定 Amazon KMS key 对存储桶中的对象进行加密，可以使用 s3express:x-amz-server-side-encryption-aws-kms-key-id 条件键。要指定 KMS 密钥，必须使用 arn:aws:kms:*region*:*acct-id*:key/*key-id* 格式的键 Amazon 资源名称（ARN）。Amazon Identity and Access Management 不验证 s3express:x-amz-server-side-encryption-aws-kms-key-id 的字符串是否存在。Amazon S3 用于对象加密的 Amazon KMS 密钥 ID 必须与策略中的 Amazon KMS 密钥 ID 匹配，否则 Amazon S3 会拒绝请求。

有关如何将 SSE-KMS 用于新对象上传的更多信息，请参阅为目录存储桶中的新对象上传指定具有 Amazon KMS 的服务器端加密（SSE-KMS）。

有关目录存储桶的特定条件键的完整列表，请参阅使用 IAM 对区域端点 API 操作进行授权。

加密上下文

对于目录存储桶，加密上下文 是一组键值对，其中包含有关数据的上下文信息。不支持额外的加密上下文值。有关加密上下文的更多信息，请参阅加密上下文。

默认情况下，如果您在目录存储桶上使用 SSE-KMS，Amazon S3 将使用存储桶 Amazon 资源名称（ARN）作为加密上下文对：

```
arn:aws:s3express:region:account-id:bucket/bucket-base-name--zone-id--x-s3
```

确保 IAM 策略或 Amazon KMS 密钥策略使用存储桶 ARN 作为加密上下文。

可以选择通过在可用区端点 API 请求（例如 CreateSession）中使用 `x-amz-server-side-encryption-context` 标头，来提供显式加密上下文对。此标头的值是 UTF-8 编码的 JSON 的 Base64 编码字符串，其中包含作为键值对的加密上下文。对于目录存储桶，加密上下文必须与默认加密上下文 [即存储桶 Amazon 资源名称（ARN）] 相匹配。此外，由于加密上下文未加密，请确保它不包含敏感信息。

您可以使用加密上下文来标识和分类加密操作。还可以通过查看哪个目录存储桶 ARN 与哪个加密密钥一起使用，来使用默认加密上下文 ARN 值跟踪 Amazon CloudTrail 中的相关请求。

在 CloudTrail 日志文件的 `requestParameters` 字段中，如果您在目录存储桶上使用 SSE-KMS，则加密上下文值为存储桶的 ARN。

```
"encryptionContext": {
    "aws:s3express:arn": "arn:aws:s3:::arn:aws:s3express:region:account-
id:bucket/bucket-base-name--zone-id--x-s3"
}
```

此外，要在目录存储桶中使用 SSE-KMS 为对象加密，Amazon KMS CloudTrail 事件将记录存储桶 ARN 而不是对象 ARN。

发送对 Amazon KMS 加密对象的请求

只能通过 HTTPS（TLS）访问目录存储桶。此外，目录存储桶使用 Amazon 签名版本 4（SigV4）对请求进行签名。有关发送针对 Amazon KMS 加密对象的请求的更多信息，请参阅发送对 Amazon KMS 加密对象的请求。

如果对象使用 SSE-KMS，则不应对 `GET` 请求和 `HEAD` 请求发送加密请求标头。否则，您会收到 HTTP 400 错误请求错误。

审计目录存储桶中的 SSE-KMS 加密

要审计为 SSE-KMS 加密数据使用 Amazon KMS 密钥的情况，您可以使用 Amazon CloudTrail 日志。您可以深入了解自己的加密操作，例如 GenerateDataKey 和 Decrypt。CloudTrail 支持多种属性值来筛选您的搜索，包括事件名称、用户名和事件源。

主题


- 为目录存储桶中的新对象上传指定具有 Amazon KMS 的服务器端加密（SSE-KMS）


## 为目录存储桶中的新对象上传指定具有 Amazon KMS 的服务器端加密（SSE-KMS）

对于目录存储桶，要使用服务器端加密来加密您的数据，可以使用具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）（默认设置）或具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）。我们建议存储桶的默认加密使用所需的加密配置，并且不要在 `CreateSession` 请求或 PUT 对象请求中覆盖存储桶默认加密。然后，使用所需的加密设置自动对新对象进行加密。有关目录存储桶中加密覆盖行为的更多信息，请参阅 Specifying server-side encryption with Amazon KMS for new object uploads。

默认情况下，所有 Amazon S3 存储桶都配置了加密，所有上传到 S3 存储桶的新对象都会自动静态加密。具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）是 Amazon S3 中每个存储桶的默认加密配置。如果要为目录存储桶指定不同的加密类型，可以使用具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）。要使用 SSE-KMS 加密目录存储桶中的新对象，必须将具有 KMS 密钥（特别是 customer managed key）的 SSE-KMS 指定为目录存储桶的默认加密配置。Amazon 托管式密钥 (`aws/s3`) 不受支持。在存储桶的生命周期内，SSE-KMS 配置只能支持每个目录存储桶 1 个 customer managed key。在为 SSE-KMS 指定客户自主管理型密钥后，无法覆盖存储桶的 SSE-KMS 配置的客户自主管理型密钥。然后，当您使用 SSE-KMS 为新的对象指定服务器端加密设置时，必须确保加密密钥与您为目录存储桶的默认加密配置指定的客户自主管理型密钥相同。要对数据使用新的客户自主管理型密钥，我们建议使用新的客户自主管理型密钥将现有对象复制到新的目录存储桶中。

当您上传新对象或复制现有对象时，您可以应用加密。如果更改对象的加密，则会创建一个新对象来替换旧对象。

可以使用 REST API 操作、Amazon SDK 和 Amazon Command Line Interface（Amazon CLI）指定 SSE-KMS。

> **Note**
>
> - 对于目录存储桶，加密覆盖行为如下所示：
>   - 当您将 CreateSession 与 REST API 结合使用来验证可用区端点 API 请求并对其进行授权（CopyObject 和 UploadPartCopy 除外）时，仅当之前使用 SSE-KMS 指定了存储桶的默认加密时，才能将加密设置覆盖为 SSE-S3 或 SSE-KMS。

- 当您将 CreateSession 与 Amazon CLI 或 Amazon SDK 结合使用来验证可用区端点 API 请求并对其进行授权（CopyObject 和 UploadPartCopy 除外）时，您根本无法覆盖加密设置。
- 在发出 CopyObject 请求时，仅当之前使用 SSE-KMS 指定了存储桶的默认加密时，才能将加密设置覆盖为 SSE-S3 或 SSE-KMS。当您发出 UploadPartCopy 请求时，无法覆盖加密设置。

- 您可以在 Amazon S3 中使用多区域 Amazon KMS keys。但是，Amazon S3 目前将多区域密钥视为单区域密钥，且不使用密钥的多区域特征。有关更多信息，请参阅 Amazon Key Management Service 开发人员指南中的使用多区域密钥。
- 如果您希望使用其它账户拥有的 KMS 密钥，您必须有权使用该密钥。有关 KMS 密钥的跨账户权限的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的创建其他账户可以使用的 KMS 密钥。

使用 REST API

> **Note**
>
> 在存储桶的生命周期内，对于每个目录存储桶只支持 1 个 customer managed key。Amazon 托管式密钥 (aws/s3) 不受支持。将具有客户自主管理型密钥的 SSE-KMS 指定为存储桶的默认加密配置后，您无法更改存储桶的 SSE-KMS 配置的客户自主管理型密钥。

对于除 CopyObject 和 UploadPartCopy 之外的可用区端点（对象级）API 操作，可以通过 CreateSession 验证请求和为请求授权，以实现低延迟。我们建议存储桶的默认加密使用所需的加密配置，并且不要在 CreateSession 请求或 PUT 对象请求中覆盖存储桶默认加密。然后，使用所需的加密设置自动对新对象进行加密。要使用 SSE-KMS 加密目录存储桶中的新对象，必须将具有 KMS 密钥（特别是 customer managed key）的 SSE-KMS 指定为目录存储桶的默认加密配置。然后，在为可用区端点 API 操作创建会话时，将在会话期间使用 SSE-KMS 和 S3 存储桶密钥自动加密和解密新对象。有关目录存储桶中加密覆盖行为的更多信息，请参阅 Specifying server-side encryption with Amazon KMS for new object uploads。

在使用 REST API 的可用区端点 API 调用（CopyObject 和 UploadPartCopy 除外）中，您无法覆盖 CreateSession 请求中加密设置（x-amz-server-side-encryption、x-amz-server-side-encryption-aws-kms-key-id、x-amz-server-side-encryption-context 和 x-amz-server-side-encryption-bucket-key-enabled）的值。无需在可用区端点 API 调用中显式指

定这些加密设置值，Amazon S3 将使用 `CreateSession` 请求中的加密设置值来保护目录存储桶中的新对象。

> **Note**
>
> 当您使用 Amazon CLI 或 Amazon SDK 时，对于 `CreateSession`，会话令牌会自动刷新，以避免在会话到期时服务中断。Amazon CLI 或 Amazon SDK 将存储桶的默认加密配置用于 `CreateSession` 请求。不支持覆盖 `CreateSession` 请求中的加密设置值。此外，在可用区端点 API 调用（CopyObject 和 UploadPartCopy 除外）中，不支持覆盖 `CreateSession` 请求中加密设置的值。

对于 CopyObject，要使用 SSE-KMS 加密目录存储桶中新的对象副本，必须将具有 KMS 密钥（特别是 customer managed key）的 SSE-KMS 指定为目录存储桶的默认加密配置。然后，当您使用 SSE-KMS 为新的对象副本指定服务器端加密设置时，必须确保加密密钥与您为目录存储桶的默认加密配置指定的客户自主管理型密钥相同。对于 UploadPartCopy，要使用 SSE-KMS 加密目录存储桶中新的对象分段副本，必须将具有 KMS 密钥（特别是 customer managed key）的 SSE-KMS 指定为目录存储桶的默认加密配置。无法在 UploadPartCopy 请求标头中使用 SSE-KMS 为新的对象分段副本指定服务器端加密设置。此外，您在 CreateMultipartUpload 请求中提供的加密设置必须与目标存储桶的默认加密配置相匹配。

主题

- 支持 SSE-KMS 的 Amazon S3 REST API 操作
- 加密上下文（x-amz-server-side-encryption-context）
- Amazon KMS 密钥 ID（x-amz-server-side-encryption-aws-kms-key-id）
- S3 桶密钥（x-amz-server-side-encryption-aws-bucket-key-enabled）

## 支持 SSE-KMS 的 Amazon S3 REST API 操作

目录存储桶中的以下对象级 REST API 操作接受 `x-amz-server-side-encryption`、`x-amz-server-side-encryption-aws-kms-key-id` 和 `x-amz-server-side-encryption-context` 请求标头。

- CreateSession：当您使用可用区端点（对象级）API 操作（CopyObject 和 UploadPartCopy 除外）时，可以指定这些请求标头。
- PutObject – 使用 PUT API 操作上传数据时，您可以指定这些请求标头。

- CopyObject – 复制对象时，您同时具有源对象和目标对象。如果使用 CopyObject 操作传递 SSE-KMS 标头，这些标头仅应用于目标对象。
- CreateMultipartUpload – 使用分段上传 API 操作上传大型对象时，可以指定这些标头。您可以在 CreateMultipartUpload 请求中指定这些标头。

使用服务器端加密存储对象时，以下 REST API 操作的响应标头将返回 x-amz-server-side-encryption 标头。

- CreateSession
- PutObject
- CopyObject
- POST Object
- CreateMultipartUpload
- UploadPart
- UploadPartCopy
- CompleteMultipartUpload
- GetObject
- HeadObject

> **Important**
>
> - 如果您针对受 Amazon KMS 保护的对象发出 GET 和 PUT 请求时未使用传输层安全性协议（TLS）或签名版本 4，则所有这些请求都将失败。
> - 如果对象使用 SSE-KMS，则不应对 GET 请求和 HEAD 请求发送加密请求标头，否则将显示 HTTP 400 BadRequest 错误。

加密上下文（**x-amz-server-side-encryption-context**）

如果您指定 x-amz-server-side-encryption:aws:kms，Amazon S3 API 将支持您可选提供带有 x-amz-server-side-encryption-context 标头的显式加密上下文。对于目录存储桶，加密上下文是一组键值对，其中包含有关数据的上下文信息。该值必须与默认加密上下文 [即存储桶的 Amazon 资源名称（ARN）] 相匹配。不支持额外的加密上下文值。

有关目录存储桶中加密上下文的信息，请参阅加密上下文。有关加密上下文的一般信息，请参阅 Amazon Key Management Service 开发人员指南中的 Amazon Key Management Service 概念 - 加密上下文。

Amazon KMS 密钥 ID（**`x-amz-server-side-encryption-aws-kms-key-id`**）

您可以使用 `x-amz-server-side-encryption-aws-kms-key-id` 标头指定用于保护数据的客户自主管理型密钥的 ID。

在存储桶的生命周期内，SSE-KMS 配置只能支持每个目录存储桶 1 个 customer managed key。Amazon 托管式密钥 (`aws/s3`) 不受支持。此外，在为 SSE-KMS 指定客户自主管理型密钥后，无法覆盖存储桶的 SSE-KMS 配置的客户自主管理型密钥。

可以通过以下方式，确定您为存储桶的 SSE-KMS 配置指定的客户自主管理型密钥：

- 您发出 `HeadObject` API 操作请求以查找响应中 `x-amz-server-side-encryption-aws-kms-key-id` 的值。

要对数据使用新的客户自主管理型密钥，我们建议使用新的客户自主管理型密钥将现有对象复制到新的目录存储桶中。

有关目录存储桶中加密上下文的信息，请参阅Amazon KMS keys。

S3 桶密钥（**`x-amz-server-side-encryption-aws-bucket-key-enabled`**）

始终为目录存储桶中的 `GET` 和 `PUT` 操作启用 S3 存储桶密钥，并且不能禁用。当您通过 CopyObject、UploadPartCopy、批量操作中的 Copy 操作或 import 任务，将 SSE-KMS 加密的对象从通用存储桶复制到目录存储桶、从目录存储桶复制到通用存储桶，或在目录存储桶之间复制时，不支持 S3 存储桶密钥。在这种情况下，每次对 KMS 加密的对象发出复制请求时，Amazon S3 都会调用 Amazon KMS。有关目录存储桶中 S3 存储桶密钥的信息，请参阅加密上下文。

使用 Amazon CLI

> **Note**
>
> 当您使用 Amazon CLI 时，对于 `CreateSession`，会话令牌会自动刷新，以避免在会话到期时服务中断。不支持覆盖 `CreateSession` 请求的加密设置值。此外，在可用区端点 API 调用（CopyObject 和 UploadPartCopy 除外）中，不支持覆盖 `CreateSession` 请求中加密设置的值。

要使用 SSE-KMS 加密目录存储桶中的新对象，必须将具有 KMS 密钥（特别是客户自主管理型密钥）的 SSE-KMS 指定为目录存储桶的默认加密配置。然后，在为可用区端点 API 操作创建会话时，将在会话期间使用 SSE-KMS 和 S3 存储桶密钥自动加密和解密新对象。

要使用以下示例 Amazon CLI 命令，请将 *user input placeholders* 替换为您自己的信息。

当您上传新对象或复制现有对象时，可以指定使用具有 Amazon KMS 密钥的服务器端加密来加密数据。为此，请使用 `put-bucket-encryption` 命令将目录存储桶的默认加密配置设置为 SSE-KMS (`aws:kms`)。具体而言，就是将 `--server-side-encryption aws:kms` 标头添加到请求。使用 `--ssekms-key-id` *example-key-id* 添加您创建的客户托管式 Amazon KMS 密钥。如果您指定 `--server-side-encryption aws:kms`，则必须提供客户自主管理型密钥的 Amazon KMS 密钥 ID。目录存储桶不使用 Amazon 托管式密钥。有关示例命令，请参阅 使用 Amazon CLI。

然后，当您使用以下命令上传新对象时，Amazon S3 默认情况下使用存储桶默认加密设置来加密该对象。

```
aws s3api put-object --bucket bucket-base-name--zone-id--x-s3 --key example-object-key
 --body filepath
```

您不需要在可用区端点 API 操作命令中显式添加 `-\-bucket-key-enabled`。始终为目录存储桶中的 GET 和 PUT 操作启用 S3 存储桶密钥，并且不能禁用。当您通过 CopyObject、UploadPartCopy、批量操作中的 Copy 操作或 import 任务，将 SSE-KMS 加密的对象从通用存储桶复制到目录存储桶、从目录存储桶复制到通用存储桶，或在目录存储桶之间复制时，不支持 S3 存储桶密钥。在这种情况下，每次对 KMS 加密的对象发出复制请求时，Amazon S3 都会调用 Amazon KMS。

可以将对象从源存储桶（例如通用存储桶）复制到新的存储桶（例如目录存储桶），然后对目标对象使用 SSE-KMS 加密。为此，请使用 `put-bucket-encryption` 命令将目标存储桶（例如目录存储桶）的默认加密配置设置为 SSE-KMS (`aws:kms`)。有关示例命令，请参阅 使用 Amazon CLI。然后，当您使用以下命令复制对象时，Amazon S3 默认情况下使用存储桶默认加密设置来加密该对象。

```
aws s3api copy-object --copy-source amzn-s3-demo-bucket/example-object-key --
bucket bucket-base-name--zone-id--x-s3 --key example-object-key
```

使用 Amazon SDK

使用 Amazon SDK 时，您可以请求 Amazon S3 使用 Amazon KMS keys 进行服务器端加密。以下示例展示了如何将 SSE-KMS 与适用于 Java 和 .NET 的 Amazon SDK 结合使用。有关其它 SDK 的信息，请参阅 Amazon 开发人员中心上的示例代码和库。

> **Note**
>
> 当您使用 Amazon SDK 时，对于 `CreateSession`，会话令牌会自动刷新，以避免在会话到期时服务中断。不支持覆盖 `CreateSession` 请求的加密设置值。此外，在可用区端点 API 调用（CopyObject 和 UploadPartCopy 除外）中，不支持覆盖 `CreateSession` 请求中加密设置的值。
>
> 要使用 SSE-KMS 加密目录存储桶中的新对象，必须将具有 KMS 密钥（特别是客户自主管理型密钥）的 SSE-KMS 指定为目录存储桶的默认加密配置。然后，在为可用区端点 API 操作创建会话时，将在会话期间使用 SSE-KMS 和 S3 存储桶密钥自动加密和解密新对象。
>
> 有关使用 Amazon SDK 将目录存储桶的默认加密配置设置为 SSE-KMS 的更多信息，请参阅使用 Amazon SDK。

> **Important**
>
> 在 Amazon S3 中使用 Amazon KMS key 进行服务器端加密时，您必须选择对称加密 KMS 密钥。Amazon S3 仅支持对称加密 KMS 密钥。有关这些密钥的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的对称加密 KMS 密钥。

有关创建客户托管密钥的更多信息，请参阅 Amazon Key Management Service 开发人员指南中的对 Amazon KMS API 进行编程。

## 传输中加密

目录存储桶使用区域和可用区 API 端点。根据您使用的 Amazon S3 API 操作，需要区域端点或可用区端点。您可以通过网关虚拟私有云（VPC）端点访问区域端点和可用区端点。使用网关端点不会发生任何额外费用。要了解有关区域和可用区 API 端点的更多信息，请参阅目录存储桶的联网。

### 数据删除

您可以使用 Amazon S3 控制台、Amazon SDK、Amazon Command Line Interface（Amazon CLI）或 Amazon S3 REST API，直接从目录存储桶删除一个或多个对象。由于目录存储桶中的所有对象都会产生存储费用，因此建议您删除不再需要的对象。

删除存储在目录存储桶中的对象也会递归地删除所有父目录，前提是在要删除的对象之外，这些父目录不包含其他任何对象。

> **Note**
>
> S3 Express One Zone 不支持多重身份验证（MFA）删除和 S3 版本控制。

## 对请求进行身份验证和授权

默认情况下，目录存储桶为私有，只有被明确授予访问权限的用户才可以访问。目录存储桶的访问控制边界仅在存储桶级设置。与之相对，通用存储桶的访问控制边界可以在存储桶、前缀或对象标签级设置。这种不同意味着，对于 S3 Express One Zone 访问权限，目录存储桶是唯一可以包括在存储桶策略或 IAM 身份策略中的资源。

Amazon S3 Express One Zone 同时支持 Amazon Identity and Access Management（Amazon IAM）授权和基于会话的授权：

- 要在 S3 Express One Zone 中使用区域端点 API 操作（桶级或控制面板操作），请使用 IAM 授权模型，该模型不涉及会话管理。对于操作，将单独授予权限。有关更多信息，请参阅 使用 IAM 对区域端点 API 操作进行授权。
- 要使用可用区端点 API 操作（对象级或数据面板操作），但 `CopyObject` 和 `HeadBucket` 除外，可以使用 `CreateSession` API 操作来创建和管理会话，这些会话经过优化，可为数据请求提供低延迟的授权。要检索和使用会话令牌，您必须在基于身份的策略或存储桶策略中，允许对目录存储桶执行 `s3express:CreateSession` 操作。有关更多信息，请参阅 使用 IAM 对区域端点 API 操作进行授权。如果您在 Amazon S3 控制台中通过 Amazon Command Line Interface（Amazon CLI）或使用 Amazon SDK 访问 S3 Express One Zone，S3 Express One Zone 会代表您创建会话。

使用 `CreateSession` API 操作时，可以通过新的基于会话的机制，对请求进行身份验证和授权。您可以使用 `CreateSession` 来请求临时凭证，以便提供对存储桶的低延迟访问。这些临时凭证的作用范围限制为特定的目录存储桶。

要使用 CreateSession，我们建议使用最新版本的 Amazon SDK 或者使用 Amazon Command Line Interface（Amazon CLI）。支持的 Amazon SDK 以及 Amazon CLI 代表您处理会话的建立、刷新和终止。

您可以使用会话令牌以及仅限可用区（对象级）的操作（CopyObject 和 HeadBucket 除外），在一个会话中的多个请求上分配与授权关联的延迟。对于区域端点 API 操作（存储桶级操作），您可以使用 IAM 授权，这不涉及对会话的管理。有关更多信息，请参阅使用 IAM 对区域端点 API 操作进行授权和使用 CreateSession 对可用区端点 API 操作进行授权。

## 如何对 API 操作进行身份验证和授权

下表列出了目录存储桶 API 操作的身份验证和授权信息。对于每个 API 操作，表中显示了 API 操作名称、IAM 策略操作、端点类型（区域或可用区）和授权机制（IAM 或基于会话）。此表还指出了是否支持跨账户访问。对存储桶级操作的访问权限，只能在基于 IAM 身份的策略（用户或角色）中授予，不能在存储桶策略中授予。

| API | 端点类型 | IAM 操作 | 跨账户访问 |
| --- | --- | --- | --- |
| CreateBucket | 区域性 | s3express:CreateBucket | 否 |
| DeleteBucket | 区域性 | s3express:DeleteBucket | 否 |
| ListDirectoryBuckets | 区域性 | s3express:ListAllMyDirectoryBuckets | 否 |
| PutBucketPolicy | 区域性 | s3express:PutBucketPolicy | 否 |
| GetBucketPolicy | 区域性 | s3express:GetBucketPolicy | 否 |
| DeleteBucketPolicy | 区域性 | s3express:DeleteBucketPolicy | 否 |
| CreateSession | 可用区 | s3express:CreateSession | 是 |
| CopyObject | 可用区 | s3express:CreateSession | 是 |
| DeleteObject | 可用区 | s3express:CreateSession | 是 |

| API | 端点类型 | IAM 操作 | 跨账户访问 |
| --- | --- | --- | --- |
| DeleteObjects | 可用区 | s3express:CreateSession | 是 |
| HeadObject | 可用区 | s3express:CreateSession | 是 |
| PutObject | 可用区 | s3express:CreateSession | 是 |
| GetObject Attributes | 可用区 | s3express:CreateSession | 是 |
| ListObjectsV2 | 可用区 | s3express:CreateSession | 是 |
| HeadBucket | 可用区 | s3express:CreateSession | 是 |
| CreateMultipartUpload | 可用区 | s3express:CreateSession | 是 |
| UploadPart | 可用区 | s3express:CreateSession | 是 |
| UploadPartCopy | 可用区 | s3express:CreateSession | 是 |
| CompleteMultipartUpload | 可用区 | s3express:CreateSession | 是 |
| AbortMultipartUpload | 可用区 | s3express:CreateSession | 是 |
| ListParts | 可用区 | s3express:CreateSession | 是 |
| ListMultipartUploads | 可用区 | s3express:CreateSession | 是 |
| ListAccessPointsForDirectoryBuckets | 可用区 | s3express:ListAccessPointsForDirectoryBuckets | 是 |

| API | 端点类型 | IAM 操作 | 跨账户访问 |
| --- | --- | --- | --- |
| GetAccessPointScope | 可用区 | s3express:GetAccessPointScope | 是 |
| PutAccessPointScope | 可用区 | s3express:PutAccessPointScope | 是 |
| DeleteAccessPointScope | 可用区 | s3express:DeleteAccessPointScope | 是 |

主题

- 使用 IAM 对区域端点 API 操作进行授权
- 使用 CreateSession 对可用区端点 API 操作进行授权

## 使用 IAM 对区域端点 API 操作进行授权

Amazon Identity and Access Management（IAM）是一项 Amazon Web Services 服务，有助于管理员安全地控制对 Amazon 资源的访问。IAM 管理员可控制哪些用户能够通过身份验证（登录）和获得授权（拥有权限），使用 S3 Express One Zone 中的 Amazon S3 资源。使用 IAM 不会产生额外的费用。

默认情况下，用户没有目录存储桶和 S3 Express One Zone 操作的权限。要授予对目录存储桶的访问权限，您可以使用 IAM 创建用户、组或角色，然后将权限附加到这些身份。有关 IAM 的更多信息，请参阅《IAM 用户指南》中的安全最佳实践。

要提供访问权限，您可以通过以下方法为用户、组或角色添加权限：

- Amazon IAM Identity Center 中的用户和组 – 创建权限集。按照《Amazon IAM Identity Center 用户指南》中创建权限集的说明进行操作。
- 通过身份提供商在 IAM 中管理的用户 – 创建身份联合验证角色。按照《IAM 用户指南》中为第三方身份提供商创建角色（联合身份验证）的说明进行操作。
- IAM 角色和用户 – 创建您的用户可以代入的角色。请按照《IAM 用户指南》的创建向 IAM 用户委派权限的角色中的说明进行操作。

有关为 S3 Express One Zone 设置 IAM 的更多信息，请参阅以下主题。

主题


- 主体
- 资源
- 目录存储桶的操作
- 目录存储桶的条件键
- 目录存储桶的 IAM 基于身份的策略
- 目录存储桶的存储桶策略示例


主体

创建基于资源的策略以授予对存储桶的访问权限时，您必须使用 `Principal` 元素来指定可请求对该资源执行某个操作或运算的人员或应用程序。对于目录存储桶策略，您可以使用以下主体：

- Amazon 账户
- IAM 用户
- IAM 角色
- 联合用户

有关更多信息，请参阅 IAM 用户指南中的 Principal。

资源

目录存储桶的 Amazon 资源名称（ARN）包含 `s3express` 命名空间、Amazon Web Services 区域、Amazon 账户 ID 和目录存储桶名称（包括可用区 ID）。要访问目录存储桶并对其执行操作，您必须使用以下 ARN 格式：

```
arn:aws:s3express:region:account-id:bucket/base-bucket-name--zone-id--x-s3
```

有关更多信息，请参阅《IAM 用户指南》中的 Amazon Resource Names (ARNs)。有关资源的更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：Resource。

目录存储桶的操作

在基于 IAM 身份的策略或基于资源的策略中，您可以定义要允许或拒绝的 S3 操作。这些操作对应于特定的 API 操作。使用目录存储桶时，您可以使用 S3 Express One Zone 命名空间来授予权限。此命名空间是 `s3express`。

当您允许 `s3express:CreateSession` 权限时，这会让 `CreateSession` API 操作能够在访问可用区端点 API（或对象级）操作时检索会话令牌。这些会话令牌返回的凭证用于授予对其他所有可用区端点 API 操作的访问权限。因此，您不必使用 IAM 策略授予对可用区 API 操作的访问权限，而是通过会话令牌来允许访问。有关区域端点 API 操作和权限的列表，请参阅对请求进行身份验证和授权。

有关可用区和区域端点 API 操作的更多信息，请参阅 目录存储桶的联网。要了解有关 `CreateSession` API 操作的更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 CreateSession。

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 Amazon 中执行操作的权限。当您在策略中使用一项操作时，通常会允许或拒绝使用具有相同名称的 API 操作。但在某些情况下，单个操作可控制对多个 API 操作的访问。对存储桶级操作的访问权限，只能在基于 IAM 身份的策略（用户或角色）中授予，不能在存储桶策略中授予。

> **Note**
>
> 如果要使用目录存储桶的接入点来控制对存储桶或对象操作的访问权限，请注意以下几点：
>
> - 有关使用接入点控制对存储桶操作的访问权限的信息，请参阅目录存储桶的接入点策略中的存储桶操作。
> - 有关使用接入点控制对于对象操作的访问权限的信息，请参阅目录存储桶的接入点策略中的对象操作。
> - 有关如何配置接入点策略的更多信息，请参阅配置 IAM 策略以使用目录存储桶的接入点。

下表显示了相应的操作和条件键。

| 操作 | API | 描述 | 访问级别 | 条件键 |
| --- | --- | --- | --- | --- |
| `s3express:CreateBucket` | `CreateBucket` | 授予权限以创建新的存储桶。 | 写入 | `s3express:authType` |

| 操作 | API | 描述 | 访问级别 | 条件键 |
| --- | --- | --- | --- | --- |
| | | | | s3express:LocationName<br>s3express:ResourceAccount<br>s3express:signatureversion<br>s3express:TlsVersion<br>s3express:x-amz-content-sha256 |

| 操作 | API | 描述 | 访问级别 | 条件键 |
| --- | --- | --- | --- | --- |
| s3express:CreateSession | 可用区端点 API 操作 | 授予权限以创建会话令牌，该令牌用于授予对所有可用区（对象级）API 操作的访问权限，例如 CopyObject 、PutObject 、GetObject 、HeadBucket 等。 | 写入 | s3express:authType<br><br>s3express:SessionMode<br><br>s3express:ResourceAccount<br><br>s3express:signatureversion<br><br>s3express:signatureAge<br><br>s3express:TlsVersion<br><br>s3express:x-amz-content-sha256<br><br>s3express:x-amz-server-side-encryption<br><br>s3express:x-amz-server-side |

| 操作 | API | 描述 | 访问级别 | 条件键 |
| --- | --- | --- | --- | --- |
| | | | | -encryption-aws-kms-key-id |
| s3express:DeleteBucket | DeleteBucket | 授予权限以删除在 URI 中指定的存储桶。 | 写入 | s3express:authType<br><br>s3express:ResourceAccount<br><br>s3express:signatureversion<br><br>s3express:TlsVersion<br><br>s3express:x-amz-content-sha256 |

| 操作 | API | 描述 | 访问级别 | 条件键 |
| --- | --- | --- | --- | --- |
| s3express:DeleteBucketPolicy | DeleteBucketPolicy | 授予权限以删除指定存储桶上的策略。 | 权限管理 | s3express:authType<br><br>s3express:ResourceAccount<br><br>s3express:signatureversion<br><br>s3express:TlsVersion<br><br>s3express:x-amz-content-sha256 |

| 操作 | API | 描述 | 访问级别 | 条件键 |
| --- | --- | --- | --- | --- |
| s3express:GetBucketPolicy | GetBucketPolicy | 授予权限以返回指定存储桶的策略。 | 读取 | s3express:authType<br>s3express:ResourceAccount<br>s3express:signatureversion<br>s3express:TlsVersion<br>s3express:x-amz-content-sha256 |

| 操作 | API | 描述 | 访问级别 | 条件键 |
| --- | --- | --- | --- | --- |
| s3express:GetEncryptionConfiguration | GetBucketEncryption | 授予权限以返回目录存储桶的默认加密配置。 | 读取 | s3express:authType<br><br>s3express:ResourceAccount<br><br>s3express:signatureversion<br><br>s3express:TlsVersion<br><br>s3express:x-amz-content-sha256 |

| 操作 | API | 描述 | 访问级别 | 条件键 |
| --- | --- | --- | --- | --- |
| s3express:ListAllMyDirectoryBuckets | ListDirectoryBuckets | 授予权限，以列出由已通过身份验证的请求发出方拥有的所有目录存储桶。 | 列表 | s3express:authType<br><br>s3express:ResourceAccount<br><br>s3express:signatureversion<br><br>s3express:TlsVersion<br><br>s3express:x-amz-content-sha256 |

| 操作 | API | 描述 | 访问级别 | 条件键 |
| --- | --- | --- | --- | --- |
| s3express:PutBucketPolicy | PutBucketPolicy | 授予权限以在存储桶上添加或替换存储桶策略。 | 权限管理 | s3express:authType<br><br>s3express:ResourceAccount<br><br>s3express:signatureversion<br><br>s3express:TlsVersion<br><br>s3express:x-amz-content-sha256 |

| 操作 | API | 描述 | 访问级别 | 条件键 |
| --- | --- | --- | --- | --- |
| s3express:PutBucketPolicy | PutBucketPolicy | 授予权限以在存储桶上添加或替换存储桶策略。 | 权限管理 | s3express:authType<br>s3express:ResourceAccount<br>s3express:signatureversion<br>s3express:TlsVersion<br>s3express:x-amz-content-sha256 |

| 操作 | API | 描述 | 访问级别 | 条件键 |
| --- | --- | --- | --- | --- |
| s3express:PutEncryptionConfiguration | PutBucketEncryption 或 DeleteBucketEncryption | 授予权限以设置目录存储桶的加密配置 | 写入 | s3express:authType<br><br>s3express:ResourceAccount<br><br>s3express:signatureversion<br><br>s3express:TlsVersion<br><br>s3express:x-amz-content-sha256 |

| 操作 | API | 描述 | 访问级别 | 条件键 |
| --- | --- | --- | --- | --- |
| s3express:CreateAccessPoint | CreateAccessPoint | 授予创建与目录存储桶关联的接入点的权限。 | 写入 | s3express:DataAccessPointAccount<br><br>s3express:DataAccessPointArn<br><br>s3express:AccessPointNetworkOrigin<br><br>s3express:authType<br><br>s3express:LocationName<br><br>s3express:ResourceAccount<br><br>s3express:signatureversion<br><br>s3express:TlsVersion<br><br>s3express:x-amz-content-sha256 |

| 操作 | API | 描述 | 访问级别 | 条件键 |
| --- | --- | --- | --- | --- |
| s3express:ListAccessPointsForDirectoryBuckets | ListAccessPointsForDirectoryBuckets | 授予列出接入点的权限。 | 列表 | s3express:authType<br><br>s3express:ResourceAccount<br><br>s3express:signatureversion<br><br>s3express:TlsVersion<br><br>s3express:x-amz-content-sha256 |

| 操作 | API | 描述 | 访问级别 | 条件键 |
| --- | --- | --- | --- | --- |
| s3express:GetAccessPoint | GetAccessPoint | 授予返回有关指定接入点的配置信息的权限。 | 读取 | s3express:DataAccessPointAccount<br><br>s3express:DataAccessPointAccount<br><br>s3express:DataAccessPointArn<br><br>s3express:AccessPointNetworkOrigin<br><br>s3express:authType<br><br>s3express:ResourceAccount<br><br>s3express:signatureversion<br><br>s3express:TlsVersion<br><br>s3express:x-amz-content-sha256 |

| 操作 | API | 描述 | 访问级别 | 条件键 |
| --- | --- | --- | --- | --- |
| s3express:DeleteAccessPoint | DeleteAccessPoint | 授予删除在 URI 中命名的接入点的权限。 | 写入 | s3express:DataAccessPointAccount<br><br>s3express:DataAccessPointAccount<br><br>s3express:DataAccessPointArn<br><br>s3express:AccessPointNetworkOrigin<br><br>s3express:authType<br><br>s3express:ResourceAccount<br><br>s3express:signatureversion<br><br>s3express:TlsVersion<br><br>s3express:x-amz-content-sha256 |

| 操作 | API | 描述 | 访问级别 | 条件键 |
| --- | --- | --- | --- | --- |
| s3express:DeleteAccessPointPolicy | DeleteAccessPointPolicy | 授予删除指定接入点上的策略的权限。 | 权限管理 | s3express:DataAccessPointAccount<br>s3express:DataAccessPointArn<br>s3express:AccessPointNetworkOrigin<br>s3express:authType<br>s3express:ResourceAccount<br>s3express:signatureversion<br>s3express:TlsVersion<br>s3express:x-amz-content-sha256 |

| 操作 | API | 描述 | 访问级别 | 条件键 |
| --- | --- | --- | --- | --- |
| s3express:GetAccessPointPolicy | GetAccessPointPolicy | 授予返回与指定接入点关联的接入点策略的权限。 | 读取 | s3express:DataAccessPointAccount<br><br>s3express:DataAccessPointAccount<br><br>s3express:DataAccessPointArn<br><br>s3express:AccessPointNetworkOrigin<br><br>s3express:authType<br><br>s3express:ResourceAccount<br><br>s3express:signatureversion<br><br>s3express:TlsVersion<br><br>s3express:x-amz-content-sha256 |

| 操作 | API | 描述 | 访问级别 | 条件键 |
| --- | --- | --- | --- | --- |
| s3express:PutAccessPointPolicy | PutAccessPointPolicy | 授予将接入点策略与指定接入点关联的权限。 | 权限管理 | s3express:DataAccessPointAccount<br><br>s3express:DataAccessPointArn<br><br>s3express:AccessPointNetworkOrigin<br><br>s3express:authType<br><br>s3express:ResourceAccount<br><br>s3express:signatureversion<br><br>s3express:TlsVersion<br><br>s3express:x-amz-content-sha256 |

| 操作 | API | 描述 | 访问级别 | 条件键 |
| --- | --- | --- | --- | --- |
| s3express:DeleteAccessPointScope | DeleteAccessPointScope | 授予删除指定接入点上的范围配置的权限。 | 权限管理 | s3express:DataAccessPointAccount<br><br>s3express:DataAccessPointArn<br><br>s3express:AccessPointNetworkOrigin<br><br>s3express:authType<br><br>s3express:ResourceAccount<br><br>s3express:signatureversion<br><br>s3express:TlsVersion<br><br>s3express:x-amz-content-sha256 |

| 操作 | API | 描述 | 访问级别 | 条件键 |
| --- | --- | --- | --- | --- |
| s3express:GetAccessPointScope | GetAccessPointScope | 授予返回与指定接入点关联的范围配置的权限。 | 读取 | s3express:DataAccessPointAccount<br><br>s3express:DataAccessPointArn<br><br>s3express:AccessPointNetworkOrigin<br><br>s3express:authType<br><br>s3express:ResourceAccount<br><br>s3express:signatureversion<br><br>s3express:TlsVersion<br><br>s3express:x-amz-content-sha256 |

| 操作 | API | 描述 | 访问级别 | 条件键 |
| --- | --- | --- | --- | --- |
| s3express:PutAccessPointScope | PutAccessPointScope | 授予将接入点与指定的接入点范围配置相关联的权限。 | 权限管理 | s3express:DataAccessPointAccount<br><br>s3express:DataAccessPointArn<br><br>s3express:AccessPointNetworkOrigin<br><br>s3express:authType<br><br>s3express:ResourceAccount<br><br>s3express:signatureversion<br><br>s3express:TlsVersion<br><br>s3express:x-amz-content-sha256 |

目录存储桶的条件键

以下是可用于 IAM 策略的 Condition 元素的条件键。您可以使用这些键进一步细化应用策略语句的条件。

| 条件键 | 描述 | 类型 |
| --- | --- | --- |
| s3express:authType | 按身份验证方法筛选访问。要限定传入的请求使用特定的身份认证方法，您可以使用此可选条件键。例如，您可以使用此条件键以仅允许在请求身份认证中使用 HTTP Authorization 标头。<br><br>有效值：REST-HEADER 、REST-QUERY-STRING | 字符串 |
| s3express:LocationName | 按特定的可用区 ID（AZ ID）筛选对 CreateBucket API 操作的访问权限，例如 usw2-az1。<br><br>示例值：usw2-az1 | 字符串 |
| s3express:ResourceAccount | 按资源拥有者的 Amazon Web Services 账户 ID 筛选访问权限。<br><br>要限制用户、角色或应用程序对特定 Amazon Web Services 账户 ID 所拥有的目录桶的访问权限，您可以使用 aws:ResourceAccount 或 s3express:ResourceAccount 条件键。您可以在 Amazon Identity and Access Management（IAM）身份策略或虚拟私有云（VPC）端点策略中使用此条件键。例如，您可以使用此条件键来限制 VPC 内的客户端访问非您拥有的桶。<br><br>示例值：111122223333 | 字符串 |
| s3express:SessionMode | 按照 CreateSession API 操作请求的权限来筛选访问权限。默认情况下，会话为 ReadWrite 。您可以使用此条件键将访问权限限制为 ReadOnly，或者明确拒绝 ReadWrite 访问。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的目录存储桶的存储桶策略示例和 CreateSession。 | 字符串 |

| 条件键 | 描述 | 类型 |
| --- | --- | --- |
| | 有效值：ReadWrite 、ReadOnly | |
| s3express:signatureAge | 按请求签名的生存期（以毫秒为单位）筛选访问。此条件仅适用于预签名 URL。<br><br>在 Amazon 签名版本 4 中，签名密钥的有效期最长为 7 天。因此，签名的有效期最初也为 7 天。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 签名请求简介。您可以使用此条件进一步限制签名有效期。<br><br>示例值：600000 | 数值 |
| s3express:signatureversion | 标识您希望支持的 Amazon 签名的版本，以将其用于经过身份验证的请求。对于经过身份验证的请求，支持签名版本 4。<br><br>有效值："AWS4-HMAC-SHA256" （标识签名版本 4） | 字符串 |
| s3express:TlsVersion | 按客户端使用的 TLS 版本筛选访问权限。<br><br>您可以使用 s3:TlsVersion 条件键来编写 IAM、虚拟私有云端点（VPCE）或桶策略，以便根据客户端使用的 TLS 版本，限制用户或应用程序对目录桶的访问权限。您还可以使用此条件键来编写具有最低 TLS 版本要求的策略。<br><br>示例值：1.3 | 数值 |

| 条件键 | 描述 | 类型 |
| --- | --- | --- |
| s3express:x-amz-content-sha256 | 按存储桶中未签名内容筛选访问权限。<br><br>您可以使用此条件键禁止存储桶中未签名的内容。<br><br>使用签名版本 4 时，对于使用 Authorization 标头的请求，您需要在签名计算中添加 x-amz-content-sha256 标头，然后将其值设置为哈希负载。<br><br>您可以在存储桶策略中使用此条件键来拒绝上传任何未签名的有效负载。例如：<br><br>• 拒绝使用 Authorization 标头对请求进行身份认证，但未对有效负载进行签名的上传。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的在单个区块中传输有效负载。<br>• 拒绝使用预签名 URL 的上传。预签名 URL 始终有一个 UNSIGNED_PAYLOAD 。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的对请求进行身份认证和身份认证方法。<br><br>有效值：UNSIGNED-PAYLOAD | 字符串 |
| s3express:x-amz-server-side-encryption | 通过服务器端加密来筛选访问<br><br>有效值："AWS256"、aws:kms | 字符串 |
| s3express:x-amz-server-side-encryption-aws-kms-key-id | 通过将 Amazon KMS 客户自主管理型密钥用于服务器端加密来筛选访问<br><br>示例值："arn:aws:kms: *region*:*acct-id*:key/*key-id*" | ARN |

### 目录存储桶的 IAM 基于身份的策略

在创建目录存储桶之前，您必须向 Amazon Identity and Access Management（IAM）角色或用户授予必要的权限。此示例策略允许使用 `CreateSession` API 操作 [用于可用区端点（对象级）API 操作] 和所有区域端点（存储桶级）API 操作。此策略允许将 `CreateSession` API 操作用于所有目录存储桶，但仅允许将区域端点 API 操作用于指定的目录存储桶。要使用此示例策略，请将 *`user input placeholders`* 替换为您自己的信息。

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Sid": "AllowAccessRegionalEndpointAPIs",
             "Effect": "Allow",
             "Action": [
                 "s3express:DeleteBucket",
                 "s3express:DeleteBucketPolicy",
                 "s3express:CreateBucket",
                 "s3express:PutBucketPolicy",
                 "s3express:GetBucketPolicy",
                 "s3express:ListAllMyDirectoryBuckets"
             ],

             "Resource": "arn:aws:s3express:region:account_id:bucket/bucket-base-
name--zone-id--x-s3/*"
         },
         {
             "Sid": "AllowCreateSession",
             "Effect": "Allow",
             "Action": "s3express:CreateSession",
             "Resource": "*"
         }
     ]
 }
```

### 目录存储桶的存储桶策略示例

本节提供存储桶策略示例。要使用这些策略，请将 *`user input placeholders`* 替换为您自己的信息。

以下示例存储桶策略允许 Amazon Web Services 账户 ID *111122223333* 在指定目录存储桶的默认 `ReadWrite` 会话中使用 `CreateSession` API 操作。此策略授予对可用区端点（对象级）API 操作的访问权限。

Example – 允许通过默认 **`ReadWrite`** 会话执行 **`CreateSession`** 调用的存储桶策略

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadWriteAccess",
            "Effect": "Allow",
            "Resource": "arn:aws:s3express:us-west-2:account-id:bucket/bucket-base-name--zone-id--x-s3",
            "Principal": {
                "AWS": [
                    "111122223333"
                ]
            },
            "Action": [
                "s3express:CreateSession"
            ]
        }
    ]
}
```

Example – 允许通过 **`ReadOnly`** 会话执行 **`CreateSession`** 调用的存储桶策略

以下示例存储桶策略允许 Amazon Web Services 账户 ID *111122223333* 使用 `CreateSession` API 操作。此策略使用 `s3express:SessionMode` 条件键以及 `ReadOnly` 值来设置只读会话。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadOnlyAccess",
            "Effect": "Allow",
            "Principal": {
                "AWS": "111122223333"
            },
```

```
            "Action": "s3express:CreateSession",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "s3express:SessionMode": "ReadOnly"
                }
            }
        }
    ]
}
```

Example – 允许 **CreateSession** 调用进行跨账户访问的存储桶策略

以下示例存储桶策略允许 Amazon Web Services 账户 ID *111122223333* 在由 Amazon Web Services 账户 ID *444455556666* 拥有的指定目录存储桶中，使用 CreateSession API 操作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CrossAccount",
            "Effect": "Allow",
            "Principal": {
                "AWS": "111122223333"
            },
            "Action": [
                "s3express:CreateSession"
            ],
            "Resource": "arn:aws:s3express:us-west-2:444455556666:bucket/bucket-base-name--zone-id--x-s3"

        }
    ]
}
```

## 使用 **CreateSession** 对可用区端点 API 操作进行授权

要使用可用区端点 API 操作（对象级或数据面板操作），但 CopyObject 和 HeadBucket 除外，可以使用 CreateSession API 操作来创建和管理会话，这些会话经过优化，可为数据请求提供低延迟

的授权。要检索和使用会话令牌，您必须在基于身份的策略或存储桶策略中，允许对目录存储桶执行 `s3express:CreateSession` 操作。有关更多信息，请参阅 使用 IAM 对区域端点 API 操作进行授权。如果您在 Amazon S3 控制台中通过 Amazon Command Line Interface（Amazon CLI）或使用 Amazon SDK 访问 S3 Express One Zone，S3 Express One Zone 会代表您创建会话。

如果您使用 Amazon S3 REST API，则可以使用 `CreateSession` API 操作获取临时安全凭证，其中包括访问密钥 ID、秘密访问密钥、会话令牌和到期时间。临时凭证提供的权限与长期安全凭证（例如 IAM 用户凭证）相同，但临时安全凭证必须包括会话令牌。

会话模式

会话模式定义会话的范围。在存储桶策略中，您可以指定 `s3express:SessionMode` 条件密钥，以便控制谁可以创建 `ReadWrite` 或 `ReadOnly` 会话。有关 `ReadWrite` 或 `ReadOnly` 会话的更多信息，请参阅《Amazon S3 API 参考》中 CreateSession 的 `x-amz-create-session-mode` 参数。有关要创建的存储桶策略的更多信息，请参阅 目录存储桶的存储桶策略示例。

会话令牌

当您使用临时安全凭证进行调用时，调用必须包含会话令牌。会话令牌与临时凭证一起返回。会话令牌的范围仅限于您的目录存储桶，用于验证安全凭证是否有效且未过期。为了保护您的会话，临时安全凭证在 5 分钟后过期。

**`CopyObject` 和 `HeadBucket`**

临时安全凭证的范围限定为特定的目录存储桶，并且对于发送到给定目录存储桶的所有可用区（对象级）操作 API 调用，将自动启用临时安全凭证。与其他可用区端点 API 操作不同，`CopyObject` 和 `HeadBucket` 不使用 `CreateSession` 身份验证。所有 `CopyObject` 和 `HeadBucket` 请求都必须使用 IAM 凭证进行身份验证和签名。但是，`CopyObject` 和 `HeadBucket` 与其他可用区端点 API 操作一样，仍由 `s3express:CreateSession` 授权。

有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 CreateSession。

## 目录存储桶的安全最佳实践

使用目录存储桶时需要考虑的许多安全功能。以下最佳实操是一般准则，并不代表完整的安全解决方案。这些最佳实践可能不适合您的环境或不满足您的环境要求，请将其视为有用的建议而不是惯例。

### 默认屏蔽公共访问权限和对象所有权设置

目录存储桶支持 S3 屏蔽公共访问权限和 S3 对象所有权。这些 S3 功能用于审计和管理对存储桶及对象的访问。

默认情况下，所有的目录存储桶都启用了屏蔽公共访问权限设置。此外，对象所有权设置为强制存储桶拥有者，这意味着访问控制列表（ACL）已禁用。无法修改这些设置。有关使用这些功能的更多信息，请参阅the section called “阻止公有访问”和the section called “控制对象所有权”。

> **Note**
>
> 您无法授予对存储在目录存储桶中的对象的访问权限。您只能授予对目录存储桶的访问权限。S3 Express One Zone 的授权模式与 Amazon S3 的授权模式不同。有关更多信息，请参阅 使用 CreateSession 对可用区端点 API 操作进行授权。

## 身份验证和授权

根据您是向可用区端点 API 操作发出请求还是向区域端点 API 操作发出请求，目录存储桶的身份验证和授权机制会有所不同。可用区 API 操作是对象级（数据面板）操作。区域 API 操作是存储桶级（控制面板）操作。

您可以通过基于会话的全新机制，对针对可用区端点 API 操作的请求进行身份验证和授权，该机制经过优化，可提供极低的延迟。通过基于会话的身份验证，Amazon SDK 使用 `CreateSession` API 操作来请求临时凭证，以提供对目录存储桶的低延迟访问。这些临时凭证的作用范围限制为特定的目录存储桶，并在 5 分钟后过期。您可以使用这些临时凭证对可用区（对象级）API 调用签名。有关更多信息，请参阅 使用 CreateSession 对可用区端点 API 操作进行授权。

使用目录存储桶管理凭证对请求进行签名

您可以通过您的凭证，使用 Amazon 签名版本 4 并将 `s3express` 作为服务名称，对可用区端点（对象级）API 请求进行签名。在对请求签名时，请使用从 `CreateSession` 返回的密钥，还要通过 `x-amzn-s3session-token header` 提供会话令牌。有关更多信息，请参阅 CreateSession。

受支持的 Amazon SDK 负责管理凭证和签名事宜。我们建议使用 Amazon SDK 来刷新凭证并为您签名请求。

使用 IAM 凭证对请求签名

所有区域（存储桶级）API 调用都必须通过 Amazon Identity and Access Management（IAM）凭证（而不是临时会话凭证）进行身份验证和签名。IAM 凭证由 IAM 身份的访问密钥 ID 和秘密访问密钥组成。所有 `CopyObject` 和 `HeadBucket` 请求还必须使用 IAM 凭证进行身份验证和签名。

为了尽可能减少可用区（对象级）操作调用的延迟，我们建议使用通过调用 `CreateSession` 获得的凭证来对您的请求签名，但 `CopyObject` 和 `HeadBucket` 的请求除外。

## 使用 Amazon CloudTrail

Amazon CloudTrail 提供用户、角色或 Amazon Web Services 服务在 Amazon S3 中执行的操作的记录。您可以使用 CloudTrail 收集的信息确定以下事项：

- 向 Amazon S3 发出的请求
- 发出请求的 IP 地址
- 谁发出了请求
- 发出请求的时间
- 有关该请求的其他详细信息

当您设置 Amazon Web Services 账户时，CloudTrail 管理事件默认处于启用状态。以下区域端点 API 操作（存储桶级或控制面板 API 操作）将记录到 CloudTrail 中。

- CreateBucket
- DeleteBucket
- DeleteBucketPolicy
- PutBucketPolicy
- GetBucketPolicy
- ListDirectoryBuckets
- ListMultipartUploads
- PutBucketEncryption
- GetBucketEncryption
- DeleteBucketEncryption

> **Note**
>
> `ListMultipartUploads` 是可用区端点 API 操作。但是，它会作为管理事件记录到 CloudTrail 中。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 ListMultipartUploads。

默认情况下，CloudTrail 跟踪不记录数据事件，但您可以将跟踪配置为记录您指定的目录存储桶的数据事件，或记录您的 Amazon 账户中所有目录存储桶的数据事件。以下可用区端点 API 操作（对象级或数据面板 API 操作）将记录到 CloudTrail 中。

- AbortMultipartUpload
- CompleteMultipartUpload
- CreateSession
- CopyObject
- CreateMultipartUpload
- DeleteObject
- DeleteObjects
- GetObject
- GetObjectAttributes
- HeadBucket
- HeadObject
- ListObjectsV2
- ListParts
- PutObject
- UploadPart
- UploadPartCopy

有关将 Amazon CloudTrail 与目录存储桶配合使用的更多信息，请参阅使用 Amazon CloudTrail 对目录存储桶进行日志记录。

使用 Amazon 监控工具实施监控

监控是保持 Amazon S3 和您的 Amazon 解决方案的可靠性、安全性、可用性和性能的重要部分。Amazon 提供了一些可用来监控 Amazon S3 和您的其他 Amazon Web Services 服务的工具和服务。例如，您可以监控 Amazon S3 的 Amazon CloudWatch 指标，特别是 `BucketSizeBytes` 和 `NumberOfObjects` 存储指标。

存储在目录存储桶中的对象不会反映在 Amazon S3 的 `BucketSizeBytes` 和 `NumberOfObjects` 存储指标中。但是，目录存储桶支持 `BucketSizeBytes` 和 `NumberOfObjects` 存储指标。要查看您选择的指标，您可以通过指定 `StorageType` 维度来区分 Amazon S3 存储类。有关更多信息，请参阅使用 Amazon CloudWatch 监控指标。

有关更多信息，请参阅使用 Amazon CloudWatch 监控指标和Amazon S3 中的日志记录和监控。

# 通过接入点管理对目录存储桶中共享数据集的访问权限

访问点可简化对 Amazon S3 中的共享数据集的大规模数据访问管理。接入点是您创建的具有唯一性的主机名，用于对通过接入点发出的所有请求强制实施不同的权限和网络控制。您可以为每个存储桶创建数百个接入点，每个接入点都有不同的名称和为每个应用程序自定义的权限。每个接入点都与附加到底层存储桶的存储桶策略结合使用。

在目录存储桶中，接入点名称由您提供的基本名称组成，后跟区域 ID，然后为 `--xa-s3`。例如 *`accesspointname`*`--`*`zoneID`*`--xa-s3`。创建接入点后，无法更改名称或可用区 ID。仅在 Amazon 专用本地区域中才支持目录存储桶的接入点。

借助目录存储桶的接入点，可以使用接入点范围来限制对特定前缀或 API 操作的访问权限。可以指定任意数量的前缀，但所有前缀的字符总长度必须小于 256 字节。

为了限制 Amazon S3 数据访问提供网络，您可以将任何接入点配置为仅接受来自私有云（VPC）的请求。

在本节中，各主题说明了如何使用目录存储桶的接入点。有关目录存储桶的信息，请参阅使用目录存储桶。

主题

- 目录存储桶的接入点命名规则、限制和局限性
- 引用目录存储桶的接入点
- 目录存储桶的接入点的对象操作
- 配置 IAM 策略以使用目录存储桶的接入点
- 监控和记录目录存储桶的接入点
- 创建目录存储桶的接入点
- 管理目录存储桶的接入点

## 目录存储桶的接入点命名规则、限制和局限性

访问点可简化对 Amazon S3 中的共享数据集的大规模数据访问管理。以下主题提供有关接入点命名规则以及限制和局限性的信息。

主题

- 目录存储桶的接入点的命名规则
- 目录存储桶的接入点的限制和局限性


## 目录存储桶的接入点的命名规则

必须在存储桶所在的同一可用区中创建接入点。接入点名称在可用区内必须是唯一的。

接入点名称必须符合 DNS，并且必须满足以下条件：

- 必须以数字或小写字母开头
- 您提供的基本名称长度必须在 3 到 50 个字符之间
- 不能以连字符（-）开头或结尾
- 不能包含下划线 (_)、大写字母、空格或句点 (.)
- 必须以后缀 *zoneid*`--xa--s3` 结尾。

## 目录存储桶的接入点的限制和局限性

目录存储桶的接入点具有以下限制和局限性：

- 仅在 Amazon 专用本地区域中才支持目录存储桶的接入点。
- 每个接入点都与一个目录存储桶相关联。创建接入点后，您无法将它与另一个存储桶关联。但是，您可以删除接入点，然后创建一个同名的新接入点，并将其与另一个存储桶相关联。
- 创建接入点后，无法更改其 Virtual Private Cloud（VPC）配置。
- 接入点策略的大小限制为 20 KB。
- 接入点范围前缀的总大小限制为 256 字节。
- 每个 Amazon Web Services 区域中的每个 Amazon Web Services 账户最多可以创建 10000 个接入点。如果您需要在单个区域为一个账户使用超过 10000 个接入点，则可以请求增加服务限额。有关服务限额和请求增加限额的更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon 服务限额。
- 您只能使用接入点来执行对象操作。您不能使用接入点来执行 Amazon S3 存储桶操作，例如修改或删除存储桶。有关支持的操作的完整列表，请参阅目录存储桶的接入点的对象操作。
- 您可以按名称、接入点别名或虚拟托管类型 URI 来引用接入点。您无法按 ARN 对接入点进行寻址。有关更多信息，请参阅 引用目录存储桶的接入点。
- 控制接入点功能的 API 操作（例如 `PutAccessPointPolicy` 和 `GetAccessPointPolicy`）必须指定拥有该接入点的 Amazon 账户。

- 使用 REST API 向接入点发出请求时，必须使用 Amazon 签名版本 4。有关对请求进行身份验证的更多信息，请参阅《Amazon Simple Storage Service API 参考》中的验证请求（Amazon 签名版本 4）。
- 接入点仅支持通过 HTTPS 发出请求。对于通过 HTTP 发出的任何请求，Amazon S3 都会自动以 HTTP 重定向来进行响应，以便将请求升级到 HTTPS。
- 接入点不支持匿名访问。
- 如果您为其它账户拥有的存储桶创建接入点（跨账户接入点），则在存储桶拥有者授予您访问该存储桶的权限之前，该跨账户接入点不会授予您访问数据的权限。存储桶拥有者始终保留对数据访问的最终控制权，并且必须更新存储桶策略才能授权来自跨账户接入点的请求。要查看存储桶策略示例，请参阅配置 IAM 策略以使用目录存储桶的接入点。

## 引用目录存储桶的接入点

创建接入点后，您可以将其用作端点来执行对象操作。对于目录存储桶的接入点，接入点别名与接入点名称相同。您可以对所有数据操作使用接入点名称，而不是存储桶名称。有关这些支持的操作的列表，请参阅目录存储桶的接入点的对象操作。

### 通过虚拟托管类型 URI 引用接入点

访问点仅支持虚拟主机式寻址。接入点使用与目录存储桶端点相同的格式。有关更多信息，请参阅 目录存储桶的区域和可用区端点。

S3 接入点不支持通过 HTTP 进行访问。接入点仅支持通过 HTTPS 进行安全访问。

## 目录存储桶的接入点的对象操作

您可以使用接入点通过以下 S3 数据操作来访问对象。

- AbortMultipartUpload
- CompleteMultipartUpload
- CopyObject
- CreateMultipartUpload
- CreateSession
- DeleteObject
- DeleteObjects
- GetObject

- GetObjectAttributes
- HeadBucket
- HeadObject
- ListMultipartUploads
- ListObjectsV2
- ListParts
- PutObject
- UploadPart
- UploadPartCopy

## 配置 IAM 策略以使用目录存储桶的接入点

接入点支持 Amazon Identity and Access Management（IAM）资源策略，这些策略可让您按资源、用户或其它条件控制接入点的使用。要使应用程序或用户可通过接入点访问对象，接入点和底层存储桶策略都必须允许该请求。

> **Important**
>
> 当直接通过存储桶的名称访问目录存储桶时，向该存储桶添加接入点不会改变存储桶的行为。针对存储桶的所有现有操作将继续像以前一样运行。您在接入点策略或接入点范围中包括的限制仅适用于通过该接入点发出的请求。

使用 IAM 资源策略时，请确保在保存策略之前，解决来自 Amazon Identity and Access Management Access Analyzer 的安全警告、错误、一般警告和建议。IAM Access Analyzer 将根据 IAM 策略语法和最佳实践运行策略检查，以验证您的策略。这些检查项生成调查结果并提供建议，可帮助您编写可操作且符合安全最佳实践的策略。

要了解有关使用 IAM Access Analyzer 验证策略的更多信息，请参阅《IAM 用户指南》中的 IAM Access Analyzer 策略验证。要查看 IAM Access Analyzer 返回的警告、错误和建议的列表，请参阅 IAM Access Analyzer 策略检查引用。

### 目录存储桶的接入点策略示例

以下接入点策略演示了如何控制对目录存储桶的请求。接入点策略需要存储桶 ARN 或接入点 ARN。策略中不支持接入点别名。以下是接入点 ARN 的示例：

```
arn:aws:s3express:region:account-id:accesspoint/myaccesspoint--zoneID--xa-s3
```

您可以在接入点的详细信息中查看接入点 ARN。有关更多信息，请参阅 查看目录存储桶的接入点的详细信息。

> **Note**
>
> 在接入点策略中授予的权限仅在底层存储桶也允许相同的访问时才有效。您可以通过两种方式实现这一点：
>
> 1. （推荐）将存储桶的访问控制委派给接入点，如将访问控制委派到接入点中所述。
> 2. 将接入点策略中包含的权限添加到底层存储桶的策略中。

Example 1 – 将接入点限制为 VPC 网络起源的服务控制策略

以下服务控制策略要求使用虚拟私有云（VPC）网络起源创建所有新的接入点。实施此策略后，组织中的用户无法创建任何可通过互联网访问的接入点。

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Effect": "Deny",
        "Action": "s3express:CreateAccessPoint",
        "Resource": "*",
        "Condition": {
            "StringNotEquals": {
                "s3express:AccessPointNetworkOrigin": "VPC"
            }
        }
    }
  ]
}
```

Example 2 – 接入点策略，用于将存储桶访问权限限制为具有 VPC 网络来源的接入点

以下接入点策略将对存储桶 *amzn-s3-demo-bucket--zoneID--x-s3* 的所有访问权限限制为具有 VPC 网络来源的接入点内。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Principal": "*",
            "Action": "s3express:CreateSession",
            "Effect": "Deny",
            "Resource": "arn:aws:s3express:region:111122223333:bucket/amzn-s3-demo-
bucket--zoneID--x-s3",
            "Condition": {
                "StringNotEqualsIfExists": {
                    "s3express:AccessPointNetworkOrigin": "VPC"
                }
            }
        }
    ]
}
```

## 条件键

目录存储桶的接入点具有条件键，您可以在 IAM 策略中使用这些键来控制对资源的访问。以下条件键仅代表 IAM 策略的一部分。有关完整策略示例，请参阅目录存储桶的接入点策略示例、将访问控制委派到接入点和授予跨账户接入点的权限。

### s3express:DataAccessPointArn

此示例说明如何按接入点的 Amazon 资源名称（ARN）筛选访问权限，并匹配区域 *region* 中 Amazon Web Services 账户 *111122223333* 的所有接入点：

```
"Condition" : {
    "StringLike": {
        "s3express:DataAccessPointArn":
 "arn:aws:s3express:region:111122223333:accesspoint/*"
    }
}
```

### s3express:DataAccessPointAccount

此示例显示一个字符串运算符，您可以使用它匹配接入点拥有者的账户 ID。以下示例匹配 Amazon Web Services 账户 *111122223333* 拥有的所有接入点。

```
"Condition" : {
    "StringEquals": {
        "s3express:DataAccessPointAccount": "111122223333"
    }
}
```

### s3express:AccessPointNetworkOrigin

此示例显示一个字符串运算符，您可以使用它来匹配网络起源（Internet 或 VPC）。以下示例仅匹配起源为 VPC 的接入点。

```
"Condition" : {
    "StringEquals": {
        "s3express:AccessPointNetworkOrigin": "VPC"
    }
}
```

### s3express:Permissions

您可以使用 s3express:Permissions 来限制对接入点范围中特定 API 操作的访问权限。支持以下 API 操作：

- PutObject
- GetObject
- DeleteObject
- ListBucket（对于 ListObjectsV2 是必需的）
- GetObjectAttributes
- AbortMultipartUpload
- ListBucketMultipartUploads
- ListMultipartUploadParts

> **Note**
>
> 使用多值条件键时，我们建议您将 ForAllValues 与 Allow 语句结合使用，并将 ForAnyValue 与 Deny 语句结合使用。有关更多信息，请参阅《IAM 用户指南》中的多值上下文键。

有关在 Amazon S3 中使用条件键的更多信息，请参阅《Service Authorization Reference》中的 Actions, resources, and condition keys for Amazon S3。

有关 S3 资源类型对 S3 API 操作所需权限的更多信息，请参阅 Amazon S3 API 操作所需的权限。

## 将访问控制委派到接入点

您可以将访问控制从存储桶策略委派到接入点策略。以下示例存储桶策略允许对存储桶拥有者账户所拥有的所有接入点进行完全访问。在应用此策略后，对此存储桶的所有访问权限都由接入点策略控制。我们建议您以这种方式为所有不需要直接访问存储桶的使用案例配置存储桶。

Example 将访问控制委派给接入点的存储桶策略

```
{
    "Version": "2012-10-17",
    "Statement" : [
    {
        "Effect": "Allow",
        "Principal" : { "AWS": "*" },
        "Action" : "*",
        "Resource" : [ "Bucket ARN",
        "Condition": {
            "StringEquals" : { "s3express:DataAccessPointAccount" : "Bucket owner's
 account ID" }
        }
    }]
}
```

## 授予跨账户接入点的权限

要为另一个账户拥有的存储桶创建接入点，您必须首先通过指定存储桶名称和账户拥有者 ID 来创建接入点。然后，存储桶拥有者必须更新存储桶策略以授权来自接入点的请求。创建接入点与创建 DNS CNAME 类似，因为接入点不提供对存储桶内容的访问权限。所有存储桶访问权限均由存储桶策略控制。以下示例存储桶策略允许从受信任 Amazon Web Services 账户拥有的接入点对存储桶进行 GET 和 LIST 请求。

将 *Bucket ARN* 替换为桶的 ARN。

Example ：将权限委派给其它 Amazon Web Services 账户的存储桶策略

```
{
    "Version": "2012-10-17",
    "Statement" : [
    {
        "Effect": "Allow",
        "Principal" : { "AWS": "*" },
        "Action" : "s3express:CreateSession",
        "Resource" : [ "Bucket ARN" ],
        "Condition": {
            "StringEquals" : {
                "s3express:DataAccessPointAccount": "Access point owner's account ID"
            },
            "ForAllValues:StringEquals": {
                "s3express:Permissions": [
                    "GetObject",
                    "ListBucket"
                ]
            }
        }
    }]
}
```

## 监控和记录目录存储桶的接入点

可以通过使用 Amazon CloudTrail，记录通过接入点发出的请求和对管理接入点（如 `CreateAccessPoint` 和 `GetAccessPointPolicy`，）的 API 发出的请求。通过接入点发出的请求的 CloudTrail 日志条目将在日志的 `resources` 部分中包含接入点 ARN（其中包括接入点名称）。

例如，假设您有以下配置：

- 区域 `region` 中名为 *`amzn-s3-demo-bucket`*`--`*`zone-id`*`--x-s3` 的存储桶，包含名为 `my-image.jpg` 的对象。
- 与 *`amzn-s3-demo-bucket`*`--`*`zone-id`*`--x-s3` 关联且名为 `my-bucket-ap--zoneID--xa-s3` 的接入点
- `123456789012` 的 Amazon Web Services 账户 ID

以下示例显示了上述配置的CloudTrail 日志条目的 `resources` 部分：

```
"resources": [
        {"type": "AWS::S3Express::Object",
```

```
            "ARN": "arn:aws:s3express-region:123456789012:bucket/amzn-s3-demo-
bucket--zone-id--x-s3/my-image.jpg"
        },
        {"accountId": "c",
            "type": "AWS::S3Express::DirectoryBucket",
            "ARN": "arn:aws::s3express:region:123456789012:bucket/amzn-s3-demo-
bucket--zone-id--x-s3"
        },
        {"accountId": "123456789012",
            "type": "AWS::S3::AccessPoint",
            "ARN": "arn:aws:s3express:region:123456789012:accesspoint/my-bucket-ap--
zoneID--xa-s3"
        }
    ]
```

有关 Amazon CloudTrail 的更多信息，请参阅《Amazon CloudTrail 用户指南》中的什么是 Amazon CloudTrail？。

## 创建目录存储桶的接入点

您可以使用 Amazon CLI、REST API 或 Amazon SDK 为任何目录存储桶创建接入点。每个接入点都与单个目录存储桶相关联，并且可以为每个存储桶创建数百个接入点。创建接入点时，您可以选择接入点的名称以及要与之关联的目录存储桶。接入点名称由您提供的基本名称和包含存储桶位置的可用区 ID 的后缀组成，后跟 `--xa-s3`。例如 *myaccesspoint-zoneID*`--xa-s3`。

创建接入点时，还可以通过虚拟私有云（VPC）限制对接入点的访问。然后，您可以使用接入点的名称立即开始通过接入点读取和写入数据，就像使用目录存储桶名称一样。

创建接入点后，您可以配置接入点 IAM 资源策略，并使用接入点范围来限制对特定前缀或 API 操作或两者组合的访问权限。有关更多信息，请参阅 管理目录存储桶的接入点。

使用 Amazon CLI

以下示例命令为账户 *111122223333* 中的存储桶 *amzn-s3-demo-bucket--zone-id--x-s3* 创建了一个名为 *example-ap* 的接入点。

```
aws s3control create-access-point --name example-ap--zoneID--xa-s3 --account-
id 111122223333 --bucket amzn-s3-demo-bucket--zone-id--x-s3
```

要限制通过 VPC 访问接入点，请包括 `--vpc` 参数和 VPC ID。

```
aws s3control create-access-point --name example-ap--zoneID--xa-s3 --account-
id 111122223333 --bucket amzn-s3-demo-bucket--zone-id--x-s3 --vpc vpc-id
```

在为跨账户存储桶创建接入点时，请包含 --bucket-account-id 参数。以下示例命令在 Amazon Web Services 账户 *111122223333* 中，为存储桶 *amzn-s3-demo-bucket--zone-id--x-s3* 创建一个接入点（由 Amazon Web Services 账户 *444455556666* 拥有）。

```
aws s3control create-access-point --name example-ap--zoneID--xa-s3 --account-
id 111122223333 --bucket amzn-s3-demo-bucket--zone-id--x-s3 --bucket-account-
id 444455556666
```

有关更多信息和示例，请参阅《Amazon CLI Command Reference》中的 create-access-point。

使用 REST API

以下示例命令为账户 *111122223333* 中的存储桶 *amzn-s3-demo-bucket--zone-id--x-s3* 创建了一个名为 *example-ap* 的接入点，并通过 VPC *vpc-id* 限制访问权限（可选）。

```
PUT /v20180820/accesspoint/example-ap--zoneID--xa-s3 HTTP/1.1
Host: s3express-control.region.amazonaws.com
x-amz-account-id: 111122223333
<?xml version="1.0" encoding="UTF-8"?>
<CreateAccessPointRequest>
   <Bucket>amzn-s3-demo-bucket--zone-id--x-s3s</Bucket>
   <BucketAccountId>111122223333</BucketAccountId>
   <VpcConfiguration>
       <VpcId>vpc-id</VpcId>
   </VpcConfiguration>
</CreateAccessPointRequest>
```

响应：

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<CreateAccessPointResult>
   <AccessPointArn>
       "arn:aws:s3express:region:111122223333:accesspoint/example-ap--zoneID--xa-s3"
   </AccessPointArn>
```

```
   <Alias>example-ap--zoneID--xa-s3</Alias>
</CreateAccessPointResult>
```

使用 Amazon SDK

可以使用 Amazon SDK 创建接入点。有关更多信息，请参阅《Amazon Simple Storage Service API Reference》中的 list of supported SDKs。

# 管理目录存储桶的接入点

本节介绍如何使用 Amazon Command Line Interface、Amazon S3 REST API 或 Amazon SDK 来管理目录存储桶的接入点。

主题


- 列出目录存储桶的接入点
- 查看目录存储桶的接入点的详细信息
- 查看、编辑或删除接入点策略
- 管理目录存储桶的接入点的范围
- 删除目录存储桶的接入点


## 列出目录存储桶的接入点

本节说明如何使用 Amazon Command Line Interface（Amazon CLI）、REST API 或 Amazon SDK 来列出目录存储桶的接入点。

使用 Amazon CLI

以下 `list-access-points-for-directory-buckets` 示例命令显示了如何使用 Amazon CLI 来列出由 Amazon 账户拥有且与目录存储桶关联的接入点。

以下命令列出了 Amazon Web Services 账户 *111122223333* 的附加到存储桶 *amzn-s3-demo-bucket--zone-id--x-s3* 的接入点。

```
aws s3control list-access-points-for-directory-buckets --account-id 111122223333 --
directory-bucket amzn-s3-demo-bucket--zone-id--x-s3
```

有关更多信息和示例，请参阅《Amazon CLI Command Reference》中的 list-access-points-for-directory-buckets。

使用 REST API

以下示例显示了如何使用 REST API 列出您的接入点。

```
GET /v20180820/directoryaccesspoint?directoryBucket=amzn-s3-demo-bucket--zone-id--x-s3
&maxResults=maxResults HTTP/1.1
Host: s3express-control.region.amazonaws.com
x-amz-account-id: 111122223333
```

Example ：**ListAccessPointsForDirectoryBuckets** 响应

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<ListDirectoryAccessPointsResult>
    <AccessPointList>
        <AccessPoint>
            <AccessPointArn>arn:aws:s3express:region:111122223333:accesspoint/example-
access-point--zoneID--xa-s3</AccessPointArn>
            <Alias>example-access-point--zoneID--xa-s3</Alias>
            <Bucket>amzn-s3-demo-bucket--zone-id--x-s3</Bucket>
            <BucketAccountId>111122223333</BucketAccountId>
            <Name>example-access-point--zoneID--xa-s3</Name>
            <NetworkOrigin>VPC</NetworkOrigin>
            <VpcConfiguration>
                <VpcId>VPC-1</VpcId>
            </VpcConfiguration>
        </AccessPoint>
    </AccessPointList>
</ListDirectoryAccessPointsResult>
```

使用 Amazon SDK

可以使用 Amazon SDK 列出接入点。有关更多信息，请参阅《Amazon Simple Storage Service API Reference》中的 list of supported SDKs。

## 查看目录存储桶的接入点的详细信息

本节介绍如何使用 Amazon Command Line Interface或 REST API 查看目录存储桶的接入点的详细信息。

使用 Amazon CLI

以下 `get-access-point` 示例命令显示了如何使用 Amazon CLI 来查看接入点的详细信息。

以下命令列出了 Amazon Web Services 账户 *111122223333* 的接入点 *my-access-point--zoneID--xa-s3* 的详细信息。

```
aws s3control get-access-point --name my-access-point--zoneID--xa-s3 --account-
id 111122223333
```

Example **`get-access-point`** 命令的输出

```
{
    "Name": "example-access-point--zoneID--xa-s3",
    "Bucket": "amzn-s3-demo-bucket--zone-id--x-s3",
    "NetworkOrigin": "Internet",
    "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": true,
        "IgnorePublicAcls": true,
        "BlockPublicPolicy": true,
        "RestrictPublicBuckets": true
    },
    "CreationDate": "2025-04-23T18:26:22.146000+00:00",
    "Alias": "example-access-point--zoneID--xa-s3",
    "AccessPointArn": "arn:aws:s3express:region:111122223333:accesspoint/example-
access-point--zoneID--xa-s3",
    "BucketAccountId": "296805379465"
}
```

有关更多信息和示例，请参阅《Amazon CLI 命令参考》中的 get-access-point。

使用 REST API

可以使用 REST API 查看接入点的详细信息。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 GetAccessPoint。

使用 Amazon SDK

可以使用 Amazon SDK 查看接入点的详细信息。有关更多信息，请参阅《Amazon Simple Storage Service API Reference》中的 list of supported SDKs。

## 查看、编辑或删除接入点策略

您可以使用 Amazon Identity and Access Management（IAM）接入点策略来控制可以访问接入点的主体和资源。接入点范围管理接入点的前缀和 API 权限。可以使用 Amazon Command Line Interface、REST API 或 Amazon SDK 创建、编辑和删除接入点策略。有关接入点范围的更多信息，请参阅管理目录存储桶的接入点的范围。

> **Note**
>
> 由于目录存储桶使用基于会话的授权，因此策略必须始终包含 `s3express:CreateSession` 操作。

使用 Amazon CLI

可以使用 `get-acccess-point-policy`、`put-access-point-policy` 和 `delete-access-point-policy` 命令来查看、编辑或删除接入点策略。有关更多信息，请参阅《Amazon CLI Command Reference》中的 get-access-point-policy、put-access-point-policy 或 delete-access-point-policy。

使用 REST API

可以使用 REST API `GetAccessPointPolicy`、`DeleteAccessPointPolicy` 和 `PutAccessPointPolicy` 操作来查看、删除或编辑接入点策略。有关更多信息，请参阅《Amazon Simple Storage Service API Reference》中的 PutAccessPointPolicy、GetAccessPointPolicy 或 DeleteAccessPointPolicy。

使用 Amazon SDK

您可以使用 Amazon SDK 来查看、删除或编辑接入点策略。有关更多信息，请参阅《Amazon Simple Storage Service API Reference》中的 GetAccessControlPolicy、DeleteAccessControlPolicy 和 PutAccessControlPolicy 支持的 SDK 列表。

## 管理目录存储桶的接入点的范围

本节介绍如何使用 Amazon Command Line Interface、REST API 或 Amazon SDK 来查看和修改目录存储桶的接入点的范围。可以使用接入点范围来限制对特定前缀或 API 操作的访问。

主题


- 查看目录存储桶的接入点的范围

- 修改目录存储桶的接入点的范围
- 删除目录存储桶的接入点的范围

### 查看目录存储桶的接入点的范围

您可以使用 Amazon Command Line Interface、REST API 或 Amazon SDK 来查看目录存储桶的接入点的范围。

#### 使用 Amazon CLI

以下 `get-access-point-scope` 示例命令显示了如何使用 Amazon CLI 来查看接入点的范围。

以下命令显示了 Amazon Web Services 账户 *111122223333* 的接入点 *my-access-point--zoneID*--xa-s3 的范围。

```
aws s3control get-access-point-scope --name my-access-point--zoneID--xa-s3 --account-id 111122223333
```

有关更多信息和示例，请参阅《Amazon CLI Command Reference》中的 get-access-point-scope。

Example ：**`get-access-point-scope`** 的结果

```
{
    "Scope": {
        "Permissions": [
            "ListBucket",
            "PutObject"
        ]
  "Prefixes": [
            "Prefix": "MyPrefix1*",
            "Prefix": "MyObjectName.csv"
        ]
    }
}
```

#### 使用 REST API

以下 `GetAccessPointScope` 示例请求显示了如何使用 REST API 来查看接入点的范围。

以下请求显示了 Amazon Web Services 账户 *111122223333* 的接入点 *my-access-point*--*region*-*zoneID*--xa-s3 的范围。

```
GET /v20180820/accesspoint/my-access-point--zoneID--xa-s3/scope HTTP/1.1
Host: s3express-control.region.amazonaws.com
x-amz-account-id: 111122223333
```

Example ：**GetAccessPointScope** 的结果

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<GetAccessPointScopeResult>
    <Scope>
        <Prefixes>
            <Prefix>MyPrefix1*</Prefix>
            <Prefix>MyObjectName.csv</Prefix>
        </Prefixes>
        <Permissions>
            <Permission>ListBucket</Permission>
            <Permission>PutObject</Permission>
        </Permissions>
        <Scope>
</GetAccessPointScopeResult>
```

使用 Amazon SDK

可以使用 Amazon SDK 来查看接入点的范围。有关更多信息，请参阅《Amazon Simple Storage Service API Reference》中的 list of supported SDKs。

修改目录存储桶的接入点的范围

可以使用 Amazon Command Line Interface、REST API 或 Amazon SDK 来修改目录存储桶的接入点的范围。接入点范围用于限制对特定前缀、API 操作或两者组合的访问。

您可以包含以下一个或多个 API 操作作为权限：

- `PutObject`
- `GetObject`

- DeleteObject
- ListBucket（对于 ListObjectsV2 是必需的）
- GetObjectAttributes
- AbortMultipartUploads
- ListBucketMultipartUploads
- ListMultipartUploadParts

> **Note**
>
> - 您可以指定任意数量的前缀，但所有前缀的字符总长度的大小必须小于 256 字节。
> - 修改接入点的范围时，将替换现有范围。

使用 Amazon CLI

以下 put-access-point-scope 示例命令显示了如何使用 Amazon CLI 来修改接入点的范围。

以下命令修改 Amazon Web Services 账户 *111122223333* 的 *my-access-point*--*zoneID*--xa-s3 的接入点范围。

> **Note**
>
> 您可以使用星号（*）字符在前缀中使用通配符。如果要将星号字符用作文字，请在它之前添加一个反斜杠字符（\）以对它进行转义。
> 此外，所有前缀都有一个隐含的“*”结尾，这意味着所有带有该前缀的路径都将被包括在内。

```
aws s3control put-access-point-scope --name my-access-point--zoneID--xa-s3 --account-
id 111122223333 --scope Prefixes=string,Permissions=string
```

有关更多信息和示例，请参阅《Amazon CLI Command Reference》中的 put-access-point-scope。

使用 REST API

以下 PutAccessPointScope 示例请求显示了如何使用 REST API 来修改接入点的范围。

以下请求修改 Amazon Web Services 账户 *111122223333* 的 *my-access-point*--*zoneID*--xa-s3 的接入点范围。

> **Note**
>
> 您可以使用星号（*）字符在前缀中使用通配符。如果要将星号字符用作文字，请在它之前添加一个反斜杠字符（\）以对它进行转义。
> 此外，所有前缀都有一个隐含的“*”结尾，这意味着所有带有该前缀的路径都将被包括在内。

```
PUT /v20180820/accesspoint/my-access-point--zoneID--xa-s3/scope HTTP/1.1
Host: s3express-control.region.amazonaws.com
x-amz-account-id: 111122223333
<?xml version="1.0" encoding="UTF-8"?>
<PutAccessPointScopeRequest>
        <Scope>
            <Prefixes>
                <Prefix>Jane/*</Prefix>
            </Prefixes>
            <Permissions>
                <Permission>PutObject</Permission>
                <Permission>GetObject</Permission>
            </Permissions>
            <Scope>
    </PutAccessPointScopeRequest>
```

使用 Amazon SDK

可以使用 Amazon CLI、Amazon SDK 或 REST API 来修改接入点的范围。有关更多信息，请参阅《Amazon Simple Storage Service API Reference》中的 list of supported SDKs。

删除目录存储桶的接入点的范围

可以使用 Amazon Command Line Interface、REST API 或 Amazon SDK 来删除目录存储桶的接入点的范围。

> **Note**
>
> 删除接入点的范围时，将删除所有前缀和权限。

使用 Amazon CLI

以下 `delete-access-point-scope` 示例命令显示了如何使用 Amazon CLI 来删除接入点的范围。

以下命令删除 Amazon Web Services 账户 *111122223333* 的接入点 *my-access-point*--*zoneID*--xa-s3 的范围。

```
aws s3control delete-access-point-scope --name my-access-point--region-zoneID--xa-s3 --
account-id 111122223333
```

有关更多信息和示例，请参阅《Amazon CLI Command Reference》中的 delete-access-point-scope。

使用 REST API

以下请求删除 Amazon Web Services 账户 *111122223333* 的接入点 *my-access-point*--*zoneID*--xa-s3 的范围。

```
DELETE /v20180820/accesspoint/my-access-point--zoneID--xa-s3/scope HTTP/1.1
Host: s3express-control.region.amazonaws.com
x-amz-account-id: 111122223333
```

使用 Amazon SDK

可以使用 Amazon SDK 来删除接入点的范围。有关更多信息，请参阅《Amazon Simple Storage Service API Reference》中的 list of supported SDKs。

## 删除目录存储桶的接入点

本节介绍如何使用 Amazon Command Line Interface、REST API 或 Amazon SDK 来删除接入点。

> **Note**
>
> 在删除附加到接入点的目录存储桶之前，必须先删除该接入点。

使用 Amazon CLI

以下 `delete-access-point` 示例命令显示了如何使用 Amazon CLI 删除接入点。

以下命令删除 Amazon Web Services 账户 *111122223333* 的接入点 *my-access-point--zoneID*--xa-s3。

```
aws s3control delete-access-point --name my-access-point--zoneID--xa-s3 --account-
id 111122223333
```

有关更多信息和示例，请参阅《Amazon CLI 命令参考》中的 delete-access-point。

使用 REST API

可以使用 REST API 来删除接入点。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 DeleteAccessPoint。

使用 Amazon SDK

可以使用 Amazon SDK 来删除接入点。有关更多信息，请参阅《Amazon Simple Storage Service API Reference》中的 list of supported SDKs。

# 使用 Amazon CloudTrail 对目录存储桶进行日志记录

Amazon S3 与 Amazon CloudTrail 集成，后者是一项提供由用户、角色或 Amazon 服务所采取操作的记录的服务。CloudTrail 将 Amazon S3 的所有 API 调用作为事件捕获。借助通过 CloudTrail 收集的信息，您可以确定向 Amazon S3 发出哪些请求、发出请求的 IP 地址、请求的发出时间以及其它详细信息。当 Amazon S3 中发生受支持的事件活动时，该活动将记录在 CloudTrail 事件中。可以使用 Amazon CloudTrail 跟踪来记录目录存储桶的管理事件和数据事件。有关更多信息，请参阅 Amazon S3 CloudTrail 事件和《Amazon CloudTrail 用户指南》中的 What is Amazon CloudTrail?

## 目录存储桶的 CloudTrail 管理事件

默认情况下，CloudTrail 将目录存储桶的存储桶级操作记录为管理事件。目录存储桶的 CloudTrail 管理事件的 `eventsource` 是 `s3express.amazonaws.com`。当您设置 Amazon 账户时，CloudTrail 管理事件默认处于启用状态。以下区域端点 API 操作（存储桶级或控制面板 API 操作）将记录到 CloudTrail 中。

- `CreateBucket`
- `DeleteBucket`
- `DeleteBucketPolicy`
- `PutBucketPolicy`
- `GetBucketPolicy`

- ListDirectoryBuckets
- ListMultipartUploads
- GetBucketEncryption
- PutBucketEncryption
- DeleteBucketEncryption

> **Note**
>
> ListMultipartUploads 是可用区端点 API 操作。但是，此 API 操作会作为管理事件记录到 CloudTrail 中。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 ListMultipartUploads。

有关 CloudTrail 管理事件的更多信息，请参阅《Amazon CloudTrail 用户指南》中的 Logging management events。

## 目录存储桶的 CloudTrail 数据事件

数据事件可提供对资源或在资源中所执行资源操作（例如，读取或写入 Amazon S3 对象）的相关信息。这些也称为数据层面操作。数据事件通常是高容量活动。默认情况下，CloudTrail 跟踪不记录数据事件，但您可以将跟踪配置为记录存储在通用存储桶和目录存储桶中的对象的数据事件。有关更多信息，请参阅使用控制台为存储桶中的对象启用日志记录功能。

在 CloudTrail 中记录跟踪的数据事件时，您可以选择使用高级事件选择器或基本事件选择器。要记录存储在目录存储桶中的对象的数据事件，必须使用高级事件选择器。配置高级资源选择器时，您将需要选择或指定资源类型，即 Amazon::S3Express::Object。

以下可用区端点 API 操作（对象级或数据面板 API 操作）将记录到 CloudTrail 中。

- AbortMultipartUpload
- CompleteMultipartUpload
- CreateSession
- CopyObject
- CreateMultipartUpload
- DeleteObject
- DeleteObjects

- GetObject
- GetObjectAttributes
- HeadBucket
- HeadObject
- ListObjectsV2
- ListParts
- PutObject
- UploadPart
- UploadPartCopy

有关 CloudTrail 数据事件的更多信息，请参阅《Amazon CloudTrail 用户指南》中的 Logging data events。

有关目录存储桶的 CloudTrail 事件的更多信息，请参阅以下主题：

主题

- 目录存储桶的 CloudTrail 日志文件示例

## 目录存储桶的 CloudTrail 日志文件示例

CloudTrail 日志文件包括有关所请求 API 操作的信息、操作的日期和时间和请求参数等。本主题介绍目录存储桶的 CloudTrail 数据事件和管理事件示例。

主题

- 目录存储桶的 CloudTrail 数据事件日志文件示例

### 目录存储桶的 CloudTrail 数据事件日志文件示例

下面的示例显示了一个 CloudTrail 日志文件示例，该示例演示了 CreateSession。

```
{
    "eventVersion": "1.09",
    "userIdentity": {
      "type": "AssumedRole",
      "principalId": "AROAIDPPEZS35WEXAMPLE:AssumedRoleSessionName",
      "arn": "arn:aws:sts::111122223333assumed-role/RoleToBeAssumed/MySessionName",
```

```
          "accountId": "111122223333",
          "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
          "sessionContext": {
            "sessionIssuer": {
              "type": "Role",
              "principalId": "AROAIDPPEZS35WEXAMPLE",
              "arn": "arn:aws:iam::111122223333:role/RoleToBeAssumed",
              "accountId": "111122223333",
              "userName":"RoleToBeAssumed
            },

            "attributes": {
              "creationDate": "2024-07-02T00:21:16Z",
            "mfaAuthenticated": "false"
            }
          }
        },
        "eventTime": "2024-07-02T00:22:11Z",
        "eventSource": "s3express.amazonaws.com",
        "eventName": "CreateSession",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "72.21.198.68",
        "userAgent": "aws-sdk-java/2.20.160-SNAPSHOT
 Linux/5.10.216-225.855.amzn2.x86_64 OpenJDK_64-Bit_Server_VM/11.0.23+9-LTS
 Java/11.0.23 vendor/Amazon.com_Inc. md/internal exec-env/AWS_Lambda_java11 io/sync
 http/Apache cfg/retry-mode/standard",
        "requestParameters": {
          "bucketName": "bucket-base-name--usw2-az1--x-s3".
            "host": "bucket-base-name--usw2-az1--x-s3.s3express-usw2-az1.us-
west-2.amazonaws.com",
            "x-amz-create-session-mode": "ReadWrite"
        },
        "responseElements": {
            "credentials": {
                "accessKeyId": "AKIAI44QH8DHBEXAMPLE"
                "expiration": ""Mar 20, 2024, 11:16:09 PM",
                "sessionToken": "<session token string>"
           },
        },
        "additionalEventData": {
            "SignatureVersion": "SigV4",
            "cipherSuite": "TLS_AES_128_GCM_SHA256",
            "bytesTransferredIn": 0,
            "AuthenticationMethod": "AuthHeader",
```

```
            "xAmzId2": "q6xhNJYmhg",
            "bytesTransferredOut": 1815,
            "availabilityZone": "usw2-az1"
          },
          "requestID": "28d2faaf-3319-4649-998d-EXAMPLE72818",
          "eventID": "694d604a-d190-4470-8dd1-EXAMPLEe20c1",
          "readOnly": true,
          "resources": [
            {
              "type": "AWS::S3Express::Object",
              "ARNPrefix": "arn:aws:s3express:us-west-2:111122223333:bucket-base-name--
usw2-az1--x-s3"
            },
            {
              "accountId": "111122223333"
              "type": "AWS::S3Express::DirectoryBucket",
              "ARN": "arn:aws:s3express:us-west-2:111122223333:bucket-base-name--usw2-
az1--x-s3"
             }
           ],
           "eventType": "AwsApiCall",
           "managementEvent": false,
           "recipientAccountId": "111122223333",
           "eventCategory": "Data",
           "tlsDetails": {
             "tlsVersion": "TLSv1.3",
             "cipherSuite": "TLS_AES_128_GCM_SHA256",
             "clientProvidedHostHeader": "bucket-base-name--usw2-az1--x-s3.s3express-
usw2-az1.us-west-2.amazonaws.com"
            }
          }
```

要使用可用区端点 API 操作（对象级或数据面板操作），可以使用 CreateSession API 操作来创建和管理会话，这些会话经过优化，可为数据请求提供低延迟的授权。也可以使用 CreateSession 来减少日志记录量。要确定在会话期间执行了哪些可用区 API 操作，可以将 CreateSession 日志文件中 responseElements 下的 accessKeyId 与其它可用区 API 操作的日志文件中的 accessKeyId 进行匹配。有关更多信息，请参阅 CreateSession 授权。

下面的示例显示了一个 CloudTrail 日志文件示例，该示例演示了通过 CreateSession 进行身份验证的 GetObject API 操作。

```
    {
```

```
        "eventVersion": "1.09",
        "userIdentity": {
          "type": "AssumedRole",
          "principalId": "AROAIDPPEZS35WEXAMPLE:AssumedRoleSessionName",
          "arn": "arn:aws:sts::111122223333assumed-role/RoleToBeAssumed/MySessionName",
          "accountId": "111122223333",
          "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
          "sessionContext": {
            "attributes": {
              "creationDate": "2024-07-02T00:21:49Z"
            }
          }
        },
        "eventTime": "2024-07-02T00:22:01Z",
        "eventSource": "s3express.amazonaws.com",
        "eventName": "GetObject",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "72.21.198.68",
        "userAgent": "aws-sdk-java/2.25.66 Linux/5.10.216-225.855.amzn2.x86_64
 OpenJDK_64-Bit_Server_VM/17.0.11+9-LTS Java/17.0.11 vendor/Amazon.com_Inc. md/internal
 exec-env/AWS_Lambda_java17 io/sync http/Apache cfg/retry-mode/legacy",
        "requestParameters": {
          "bucketName": "bucket-base-name--usw2-az1--x-s3",
          "x-amz-checksum-mode": "ENABLED",
          "Host": "bucket-base-name--usw2-az1--x-s3.s3express-usw2-az1.us-
west-2.amazonaws.com",
          "key": "test-get-obj-with-checksum"
        },
        "responseElements": null,
        "additionalEventData": {
          "SignatureVersion": "Sigv4",
          "CipherSuite": "TLS_AES_128_GCM_SHA256",
          "bytesTransferredIn": 0,
          "AuthenticationMethod": "AuthHeader",
          "x-amz-id-2": "oOy6w8K7LFsyFN",
          "bytesTransferredOut": 9,
          "availabilityZone": "usw2-az1",
          "sessionModeApplied": "ReadWrite"
         },
          "requestID": "28d2faaf-3319-4649-998d-EXAMPLE72818",
          "eventID": "694d604a-d190-4470-8dd1-EXAMPLEe20c1",
          "readOnly": true,
          "resources": [
            {
```

```
              "type": "AWS::S3Express::Object",
              "ARNPrefix": "arn:aws:s3express:us-west-2:111122223333:bucket-base-name--
usw2-az1--x-s3"
            },
            {
              "accountId": "111122223333",
              "type": "AWS::S3Express::DirectoryBucket",
              "ARN": "arn:aws:s3express:us-west-2:111122223333:bucket-base-name--usw2-
az1--x-s3"
             }
           ],
           "eventType": "AwsApiCall",
           "managementEvent": false,
           "recipientAccountId": "111122223333",
           "eventCategory": "Data",
           "tlsDetails": {
             "tlsVersion": "TLSv1.3",
             "cipherSuite": "TLS_AES_128_GCM_SHA256",
             "clientProvidedHostHeader": "bucket-base-name--usw2-az1--x-s3.s3express-
usw2-az1.us-west-2.amazonaws.com"
            }
          }
```

在上面的 GetObject 日志文件示例中，accessKeyId（AKIAI44QH8DHBEXAMPLE）与 CreateSession 日志文件示例中 responseElements 下的 accessKeyId 相匹配。匹配的 accessKeyId 表示在哪个会话中执行了 GetObject 操作。

以下示例展示了一个 CloudTrail 日志条目，该条目演示了由 S3 生命周期调用的针对目录存储桶的 DeleteObjects 操作。有关更多信息，请参阅 Working with S3 Lifecycle for directory buckets。

```
eventVersion:"1.09",
  userIdentity:{

    type:"AWSService",
    invokedBy:"lifecycle.s3.amazonaws.com"
  },
  eventTime:"2024-09-11T00:55:54Z",
  eventSource:"s3express.amazonaws.com",
  eventName:"DeleteObjects",
  awsRegion:"us-east-2",
  sourceIPAddress:"lifecycle.s3.amazonaws.com",
  userAgent:"gamma.lifecycle.s3.amazonaws.com",
  requestParameters:{
```

```
    bucketName:"amzn-s3-demo-bucket--use2-az2--x-s3",
    'x-amz-expected-bucket-owner':"637423581905",
    Host:"amzn-s3-demo-bucket--use2-az2--x-s3.gamma.use2-az2.express.s3.aws.dev",
    delete:"",
    'x-amz-sdk-checksum-algorithm':"CRC32C"
  },
  responseElements:null,
  additionalEventData:{

    SignatureVersion:"Sigv4",
    CipherSuite:"TLS_AES_128_GCM_SHA256",
    bytesTransferredIn:41903,
    AuthenticationMethod:"AuthHeader",
    'x-amz-id-2':"9H5YWZY0",
    bytesTransferredOut:35316,
    availabilityZone:"use2-az2",
    sessionModeApplied:"ReadWrite"
  },
  requestID:"011eeadd04000191",
  eventID:"d3d8b116-219d-4ee6-a072-5f9950733c74",
  readOnly:false,
  resources:[

    {

      type:"AWS::S3Express::Object",
      ARNPrefix:"arn:aws:s3express:us-east-2:637423581905:bucket/amzn-s3-demo-bucket--
use2-az2--x-s3/"
    },
    {

      accountId:"637423581905",
      type:"AWS::S3Express::DirectoryBucket",
      ARN:"arn:aws:s3express:us-east-2:637423581905:bucket/amzn-s3-demo-bucket--use2-
az2--x-s3"
    }
  ],
  eventType:"AwsApiCall",
  managementEvent:false,
  recipientAccountId:"637423581905",
  sharedEventID:"59f877ac-1dd9-415d-b315-9bb8133289ce",
  eventCategory:"Data"
```

```
}
```

以下示例显示了一个 CloudTrail 日志条目，该条目演示了由 S3 生命周期调用的 `CreateSession` 操作上的 `Access Denied` 请求。有关更多信息，请参阅 CreateSession。

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "gamma.lifecycle.s3.amazonaws.com"
    },
    "eventTime": "2024-09-11T18:13:08Z",
    "eventSource": "s3express.amazonaws.com",
    "eventName": "CreateSession",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "gamma.lifecycle.s3.amazonaws.com",
    "userAgent": "gamma.lifecycle.s3.amazonaws.com",
    "errorCode": "AccessDenied",
    "errorMessage": "Access Denied",
    "requestParameters": {
        "bucketName": "amzn-s3-demo-bucket--use2-az2--x-s3",
        "Host": "amzn-s3-demo-bucket--use2-az2--x-s3.gamma.use2-
az2.express.s3.aws.dev",
        "x-amz-create-session-mode": "ReadWrite",
        "x-amz-server-side-encryption": "AES256"
    },
    "responseElements": null,
    "additionalEventData": {
        "SignatureVersion": "Sigv4",
        "CipherSuite": "TLS_AES_128_GCM_SHA256",
        "bytesTransferredIn": 0,
        "AuthenticationMethod": "AuthHeader",
        "x-amz-id-2": "zuDDC1VNbC4LoNwUIc5",
        "bytesTransferredOut": 210,
        "availabilityZone": "use2-az2"
    },
    "requestID": "010932f174000191e24a0",
    "eventID": "dce7cc46-4cd3-46c0-9a47-d1b8b70e301c",
    "readOnly": true,
    "resources": [{
            "type": "AWS::S3Express::Object",
            "ARNPrefix": "arn:aws:s3express:us-east-2:637423581905:bucket/amzn-s3-demo-
bucket--use2-az2--x-s3/"
```

```
        },
        {
            "accountId": "637423581905",
            "type": "AWS::S3Express::DirectoryBucket",
            "ARN": "arn:aws:s3express:us-east-2:637423581905:bucket/amzn-s3-demo-
bucket--use2-az2--x-s3"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "637423581905",
    "sharedEventID": "da96b5bd-6066-4a8d-ad8d-f7f427ca7d58",
    "eventCategory": "Data"
}
```

# 优化目录存储桶性能

要在使用目录存储桶时获得最佳性能，我们建议遵循以下准则。

## 使用基于会话的身份验证

目录存储桶支持基于会话的新型授权机制，用于对发送到目录存储桶的请求进行身份验证和授权。使用基于会话的身份验证，Amazon SDK 会自动使用 `CreateSession` API 操作创建临时会话令牌，该令牌可用于对发送到目录存储桶的数据请求进行低延迟授权。

Amazon SDK 使用 `CreateSession` API 操作请求临时凭证，然后代表您每 5 分钟自动创建和刷新令牌。为了充分利用目录存储桶的性能优势，我们建议您使用 Amazon SDK 来启动和管理 `CreateSession` API 请求。有关此基于会话的模型的更多信息，请参阅 [使用 CreateSession 对可用区端点 API 操作进行授权]。

## 其他 S3 校验和最佳实践

目录存储桶为您提供了选择校验和算法的选项，该算法用于在上传或下载期间验证数据。您可以选择以下安全哈希算法（SHA）或循环冗余校验（CRC）数据完整性检查算法之一：CRC32、CRC32C、SHA-1 和 SHA-256。S3 Express One Zone 存储类不支持基于 MD5 的校验和。

CRC32 是 Amazon SDK 在对目录存储桶往返传输数据时默认使用的校验和。我们建议使用 CRC32 和 CRC32C，以便在目录存储桶上获得最佳性能。

## 使用最新版本的 Amazon SDK 和通用运行时库

一些 Amazon SDK 还提供 Amazon 通用运行时（CRT）库，以进一步提高 S3 客户端的性能。这些 SDK 包括 Amazon SDK for Java 2.x、适用于 C++ 的 Amazon SDK 和 适用于 Python (Boto3) 的 Amazon SDK。基于 CRT 的 S3 客户端通过自动使用分段上传 API 操作和字节范围提取来自动进行横向扩展连接，从而以高性能和可靠性向目录存储桶往返传输数据。

要使用目录存储桶实现卓越的性能，我们建议使用包含 CRT 库的 Amazon SDK 的最新版本，或者使用 Amazon Command Line Interface（Amazon CLI）。

# 使用目录存储桶进行开发

创建目录存储桶后，您便可立即开始实现非常低延迟的读取和写入。您可以通过虚拟私有云（VPC），使用端点连接与目录存储桶进行通信，也可以使用可用区和区域 API 操作管理对象和目录存储桶。可以通过 Amazon SDK、Amazon S3 控制台、Amazon 命令行界面（Amazon CLI）和 Amazon S3 REST API 使用目录存储桶。

主题

- 目录存储桶的区域和可用区端点
- 使用 S3 控制台、Amazon CLI 和 Amazon SDK 处理目录存储桶
- 目录存储桶 API 操作

## 目录存储桶的区域和可用区端点

要从虚拟私有云（VPC）中访问目录存储桶的区域和可用区端点，您可以使用网关 VPC 端点。创建网关端点后，您可以将其添加为路由表中的目标，用于从您的 VPC 流向存储桶的流量。使用网关端点不会发生任何额外费用。有关如何配置网关 VPC 端点的更多信息，请参阅 目录存储桶的联网。

存储桶级（控制面板）API 操作可通过区域端点使用，称为区域端点 API 操作。区域端点 API 操作的示例包括 `CreateBucket` 和 `DeleteBucket`。

您可以使用可用区（对象级，或数据面板端点 API 操作）来上传和管理对象。可用区端点 API 操作可通过可用区端点执行。可用区 API 操作的示例包括 `PutObject` 和 `CopyObject`。

有关可用区中目录存储桶的区域端点和可用区端点的更多信息，请参阅可用区中适用于目录存储桶的区域和可用区端点。

有关 Local Zones 中目录存储桶的区域端点和可用区端点的更多信息，请参阅Local Zones 中目录存储桶的概念。

# 使用 S3 控制台、Amazon CLI 和 Amazon SDK 处理目录存储桶

您可以通过 Amazon SDK、Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）和 Amazon S3 REST API 使用 S3 Express One Zone 存储类和目录存储桶。

## S3 控制台

要开始使用 S3 控制台，请执行以下步骤：

- 在可用区中创建目录存储桶
- 清空目录存储桶
- 删除目录存储桶

有关完整教程，请参阅教程：开始使用 S3 Express One Zone。

## Amazon SDK

S3 Express One Zone 支持以下 Amazon SDK：

- 适用于 C++ 的 Amazon SDK
- 适用于 Go 的 Amazon SDK v2
- Amazon SDK for Java 2.x
- 适用于 JavaScript 的 Amazon SDK v3
- 适用于 .NET 的 Amazon SDK
- 适用于 PHP 的 Amazon SDK
- 适用于 Python (Boto3) 的 Amazon SDK
- 适用于 Ruby 的 Amazon SDK
- 适用于 Kotlin 的 Amazon SDK
- Amazon SDK for Rust

在使用 S3 Express One Zone 时，建议您使用最新版本的 Amazon SDK。S3 Express One Zone 支持的 Amazon SDK 代表您处理会话的建立、刷新和终止。这意味着您在下载和安装 Amazon SDK 并配置必要的 IAM 权限后，便可立即开始使用 API 操作。有关更多信息，请参阅 使用 IAM 对区域端点 API 操作进行授权。

有关 Amazon SDK 的信息（包括如何下载及安装），请参阅在 Amazon 上构建所用的工具。

有关 Amazon SDK 示例，请参阅以下内容：

- 在可用区中创建目录存储桶
- 清空目录存储桶
- 删除目录存储桶

### Amazon Command Line Interface (Amazon CLI)

您可以使用 Amazon Command Line Interface（Amazon CLI）创建目录存储桶，并对 S3 Express One Zone 使用支持的区域端点和可用区端点 API 操作。

要开始使用 Amazon CLI，请参阅《Amazon CLI 命令参考》中的开始使用 Amazon CLI。

> **Note**
>
> 要通过高级 `aws s3` 命令使用目录存储桶，请将您的 Amazon CLI 更新到最新版本。有关如何安装和配置 Amazon CLI 的更多信息，请参阅《Amazon CLI 用户指南》中的安装或更新 Amazon CLI 的最新版本。

有关 Amazon CLI 示例，请参阅以下内容：

- 在可用区中创建目录存储桶
- 清空目录存储桶
- 删除目录存储桶

## 目录存储桶 API 操作

要管理目录存储桶，您可以使用区域（存储桶级或控制面板）端点 API 操作。要管理目录存储桶中的对象，您可以使用可用区（对象级或数据面板）端点 API 操作。有关更多信息，请参阅目录存储桶的联网和端点和网关 VPC 端点。

区域端点 API 操作

目录存储桶支持以下区域端点 API 操作：

- CreateBucket
- DeleteBucket

- DeleteBucketLifecycle
- DeleteBucketPolicy
- GetBucketLifecycleConfiguration
- GetBucketPolicy
- ListDirectoryBuckets
- PutBucketLifecycleConfiguration
- PutBucketPolicy

### 可用区端点 API 操作

目录存储桶支持以下可用区端点 API 操作：

- CreateSession
- CopyObject
- DeleteObject
- DeleteObjects
- GetObject
- GetObjectAttributes
- HeadBucket
- HeadObject
- ListObjectsV2
- PutObject
- AbortMultipartUpload
- CompleteMultiPartUpload
- CreateMultipartUpload
- ListMultipartUploads
- ListParts
- UploadPart
- UploadPartCopy
- PutBucketEncryption
- GetBucketEncryption
- DeleteBucketEncryption

- ListAccessPointsForDirectoryBuckets
- DeleteAccessPointScope
- GetAccessPointScope
- PutAccessPointScope

# 使用 Amazon S3 表类数据存储服务和表存储桶

Amazon S3 表类数据存储服务提供针对分析工作负载进行优化的 S3 存储，其功能旨在持续提高查询性能并降低表的存储成本。S3 表类数据存储服务专为存储表数据而设计，例如每日购买交易、流传感器数据或广告展示次数。表数据以列和行表示数据，就像在数据库表中一样。

S3 表类数据存储服务中的数据存储在新的存储桶类型中：表存储桶，它将表存储为子资源。表存储桶支持以 Apache Iceberg 格式存储表。使用标准 SQL 语句，您可以通过支持 Iceberg 的查询引擎来查询表，例如 Amazon Athena、Amazon Redshift 和 Apache Spark。

主题


- S3 表类数据存储服务的功能
- 相关服务
- 教程：S3 表类数据存储服务入门
- 表存储桶
- S3 表类数据存储服务维护
- 表命名空间
- S3 表存储桶中的表
- 访问表数据
- S3 表类数据存储服务 Amazon Web Services 区域、端点和服务配额
- S3 表类数据存储服务的安全性
- 使用 Amazon CloudTrail 对 S3 表类数据存储服务进行日志记录


## S3 表类数据存储服务的功能

专为表设计的存储

S3 表存储桶是专门为表设计的。与 S3 通用存储桶中的自行管理的表相比，表存储桶可提供更高的每秒事务数（TPS）和更好的查询吞吐量。表存储桶具有与其它 Amazon S3 存储桶类型相同的耐久性、可用性和可扩展性。

对 Apache Iceberg 的内置支持

表存储桶中的表以 Apache Iceberg 格式存储。您可以在支持 Iceberg 的查询引擎中使用标准 SQL 查询这些表。Iceberg 具有多种优化查询性能的功能，包括架构演变和分区演进。

借助 Iceberg，您可以更改数据的组织方式，使其能够随着时间推移而演变，而无需重写查询或重建数据结构。Iceberg 旨在通过其对事务的支持来协助确保数据一致性和可靠性。为了有助于更正问题或执行时空旅行查询，您可以跟踪数据如何随时间变化和回滚到历史版本。

自动表优化

为了优化您的表以进行查询，S3 会持续执行自动维护操作，例如压缩、快照管理和未引用文件移除。这些操作通过将较小的对象压缩成更少、更大的文件来提高表性能。维护操作还可以通过清理未使用的对象来降低存储成本。这种自动维护通过减少对手动表维护的需求，大规模简化了数据湖的运营。对于每个表和表存储桶，您可以自定义维护配置。

访问管理和安全性

您可以在 Amazon Organizations 中使用 Amazon Identity and Access Management（IAM）和 Service Control Policies 来管理对表存储桶和单个表的访问权限。S3 表类数据存储服务使用的服务命名空间与 Amazon S3 不同：s3tables 命名空间。因此，可以专门为 S3 表类数据存储服务及其资源设计策略。可以设计策略来授予对单个表、表命名空间内的所有表或整个表存储桶的访问权限。所有 Amazon S3 屏蔽公共访问权限设置均始终为表存储桶启用，无法禁用。

与 Amazon 分析服务集成

可以通过 S3 控制台自动将 Amazon S3 表存储桶与 Amazon SageMaker 智能湖仓集成。这种集成支持 Amazon 分析服务通过 Amazon Glue Data Catalog 自动发现和访问表数据。集成后，可以使用诸如 Amazon Athena、Amazon Redshift、QuickSight 等分析服务来处理您的表。有关集成工作原理的更多信息，请参阅将 Amazon S3 表类数据存储服务与 Amazon 分析服务结合使用。

# 相关服务

可以将以下 Amazon Web Services 服务 与 S3 表类数据存储服务结合使用，来支持您的特定分析应用程序。

- Amazon Athena：Athena 是一种交互式查询服务，可用于通过使用标准 SQL 直接分析 Amazon S3 中的数据。还可以使用 Athena，通过 Apache Spark 以交互方式运行数据分析，而无需规划、配置或管理资源。在 Athena 上运行 Apache Spark 应用程序时，您需要提交 Spark 代码以供处理并直接接收结果。
- Amazon Glue：Amazon Glue 是一项无服务器数据集成服务，可让您轻松发现、准备、移动和集成来自多个来源的数据。可以使用 Amazon Glue 进行分析、机器学习（ML）和应用程序开发。Amazon Glue 还包括用于编写、运行任务和实施业务工作流程的额外生产率和数据操作工具。

- Amazon EMR：Amazon EMR 是一个托管式集群平台，可简化在 Amazon 上运行大数据框架（如 Apache Hadoop 和 Apache Spark）来处理和分析海量数据的过程。
- Amazon Redshift：Amazon Redshift 是一项 PB 级云中数据仓库服务。可以使用 Amazon Redshift Serverless 来访问和分析数据，而无需对预置数据仓库执行所有配置操作。系统将自动预置资源，数据仓库的容量会智能扩展，即使面对要求最为苛刻且不可预测的工作负载也能提供高速性能。数据仓库空闲时不会产生费用，您只需为实际使用的资源付费。您可以在 Amazon Redshift 查询编辑器 v2 或您最喜欢的商业智能（BI，Business Intelligence）工具中，直接加载数据并开始查询。
- QuickSight：QuickSight 是一项业务分析服务，可用于构建可视化内容，执行临时分析，并快速从您的数据中获得业务见解。QuickSight 无缝地发现 Amazon 数据来源，并通过使用 QuickSight 超快、并行、内存、计算引擎（SPICE）提供快速的响应式查询性能。
- Amazon Lake Formation：Lake Formation 是一项托管式服务，可简化设置、保护和管理数据湖的流程。Lake Formation 可帮助您探索数据来源，然后对数据进行编目、清理和转换。借助 Lake Formation，可以对 Amazon S3 上的数据湖数据及其在 Amazon Glue Data Catalog 中的元数据进行精细访问控制。

# 教程：S3 表类数据存储服务入门

在本教程中，您将创建一个表存储桶，并将您区域中的表存储桶与 Amazon 分析服务集成。接下来，您将使用 Amazon CLI 在表存储桶中创建第一个命名空间和表。然后，您可以使用 Amazon Lake Formation 授予对表的权限，这样您就可以开始使用 Athena 查询表了。

> **Tip**
>
> 如果您要将表格数据从通用存储桶迁移到表存储桶，Amazon 解决方案库提供了指导性解决方案来为您提供助力。此解决方案通过将 Amazon Step Functions 和 Amazon EMR 与 Apache Spark 结合使用，自动将在 Amazon Glue Data Catalog 中注册并存储在通用存储桶中的 Apache Iceberg 和 Apache Hive 表移到表存储桶。有关更多信息，请参阅 Amazon 解决方案库中的将表格数据从 Amazon S3 迁移到 S3 表的指南。

主题


- 步骤 1：创建表存储桶并将其与 Amazon 分析服务集成
- 步骤 2：创建表命名空间和表
- （可选）步骤 3：授予对表的 Lake Formation 权限
- 步骤 4：在 Athena 中使用 SQL 查询数据

# 步骤 1：创建表存储桶并将其与 Amazon 分析服务集成

在此步骤中，您使用 Amazon S3 控制台来创建第一个表存储桶。有关创建表存储桶的其它方法，请参阅 Creating a table bucket。

> **Note**
>
> 默认情况下，Amazon S3 控制台会自动将表存储桶与 Amazon SageMaker 智能湖仓集成，从而支持 Amazon 分析服务自动发现和访问您的 S3 表类数据存储服务数据。如果您使用 Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 REST API 以编程方式创建第一个表存储桶，则必须手动完成 Amazon 分析服务集成。有关更多信息，请参阅 将 Amazon S3 表类数据存储服务与 Amazon 分析服务结合使用。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在页面顶部的导航栏中，选择当前所显示 Amazon Web Services 区域的名称。接下来，选择要在其中创建表存储桶的区域。
3. 在左侧导航窗格中，选择表存储桶。
4. 选择创建表存储桶。
5. 在常规配置下，输入表存储桶的名称。

   表存储桶名称必须满足以下要求：

   - 在当前区域中对于您的 Amazon Web Services 账户是唯一的。
   - 长度必须介于 3 到 63 个字符之间。
   - 只能由小写字母、数字和连字符 (-) 组成。
   - 以字母或数字开头和结尾。

   创建表存储桶后，便无法更改其名称。创建表存储桶的 Amazon Web Services 账户拥有该存储桶。有关命名表存储桶的更多信息，请参阅表存储桶命名规则。
6. 在与 Amazon 分析服务集成部分中，确保选中启用集成复选框。

   如果在使用控制台创建第一个表存储桶时选择了启用集成，则 Amazon S3 会尝试将表存储桶与 Amazon 分析服务集成。这种集成可让您使用 Amazon 分析服务来访问当前区域中的所有表。有关更多信息，请参阅 将 Amazon S3 表类数据存储服务与 Amazon 分析服务结合使用。

7. 选择 创建存储桶 。

## 步骤 2：创建表命名空间和表

对于此步骤，可以在表存储桶中创建一个命名空间，然后在该命名空间下创建一个新表。可以使用控制台或 Amazon CLI 创建表命名空间和表。

> **Important**
>
> 创建表时，请确保在表名称和表定义中全部使用小写字母。例如，请确保列名称全部为小写。如果表名称或表定义包含大写字母，则 Amazon Lake Formation 或 Amazon Glue Data Catalog 不支持该表。在这种情况下，Amazon Athena 等 Amazon 分析服务将无法看到您的表，即使表存储桶与 Amazon 分析服务集成，也不例外。
> 如果表定义包含大写字母，则在 Athena 中运行 SELECT 查询时会收到以下错误消息：“GENERIC_INTERNAL_ERROR: Get table request failed: com.amazonaws.services.glue.model.ValidationException: Unsupported Federation Resource - Invalid table or column names.”

使用 S3 控制台和 Amazon Athena

以下过程使用 Amazon S3 控制台通过 Amazon Athena 来创建命名空间和表。

创建表命名空间和表

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择表存储桶。
3. 在表存储桶页面上，选择要在其中创建表的表存储桶。
4. 在表存储桶详细信息页面上，选择使用 Athena 创建表。
5. 在使用 Athena 创建表对话框中，选择创建命名空间，然后在命名空间名称字段中输入名称。命名空间名称必须为 1 到 255 个字符，并且在表存储桶中是唯一的。有效字符为 a–z、0–9 和下划线 (_)。命名空间名称的开头不支持使用下划线。
6. 选择 Create namespace (创建命名空间)。
7. 选择使用 Athena 创建表。
8. Amazon Athena 控制台将打开，并出现 Athena 查询编辑器。查询编辑器中填充了一个可用于创建表的示例查询。修改此查询，以指定您希望表具有的表名称和列。

9. 修改完查询后，选择运行来创建表。

如果表创建取得成功，则新表的名称将显示在 Athena 中的表列表中。当您导航回 Amazon S3 控制台时，刷新列表后，新表将出现在表存储桶的详细信息页面上的表列表中。

使用 Amazon CLI

要使用以下 Amazon CLI 示例命令在表存储桶中创建命名空间，然后在该命名空间下使用架构创建新表，请将 *user input placeholder* 值替换为您自己的值。

先决条件

- 将 AmazonS3TablesFullAccess 策略附加到您的 IAM 身份。
- 安装 Amazon CLI 版本 2.23.10 或更高版本。有关更多信息，请参阅《Amazon Command Line Interface 用户指南》中的安装或更新最新版本的 Amazon CLI。

1. 通过运行以下命令，在表存储桶中创建新的命名空间：

```
aws s3tables create-namespace \
--table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-bucket \
--namespace my_namespace
```

   - 通过运行以下命令，确认您的命名空间已成功创建：

```
aws s3tables list-namespaces \
--table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-bucket
```

2. 通过运行以下命令，使用表架构创建新表：

```
aws s3tables create-table --cli-input-json file://mytabledefinition.json
```

   对于 mytabledefinition.json 文件，请使用以下示例表定义：

```
{
    "tableBucketARN": "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-bucket",
    "namespace": "my_namespace",
```

```
    "name": "my_table",
    "format": "ICEBERG",
    "metadata": {
        "iceberg": {
            "schema": {
                "fields": [
                    {"name": "id", "type": "int","required": true},
                    {"name": "name", "type": "string"},
                    {"name": "value", "type": "int"}
                ]
            }
        }
    }
}
```

## （可选）步骤 3：授予对表的 Lake Formation 权限

对于此步骤，请向其它 IAM 主体授予对新表的 Lake Formation 权限。这些权限可让除您之外的其它主体使用 Athena 和其它 Amazon 分析服务来访问表存储桶资源。有关更多信息，请参阅 授予对表或数据库的权限。如果您是唯一将访问表的用户，则可以跳过此步骤。

1. 打开 Amazon Lake Formation 控制台（网址为 https://console.amazonaws.cn/lakeformation/），并以数据湖管理员身份登录。有关如何创建数据湖管理员的更多信息，请参阅 Create a data lake administrator。
2. 在导航窗格中，选择数据权限，然后选择授予。
3. 在授予权限页面的主体下，选择 IAM 用户和角色，然后选择您要支持对表运行查询的 IAM 用户或角色。
4. 在 LF 标签或目录资源下，选择命名 Data Catalog 资源。
5. 根据您是要授予对账户中所有表的访问权限，还是只想授予对您创建的表存储桶中资源的访问权限，执行以下操作之一：
   - 对于目录，选择您在集成表存储桶时创建的账户级目录。例如 *111122223333*:s3tablescatalog。
   - 对于目录，为表存储桶选择子目录。例如 *111122223333*:s3tablescatalog/*amzn-s3-demo-table-bucket*。
6. （可选）如果您为表存储桶选择了子目录，请执行以下一项或两项操作：
   - 对于数据库，选择您创建的表存储桶命名空间。
   - 对于表，请选择您在表存储桶中创建的表，或选择所有表。

7. 根据您选择的是目录还是子目录，以及随后选择的是数据库还是表，您可以在目录级别、数据库级别或表级别设置权限。有关 Lake Formation 权限的更多信息，请参阅《Amazon Lake Formation Developer Guide》中的 Managing Lake Formation permissions。

   请执行以下操作之一：

   - 对于目录权限，请选择 Super 来向另一个主体授予对目录的所有权限，或者选择更精细的权限，例如描述。
   - 对于数据库权限，您不能选择 Super 来向另一个主体授予对数据库的所有权限。而是应选择更精细的权限，例如描述。
   - 对于表权限，请选择 Super 来向另一个主体授予对表的所有权限，或者选择更精细的权限，例如选择或描述。

   > **Note**
   >
   > 当您将对数据目录资源的 Lake Formation 权限授予外部账户或直接授予其他账户中的 IAM 主体时，Lake Formation 会使用 Amazon Resource Access Manager (Amazon RAM) 服务共享该资源。如果被授权者账户与授予者账户在同一个组织中，则被授权者立即可以使用共享资源。如果被授权者账户不在同一个组织中，则 Amazon RAM 会向被授权者账户发送邀请，以便其接受或拒绝资源授权。然后，要使共享资源可用，被授权者账户中的数据湖管理员必须使用 Amazon RAM 控制台或 Amazon CLI 接受邀请。有关跨账户数据共享的更多信息，请参阅《Amazon Lake Formation Developer Guide》中的 Cross-account data sharing in Lake Formation。

8. 选择授权。

## 步骤 4：在 Athena 中使用 SQL 查询数据

可以在 Athena 中使用 SQL 查询表。Athena 对于 S3 表类数据存储服务支持数据定义语言（DDL）、数据操作语言（DML）和数据查询语言（DQL）查询。

您可以从 Amazon S3 控制台或通过 Amazon Athena 控制台访问 Athena 查询。

使用 S3 控制台和 Amazon Athena

以下过程使用 Amazon S3 控制台访问 Athena 查询编辑器，以便您可以使用 Amazon Athena 查询表。

查询表

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择表存储桶。
3. 在表存储桶页面上，选择包含要查询的表的表存储桶。
4. 在表存储桶详细信息页面上，选择要查询的表名称旁边的选项按钮。
5. 选择使用 Athena 查询表。
6. Amazon Athena 控制台打开，Athena 查询编辑器随即出现，其中包含为您加载的示例 SELECT 查询。根据您的用例需要修改此查询。
7. 要运行查询，请选择 Run（运行）。

使用 Amazon Athena 控制台

查询表

1. 从 https://console.aws.amazon.com/athena/ 打开 Athena 控制台。
2. 查询表。下面是您可以修改的示例查询。确保将 *user input placeholders* 替换为您自己的信息。

```
SELECT * FROM "s3tablescatalog/amzn-s3-demo-table-bucket"."my_namespace"."my_table"
 LIMIT 10
```

3. 要运行查询，请选择 Run（运行）。

# 表存储桶

Amazon S3 表存储桶是一种 S3 存储桶类型，可用于创建表并将其存储为 S3 资源。表存储桶用于将表数据和元数据存储为对象，以便在分析工作负载中使用。S3 会自动在表存储桶中执行维护，有助于降低表存储成本。有关更多信息，请参阅 Amazon S3 表存储桶维护。

要与存储在表存储桶中的表进行交互，可以将表存储桶与支持 Apache Iceberg 的分析应用程序集成。表存储桶通过 Amazon Glue Data Catalog 与 Amazon 分析服务集成。有关更多信息，请参阅 将 Amazon S3 表类数据存储服务与 Amazon 分析服务结合使用。还可以使用适用于 Apache Iceberg 的 Amazon S3 表类数据存储服务目录，通过开源查询引擎与表进行交互。有关更多信息，请参阅 使用 Amazon S3 表类数据存储服务 Iceberg REST 端点访问表。

每个表存储桶都有一个唯一的 Amazon 资源名称（ARN）和附加到它的资源策略。表存储桶 ARN 采用以下格式：

```
arn:aws:s3tables:Region:OwnerAccountID:bucket/bucket-name
```

所有表存储桶和表都是私有的，不能使之成为公有的。只有被明确授予访问权限的用户才可以访问这些资源。要授予访问权限，您可以对表存储桶和表使用基于 IAM 资源的策略，并对用户和角色使用基于 IAM 身份的策略。

默认情况下，您可以在 Amazon Web Services 账户中为每个 Amazon Web Services 区域创建最多 10 个表存储桶。要请求增加表存储桶或表的配额，请联系 Amazon Web Services 支持。

Amazon S3 存储桶有几种类型。在创建存储桶之前，请确保选择最适合应用程序和性能要求的存储桶类型。有关各种存储桶类型以及每种类型的相应用例的更多信息，请参阅存储桶。

主题


- Amazon S3 表存储桶、表和命名空间命名规则
- 创建表存储桶
- 删除表存储桶
- 查看有关 Amazon S3 表存储桶的详细信息
- 管理表存储桶策略


## Amazon S3 表存储桶、表和命名空间命名规则

创建表存储桶时，您选择存储桶名称和 Amazon Web Services 区域，该名称在所选区域中对于您的账户必须是唯一的。创建表存储桶后，无法更改存储桶名称或区域。表存储桶名称必须遵循特定的命名规则。有关表存储桶及其中的表和命名空间的命名规则的更多信息，请参阅以下主题。

主题


- 表存储桶命名规则
- 表和命名空间的命名规则


### 表存储桶命名规则

创建 Amazon S3 表存储桶时，需要指定表存储桶名称。与其它存储桶类型一样，无法重命名表存储桶。与其它存储桶类型不同，表存储桶不在全局命名空间中，因此，您账户中的每个存储桶名称只需要在当前 Amazon 区域内保持唯一即可。

有关通用存储桶命名规则，请参阅通用存储桶命名规则。有关目录存储桶命名规则的信息，请参阅目录存储桶命名规则。

以下命名规则适用于表存储桶。

- 存储桶名称必须介于 3 到 63 个字符之间。
- 存储桶名称只能由小写字母、数字和连字符 (-) 组成。
- 存储桶名称必须以字母或数字开头和结尾。
- 存储桶名称不得包含任何下划线 (_) 或句点 (.)。
- 存储桶名称不得以下面的任何前缀开头：
  - `xn--`
  - `sthree-`
  - `amzn-s3-demo-`
- 存储桶名称不得以下面的任何后缀结尾：
  - `-s3alias`
  - `--ol-s3`
  - `--x-s3`
  - `--table-s3`

## 表和命名空间的命名规则

以下命名规则适用于表存储桶中的表和命名空间。

- 名称长度必须介于 1 到 225 个字符之间。
- 名称只能由小写字母、数字和下划线 (_) 组成。命名空间名称的开头不支持使用下划线。
- 名称必须以字母或数字开头和结尾。
- 名称不得包含连字符 (-) 或句点 (.)。
- 表名称在命名空间内必须是唯一的。
- 命名空间在表存储桶中必须是唯一的。
- 不能将 `aws_s3_metadata` 用作命名空间。`aws_s3_metadata` 保留用于元数据表。有关更多信息，请参阅 使用 S3 元数据加快数据发现速度。

# 创建表存储桶

Amazon S3 表存储桶是一种 S3 存储桶类型，可用于创建表并将其存储为 S3 资源。要开始使用 S3 表类数据存储服务，您需要创建一个用于存储和管理表的表存储桶。创建表存储桶时，请选择存储桶名称和 Amazon Web Services 区域。表存储桶名称在所选区域中对于您的账户必须是唯一的。创建表存储桶后，无法更改存储桶名称或区域。有关命名表存储桶的信息，请参阅 Amazon S3 表存储桶、表和命名空间命名规则。

表存储桶具有以下 Amazon 资源名称（ARN）格式：

```
arn:aws:s3tables:region:owner-account-id:bucket/bucket-name
```

默认情况下，可以在 Amazon Web Services 账户中为每个区域创建最多 10 个表存储桶。要请求增加表存储桶或表的配额，请联系 Amazon Web Services 支持。

创建表存储桶时，可以为其指定加密类型，该加密类型将用于加密您在该存储桶中创建的表。有关存储桶加密选项的更多信息，请参阅the section called “加密”。

创建表存储桶的先决条件

要创建表存储桶，首先必须执行以下操作：

- 确保您对 `s3tables:CreateTableBucket` 拥有 Amazon Identity and Access Management（IAM）权限。

> **Note**
>
> 如果您选择 SSE-KMS 作为默认加密类型，则必须对 `s3tables:PutTableBucketEncryption` 拥有权限，并且对所选 Amazon KMS 密钥具有 `DescribeKey` 权限。此外，您使用的 Amazon KMS 密钥需要向 S3 表类数据存储服务授予执行自动表维护的权限。有关更多信息，请参阅 S3 表类数据存储服务 SSE-KMS 加密的权限要求。

要创建表存储桶，可以使用 Amazon S3 控制台、Amazon S3 REST API、Amazon Command Line Interface（Amazon CLI）或 Amazon SDK。

使用 S3 控制台

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在页面顶部的导航栏中，选择当前所显示 Amazon Web Services 区域的名称。接下来，选择要在其中创建存储桶的区域。
3. 在左侧导航窗格中，选择表存储桶。
4. 选择创建表存储桶以打开创建表存储桶页面。
5. 在属性下，输入表存储桶的名称。

   表存储桶名称必须满足以下要求：

   - 在当前区域中对于您的账户是唯一的。
   - 长度介于 3 到 63 个字符之间。
   - 只能由小写字母、数字和连字符（-）组成。
   - 以字母或数字开头和结尾。

   创建存储桶后，便无法更改其名称。创建存储桶的 Amazon Web Services 账户 拥有该存储桶。有关命名表存储桶的信息，请参阅 Amazon S3 表存储桶、表和命名空间命名规则。
6. 如果要将表存储桶与 Amazon 分析服务集成，请确保在与 Amazon 分析服务集成下选择启用集成。

   > **Note**
   >
   > 当您使用控制台并且选择了启用集成选项来创建第一个表存储桶时，Amazon S3 会尝试自动将您的表存储桶与 Amazon 分析服务集成。这种集成可让您使用 Amazon 分析服务来查询当前区域中的所有表。有关更多信息，请参阅将 Amazon S3 表类数据存储服务与 Amazon 分析服务结合使用。
7. 要配置默认加密，请在加密类型下，选择以下选项之一：

   - 具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）
   - 具有 Amazon Key Management Service 密钥的服务器端加密（SSE-KMS）

   有关表数据的加密选项的更多信息，请参阅使用加密保护 S3 表数据。
8. 选择创建存储桶。

使用 Amazon CLI

此示例说明如何使用 Amazon CLI 创建表存储桶。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3tables create-table-bucket \
    --region us-east-2 \
    --name amzn-s3-demo-bucket1
```

默认情况下，S3 表存储桶使用 SSE-S3 作为其默认加密设置，但是，您可以使用可选的 `--encryption-configuration` 参数来指定不同的加密类型。以下示例说明如何创建使用 SSE-KMS 加密的存储桶。有关表存储桶的加密设置的更多信息，请参阅使用加密保护 S3 表数据。

```
aws s3tables create-table-bucket \
    --region us-east-2 \
    --name amzn-s3-demo-bucket1
    --encryption-configuration '{
                    "sseAlgorithm": "aws:kms",
                    "kmsKeyArn":
 "arn:aws:kms:Region:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab" }'
```

## 删除表存储桶

您可以使用 Amazon S3 API、Amazon Command Line Interface 或 Amazon SDK 来删除表存储桶。在删除表存储桶之前，必须删除该存储桶中的所有命名空间和表。

使用 Amazon CLI

此示例说明如何使用 Amazon CLI 删除表存储桶。要使用此示例，请将####### 替换为您自己的信息。

```
aws s3tables delete-table-bucket \
    --region us-east-2 \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
bucket1
```

# 查看有关 Amazon S3 表存储桶的详细信息

您可以使用 S3 表类数据存储服务 REST API、Amazon CLI 或 Amazon SDK，以编程方式查看 Amazon S3 表存储桶的详细信息。

使用 Amazon CLI

此示例说明如何使用 Amazon CLI 获取有关表存储桶的详细信息。要使用此示例，请将*#######* 替换为您自己的信息。

```
aws s3tables get-table-bucket --table-bucket-arn arn:aws:s3tables:us-
east-1:111122223333:bucket/amzn-s3-demo-bucket1
```

# 管理表存储桶策略

可以使用 Amazon S3 REST API、Amazon SDK 和 Amazon Command Line Interface（Amazon CLI）来添加、删除、更新和查看 Amazon S3 表存储桶的存储桶策略。有关更多信息，请参阅以下主题。

有关更多信息，请参阅以下主题。有关 Amazon S3 表类数据存储服务支持的 Amazon Identity and Access Management（IAM）操作和条件键的更多信息，请参阅 S3 表类数据存储服务的访问管理。有关表存储桶的存储桶策略示例，请参阅 S3 表类数据存储服务的基于资源的策略。

## 添加表存储桶策略

要向表存储桶添加存储桶策略，请使用以下 Amazon CLI 示例。

使用 Amazon CLI

此示例说明如何使用 Amazon CLI 创建表存储桶策略。要使用此命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3tables put-table-bucket-policy \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
bucket1  \
    --resource-policy your-policy-JSON
```

## 查看表存储桶策略

要查看附加到表存储桶的存储桶策略，请使用以下 Amazon CLI 示例。

使用 Amazon CLI

此示例说明如何使用 Amazon CLI 查看附加到表存储桶的策略。要使用此命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3tables get-table-bucket-policy --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1
```

### 删除表存储桶策略

要删除附加到表存储桶的存储桶策略，请使用以下 Amazon CLI 示例。

使用 Amazon CLI

此示例说明如何使用 Amazon CLI 删除表存储桶策略。要使用此命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3tables delete-table-bucket-policy --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1
```

## S3 表类数据存储服务维护

Amazon S3 提供维护，以提高 S3 表或表存储桶的性能。这些维护选项包括文件压缩、快照管理和未引用文件移除。默认情况下，将启用这些选项。可以通过维护配置文件来编辑或禁用这些操作。

主题

- S3 表类数据存储服务维护任务状态
- Amazon S3 表存储桶维护
- S3 表类数据存储服务维护
- 维护任务的注意事项和限制

## S3 表类数据存储服务维护任务状态

S3 表类数据存储服务维护任务会定期为您的 S3 表或表存储桶运行。可以使用 `GetTableMaintenanceJobStatus` API 查询这些任务的状态。

使用 Amazon CLI 获取维护任务的状态

以下示例将使用 `GetTableMaintenanceJobStatus` API 获取维护任务的状态。

```
aws s3tables get-table-maintenance-job-status \
   --table-bucket-arn="arn:aws:s3tables:arn:aws::111122223333:bucket/amzn-s3-demo-bucket1" \
   --namespace="mynamespace" \
   --name="testtable"
```

有关更多信息，请参阅 Amazon CLI 命令参考 中的 get-table-maintenance-job-status。

S3 表类数据存储服务维护任务可以在四种可能的状态之间转换：

- `Successful`
- `Failed`
- `Disabled`
- `Not_Yet_Run`

状态为失败的任务将包含一条失败消息。下面的列表介绍了可能的失败消息。

- 尝试读取表时遇到 Iceberg 验证异常。确保您的表可读，符合 Iceberg 规范，并且仅包含以 S3 表别名开头的 S3 路径。
- Iceberg 快照管理目前不支持用户定义的标签或引用。
- Iceberg 表维护配置与“history.expire.max-snapshot-age-ms”和“history.expire.min-snapshots-to-keep”表属性不兼容。
- 当“gc.enabled”表属性为 false 时，不支持 Iceberg 快照管理和未引用文件移除。确保此属性为未设置或显式设置为 true。
- 由于元数据过期，提交失败。将在下次有机会时重试维护。
- 访问权限不足，无法执行表维护。确保用于加密表的密钥处于活动状态、存在且具有向 S3 服务主体 `maintenance.s3tables.amazonaws.com` 授予访问权限的资源策略。
- 内部错误

## Amazon S3 表存储桶维护

Amazon S3 提供维护操作，以增强表存储桶的管理和性能。默认情况下，对所有表存储桶启用了以下选项。您可以通过为表存储桶指定维护配置文件来编辑或禁用此选项。

编辑此配置需要 `s3tables:PutTableBucketMaintenanceConfiguration` 权限。

主题


- 未引用文件移除
- 注意事项和限制


## 未引用文件移除

未引用文件移除会识别并删除所有未被任何表快照引用的对象。作为未引用文件移除策略的一部分，您可以配置两个属性：unreferencedDays（默认为 3 天）和 nonCurrentDays（默认为 10 天）。

对于您的表未引用且早于 unreferencedDays 属性的任何对象，S3 将该对象标记为非当前版本。S3 会在 nonCurrentDays 属性指定的天数后删除非当前对象。

> **Note**
>
> 删除非当前对象是永久性的，无法恢复这些对象。

要查看或恢复已标记为非当前版本的对象，必须联系 Amazon Web Services 支持。有关联系 Amazon Web Services 支持 的信息，请参阅联系 Amazon 或 Amazon Web Services 支持 文档。

未引用文件移除仅根据对表的引用来确定要从该表中删除的对象。在表之外对这些对象进行的任何引用都不会阻止未引用文件移除来删除对象。

如果您禁用未引用文件移除，则任何正在进行的任务都不会受到影响。配置更改后，新配置将在下一个任务中生效。有关更多信息，请参阅 Amazon S3 定价中的定价信息。

您只能在表存储桶级配置未引用文件移除。此配置将应用于存储桶中的每个表。

使用 Amazon CLI 配置未引用文件移除

以下示例将使用 PutTableBucketMaintenanceConfiguration API 将 unreferencedDays 设置为 4 天，并将 nonCurrentDays 设置为 10 天。

```
aws s3tables put-table-bucket-maintenance-configuration \
   --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
table-bucket \
   --type icebergUnreferencedFileRemoval \
   --value '{"status":"enabled","settings":{"icebergUnreferencedFileRemoval":
{"unreferencedDays":4,"nonCurrentDays":10}}}'
```

有关更多信息，请参阅 Amazon CLI 命令参考 中的 put-table-bucket-maintenance-configuration。

### 注意事项和限制

要了解有关未引用文件移除的其它注意事项和限制的更多信息，请参阅the section called “注意事项和限制”。

## S3 表类数据存储服务维护

S3 表类数据存储服务提供维护操作，以增强表的管理和性能。默认情况下为所有表启用以下选项。可以通过为 S3 表指定维护配置文件来编辑或禁用这些选项。

编辑此配置需要 `s3tables:GetTableMaintenanceConfiguration` 和 `s3tables:PutTableMaintenanceConfiguration` 权限。

主题

- 压缩
- 快照管理
- 注意事项和限制

### 压缩

压缩可将较小的对象组合成更少、更大的对象，以提高 Iceberg 查询性能。组合对象时，压缩还会应用表中行级删除的效果。Amazon S3 根据最适合数据访问规律的目标文件大小或您指定的值来压缩表。压缩后的文件将作为表的最新快照写入。默认情况下，对所有表启用压缩功能，默认目标文件大小为 512 MB。

> **Note**
>
> 仅 Apache Parquet 文件类型支持压缩。

只能在表级配置压缩。压缩将产生额外费用。有关更多信息，请参阅 Amazon S3 定价中的定价信息。

使用 Amazon CLI 配置压缩目标文件大小

以下示例将使用 `PutTableMaintenanceConfiguration` API 将目标文件大小更改为 256 MB。

```
aws s3tables put-table-maintenance-configuration \
```

```
   --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
bucket1 \
   --type icebergCompaction \
   --namespace mynamespace \
   --name testtable \
   --value='{"status":"enabled","settings":{"icebergCompaction":
{"targetFileSizeMB":256}}}'
```

有关更多信息，请参阅 Amazon CLI 命令参考 中的 put-table-maintenance-configuration。

使用 Amazon CLI 禁用压缩

以下示例将使用 PutTableMaintenanceConfiguration API 禁用压缩。

```
aws s3tables put-table-maintenance-configuration \
   --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
table-bucket \
   --type icebergCompaction \
   --namespace mynamespace \
   --name testtable \
   --value='{"status":"disabled","settings":{"icebergCompaction":
{"targetFileSizeMB":256}}}'
```

有关更多信息，请参阅 Amazon CLI 命令参考 中的 put-table-maintenance-configuration。

### 快照管理

快照管理确定表的活动快照的数量。这基于 MinimumSnapshots（默认为 1）和 MaximumSnapshotAge（默认为 120 小时）。快照管理会根据这些配置使表快照到期和移除表快照。

快照到期后，Amazon S3 会将仅由该快照引用的任何对象标记为非当前对象。这些非当前对象将在由未引用文件移除策略中的 NoncurrentDays 属性指定的天数后被删除。

> **Note**
>
> 删除非当前对象是永久性的，无法恢复这些对象。

要查看或恢复已标记为非当前对象的对象，必须联系 Amazon Web Services 支持。有关联系 Amazon Web Services 支持 的信息，请参阅联系 Amazon 或 Amazon Web Services 支持 文档。

快照管理仅根据对该表的引用来确定要从表中删除的对象。在表之外对这些对象进行的任何引用都不会阻止快照管理删除对象。

> **Note**
>
> 快照管理不支持您在 `metadata.json` 文件中或通过 `ALTER TABLE SET TBLPROPERTIES` SQL 命令配置为 Iceberg 表属性的保留值，包括基于分支或标签的保留。当您配置基于分支或标签的保留策略，或者在 `metadata.json` 文件上配置的保留策略长度超过通过 `PutTableMaintenanceConfiguration` API 配置的值时，快照管理将被禁用。在这些情况下，S3 不会使快照到期或移除快照，您需要手动删除快照或从 Iceberg 表中移除属性，以避免产生存储费用。

只能在表级配置快照管理。有关更多信息，请参阅 Amazon S3 定价中的定价信息。

使用 Amazon CLI 配置快照管理

以下示例将使用 `PutTableMaintenanceConfiguration` API 将 `MinimumSnapshots` 设置为 10，并将 `MaximumSnapshotAge` 设置为 2500 小时。

```
aws s3tables put-table-maintenance-configuration \
--table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
table-bucket \
--namespace my_namespace \
--name my_table \
--type icebergSnapshotManagement \
--value '{"status":"enabled","settings":{"icebergSnapshotManagement":
{"minSnapshotsToKeep":10,"maxSnapshotAgeHours":2500}}}'
```

有关更多信息，请参阅 Amazon CLI 命令参考 中的 put-table-maintenance-configuration。

### 注意事项和限制

要详细了解压缩和快照管理的其它注意事项和限制，请参阅the section called “注意事项和限制”。

## 维护任务的注意事项和限制

Amazon S3 提供维护操作，以提高 S3 表或表存储桶的性能。这些选项为文件压缩、快照管理和未引用文件移除。以下是这些管理选项的限制和注意事项。

主题

- 压缩注意事项
- 快照管理注意事项
- 未引用文件移除的注意事项
- S3 表和表存储桶维护的限制

## 压缩注意事项

以下注意事项适用于压缩。有关压缩的更多信息，请参阅 the section called “表维护”。

- 仅 Apache Parquet 文件类型支持压缩。
- 压缩不支持数据类型：固定。
- 压缩不支持压缩类型：`brotli`、`lz4`。

## 快照管理注意事项

以下注意事项适用于快照管理。有关快照管理的更多信息，请参阅 the section called “表维护”。

- 只有在同时满足以下两个条件时，才会保留快照：要保留的最小快照数量和指定的保留期。
- 快照管理从 Apache Iceberg 中删除到期的快照元数据，从而防止对到期快照进行时空旅行查询，并选择性删除关联的数据文件。
- 快照管理不支持您在 `metadata.json` 文件中或通过 `ALTER TABLE SET TBLPROPERTIES` SQL 命令配置为 Iceberg 表属性的保留值，包括基于分支或标签的保留。当您配置基于分支或标签的保留策略，或者在 `metadata.json` 文件上配置的保留策略长度超过通过 `PutTableMaintenanceConfiguration` API 配置的值时，快照管理将被禁用。在这些情况下，S3 不会使快照到期或移除快照，您需要手动删除快照或从 Iceberg 表中移除属性，以避免产生存储费用。

## 未引用文件移除的注意事项

以下注意事项适用于未引用文件移除。有关未引用文件移除的更多信息，请参阅 the section called “表存储桶维护”。

- 未引用文件移除会删除 Iceberg 元数据不再引用的数据和元数据文件（如果其创建时间早于保留期）。

S3 表和表存储桶维护的限制

| 维护操作 | 属性 | 是否可在表存储桶级进行配置？ | 是否可在表级进行配置？ | 默认值 | 最小值 |
|---|---|---|---|---|---|
| 压缩 | targetFileSizeMB | 否 | 是 | 512 MB | 64MB |
| 快照管理 | minimumSnapshots | 否 | 是 | 1 | 1 |
| 快照管理 | maximumSnapshotAge | 否 | 是 | 120 小时 | 1 小时 |
| 未引用文件移除 | unreferencedDays | 是 | 否 | 3 天 | 1 天 |
| 未引用文件移除 | nonCurrentDays | 是 | 否 | 10 天 | 1 天 |

# 表命名空间

在 Amazon S3 表存储桶中创建表时，可以将它们组织成称为命名空间的逻辑分组。与 S3 表和表存储桶不同，命名空间不是资源。命名空间是有助于您以可扩展的方式组织和管理表的构造。例如，公司中属于人力资源部门的所有表都可以分组到一个公共命名空间值 `hr` 下。

要控制对特定命名空间的访问权限，可以使用表存储桶资源策略。有关更多信息，请参阅 the section called “基于资源的策略”。

以下规则适用于表命名空间：

- 每个命名空间在表存储桶内都必须是唯一的。
- 您可以为每个表存储桶创建最多 10000 个命名空间。
- 每个表名称在命名空间内都必须是唯一的。
- 每个表只能有一个级别的命名空间。命名空间不能嵌套。
- 每个表都属于单个命名空间。

- 您可以在命名空间之间移动表。

主题


- 创建命名空间
- 删除命名空间


## 创建命名空间

表命名空间是在 Amazon S3 表存储桶中对表进行分组的逻辑构造。每个表都属于单个命名空间。在表存储桶中创建表之前，必须创建一个命名空间来对表进行分组。可以使用 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）、Amazon S3 REST API、Amazon SDK 或集成查询引擎创建命名空间。

命名空间名称

以下命名规则适用于命名空间：

- 名称长度必须介于 1 到 255 个字符之间。
- 名称只能由小写字母、数字和下划线 (_) 组成。命名空间名称的开头不支持使用下划线。
- 名称必须以字母或数字开头和结尾。
- 名称不得包含连字符 (-) 或句点 (.)。

有关有效命名空间名称的更多信息，请参阅表和命名空间的命名规则。

使用 S3 控制台和 Amazon Athena

以下过程通过使用 Athena 创建表工作流程在 Amazon S3 控制台中创建命名空间。如果您不想同时使用 Amazon Athena 在命名空间中创建表，则可以在创建命名空间后取消该工作流程。

创建命名空间

1. 登录到Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择表存储桶。
3. 在表存储桶页面上，选择要在其中创建命名空间的存储桶。
4. 在存储桶详细信息页面上，选择使用 Athena 创建表。

5. 在使用 Athena 创建表对话框中，选择创建命名空间，然后选择创建命名空间。
6. 在命名空间名称字段中输入名称。命名空间名称必须为 1 到 255 个字符，并且在表存储桶中是唯一的。有效字符为 a–z、0–9 和下划线 (_)。命名空间名称的开头不支持使用下划线。
7. 选择 Create namespace (创建命名空间)。
8. 如果您还想创建表，请选择使用 Athena 创建表。有关使用 Athena 创建表的更多信息，请参阅the section called “使用 S3 控制台和 Amazon Athena”。如果您不想立即创建表，请选择取消。

使用 Amazon CLI

此示例说明如何使用 Amazon CLI 创建表命名空间。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3tables create-namespace \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1 \
    --namespace example_namespace
```

使用查询引擎

您可以在连接到 Amazon S3 表存储桶的 Apache Spark 会话中创建命名空间。

此示例向您展示如何在与 S3 表类数据存储服务集成的查询引擎中使用 CREATE 语句来创建表。要使用此示例，请将####### 替换为您自己的信息。

```
spark.sql("CREATE NAMESPACE IF NOT EXISTS s3tablesbucket.my_namespace")
```

## 删除命名空间

在从 Amazon S3 表存储桶中删除表命名空间之前，必须删除该命名空间中的所有表，或者将它们移到另一个命名空间下。可以使用 Amazon S3 REST API、Amazon SDK、Amazon Command Line Interface（Amazon CLI）或集成查询引擎来删除命名空间。

有关删除命名空间所需的权限的信息，请参阅《Amazon Simple Storage Service API Reference》中的 DeleteNamespace。

使用 Amazon CLI

此示例说明如何使用 Amazon CLI 删除表命名空间。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3tables delete-namespace \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1 \
    --namespace example_namespace
```

# S3 表存储桶中的表

S3 表表示由基础表数据和相关元数据组成的结构化数据集。该数据作为子资源存储在表存储桶中。表存储桶中的所有表均以 Apache Iceberg 表格式存储。Amazon S3 通过自动文件压缩和快照管理来管理表的维护。有关更多信息，请参阅 S3 表类数据存储服务维护。

要使 Amazon 分析服务可以访问您账户中的表，您可以将 Amazon S3 表存储桶与 Amazon SageMaker 智能湖仓集成。这种集成支持 Amazon Athena 和 Amazon Redshift 等 Amazon 分析服务自动发现和访问您的表数据。

创建表时，Amazon S3 会自动为表生成仓库位置。这是一个唯一的 S3 位置，用于存储与表关联的对象。以下示例显示了仓库位置的格式：

```
s3://63a8e430-6e0b-46f5-k833abtwr6s8tmtsycedn8s4yc3xhuse1b--table-s3
```

在表存储桶中，可以将表组织成称为命名空间的逻辑分组。有关更多信息，请参阅 表命名空间。

您可以重命名表，但每个表都有自己唯一的 Amazon 资源名称（ARN）和唯一的表 ID。每个表还附加了资源策略。可以使用此策略来管理对表的访问权限。

表 ARN 使用以下格式：

```
arn:aws:s3tables:region:owner-account-id:bucket/bucket-name/table/table-id
```

默认情况下，您可以在表存储桶中创建多达 10000 个表。要请求增加表存储桶或表的配额，请联系 Amazon Web Services 支持。

Amazon S3 在表存储桶中支持以下类型的表：

客户表

客户表是您可以读取和写入的表。您可以使用集成的查询引擎从这些表中检索数据。您可以使用 S3 API 操作或集成的查询引擎在其中插入、更新或删除数据。

Amazon 表

Amazon 表是由 Amazon Web Services 服务 代表您生成的只读表。这些表由 Amazon S3 管理，而不能由 Amazon S3 本身以外的任何 IAM 主体进行修改。您可以从这些表中检索信息，但无法修改表中的数据。Amazon 表包括 S3 元数据表，其中包含从 S3 通用存储桶内的对象中捕获的元数据。有关更多信息，请参阅 使用 S3 元数据加快数据发现速度。

主题

- 创建 Amazon S3 表
- 删除 Amazon S3 表
- 管理表策略

## 创建 Amazon S3 表

Amazon S3 表是表存储桶的子资源。表以 Apache Iceberg 格式存储，以便您通过使用查询引擎和其它支持 Apache Iceberg 的应用程序来处理这些表。Amazon S3 会持续优化表，以有助于降低存储成本并提高分析查询性能。

创建表时，Amazon S3 会自动为表生成仓库位置。仓库位置是一个唯一的 S3 位置，您可以在其中读取和写入与表关联的对象。以下示例显示了仓库位置的格式：

```
s3://63a8e430-6e0b-46f5-k833abtwr6s8tmtsycedn8s4yc3xhuse1b--table-s3
```

表具有以下 Amazon 资源名称（ARN）格式：

```
arn:aws:s3tables:region:owner-account-id:bucket/bucket-name/table/table-id
```

默认情况下，您可以在表存储桶中创建多达 10000 个表。要请求增加表存储桶或表的配额，请联系 Amazon Web Services 支持。

可以使用 Amazon S3 控制台、Amazon S3 REST API、Amazon SDK、Amazon Command Line Interface（Amazon CLI）或连接到表存储桶的查询引擎来创建表。

创建表时，您可以为该表指定加密设置，除非您使用 Athena 创建表。如果您未指定加密设置，则将使用表存储桶的默认设置对表进行加密。有关更多信息，请参阅 为表指定加密。

创建表的先决条件

要创建表，首先必须执行以下操作：

- 创建表存储桶.
- 在表存储桶中创建命名空间。
- 确保您对 `s3tables:CreateTable` 和 `s3tables:PutTableData` 具有 Amazon Identity and Access Management（IAM）权限。
- 

> **Note**
>
> 如果您对表使用 SSE-KMS 加密，则需要对 `s3tables:PutTableEncryption` 拥有权限，并对所选 Amazon KMS 密钥拥有 `DescribeKey` 权限。此外，您使用的 Amazon KMS 密钥需要向 S3 表类数据存储服务授予执行自动表维护的权限。有关更多信息，请参阅 S3 表类数据存储服务 SSE-KMS 加密的权限要求。

有关有效表名称的信息，请参阅表和命名空间的命名规则。

> **Important**
>
> 创建表时，请确保在表名称和表定义中全部使用小写字母。例如，请确保列名称全部为小写。如果表名称或表定义包含大写字母，则 Amazon Lake Formation 或 Amazon Glue Data Catalog 不支持该表。在这种情况下，Amazon Athena 等 Amazon 分析服务将无法看到您的表，即使表存储桶与 Amazon 分析服务集成，也不例外。
> 如果表定义包含大写字母，则在 Athena 中运行 `SELECT` 查询时会收到以下错误消息：“GENERIC_INTERNAL_ERROR: Get table request failed: com.amazonaws.services.glue.model.ValidationException: Unsupported Federation Resource - Invalid table or column names.”

使用 S3 控制台和 Amazon Athena

以下过程使用 Amazon S3 控制台通过 Amazon Athena 来创建表。如果您尚未在表存储桶中创建命名空间，则可以在此过程中创建命名空间。在执行以下步骤之前，请确保您已在此区域中将表存储桶与 Amazon 分析服务集成。有关更多信息，请参阅 the section called “将 S3 表类数据存储服务与 Amazon 分析服务结合使用”。

> **Note**
>
> 当您使用 Athena 创建表时，该表将从表存储桶继承默认加密设置。如果要使用不同的加密类型，则需要使用另一种方法创建表。

创建表

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择表存储桶。
3. 在表存储桶页面上，选择要在其中创建表的存储桶。
4. 在存储桶详细信息页面上，选择使用 Athena 创建表。
5. 在使用 Athena 创建表对话框中，执行下列操作之一：
   - 创建新的命名空间。选择创建命名空间，然后在命名空间名称字段中输入名称。命名空间名称必须为 1 到 255 个字符，并且在表存储桶中是唯一的。有效字符为 a–z、0–9 和下划线 (_)。命名空间名称的开头不支持使用下划线。
   - 选择 Create namespace (创建命名空间)。
   - 指定现有的命名空间。选择指定此表存储桶中的现有命名空间。然后选择从现有命名空间中选择或输入现有命名空间名称。如果存储桶中有超过 1000 个命名空间，则当命名空间名称未出现在列表中时，必须输入该名称。
6. 选择使用 Athena 创建表。
7. Amazon Athena 控制台将打开，并出现 Athena 查询编辑器。目录字段中应填充 s3tablescatalog/，后跟表存储桶的名称，例如 s3tablescatalog/***amzn-s3-demo-bucket***。数据库字段中应填充您之前创建或选择的命名空间。

   > **Note**
   >
   > 如果您在目录和数据库字段中看不到这些值，请确保您已在该区域中将表存储桶与 Amazon 分析服务集成。有关更多信息，请参阅 the section called “将 S3 表类数据存储服务与 Amazon 分析服务结合使用”。

8. 查询编辑器中填充了一个可用于创建表的示例查询。修改此查询，以指定您希望表具有的表名称和列。
9. 修改完查询后，选择运行来创建表。

   > **Note**
   >
   > - 如果您在尝试在 Athena 中运行查询时收到错误“权限不足，无法执行查询。主体对指定的资源没有任何权限”，则必须向您授予对于表的必需 Lake Formation 权限。有关更多信息，请参阅 the section called “授予对表或数据库的权限”。

- 如果您在尝试在 Athena 中运行查询时收到错误“Iceberg 无法访问所请求的资源”，请转到 Amazon Lake Formation 控制台，并确保您已授予自己对您创建的表存储桶目录和数据库（命名空间）的权限。授予这些权限时请勿指定表。有关更多信息，请参阅 the section called “授予对表或数据库的权限”。
- 如果在 Athena 中运行 SELECT 查询时收到以下错误消息，则此消息是由表名称中或表定义的列名称中具有大写字母而引起的：“GENERIC_INTERNAL_ERROR: Get table request failed: com.amazonaws.services.glue.model.ValidationException: Unsupported Federation Resource - Invalid table or column names.” 确保表名称和列名称全部为小写。

如果表创建取得成功，则新表的名称将显示在 Athena 中的表列表中。当您导航回 Amazon S3 控制台时，刷新列表后，新表将出现在表存储桶的存储桶详细信息页面上的表列表中。

使用 Amazon CLI

此示例展示了如何使用 Amazon CLI 并使用 JSON 指定表元数据，来通过架构创建表。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3tables create-table --cli-input-json file://mytabledefinition.json
```

对于 mytabledefinition.json 文件，请使用以下示例表定义。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
{
    "tableBucketARN": "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-bucket",
    "namespace": "your_namespace",
    "name": "example_table",
    "format": "ICEBERG",
    "metadata": {
        "iceberg": {
            "schema": {
                "fields": [
                     {"name": "id", "type": "int","required": true},
                     {"name": "name", "type": "string"},
                     {"name": "value", "type": "int"}
                ]
            }
        }
```

```
    }
}
```

使用查询引擎

您可以在连接到表存储桶的受支持的查询引擎中创建表，例如在 Amazon EMR 上的 Apache Spark 会话中。

以下示例说明如何通过 Spark 使用 CREATE 语句创建表，以及如何使用 INSERT 语句或从现有文件中读取数据来添加表数据。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
spark.sql(
" CREATE TABLE IF NOT EXISTS s3tablesbucket.example_namespace.`example_table` (
    id INT,
    name STRING,
    value INT
)
USING iceberg "
)
```

创建表后，可以将数据加载到表中。从以下方法中进行选择：

- 使用 INSERT 语句向表中添加数据。

  ```
  spark.sql(
  """
      INSERT INTO s3tablesbucket.my_namespace.my_table
      VALUES
          (1, 'ABC', 100),
          (2, 'XYZ', 200)
  """)
  ```

- 加载现有的数据文件。

  1. 将数据读入 Spark：

     ```
     val data_file_location = "Path such as S3 URI to data file"
     val data_file = spark.read.parquet(data_file_location)
     ```

  2. 将数据写入 Iceberg 表：

```
data_file.writeTo("s3tablesbucket.my_namespace.my_table").using("Iceberg").tableProperty
 ("format-version", "2").createOrReplace()
```

## 删除 Amazon S3 表

可以使用 Amazon S3 REST API、Amazon SDK、Amazon CLI 或使用集成查询引擎来删除表。

> **Note**
>
> S3 表类数据存储服务不支持 purge=false 的 DROP TABLE 操作。某些版本的 Spark 即使在运行 DROP TABLE PURGE 命令时也始终将此标志设置为 false。可以使用 purge=true 重试 DROP TABLE 或使用 S3 表类数据存储服务 DeleteTable REST API 来删除表。
> 删除表时，与该表关联的对象将变为非当前版本，可能需要多达一天的时间才能移除。

### 使用 Amazon CLI

此示例说明如何使用 Amazon CLI 删除表。要使用该命令，请将####### 替换为您自己的信息。

```
aws s3tables delete-table \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
table-bucket \
    --namespace example_namespace --name example_table
```

### 使用查询引擎

您可以在连接到 Amazon S3 表存储桶的 Apache Spark 会话中删除表。

此示例说明如何使用 DROP TABLE PURGE 命令来删除表。要使用该命令，请将####### 替换为您自己的信息。

```
spark.sql(
" DROP TABLE [IF EXISTS] s3tablesbucket.example_namespace.example_table PURGE;
```

## 管理表策略

可以使用 Amazon S3 REST API、Amazon SDK 和 Amazon CLI 来添加、删除、更新和查看表的表策略。有关更多信息，请参阅以下主题。有关 Amazon S3 表类数据存储服务支持的 Amazon Identity

and Access Management（IAM）操作和条件键的更多信息，请参阅 S3 表类数据存储服务的访问管理。有关示例表策略，请参阅 S3 表类数据存储服务的基于资源的策略。

### 添加表策略

要向表添加表策略，可以使用 Amazon S3 REST API、Amazon SDK 和 Amazon CLI。

使用 Amazon CLI

此示例说明如何使用 Amazon CLI 创建表策略。要使用该命令，请将*###### 替换为您自己的信息。

```
aws s3tables put-table-policy \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1 \
    --namespace my-namespace \
    --name my-table \
    --resource-policy your-policy-JSON
```

### 查看表策略

要查看附加到表的存储桶策略，可以使用 Amazon S3 REST API、Amazon SDK 和 Amazon CLI。

使用 Amazon CLI

此示例说明如何使用 Amazon CLI 查看附加到表的策略。要使用该命令，请将*###### 替换为您自己的信息。

```
aws s3tables get-table-policy \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1/table/tableID \
    --namespace my-namespace \
    --name my-table
```

### 删除表策略

要删除附加到表的策略，可以使用 Amazon S3 REST API、Amazon SDK 和 Amazon CLI。

使用 Amazon CLI

此示例说明如何使用 Amazon CLI 删除表策略。要使用该命令，请将*###### 替换为您自己的信息。

```
aws s3tables delete-table-policy \
```

```
    --table-ARN arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1/
table/tableID \
    --namespace your-namespace \
    --name your-table
```

# 访问表数据

有多种方法可以访问 Amazon S3 表存储桶中的表，您可以使用 Amazon SageMaker 智能湖仓将表与 Amazon 分析服务集成，也可以直接使用 Amazon S3 表类数据存储服务 Iceberg REST 端点或适用于 Apache Iceberg 的 Amazon S3 表类数据存储服务目录来访问表。您使用的访问方法将取决于您的目录设置、治理模式和访问控制需要。下文概述了这些访问方法。

Amazon SageMaker 智能湖仓集成

这是处理 S3 表存储桶中的表的推荐访问方法。该集成为您提供了统一的表管理、集中式治理以及跨多个 Amazon 分析服务的精细访问控制。

直接访问

如果您需要使用 Amazon Partner Network（APN）目录实现、自定义目录实现，或者只需要对单个表存储桶中的表执行基本读/写操作，请使用此方法。

> **Note**
>
> 要访问表，您使用的 IAM 身份需要访问您的表资源和 S3 表类数据存储服务操作。有关更多信息，请参阅 S3 表类数据存储服务的访问管理。

## 通过 Amazon SageMaker 智能湖仓集成访问表

您可以将 S3 表存储桶与 Amazon SageMaker 智能湖仓集成，以便通过 Amazon 分析服务访问表，例如 Amazon Athena、Amazon Redshift 和 QuickSight。Amazon SageMaker 智能湖仓统一了您在 Amazon S3 数据湖和 Amazon Redshift 数据仓库中的数据，因此，您可以在单个数据副本上构建分析、机器学习（ML）和生成式人工智能应用程序。该集成会使用您的表资源填充 Amazon Glue Data Catalog，并与 Amazon Lake Formation 联合访问这些资源。有关集成的更多信息，请参阅将 Amazon S3 表类数据存储服务与 Amazon 分析服务结合使用。

该集成通过 Amazon Lake Formation 支持精细的访问控制，以提供额外的安全性。Lake Formation 结合使用自己的权限模型和 IAM 权限模型，来控制对表资源和基础数据的访问权限。这意味着，访问表

的请求必须通过由 IAM 和 Lake Formation 执行的权限检查。有关更多信息，请参阅《Amazon Lake Formation Developer Guide》中的 Lake Formation permissions overview。

以下 Amazon 分析服务可以通过此集成访问表：

- Amazon Athena
- Amazon Redshift
- Amazon EMR
- QuickSight
- Amazon Data Firehose

### 使用 Amazon GlueIceberg REST 端点访问表

在将 S3 表存储桶与 Amazon SageMaker 智能湖仓集成后，还可以使用 Amazon Glue Iceberg REST 端点，从支持 Iceberg 的第三方查询引擎连接到 S3 表。有关更多信息，请参阅 使用 Amazon GlueIceberg REST 端点访问 Amazon S3 表。

当您要从 Spark、PyIceberg 或其它 Iceberg 兼容的客户端访问表时，我们建议使用 Amazon Glue Iceberg REST 端点。

以下客户端可以直接通过 Amazon Glue Iceberg REST 端点访问表：

- 任何 Iceberg 客户端，包括 Spark、PyIceberg 等。

## 直接访问表

您可以通过将 S3 表类数据存储服务管理操作与 Apache Iceberg 分析应用程序连接起来的方法，直接从开源查询引擎访问表。有两种直接访问方法：Amazon S3 表类数据存储服务 Iceberg REST 端点或适用于 Apache Iceberg 的 Amazon S3 表类数据存储服务目录。建议使用 REST 端点。

如果您访问自行管理的目录实现中的表，或者只需要对单个表存储桶中的表执行基本的读/写操作，我们建议您直接访问。对于其它访问场景，我们建议使用 Amazon SageMaker 智能湖仓集成。

对表的直接访问可通过附加到表和表存储桶的基于 IAM 身份的策略或基于资源的策略来进行管理。直接访问表时，您无需管理表的 Lake Formation 权限。

### 通过 Amazon S3 表类数据存储服务 Iceberg REST 端点访问表

您可以使用 Amazon S3 表类数据存储服务 Iceberg REST 端点，通过 HTTP 端点直接从任何 Iceberg REST 兼容的客户端访问您的表，有关更多信息，请参阅使用 Amazon S3 表类数据存储服务 Iceberg REST 端点访问表。

以下 Amazon 分析服务和查询引擎可以使用 Amazon S3 表类数据存储服务 Iceberg REST 端点直接访问表：

支持的查询引擎

- 任何 Iceberg 客户端，包括 Spark、PyIceberg 等。
- Amazon EMR
- Amazon Glue ETL

### 通过适用于 Apache Iceberg 的 Amazon S3 表类数据存储服务目录直接访问表

也可以通过使用 S3 表类数据存储服务客户端目录直接从查询引擎（例如 Apache Spark）访问表，有关更多信息，请参阅使用适用于 Apache Iceberg 的 Amazon S3 表类数据存储服务目录访问 Amazon S3 表。但是，S3 建议使用 Amazon S3 表类数据存储服务 Iceberg REST 端点进行直接访问，因为它支持更多应用程序，而无需语言或引擎特定的代码。

以下查询引擎可以使用客户端目录直接访问表：

- Apache Spark

## 将 Amazon S3 表类数据存储服务与 Amazon 分析服务结合使用

要使 Amazon 分析服务可以访问您账户中的表，您可以将 Amazon S3 表存储桶与 Amazon SageMaker 智能湖仓集成。这种集成支持 Amazon 分析服务自动发现和访问您的表数据。您可以使用此集成在以下服务中处理表：

- Amazon Athena
- Amazon Redshift
- Amazon EMR
- QuickSight
- Amazon Data Firehose

> **Note**
>
> 此集成使用 Amazon Glue 和 Amazon Lake Formation 服务，可能会产生 Amazon Glue 请求和存储成本。有关更多信息，请参阅 Amazon Glue 定价。
> 在 S3 表上运行查询需支付额外费用。有关更多信息，请参阅您使用的查询引擎的定价信息。

## 集成的工作原理

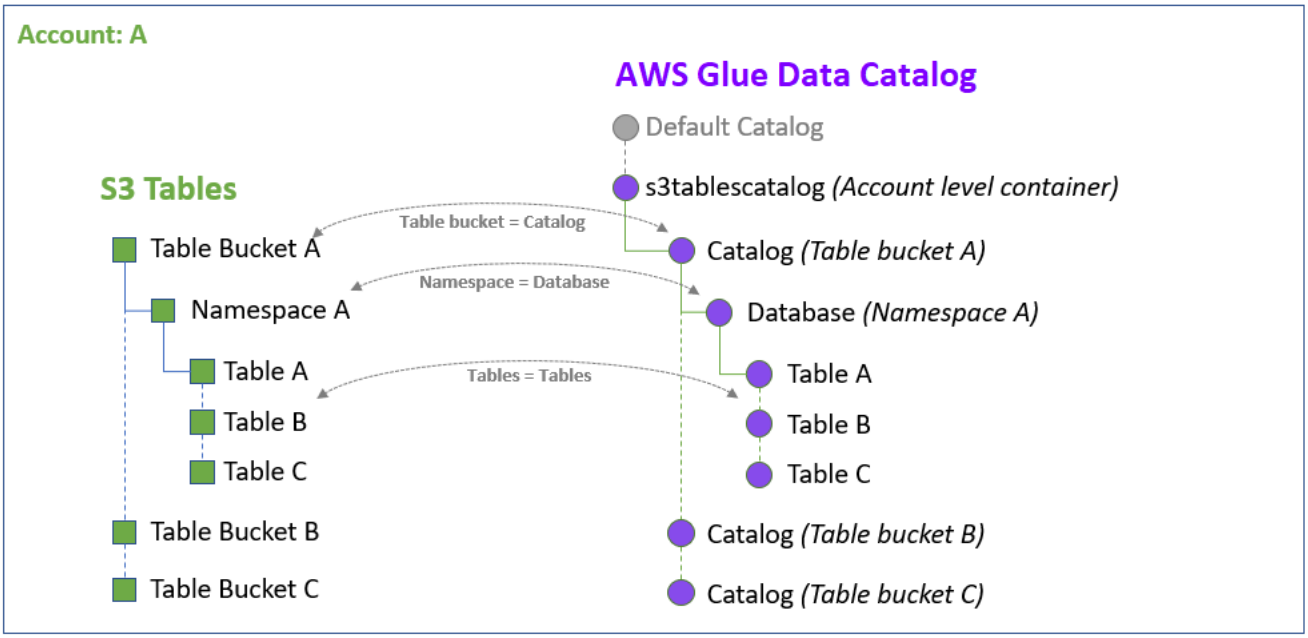
当您在控制台中创建表存储桶时，Amazon S3 会启动以下操作，来将您选择的区域中的表存储桶与 Amazon 分析服务集成：

1. 创建一个新的 Amazon Identity and Access Management（IAM）服务角色，该角色授予 Lake Formation 访问所有表存储桶的权限。
2. 使用服务角色，Lake Formation 在当前区域中注册表存储桶。这可让 Lake Formation 管理该区域中所有当前和将来的表存储桶的访问、权限和治理。
3. 将 `s3tablescatalog` 目录添加到当前区域中的 Amazon Glue Data Catalog。添加 `s3tablescatalog` 目录后，就可以在数据目录中填充所有表存储桶、命名空间和表。

> **Note**
>
> 这些操作通过 Amazon S3 控制台自动完成。如果您以编程方式执行此集成，则必须手动执行所有这些操作。

您可以为每个 Amazon 区域集成一次表存储桶。完成集成后，所有当前和将来的表存储桶、命名空间和表都将添加到该区域中的 Amazon Glue Data Catalog。

下图显示了 `s3tablescatalog` 目录如何自动将当前区域中的表存储桶、命名空间和表填充为数据目录中的相应对象。表存储桶以子目录的形式填充。表存储桶中的命名空间以数据库的形式填充到其各自的子目录中。表以表的形式填充到各自的数据库中。




权限的工作原理

我们建议将表存储桶与 Amazon 分析服务集成，以便您可以跨使用 Amazon Glue Data Catalog 作为元数据存储的服务处理表数据。该集成通过 Amazon Lake Formation 支持精细的访问控制。这种安全方法意味着，除了 Amazon Identity and Access Management（IAM）权限外，您还必须向 IAM 主体授予对表的 Lake Formation 权限，然后才能使用这些表。

Amazon Lake Formation 中有两种主要类型的权限：

- 元数据访问权限控制着在数据目录中创建、读取、更新和删除元数据数据库和表的能力。
- 基础数据访问权限控制着对数据目录资源指向的基础 Amazon S3 位置读取和写入数据的能力。

Lake Formation 结合使用自己的权限模型和 IAM 权限模型，来控制对数据目录资源和基础数据的访问权限：

- 为了使访问数据目录资源或基础数据的请求取得成功，请求必须通过由 IAM 和 Lake Formation 进行的权限检查。
- IAM 权限控制对 Lake Formation 和 Amazon Glue API 以及资源的访问权限，而 Lake Formation 权限控制对数据目录资源、Amazon S3 位置和基础数据的访问权限。

Lake Formation 权限仅适用于授予这些权限的区域，并且主体必须由数据湖管理员或其它具有必要权限的主体授权，才能获得 Lake Formation 权限。

有关更多信息，请参阅《Amazon Lake Formation 开发人员指南》中的 Lake Formation 权限概览。

请确保按照the section called “集成的先决条件”和the section called “将表存储桶与 Amazon 分析服务集成”中的步骤进行操作，以便您拥有访问 Amazon Glue Data Catalog 和表资源以及使用 Amazon 分析服务的相应权限。

> **Important**
>
> 如果您不是为您的账户执行表存储桶与 Amazon 分析服务集成的用户，则必须向您授予对表的必要 Lake Formation 权限。有关更多信息，请参阅 the section called “授予对表或数据库的权限”。

## 集成的先决条件

要将表存储桶与 Amazon 分析服务集成，需要满足以下先决条件：

- 创建表存储桶。
- 将 AWSLakeFormationDataAdmin Amazon 托管式策略附加到 Amazon Identity and Access Management（IAM）主体，以使该用户成为数据湖管理员。有关如何创建数据湖管理员的更多信息，请参阅《Amazon Lake Formation Developer Guide》中的 Create a data lake administrator。
- 向 IAM 主体添加 `glue:PassConnection` 操作的权限。
- 向 IAM 主体添加 `lakeformation:RegisterResource` 和 `lakeformation:RegisterResourceWithPrivilegedAccess` 操作的权限。
- 更新到 Amazon Command Line Interface（Amazon CLI）的最新版本。

> **Important**
>
> 创建表时，请确保在表名称和表定义中全部使用小写字母。例如，请确保列名称全部为小写。如果表名称或表定义包含大写字母，则 Amazon Lake Formation 或 Amazon Glue Data Catalog 不支持该表。在这种情况下，Amazon Athena 等 Amazon 分析服务将无法看到您的表，即使表存储桶与 Amazon 分析服务集成，也不例外。
>
> 如果表定义包含大写字母，则在 Athena 中运行 `SELECT` 查询时会收到以下错误消息：“GENERIC_INTERNAL_ERROR: Get table request failed: com.amazonaws.services.glue.model.ValidationException: Unsupported Federation Resource - Invalid table or column names.”

## 将表存储桶与 Amazon 分析服务集成

每个 Amazon 区域必须完成一次此集成。

> **Important**
>
> Amazon 分析服务集成现在可在 `registerResource` Lake Formation API 操作中使用 `WithPrivilegedAccess` 选项来注册 S3 表存储桶。现在，集成还会通过在 `CreateCatalog` Amazon Glue API 操作中使用 `AllowFullTableExternalDataAccess` 选项来在 Amazon Glue Data Catalog 中创建 `s3tablescatalog` 目录。
> 如果您使用预览版设置集成，则可以继续使用当前的集成。但是，更新的集成流程提供了性能改进，因此我们建议进行迁移。要迁移到更新的集成，请参阅the section called “迁移到更新的集成流程”。

使用 S3 控制台

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择表存储桶。
3. 选择创建表存储桶。

   此时将打开创建表存储桶页面。
4. 输入表存储桶名称，并确保选中启用集成复选框。
5. 选择创建表存储桶。Amazon S3 将尝试自动在该区域中集成您的表存储桶。

首次在任何区域中集成表存储桶时，Amazon S3 都会代表您创建一个新的 IAM 服务角色。此角色可让 Lake Formation 访问您账户中的所有表存储桶，并以联合身份验证方式访问 Amazon Glue Data Catalog 中的表。

使用 Amazon CLI

使用 Amazon CLI 集成表存储桶

以下步骤展示了如何使用 Amazon CLI 来集成表存储桶。要使用这些步骤，请将 *`user input placeholders`* 替换为您自己的信息。

1. 创建表存储桶。

```
aws s3tables create-table-bucket \
```

```
--region us-east-1 \
--name amzn-s3-demo-table-bucket
```

2. 创建可让 Lake Formation 访问表资源的 IAM 服务角色。

   a. 创建一个名为 Role-Trust-Policy.json 的文件，其中包含以下信任策略：

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Sid": "LakeFormationDataAccessPolicy",
        "Effect": "Allow",
        "Principal": {
          "Service": "lakeformation.amazonaws.com"
        },
        "Action": [
            "sts:AssumeRole",
            "sts:SetContext",
            "sts:SetSourceIdentity"
        ],
        "Condition": {
          "StringEquals": {
            "aws:SourceAccount": "111122223333"
          }
        }
      }
    ]
}
```

   使用以下命令创建 IAM 服务角色：

```
aws iam create-role \
--role-name S3TablesRoleForLakeFormation \
--assume-role-policy-document file://Role-Trust-Policy.json
```

   b. 创建一个名为 LF-GluePolicy.json 的文件，其中包含以下策略：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "LakeFormationPermissionsForS3ListTableBucket",
```

```
            "Effect": "Allow",
            "Action": [
                "s3tables:ListTableBuckets"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "LakeFormationDataAccessPermissionsForS3TableBucket",
            "Effect": "Allow",
            "Action": [
                "s3tables:CreateTableBucket",
                "s3tables:GetTableBucket",
                "s3tables:CreateNamespace",
                "s3tables:GetNamespace",
                "s3tables:ListNamespaces",
                "s3tables:DeleteNamespace",
                "s3tables:DeleteTableBucket",
                "s3tables:CreateTable",
                "s3tables:DeleteTable",
                "s3tables:GetTable",
                "s3tables:ListTables",
                "s3tables:RenameTable",
                "s3tables:UpdateTableMetadataLocation",
                "s3tables:GetTableMetadataLocation",
                "s3tables:GetTableData",
                "s3tables:PutTableData"
            ],
            "Resource": [
                "arn:aws:s3tables:us-east-1:111122223333:bucket/*"
            ]
        }
    ]
}
```

使用以下命令将策略附加到角色：

```
aws iam put-role-policy \
--role-name S3TablesRoleForLakeFormation  \
--policy-name LakeFormationDataAccessPermissionsForS3TableBucket \
--policy-document file://LF-GluePolicy.json
```

3. 创建一个名为 input.json 的文件，其中包含以下内容：

```
{
    "ResourceArn": "arn:aws:s3tables:us-east-1:111122223333:bucket/*",

    "WithFederation": true,
    "RoleArn": "arn:aws:iam::111122223333:role/S3TablesRoleForLakeFormation"
}
```

使用以下命令在 Lake Formation 中注册表存储桶：

```
aws lakeformation register-resource \
--region us-east-1 \
--with-privileged-access \
--cli-input-json file://input.json
```

4. 创建一个名为 catalog.json 的文件，其中包含以下目录：

```
{
   "Name": "s3tablescatalog",
   "CatalogInput": {
      "FederatedCatalog": {
          "Identifier": "arn:aws:s3tables:us-east-1:111122223333:bucket/*",
          "ConnectionName": "aws:s3tables"
       },
       "CreateDatabaseDefaultPermissions":[],
       "CreateTableDefaultPermissions":[],
       "AllowFullTableExternalDataAccess": "True"
   }
}
```

使用以下命令创建 s3tablescatalog 目录。创建此目录后，将使用与表存储桶、命名空间和表对应的对象填充 Amazon Glue Data Catalog。

```
aws glue create-catalog \
--region us-east-1 \
--cli-input-json file://catalog.json
```

5. 使用以下命令验证是否在 Amazon Glue 中添加了 s3tablescatalog 目录：

```
aws glue get-catalog --catalog-id s3tablescatalog
```

### 迁移到更新的集成流程

Amazon 分析服务集成流程已更新。如果您已使用预览版设置了集成，则可以继续使用当前的集成。但是，更新的集成流程提供了性能改进，因此我们建议使用以下步骤进行迁移。有关迁移或集成流程的更多信息，请参阅《Amazon Lake Formation Developer Guide》中的 Creating an Amazon S3 Tables catalog in the Amazon Glue Data Catalog。

1. 打开 Amazon Lake Formation 控制台（网址为 https://console.amazonaws.cn/lakeformation/），并以数据湖管理员身份登录。有关如何创建数据湖管理员的更多信息，请参阅《Amazon Lake Formation Developer Guide》中的 Create a data lake administrator。
2. 通过执行以下操作删除 `s3tablescatalog` 目录：
   - 在左侧导航窗格中，选择目录。
   - 在目录列表中，选择 `s3tablescatalog` 目录旁边的选项按钮。在操作 菜单上，选择删除。
3. 通过执行以下操作注销 `s3tablescatalog` 目录的数据位置：
   - 在左侧导航窗格中，转到管理部分，然后选择数据湖位置。
   - 例如，选择 `s3tablescatalog` 数据湖位置（例如 `s3://tables:region:account-id:bucket/*`）旁边的选项按钮。
   - 在操作菜单上，选择移除。
   - 在出现的确认对话框中，选择移除。
4. 现在，您已经删除了 `s3tablescatalog` 目录和数据湖位置，可以按照以下步骤，使用更新的集成流程将表存储桶与 Amazon 分析服务集成。

> **Note**
>
> 如果您想在集成的 Amazon 分析服务中使用通过 SSE-KMS 加密的表，则您使用的角色需要拥有使用您的 Amazon KMS 密钥进行加密操作的权限。有关更多信息，请参阅 向 IAM 主体授予在集成的 Amazon 分析服务中使用加密表的权限。

### 后续步骤

- 创建命名空间.
- 创建表.

## 创建指向表的命名空间的资源链接（Amazon Data Firehose）

要访问表，Amazon Data Firehose 需要一个以表的命名空间为目标的资源链接。资源链接是一个数据目录对象，它充当指向另一个数据目录资源（如数据库或表）的别名或指针。该链接存储在创建该链接的账户或区域的数据目录中。有关更多信息，请参阅《Amazon Lake Formation Developer Guide》中的 How resource links work。

将表存储桶与 Amazon 分析服务集成后，可以创建资源链接，以便在 Amazon Data Firehose 中使用表。有关创建这些链接的更多信息，请参阅the section called “Amazon Data Firehose”。

## 授予对表资源的 Lake Formation 权限

在表存储桶与 Amazon 分析服务集成后，Lake Formation 将管理对表资源的访问权限。Lake Formation 使用其自己的权限模型（Lake Formation 权限），该模型可以对数据目录资源进行精细的访问控制。Lake Formation 要求向每个 IAM 主体（用户或角色）授权对 Lake Formation 管理的资源执行操作。有关更多信息，请参阅《Amazon Lake Formation 开发人员指南》中的 Lake Formation 权限概览。有关跨账户数据共享的信息，请参阅《Amazon Lake Formation Developer Guide》中的 Cross-account data sharing in Lake Formation。

在 IAM 主体可以访问 Amazon 分析服务中的表之前，您必须向这些主体授予对这些资源的 Lake Formation 权限。

> **Note**
>
> 如果您是执行表存储桶集成的用户，则您已经拥有对表的 Lake Formation 权限。如果您是唯一将访问表的主体，则可以跳过此步骤。您只需向其它 IAM 主体授予对表的 Lake Formation 权限即可。这可让其它主体在运行查询时访问该表。有关更多信息，请参阅 授予对表或数据库的权限。

您必须向其它 IAM 主体授予对表资源的 Lake Formation 权限，才能在以下服务中使用这些资源：

- Amazon Redshift
- Amazon Data Firehose
- Amazon QuickSight
- Amazon Athena

> **Note**
>
> 对于 Amazon Data Firehose（它使用资源链接访问表），必须分别授予对资源链接和目标（链接）命名空间的权限。有关更多信息，请参阅 the section called “授予对资源链接的权限”。

授予对表或数据库的权限

您可以通过 Lake Formation 控制台或 Amazon CLI，向主体授予对表存储桶中表或数据库的 Lake Formation 权限。

> **Note**
>
> 当您将对数据目录资源的 Lake Formation 权限授予外部账户或直接授予其他账户中的 IAM 主体时，Lake Formation 会使用 Amazon Resource Access Manager (Amazon RAM) 服务共享该资源。如果被授权者账户与授予者账户在同一个组织中，则被授权者立即可以使用共享资源。如果被授权者账户不在同一个组织中，则 Amazon RAM 会向被授权者账户发送邀请，以便其接受或拒绝资源授权。然后，要使共享资源可用，被授权者账户中的数据湖管理员必须使用 Amazon RAM 控制台或 Amazon CLI 接受邀请。有关跨账户数据共享的更多信息，请参阅《Amazon Lake Formation Developer Guide》中的 Cross-account data sharing in Lake Formation。

Console

1. 打开 Amazon Lake Formation 控制台（网址为 https://console.amazonaws.cn/lakeformation/），并以数据湖管理员身份登录。有关如何创建数据湖管理员的更多信息，请参阅《Amazon Lake Formation Developer Guide》中的 Create a data lake administrator。
2. 在导航窗格中，选择数据权限，然后选择授予。
3. 在授予权限页面的主体下，执行以下操作之一：
   - 对于 Amazon Athena 或 Amazon Redshift，选择 IAM 用户和角色，然后选择您用于查询的 IAM 主体。
   - 对于 Amazon Data Firehose，选择 IAM 用户和角色，然后选择您创建的服务角色以流式传输到表中。
   - 对于 QuickSight，选择 SAML 用户和组，然后输入 QuickSight 管理员用户的 Amazon 资源名称（ARN）。
4. 在 LF 标签或目录资源下，选择命名 Data Catalog 资源。

5. 对于目录，请选择您在集成表存储桶时创建的子目录，例如 *account-id*:s3tablescatalog/*amzn-s3-demo-bucket*。
6. 对于数据库，选择您创建的 S3 表存储桶命名空间。
7. （可选）对于表，请选择您在表存储桶中创建的 S3 表。

> **Note**
>
> 如果您要在 Athena 查询编辑器中创建新表，请不要选择表。

8. 请执行以下操作之一：
   - 如果您在之前的步骤中指定了表，请为表权限选择 Super。
   - 如果您未在之前的步骤中指定表，请转到数据库权限。对于跨账户数据共享，您不能选择 Super 来向另一个主体授予对数据库的所有权限。而是应选择更精细的权限，例如描述。
9. 选择授权。

CLI

1. 务必要以数据湖管理员身份运行以下 Amazon CLI 命令。有关更多信息，请参阅《Amazon Lake Formation Developer Guide》中的 Create a data lake administrator。
2. 运行以下命令，向 IAM 主体授予对 S3 表存储桶中表的 Lake Formation 权限以访问该表。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
aws lakeformation grant-permissions \
--region us-east-1 \
--cli-input-json \
'{
    "Principal": {
        "DataLakePrincipalIdentifier": "user or role ARN, for example,
 arn:aws:iam::account-id:role/example-role"
    },
    "Resource": {
        "Table": {
            "CatalogId": "account-id:s3tablescatalog/amzn-s3-demo-bucket",
            "DatabaseName": "S3 table bucket namespace, for example,
 test_namespace",
            "Name": "S3 table bucket table name, for example test_table"
        }
    },
    "Permissions": [
```

```
        "ALL"
    ]
}'
```

# 使用 Amazon GlueIceberg REST 端点访问 Amazon S3 表

将 S3 表存储桶与 Amazon Glue Data Catalog 集成后，可以使用 Amazon Glue Iceberg REST 端点从 Apache Iceberg 兼容的客户端（例如 PyIceberg 或 Spark）连接到您的 S3 表。Amazon Glue Iceberg REST 端点实现了 Iceberg REST Catalog Open API specification，该规范提供了用于与 Iceberg 表进行交互的标准化接口。要使用端点访问 S3 表，您需要通过 IAM 策略和 Amazon Lake Formation 授权的组合来配置权限。以下各节介绍如何设置访问权限，包括创建必要的 IAM 角色、定义所需的策略以及为数据库和表级访问建立 Lake Formation 权限。

有关使用 PyIceberg 的端到端演练，请参阅 Access data in Amazon S3 Tables using PyIceberg through the Amazon Glue Iceberg REST endpoint。

先决条件

- 将表存储桶与 Amazon 分析服务集成
- 创建表命名空间
- 可以访问数据湖管理员账户

## 为客户端创建 IAM 角色

要通过 Amazon Glue 端点访问表，您需要创建一个 IAM 角色，该角色拥有执行 Amazon Glue 和 Lake Formation 操作的权限。此过程介绍如何创建此角色并配置其权限。

1. 通过 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
2. 在左侧导航窗格中，选择 Policies（策略）。
3. 选择创建策略，并在策略编辑器中选择 JSON。
4. 添加以下内联策略，该策略授予访问 Amazon Glue 和 Lake Formation 操作的权限：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
```

```
            "Action": [
                "glue:GetCatalog",
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:GetTable",
                "glue:GetTables",
                "glue:CreateTable",
                "glue:UpdateTable"
            ],
            "Resource": [
                "arn:aws:glue:<region>:<account-id>:catalog",
                "arn:aws:glue:<region>:<account-id>:catalog/s3tablescatalog",
                "arn:aws:glue:<region>:<account-id>:catalog/
s3tablescatalog/<s3_table_bucket_name>",
                "arn:aws:glue:<region>:<account-id>:table/
s3tablescatalog/<s3_table_bucket_name>/<namespace>/*",
                "arn:aws:glue:<region>:<account-id>:database/
s3tablescatalog/<s3_table_bucket_name>/<namespace>"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "lakeformation:GetDataAccess"
            ],
            "Resource": "*"
        }
    ]
}
```

5. 创建策略后，创建一个 IAM 角色，然后选择自定义信任策略作为可信实体类型。
6. 为自定义信任策略输入以下内容。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<accountid>:role/<Admin_role>"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
```

```
        }
    ]
}
```

## 在 Lake Formation 中定义访问权限

Lake Formation 为数据湖表提供精细的访问控制。当您将 S3 存储桶与 Amazon Glue Data Catalog 集成时，表会自动在 Lake Formation 中注册为资源。要访问这些表，除了 IAM 策略权限外，您还必须向您的 IAM 身份授予特定的 Lake Formation 权限。

以下步骤说明了如何应用 Lake Formation 访问控制，来支持 Iceberg 客户端连接到表。您必须以数据湖管理员身份登录，才能应用这些权限。

支持外部引擎访问表数据

在 Lake Formation 中，必须为外部引擎启用完全表访问权限，才能访问数据。这样，第三方应用程序在使用对所请求的表具有完全权限的 IAM 角色时，就可以从 Lake Formation 获取临时凭证。

通过 https://console.aws.amazon.com/lakeformation/ 打开 Lake Formation 控制台。

1. 通过 https://console.aws.amazon.com/lakeformation/ 打开 Lake Formation 控制台，并以数据湖管理员身份登录。
2. 在导航窗格中的管理下，选择应用程序集成设置。
3. 选择支持外部引擎以完全表访问权限访问 Amazon S3 位置的数据。然后选择保存。

授予 Lake Formation 对表资源的权限

接下来，向您为 Iceberg 兼容的客户端创建的 IAM 角色授予 Lake Formation 权限。这些权限将支持该角色在您的命名空间中创建和管理表。您需要同时提供数据库级和表级权限：

授予数据库权限

1. 通过 https://console.aws.amazon.com/lakeformation/ 打开 Amazon Lake Formation 控制台，然后以数据湖管理员身份登录。
2. 在导航窗格中，选择数据权限，然后选择授予。
3. 在授予权限页面的主体下，选择 IAM 用户和角色，然后选择您为访问 Amazon Glue Iceberg REST endpoint创建的 IAM 角色。
4. 在 LF 标签或目录资源下，选择命名 Data Catalog 资源。

5. 对于目录，选择为表存储桶创建的 Amazon Glue 数据目录。例如 *<accoundID>*:s3tablescatalog/*<table-bucket-name>*。
6. 对于数据库，选择 mynamespace。
7. 对于表权限，选择创建表和描述。
8. 选择授权。

授予表权限

1. 通过 https://console.aws.amazon.com/lakeformation/ 打开 Amazon Lake Formation 控制台，然后以数据湖管理员身份登录。
2. 在导航窗格中，选择数据权限，然后选择授予。
3. 在授予权限页面的主体下，选择 IAM 用户和角色，然后选择您为访问 Amazon Glue Iceberg REST endpoint创建的 IAM 角色。
4. 在 LF 标签或目录资源下，选择命名 Data Catalog 资源。
5. 对于目录，选择为表存储桶创建的 Amazon Glue 数据目录。例如 *<accoundID>*:s3tablescatalog/*<table-bucket-name>*。
6. 对于数据库，选择您创建的 S3 表存储桶命名空间。
7. 对于表，请选择 ALL_TABLES。
8. 对于表权限，选择超级。
9. 选择授权。

## 设置环境以使用端点

设置 IAM 角色（该角色具有访问表所需的权限）后，可以使用以下命令，通过您的角色配置 Amazon CLI，使用该角色从本地计算机运行 Iceberg 客户端：

```
aws sts assume-role --role-arn "arn:aws:iam::<accountid>:role/<glue-irc-role>" --role-session-name <glue-irc-role>
```

要通过 Amazon Glue REST 端点访问表，您需要在 Iceberg 兼容的客户端中初始化目录。此初始化要求指定自定义属性，包括 sigv4 属性、端点 URI 和仓库位置。按如下方式指定这些属性：

- Sigv4 属性：必须启用 Sigv4，签名名称为 glue
- 仓库位置：这是表存储桶，按以下格式指定：*<accountid>*:s3tablescatalog/*<table-bucket-name>*

- 端点 URI：有关区域特定的端点，请参阅 Amazon Glue 服务端点参考指南。

下面的示例说明如何初始化 pyIceberg 目录。

```
rest_catalog = load_catalog(
        s3tablescatalog,
**{
"type": "rest",
"warehouse": "<accountid>:s3tablescatalog/<table-bucket-name>",
"uri": "https://glue.<region>.amazonaws.com/iceberg",
"rest.sigv4-enabled": "true",
"rest.signing-name": "glue",
"rest.signing-region": region
        }
)
```

有关 Amazon Glue Iceberg REST 端点实现的更多信息，请参阅《Amazon Glue 用户指南》中的使用 Amazon GlueIceberg REST 端点连接到数据目录。

## 使用 Amazon S3 表类数据存储服务 Iceberg REST 端点访问表

您可以将 Iceberg REST 客户端连接到 Amazon S3 表类数据存储服务 Iceberg REST 端点，然后进行 REST API 调用来创建、更新或查询 S3 表存储桶中的表。该端点实现了 Apache Iceberg REST Catalog Open API specification 中指定的一组标准化 Iceberg REST API。该端点的工作原理是将 Iceberg REST API 操作转换为相应的 S3 表类数据存储服务操作。

> **Note**
>
> Amazon S3 表类数据存储服务 Iceberg REST 端点可用于访问 Amazon Partner Network（APN）目录实现或自定义目录实现中的表。如果您只需要对单个表存储桶具有基本的读/写访问权限，也可以使用它。对于其它访问场景，我们建议使用 Amazon Glue Iceberg REST 端点来连接表，这可以提供统一的表管理、集中化的治理和精细的访问控制。有关更多信息，请参阅 使用 Amazon GlueIceberg REST 端点访问 Amazon S3 表

### 配置端点

您可以使用服务端点连接到 Amazon S3 表类数据存储服务 Iceberg REST 端点。S3 表类数据存储服务 Iceberg REST 端点具有以下格式：

```
https://s3tables.<REGION>.amazonaws.com/iceberg
```

有关区域特定的端点，请参阅 S3 表类数据存储服务 Amazon Web Services 区域和端点。

目录配置属性

当使用 Iceberg 客户端将分析引擎连接到服务端点时，必须在初始化目录时指定以下配置属性。将###替换为您的区域和表存储桶的信息。

- 作为端点 URI 的区域特定的端点：`https://s3tables.<REGION>.amazonaws.com/iceberg`
- 作为仓库位置的表存储桶 ARN：`arn:aws:s3tables:<region>:<accountID>:bucket/<bucketname>`
- 用于身份验证的 Sigv4 属性。服务端点请求的 SigV4 签名名称为：`s3tables`

以下示例演示如何配置不同的客户端以使用 Amazon S3 表类数据存储服务 Iceberg REST 端点。

PyIceberg

要将 Amazon S3 表类数据存储服务 Iceberg REST 端点与 PyIceberg 结合使用，请指定以下应用程序配置属性：

```
rest_catalog = load_catalog(
  catalog_name,
  **{
    "type": "rest",
    "warehouse":"arn:aws:s3tables:<Region>:<accountID>:bucket/<bucketname>",
    "uri": "https://s3tables.<Region>.amazonaws.com/iceberg",
    "rest.sigv4-enabled": "true",
    "rest.signing-name": "s3tables",
    "rest.signing-region": "<Region>"
  }
)
```

Apache Spark

要将 Amazon S3 表类数据存储服务 Iceberg REST 端点与 Spark 结合使用，请指定以下应用程序配置属性，同时将####替换为您的区域和表存储桶的信息。

```
spark-shell \
```

```
  --packages "org.apache.iceberg:iceberg-spark-
runtime-3.5_2.12:1.4.1,software.amazon.awssdk:bundle:2.20.160,software.amazon.awssdk:url-
connection-client:2.20.160" \
  --master "local[*]" \
  --conf
 "spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions"
 \
  --conf "spark.sql.defaultCatalog=spark_catalog" \
   --conf "spark.sql.catalog.spark_catalog=org.apache.iceberg.spark.SparkCatalog" \
  --conf "spark.sql.catalog.spark_catalog.type=rest" \
  --conf "spark.sql.catalog.spark_catalog.uri=https://
s3tables.<Region>.amazonaws.com/iceberg" \
  --conf
 "spark.sql.catalog.spark_catalog.warehouse=arn:aws:s3tables:<Region>:<accountID>:bucket/
<bucketname>" \
  --conf "spark.sql.catalog.spark_catalog.rest.sigv4-enabled=true" \
  --conf "spark.sql.catalog.spark_catalog.rest.signing-name=s3tables" \
  --conf "spark.sql.catalog.spark_catalog.rest.signing-region=<Region>" \
  --conf "spark.sql.catalog.spark_catalog.io-
impl=org.apache.iceberg.aws.s3.S3FileIO" \
  --conf
 "spark.hadoop.fs.s3a.aws.credentials.provider=org.apache.hadoop.fs.s3a.SimpleAWSCredentialP
 \
  --conf "spark.sql.catalog.spark_catalog.rest-metrics-reporting-enabled=false"
```

## 对访问端点进行身份验证和授权

对 S3 表类数据存储服务的服务端点的 API 请求使用 Amazon 签名版本 4（SigV4）进行身份验证。请参阅适用于 API 请求的 Amazon 签名版本 4，以了解有关 Amazon SigV4 的更多信息。

Amazon S3 表类数据存储服务 Iceberg REST 端点请求的 SigV4 签名名称为：`s3tables`

对 Amazon S3 表类数据存储服务 Iceberg REST 端点的请求使用与 REST API 操作对应 `s3tables` IAM 操作进行授权。这些权限可以在附加到表和表存储桶的基于 IAM 身份的策略或基于资源的策略中定义。有关更多信息，请参阅 S3 表类数据存储服务的访问管理。

您可以使用 Amazon CloudTrail 跟踪通过 REST 端点向表发出的请求。请求将记录为其相应的 S3 IAM 操作。例如，`LoadTable` API 将为 `GetTableMetadataLocation` 操作生成一个管理事件，并为 `GetTableData` 操作生成一个数据事件。有关更多信息，请参阅 使用 Amazon CloudTrail 对 S3 表类数据存储服务进行日志记录。

## 前缀和路径参数

Iceberg REST 目录 API 在其请求 URL 中有一个自由格式前缀。例如，ListNamespaces API 调用使用 GET/v1/{prefix}/namespaces URL 格式。对于 S3 表类数据存储服务，REST 路径 {prefix} 始终是 url 编码的表存储桶 ARN。

例如，对于以下表存储桶 ARN：arn:aws:s3tables:*us-east-1*:111122223333:bucket/*bucketname*，前缀应为：arn%3Aaws%3As3tables%3A*us-east-1*%3A*111122223333*%3Abucket%2F*bucketname*

命名空间路径参数

Iceberg REST 目录 API 路径中的命名空间可以有多级。但是，S3 表类数据存储服务仅支持单级命名空间。要访问多级目录层次结构中的命名空间，您可以在引用命名空间时连接到命名空间之上的多级目录。与使用多级命名空间相比，这可让任何支持 catalog.namespace.table 三部分表示法的查询引擎访问 S3 表类数据存储服务的目录层次结构中的对象，而不会出现兼容性问题。

## 支持的 Iceberg REST API 操作

下表包含支持的 Iceberg REST API 以及它们与 S3 表类数据存储服务操作的对应关系。

| Iceberg REST 操作 | REST 路径 | S3 表类数据存储服务 IAM 操作 | CloudTrail EventName |
|---|---|---|---|
| getConfig | GET /v1/config | s3tables:GetTableBucket | s3tables:GetTableBucket |
| listNamespaces | GET /v1/{prefix}/namespaces | s3tables:ListNamespaces | s3tables:ListNamespaces |
| createNamespace | POST /v1/{prefix}/namespaces | s3tables:CreateNamespace | s3tables:CreateNamespace |
| loadNamespaceMetadata | GET /v1/{prefix}/namespaces/{namespace} | s3tables:GetNamespace | s3tables:GetNamespace |

| Iceberg REST 操作 | REST 路径 | S3 表类数据存储服务 IAM 操作 | CloudTrail EventName |
| --- | --- | --- | --- |
| dropNamespace | DELETE /v1/{prefix}/namespaces/{namespace} | s3tables:DeleteNamespace | s3tables:DeleteNamespace |
| listTables | GET /v1/{prefix}/namespaces/{namespace}/tables | s3tables:ListTables | s3tables:ListTables |
| createTable | POST /v1/{prefix}/namespaces/{namespace}/tables | s3tables:CreateTable ,s3tables:PutTableData | s3tables:CreateTable ,s3tables:PutObject |
| loadTable | GET /v1/{prefix}/namespaces/{namespace}/tables/{table} | s3tables:GetTableMetadataLocation , s3tables:GetTableData | s3tables:GetTableMetadataLocation , s3tables:GetObject |
| updateTable | POST /v1/{prefix}/namespaces/{namespace}/tables/{table} | s3tables:UpdateTableMetadataLocation ,s3tables:PutTableData ,s3tables:GetTableData | s3tables:UpdateTableMetadataLocation ,s3tables:PutObject ,s3tables:GetObject |

| Iceberg REST 操作 | REST 路径 | S3 表类数据存储服务 IAM 操作 | CloudTrail EventName |
|---|---|---|---|
| dropTable | DELETE /v1/{prefix}/namespaces/{namespace}/tables/{table} | s3tables:DeleteTable | s3tables:DeleteTable |
| renameTable | POST /v1/{prefix}/tables/rename | s3tables:RenameTable | s3tables:RenameTable |
| tableExists | HEAD /v1/{prefix}/namespaces/{namespace}/tables/{table} | s3tables:GetTable | s3tables:GetTable |
| namespaceExists | HEAD /v1/{prefix}/namespaces/{namespace} | s3tables:GetNamespace | s3tables:GetNamespace |

## 注意事项和限制

以下是使用 Amazon S3 表类数据存储服务 Iceberg REST 端点时的注意事项和限制。

注意事项

- CreateTable API 行为：此操作不支持 `stage-create` 选项，此选项会导致 `400 Bad Request` 错误。这意味着无法使用 `CREATE TABLE AS SELECT`（CTAS）从查询结果创建表。
- DeleteTable API 行为：您只能删除启用了清除功能的表。不支持使用 `purge=false` 删除表，这会导致 `400 Bad Request` 错误。某些版本的 Spark 即使在运行 `DROP TABLE PURGE` 命令时也始终将此标志设置为 false。可以尝试使用 `DROP TABLE PURGE` 或使用 S3 表类数据存储服务 DeleteTable 操作来删除表。

- 该端点仅支持标准的表元数据操作。要进行表维护，例如快照管理和压缩，请使用 S3 表类数据存储服务维护 API 操作。有关更多信息，请参阅 S3 表类数据存储服务维护。

限制

- 不支持多级命名空间。
- 不支持基于 OAuth 的身份验证。
- 命名空间仅支持 `owner` 属性。
- 不支持 Apache Iceberg REST Open API specification 中定义的与视图相关的 API。
- 不支持对 `metadata.json` 文件超过 5 MB 的表运行操作，否则将返回 `400 Bad Request` 错误。要控制 `metadata.json` 文件的大小，请使用表维护操作。有关更多信息，请参阅 S3 表类数据存储服务维护。

# 使用适用于 Apache Iceberg 的 Amazon S3 表类数据存储服务目录访问 Amazon S3 表

可以使用适用于 Apache Iceberg 的 Amazon S3 表类数据存储服务目录客户端目录，从开源查询引擎（例如 Apache Spark）访问 S3 表。适用于 Apache Iceberg 的 Amazon S3 表类数据存储服务目录是由 Amazon 实验室托管的开源库。它的工作原理是将查询引擎中的 Apache Iceberg 操作（例如表发现、元数据更新以及添加或移除表）转换为 S3 表类数据存储服务类 API 操作。

适用于 Apache Iceberg 的 Amazon S3 表类数据存储服务目录以名为 `s3-tables-catalog-for-iceberg.jar` 的 Maven JAR 形式分发。可以从 Amazon Labs GitHub repository 中构建客户端目录 JAR，也可以从 Maven 下载它。连接到表时，在为 Apache Iceberg 初始化 Spark 会话的过程中，客户端目录 JAR 将用作依赖关系。

## 将适用于 Apache Iceberg 的 Amazon S3 表类数据存储服务目录与 Apache Spark 结合使用

初始化 Spark 会话时，可以使用适用于 Apache Iceberg 的 Amazon S3 表类数据存储服务目录客户端目录，从开源应用程序连接到表。在会话配置中，您可以指定 Iceberg 和 Amazon S3 依赖关系，并创建将表存储桶用作元数据仓库的自定义目录。

先决条件

- 可以访问表存储桶和 S3 表类数据存储服务操作的 IAM 身份。有关更多信息，请参阅 S3 表类数据存储服务的访问管理。

使用适用于 Apache Iceberg 的 Amazon S3 表类数据存储服务目录初始化 Spark 会话

- 使用以下命令初始化 Spark。要使用该命令，请将适用于 Apache Iceberg 的 Amazon S3 表类数据存储服务目录*###*替换为 Amazon Labs GitHub repository 中的最新版本，并将*#### ARN* 替换为您自己的表存储桶 ARN。

```
spark-shell \
--packages org.apache.iceberg:iceberg-spark-
runtime-3.5_2.12:1.6.1,software.amazon.s3tables:s3-tables-catalog-for-iceberg-
runtime:0.1.4 \
--conf spark.sql.catalog.s3tablesbucket=org.apache.iceberg.spark.SparkCatalog \
--conf spark.sql.catalog.s3tablesbucket.catalog-
impl=software.amazon.s3tables.iceberg.S3TablesCatalog \
--conf spark.sql.catalog.s3tablesbucket.warehouse=arn:aws:s3tables:us-
east-1:111122223333:bucket/amzn-s3-demo-table-bucket \
--conf
 spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions
```

使用 Spark SQL 查询 S3 表

使用 Spark，您可以对 S3 表运行 DQL、DML 和 DDL 操作。查询表时，请使用完全限定的表名称，包括遵循以下规律的会话目录名称：

*CatalogName*.*NamespaceName*.*TableName*

以下示例查询显示了您可以与 S3 表进行交互的一些方式。要在查询引擎中使用这些示例查询，请将*#########*值替换为您自己的信息。

使用 Spark 查询表

- 创建命名空间

```
spark.sql(" CREATE NAMESPACE IF NOT EXISTS s3tablesbucket.my_namespace")
```

- 创建表

```
spark.sql(" CREATE TABLE IF NOT EXISTS s3tablesbucket.my_namespace.`my_table`
( id INT, name STRING, value INT ) USING iceberg ")
```

- 查询表

```
spark.sql(" SELECT * FROM s3tablesbucket.my_namespace.`my_table` ").show()
```

- 将数据插入表中

```
spark.sql(
"""
    INSERT INTO s3tablesbucket.my_namespace.my_table
    VALUES
        (1, 'ABC', 100),
        (2, 'XYZ', 200)
""")
```

- 将现有数据文件加载到表中

1. 将数据读入 Spark。

```
val data_file_location = "Path such as S3 URI to data file"
val data_file = spark.read.parquet(data_file_location)
```

2. 将数据写入 Iceberg 表。

```
data_file.writeTo("s3tablesbucket.my_namespace.my_table").using("Iceberg").tableProperty
 ("format-version", "2").createOrReplace()
```

## 使用 Athena 查询 Amazon S3 表类数据存储服务

Amazon Athena 是一种交互式查询服务，可用于通过使用标准 SQL 直接分析 Amazon S3 中的数据。有关更多信息，请参阅《Amazon Athena 用户指南》中的 什么是 Amazon Athena？。

将表存储桶与 Amazon 分析服务集成后，可以使用 Athena 对 S3 表运行数据定义语言（DDL）、数据操作语言（DML）和数据查询语言（DQL）查询。有关如何查询表存储桶中的表的更多信息，请参阅《Amazon Athena 用户指南》中的注册 S3 表存储桶目录。

还可以在 Athena 中从 Amazon S3 控制台运行查询。

使用 S3 控制台和 Amazon Athena

以下过程使用 Amazon S3 控制台访问 Athena 查询编辑器，以便您可以使用 Amazon Athena 查询表。

> **Note**
>
> 在执行以下步骤之前，请确保您已在此区域中将表存储桶与 Amazon 分析服务集成。有关更多信息，请参阅 the section called “将 S3 表类数据存储服务与 Amazon 分析服务结合使用”。

查询表

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择表存储桶。
3. 在表存储桶页面上，选择包含要查询的表的存储桶。
4. 在存储桶详细信息页面上，选择要查询的表名称旁边的选项按钮。
5. 选择使用 Athena 查询表。
6. Amazon Athena 控制台打开，Athena 查询编辑器随即出现，其中包含为您加载的示例 SELECT 查询。根据您的用例需要修改此查询。

   在查询编辑器中，目录字段中应填充 s3tablescatalog/，后跟表存储桶的名称，例如 s3tablescatalog/***amzn-s3-demo-bucket***。数据库字段中应填充在其中存储表的命名空间。

   > **Note**
   >
   > 如果您在目录和数据库字段中看不到这些值，请确保您已在该区域中将表存储桶与 Amazon 分析服务集成。有关更多信息，请参阅 the section called “将 S3 表类数据存储服务与 Amazon 分析服务结合使用”。

7. 要运行查询，请选择 Run（运行）。

   > **Note**
   >
   > - 如果您在尝试在 Athena 中运行查询时收到错误“权限不足，无法执行查询。主体对指定的资源没有任何权限”，则必须向您授予对于表的必需 Lake Formation 权限。有关更多信息，请参阅 the section called “授予对表或数据库的权限”。
   > - 如果您在尝试运行查询时收到错误“Iceberg 无法访问所请求的资源”，请转到 Amazon Lake Formation 控制台，并确保您已授予自己对您创建的表存储桶目录和数据库（命名

空间）的权限。授予这些权限时请勿指定表。有关更多信息，请参阅 the section called “授予对表或数据库的权限”。

- 如果在 Athena 中运行 SELECT 查询时收到以下错误消息，则此消息是由表名称中或表定义的列名称中具有大写字母而引起的：“GENERIC_INTERNAL_ERROR: Get table request failed: com.amazonaws.services.glue.model.ValidationException: Unsupported Federation Resource - Invalid table or column names.” 确保表名称和列名称全部为小写。

## 使用 Amazon Redshift 访问 Amazon S3 表类数据存储服务

Amazon Redshift 是一项快速且完全托管的 PB 级数据仓库服务，可让您使用现有的商业智能工具轻松且经济高效地分析所有数据。Redshift Serverless 让您可以访问和分析数据，而无需对预置数据仓库进行所有配置。有关更多信息，请参阅《Amazon Redshift 入门指南》中的 Serverless 数据仓库入门。

### 使用 Amazon Redshift 查询 Amazon S3 表

先决条件

- 将表存储桶与 Amazon 分析服务集成。
  - 创建命名空间.
  - 创建表.
- 授予对表资源的 Lake Formation 权限.

满足先决条件后，可以通过以下方式之一开始使用 Amazon Redshift 来查询表：

- 使用 Amazon Redshift 查询编辑器 V2
- 使用 SQL 客户端工具连接到 Amazon Redshift 数据仓库
- 使用 Amazon Redshift 数据 API

## 使用 Amazon EMR 访问 Amazon S3 表类数据存储服务

Amazon EMR（以前称为 Amazon Elastic MapReduce）是一个托管式集群平台，可简化在 Amazon 上运行大数据框架（如 Apache Hadoop 和 Apache Spark）的过程，以处理和分析海量数据。使用这些框架和相关的开源项目，您可以处理用于分析目的的数据和业务情报工作负载。Amazon EMR 还可让您转换大量数据，并将数据移入/移出其它 Amazon 数据存储和数据库。

通过在 Spark 会话中连接到表存储桶，您可以使用 Amazon EMR 中的 Apache Iceberg 集群来处理 S3 表类数据存储服务。要连接到 Amazon EMR 中的表存储桶，可以通过 Amazon Glue Data Catalog 使用 Amazon 分析服务集成，也可以使用适用于 Apache Iceberg 的开源 Amazon S3 表类数据存储服务目录客户端目录。

> **Note**
>
> Amazon EMR version 7.5 或更高版本支持 S3 表类数据存储服务。

## 在 Amazon EMR Iceberg 集群上使用 Spark 连接到 S3 表存储桶

在此过程中，您设置为 Apache Iceberg 配置的 Amazon EMR 集群，然后启动连接到表存储桶的 Spark 会话。您可以通过 Amazon Glue 使用 Amazon 分析服务集成来设置此项，也可以使用适用于 Apache Iceberg 的开源 Amazon S3 表类数据存储服务目录客户端目录。有关客户端目录的信息，请参阅使用 Amazon S3 表类数据存储服务 Iceberg REST 端点访问表。

从以下选项中选择在 Amazon EMR 中使用表的方法。

Amazon S3 Tables Catalog for Apache Iceberg

使用适用于 Apache Iceberg 的 Amazon S3 表类数据存储服务目录在 Amazon EMR 上通过 Spark 查询表需要满足以下先决条件。

先决条件

- 将 `AmazonS3TablesFullAccess` 策略附加到您用于 Amazon EMR 的 IAM 角色。

设置 Amazon EMR 集群以使用 Spark 查询表

1. 使用以下配置创建集群。要使用此示例，请将 *`user input placeholders`* 替换为您自己的信息。

```
aws emr create-cluster --release-label emr-7.5.0 \
--applications Name=Spark \
--configurations file://configurations.json \
--region us-east-1 \
--name My_Spark_Iceberg_Cluster \
--log-uri s3://amzn-s3-demo-bucket/ \
--instance-type m5.xlarge \
--instance-count 2 \
```

```
--service-role EMR_DefaultRole \
--ec2-attributes \

InstanceProfile=EMR_EC2_DefaultRole,SubnetId=subnet-1234567890abcdef0,KeyName=my-key-pair
```

configurations.json:

```
[{
"Classification":"iceberg-defaults",
"Properties":{"iceberg.enabled":"true"}
}]
```

2. Connect to the Spark primary node using SSH.
3. 要初始化 Iceberg 的连接到表存储桶的 Spark 会话，请输入以下命令。将 *user input placeholders* 替换为表存储桶 ARN。

```
spark-shell \
--packages software.amazon.s3tables:s3-tables-catalog-for-iceberg-runtime:0.1.3
 \
--conf spark.sql.catalog.s3tablesbucket=org.apache.iceberg.spark.SparkCatalog \
--conf spark.sql.catalog.s3tablesbucket.catalog-
impl=software.amazon.s3tables.iceberg.S3TablesCatalog \
--conf spark.sql.catalog.s3tablesbucket.warehouse=arn:aws:s3tables:us-
east-1:111122223333:bucket/amzn-s3-demo-bucket1 \
--conf spark.sql.defaultCatalog=s3tablesbucket \
--conf
 spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions
```

4. 使用 Spark SQL 查询表。有关示例查询，请参阅the section called “使用 Spark SQL 查询 S3 表”。

## Amazon analytics services integration

使用 Amazon 分析服务集成在 Amazon EMR 上通过 Spark 查询表需要满足以下先决条件。

先决条件

- 将表存储桶与 Amazon 分析服务集成。
- 创建指向命名空间的资源链接.

- 为 Amazon EMR 创建默认服务角色 (EMR_DefaultRole_V2)。有关详细信息，请参阅 Service role for Amazon EMR (EMR role)。
- 为 Amazon EMR 创建 Amazon EC2 实例配置文件 (EMR_EC2_DefaultRole)。有关详细信息，请参阅 Service role for cluster EC2 instances (EC2 instance profile)。
  - 将 AmazonS3TablesFullAccess 策略附加到 EMR_EC2_DefaultRole。

设置 Amazon EMR 集群以使用 Spark 查询表

1. 使用以下配置创建集群。要使用此示例，请将 *user input placeholder* 值替换为您自己的信息。

```
aws emr create-cluster --release-label emr-7.5.0 \
--applications Name=Spark \
--configurations file://configurations.json \
--region us-east-1 \
--name My_Spark_Iceberg_Cluster \
--log-uri s3://amzn-s3-demo-bucket/ \
--instance-type m5.xlarge \
--instance-count 2 \
--service-role EMR_DefaultRole \
--ec2-attributes \

InstanceProfile=EMR_EC2_DefaultRole,SubnetId=subnet-1234567890abcdef0,KeyName=my-key-pair
```

   configurations.json:

```
[{
"Classification":"iceberg-defaults",
"Properties":{"iceberg.enabled":"true"}
}]
```

2. Connect to the Spark primary node using SSH.
3. 输入以下命令来初始化 Iceberg 的连接到表的 Spark 会话。将 *user input placeholders* 替换为您自己的信息。

```
spark-shell \
```

```
--conf
 spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions
 \
--conf spark.sql.defaultCatalog=s3tables \
--conf spark.sql.catalog.s3tables=org.apache.iceberg.spark.SparkCatalog \
--conf spark.sql.catalog.s3tables.catalog-
impl=org.apache.iceberg.aws.glue.GlueCatalog \
--conf spark.sql.catalog.s3tables.client.region=us-east-1 \
--conf spark.sql.catalog.s3tables.glue.id=111122223333
```

4. 使用 Spark SQL 查询表。有关示例查询，请参阅the section called “使用 Spark SQL 查询 S3 表”

> **Note**
>
> 如果您在 Amazon EMR 中使用 `DROP TABLE PURGE` 命令：
>
> - Amazon EMR 版本 7.5
>
>  将 Spark 配置 `spark.sql.catalog.your-catalog-name.cache-enabled` 设置为 `false`。如果此配置设置为 `true`，请在新的会话或应用程序中运行该命令，这样就不会激活表缓存。
>
> - 高于 7.5 的 Amazon EMR 版本
>
>  不支持 `DROP TABLE`。可以使用 S3 表类数据存储服务 `DeleteTable` REST API 来删除表。

## 使用 QuickSight 实现表数据可视化

QuickSight 是一项快速业务分析服务，可用于构建可视化内容，执行临时分析，并快速地从您的数据中获得业务见解。QuickSight 无缝地发现 Amazon 数据来源，使组织可以扩展至数十万用户，并通过使用 QuickSight 超快、并行、内存、计算引擎（SPICE）提供快速的响应式查询性能。有关更多信息，请参阅《QuickSight user guide》中的 What is QuickSight?

将表存储桶与 Amazon 分析服务集成后，可以从表中创建数据集，然后通过从查询引擎中使用 SPICE 或直接 SQL 查询，来在 QuickSight 中使用这些数据集。QuickSight 支持 Athena 作为 S3 表的数据来源。

## 为 QuickSight 配置访问表的权限

在 QuickSight 中处理 S3 表数据之前，您必须向 QuickSight 服务角色、QuickSight 管理员用户授予权限，并向 Lake Formation 授予对您要访问的表的权限。

向 QuickSight 服务角色授予权限

首次在账户中设置 QuickSight 时，Amazon 会创建一个服务角色，让 QuickSight 访问其它 Amazon 服务（例如 Athena 或 Amazon Redshift）中的数据来源。默认角色名为 `aws-quicksight-service-role-v0`。

1. 通过 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
2. 选择角色，然后选择 QuickSight 服务角色。默认名称为 `aws-quicksight-service-role-v0`
3. 选择添加权限，然后选择创建内联策略。
4. 选择 JSON 以打开 JSON 策略编辑器，然后添加以下策略。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "glue:GetCatalog",
      "Resource": "*"
    }
  ]
}
```

5. 选择下一步，输入策略名称，然后创建策略。

为 QuickSight 管理员用户配置权限

1. 运行以下 Amazon CLI 命令以查找 QuickSight 管理员用户的 ARN。

```
aws quicksight list-users --aws-account-id 111122223333 --namespace default --
region region
```

2. 向 Lake Formation 授予对此 ARN 的权限 有关更多信息，请参阅 授予对表资源的 Lake Formation 权限。

### 在 QuickSight 中使用表数据

可以使用 Athena 作为数据来源连接到表数据。

先决条件

- 将表存储桶与 Amazon 分析服务集成。
  - 创建命名空间.
  - 创建表.
  - 为 QuickSight 配置访问表的权限.
- Sign up for QuickSight。

1. 登录您的 QuickSight 账户，网址为 https://quicksight.aws.amazon.com/
2. 在控制面板中，选择新分析。
3. 选择新数据集。
4. 选择 Athena。
5. 输入数据来源名称，然后选择创建数据来源。
6. 选择使用自定义 SQL。您将无法从选择您的表窗格中选择您的表。
7. 输入用于捕获要可视化的列的 Athena SQL 查询，然后选择确认查询。例如，使用以下查询选择所有列：

```
SELECT * FROM "s3tablescatalog/table-bucket-name".namespace.table-name
```

8. 选择可视化以分析数据并开始构建控制面板。有关更多信息，请参阅 Visualizing data in QuickSight 和 Exploring interactive dashboards in QuickSight

## 使用 Amazon Data Firehose 将数据流式传输到表

Amazon Data Firehose 是一项完全托管式服务，用于实时将流数据传输到目标，如 Amazon S3、Amazon Redshift、Amazon OpenSearch Service、Splunk、Apache Iceberg 表和自定义 HTTP 端点或由受支持的第三方服务提供商拥有的 HTTP 端点。在使用 Amazon Data Firehose 时，您无需编写应用程序或管理资源。您可以配置数据生成工具向 Firehose 发送数据，然后 Firehose 会将数据自动传输到您指定的目标。还可以配置 Firehose 在传输数据之前转换数据。要了解有关 Amazon Data Firehose 的更多信息，请参阅 What is Amazon Data Firehose?

将表存储桶与 Amazon 分析服务集成后，您可以执行以下操作：

1. 配置 Firehose 以将数据传输到 S3 表中。为此，您需要创建一个支持 Firehose 访问表的 Amazon Identity and Access Management（IAM）服务角色。
2. 创建指向表或表的命名空间的资源链接。
3. 通过授予对资源链接的权限，向 Firehose 服务角色授予对表或表命名空间的显式权限。
4. 创建一个 Firehose 流来将数据路由到表。

## 为 Firehose 创建一个角色以使用 S3 表作为目标

Firehose 需要具有特定权限的 IAM 服务角色，才能访问 Amazon Glue 表并将数据写入 S3 表。在创建 Firehose 流时，您需要提供此 IAM 角色。

1. 通过 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
2. 在左侧导航窗格中，选择策略
3. 选择创建策略，并在策略编辑器中选择 JSON。
4. 添加以下内联策略，来授予对数据目录中所有数据库和表的权限。如果需要，则您可以仅向特定的表和数据库授予权限。要使用这一策略，请将 *user input placeholders* 替换为您自己的信息。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3TableAccessViaGlueFederation",
      "Effect": "Allow",
      "Action": [
        "glue:GetTable",
        "glue:GetDatabase",
        "glue:UpdateTable"
      ],
      "Resource": [
        "arn:aws:glue:region:account-id:catalog/s3tablescatalog/*",
        "arn:aws:glue:region:account-id:catalog/s3tablescatalog",
        "arn:aws:glue:region:account-id:catalog",
        "arn:aws:glue:region:account-id:database/*",
        "arn:aws:glue:region:account-id:table/*/*"
      ]
    },
    {
      "Sid": "S3DeliveryErrorBucketPermission",
```

```
      "Effect": "Allow",
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::error delivery bucket",
        "arn:aws:s3:::error delivery bucket/*"
      ]
    },
    {
      "Sid": "RequiredWhenUsingKinesisDataStreamsAsSource",
      "Effect": "Allow",
      "Action": [
        "kinesis:DescribeStream",
        "kinesis:GetShardIterator",
        "kinesis:GetRecords",
        "kinesis:ListShards"
      ],
      "Resource": "arn:aws:kinesis:region:account-id:stream/stream-name"
    },
    {
      "Sid":
"RequiredWhenDoingMetadataReadsANDDataAndMetadataWriteViaLakeformation",
      "Effect": "Allow",
      "Action": [
        "lakeformation:GetDataAccess"
      ],
      "Resource": "*"
    },
    {
      "Sid": "RequiredWhenUsingKMSEncryptionForS3ErrorBucketDelivery",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": [
        "arn:aws:kms:region:account-id:key/KMS-key-id"
      ],
```

```
      "Condition": {
        "StringEquals": {
          "kms:ViaService": "s3.region.amazonaws.com"
        },
        "StringLike": {
          "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::error delivery bucket/
prefix*"
        }
      }
    },
    {
      "Sid": "LoggingInCloudWatch",
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:region:account-id:log-group:log-group-name:log-stream:log-
stream-name"
      ]
    },
    {
      "Sid": "RequiredWhenAttachingLambdaToFirehose",
      "Effect": "Allow",
      "Action": [
        "lambda:InvokeFunction",
        "lambda:GetFunctionConfiguration"
      ],
      "Resource": [
        "arn:aws:lambda:region:account-id:function:function-name:function-version"
      ]
    }
  ]
}
```

此策略有一些语句，支持访问 Kinesis Data Streams、调用 Lambda 函数和访问 Amazon KMS 密钥。如果您不使用这些资源中的任何一个，则可以删除相应的语句。

如果启用了错误日志记录，则 Firehose 还会将数据传输错误发送到您的 CloudWatch 日志组和流。为此，您必须配置日志组和日志流名称。对于日志组和日志流名称，请参阅 Monitor Amazon Data Firehose Using CloudWatch Logs。

5. 创建策略后，创建一个 IAM 角色，其中 Amazon 服务为可信实体类型。

6. 对于服务或使用案例，选择 Kinesis。对于使用案例，选择 Kinesis Firehose。
7. 选择下一步，然后选择之前创建的策略。
8. 为您的角色命名。检查角色详细信息，然后选择创建角色。该角色将具有以下信任策略。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Principal": {
                "Service": [
                    "firehose.amazonaws.com"
                ]
            }
        }
    ]
}
```

## 创建指向表命名空间的资源链接

要访问表，Amazon Data Firehose 需要一个以表的命名空间为目标的资源链接。资源链接是一个数据目录对象，它充当指向另一个数据目录资源（如数据库或表）的别名或指针。该链接存储在创建该链接的账户或区域的数据目录中。有关更多信息，请参阅《Amazon Lake Formation Developer Guide》中的 How resource links work。

将表存储桶与 Amazon 分析服务集成后，可以创建资源链接，以便在 Firehose 中使用表。

您可以创建指向表命名空间的资源链接，然后提供指向 Firehose 的链接名称，以便 Firehose 可以处理链接的表。

以下 Amazon CLI 命令创建一个资源链接，您可以使用该链接将 S3 表连接到 Firehose。要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws glue create-database --region us-east-1 \
--catalog-id "111122223333" \
--database-input \
'{
  "Name": "resource-link-name",
```

```
  "TargetDatabase": {
    "CatalogId": "111122223333:s3tablescatalog/amzn-s3-demo-table-bucket",
    "DatabaseName": "my_namespace"
  },
  "CreateTableDefaultPermissions": []
}'
```

> **Note**
>
> 必须分别授予对资源链接和目标（链接）命名空间的权限。有关更多信息，请参阅 the section called “授予对资源链接的权限”。

## 授予对资源链接的权限

使用资源链接访问表时，必须分别授予对资源链接和目标（链接）命名空间或表的权限。您可以通过 Lake Formation 控制台或 Amazon CLI，向 IAM 主体授予对链接到表命名空间的资源链接的 Lake Formation 权限。

Console

1. 打开 Amazon Lake Formation 控制台（网址为 https://console.amazonaws.cn/lakeformation/），并以数据湖管理员身份登录。有关如何创建数据湖管理员的更多信息，请参阅《Amazon Lake Formation Developer Guide》中的 Create a data lake administrator。
2. 在导航窗格中，选择数据权限，然后选择授予。
3. 在授予权限页面的主体下，选择 IAM 用户和角色，然后选择您创建的用于流式传输到表的服务角色。
4. 在 LF 标签或目录资源下，选择命名 Data Catalog 资源。
5. 对于目录，选择您的账户 ID，即默认目录。
6. 对于数据库，选择为表命名空间创建的资源链接。
7. 对于资源链接权限，选择描述。
8. 选择授权。

CLI

1. 务必要以数据湖管理员身份运行 Amazon CLI 命令。有关更多信息，请参阅《Amazon Lake Formation Developer Guide》中的 Create a data lake administrator。

2. 运行以下命令，向 IAM 主体授予对 S3 表存储桶中表的 Lake Formation 权限，以便主体可以访问该表。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。DataLakePrincipalIdentifier 值可以是 IAM 用户或角色 ARN。

```
aws lakeformation grant-permissions \


  --principal DataLakePrincipalIdentifier=arn:aws:iam::account-id:role/role-name \
  --resource Database='{CatalogId=account-id, Name=database-name}' \
  --permissions DESCRIBE
```

## 设置到 S3 表的 Firehose 流

以下过程说明如何设置 Firehose 流以使用控制台向 S3 表传输数据。要设置到 S3 表的 Firehose 流，需要满足以下先决条件。

先决条件

- 将表存储桶与 Amazon 分析服务集成。
  - 创建命名空间.
  - 创建表.
- 创建供 Firehose 访问 S3 表类数据存储服务的角色。
- 创建指向命名空间的资源链接，以成为流的目标。

> **Note**
>
> 当您为 Firehose 创建资源链接时，名称只能由大写字母、小写字母和下划线（_）组成。

- 向您创建的用于流式传输到表的 Firehose 服务角色授予对表资源的 Lake Formation 权限。

> **Note**
>
> 必须分别授予对资源链接和目标（链接）命名空间或表的权限。Firehose 需要对于资源链接的描述权限。

要在配置流时向 Firehose 提供路由信息，可以使用为命名空间创建的资源链接名称作为数据库名称和该命名空间中表的名称。可以在 Firehose 流配置的“唯一键”部分使用这些值，来将数据路由到单

个表。也可以使用这些值通过 JSON 查询表达式路由到表。有关更多信息，请参阅 Route incoming records to a single Iceberg table。

设置到 S3 表的 Firehose 流（控制台）

1. 在 https://console.aws.amazon.com/firehose/ 中打开 Firehose 控制台。
2. 选择创建 Firehose 流。
3. 对于源，选择下列源之一：
   - Amazon Kinesis Data Streams
   - Amazon MSK
   - 直接 PUT
4. 对于目标，选择 Apache Iceberg 表。
5. 输入 Firehose 流名称。
6. 配置源设置。
7. 对于目标设置，选择当前账户和要流式传输到的表的 Amazon 区域。
8. 使用唯一密钥配置、JSONQuery 表达式或在 Lambda 函数中配置数据库和表名称。有关更多信息，请参阅《Amazon Data Firehose Developer Guide》中的 Route incoming records to a single Iceberg table 和 Route incoming records to different Iceberg tables。
9. 在备份设置下，指定 S3 备份存储桶。
10. 对于高级设置下的现有 IAM 角色，选择您为 Firehose 创建的 IAM 角色。
11. 选择创建 Firehose 流。

有关您可以为流配置的其它设置的更多信息，请参阅《Amazon Data Firehose Developer Guide》中的 Set up the Firehose stream。

## 使用 Amazon Glue 对 Amazon S3 表运行 ETL 任务

Amazon Glue 是一项无服务器数据集成服务，可让使用分析功能的用户轻松发现、准备、移动和集成来自多个来源的数据。可以使用 Amazon Glue 运行提取、转换、加载（ETL）管道，来将数据加载到数据湖中。有关 Amazon Glue 的更多信息，请参阅《Amazon Glue 开发人员指南》中的什么是 Amazon Glue？。

Amazon Glue 作业将封装连接到源数据的脚本，处理该脚本，然后将其写入数据目标。通常，作业运行提取、转换和加载 (ETL) 脚本。作业可以运行专为 Apache Spark 运行时环境设计的脚本。您可以监控作业运行以了解运行时指标（例如完成状态、持续时间和开始时间）。

您可以使用 Amazon Glue 作业来处理 S3 表中的数据，方法是通过与 Amazon 分析服务的集成连接到表，或者直接使用 Amazon S3 表类数据存储服务 Iceberg REST 端点或适用于 Apache Iceberg 的 Amazon S3 表类数据存储服务目录进行连接。本指南涵盖了开始将 Amazon Glue 与 S3 表类数据存储服务结合使用的基本步骤，包括：

主题


- 先决条件
- 创建用于连接到表存储桶的脚本
- 创建用于查询表的 Amazon Glue 作业


> **Note**
>
> Amazon Glue 版本 5.0 或更高版本支持 S3 表类数据存储服务。

## 先决条件

在可以从 Amazon Glue 任务中查询表之前，必须配置 Amazon Glue 可用于运行该任务的 IAM 角色，并将适用于 Apache Iceberg 的 Amazon S3 表类数据存储服务目录 JAR 上传到 Amazon Glue 运行任务时可以访问的 S3 存储桶。

- 将表存储桶与 Amazon 分析服务集成。
- 为 Amazon Glue 创建 IAM 角色。
  - 将 `AmazonS3TablesFullAccess` 托管式策略附加到角色。
  - 将 `AmazonS3FullAccess` 托管式策略附加到角色。
- （可选）如果您使用的是适用于 Apache Iceberg 的 Amazon S3 表类数据存储服务目录，则需要下载客户端目录 JAR 并将其上传到 S3 存储桶。

  下载目录 JAR

  1. 在 Maven Central 上检查最新版本。您可以使用浏览器或使用以下命令从 Maven Central 下载 JAR。请务必将*###*替换为最新版本。

     ```
     wget https://repo1.maven.org/maven2/software/amazon/s3tables/s3-tables-catalog-for-iceberg-runtime/0.1.5/s3-tables-catalog-for-iceberg-runtime-0.1.5.jar
     ```

2. 将下载的 JAR 上传到 Amazon Glue IAM 角色可以访问的 S3 存储桶。您可以使用以下 Amazon CLI 命令来上传 JAR。请务必将###替换为最新版本，并将#####和##替换为您自己的信息。

```
aws s3 cp s3-tables-catalog-for-iceberg-runtime-0.1.5.jar s3://amzn-s3-demo-bucket/jars/
```

## 创建用于连接到表存储桶的脚本

要在运行 Amazon Glue ETL 作业时访问表数据，可以为 Apache Iceberg 配置一个 Spark 会话，用于连接到 S3 表存储桶。可以修改现有脚本以连接到表存储桶或创建新脚本。有关创建 Amazon Glue 脚本的更多信息，请参阅《Amazon Glue 开发人员指南》中的教程：编写 Amazon Glue for Spark 脚本。

可以将会话配置为通过以下任一 S3 表类数据存储服务访问方法连接到表存储桶：

- S3 表类数据存储服务与 Amazon 分析服务集成
- Amazon S3 表类数据存储服务 Iceberg REST 端点
- 适用于 Apache Iceberg 的 Amazon S3 表类数据存储服务目录

从以下访问方法中进行选择，以查看设置说明和配置示例。

Amazon analytics services integration

作为使用 Amazon 分析服务集成在 Amazon Glue 上使用 Spark 查询表的先决条件，您必须将表存储桶与 Amazon 分析服务进行集成

可以通过作业中的 Spark 会话或交互式会话中的 Amazon Glue Studio 魔法来配置与表存储桶的连接。要使用以下示例，请将####替换为您自己的表存储桶的信息。

使用 PySpark 脚本

在 PySpark 脚本中使用以下代码段，以便将 Amazon Glue 作业配置为使用集成连接到表存储桶。

```
spark = SparkSession.builder.appName("SparkIcebergSQL") \
    .config("spark.sql.extensions",
 "org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions") \
    .config("spark.sql.defaultCatalog","s3tables") \
```

```
    .config("spark.sql.catalog.s3tables",
 "org.apache.iceberg.spark.SparkCatalog") \
    .config("spark.sql.catalog.s3tables.catalog-impl",
 "org.apache.iceberg.aws.glue.GlueCatalog") \
    .config("spark.sql.catalog.s3tables.glue.id",
 "111122223333:s3tablescatalog/amzn-s3-demo-table-bucket") \
    .config("spark.sql.catalog.s3tables.warehouse", "s3://amzn-s3-demo-table-
bucket/warehouse/") \
    .getOrCreate()
```

使用交互式 Amazon Glue 会话

如果您将交互式笔记本会话与 Amazon Glue 5.0 结合使用，请在执行代码之前，在单元格中使用 %%configure 魔法指定相同的配置。

```
%%configure
{
    "conf": {
        "spark.sql.defaultCatalog": "s3tables",
        "spark.sql.extensions":
 "org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions",
        "spark.sql.catalog.s3tables": "org.apache.iceberg.spark.SparkCatalog",
        "spark.sql.catalog.s3tables.catalog-impl":
 "org.apache.iceberg.aws.glue.GlueCatalog",
        "spark.sql.catalog.s3tables.glue.id": "111122223333:s3tablescatalog/amzn-
s3-demo-table-bucket",
        "spark.sql.catalog.s3tables.warehouse": "s3://amzn-s3-demo-table-bucket/
warehouse/"
    }
}
```

## Amazon S3 Tables Iceberg REST endpoint

可以通过作业中的 Spark 会话或交互式会话中的 Amazon Glue Studio 魔法来配置与表存储桶的连接。要使用以下示例，请将####替换为您自己的表存储桶的信息。

使用 PySpark 脚本

在 PySpark 脚本中使用以下代码段，以便将 Amazon Glue 作业配置为使用端点连接到表存储桶。

```
spark = SparkSession.builder.appName("glue-s3-tables-rest") \
```

```
    .config("spark.sql.extensions",
 "org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions") \
    .config("spark.sql.defaultCatalog", "s3_rest_catalog") \
    .config("spark.sql.catalog.s3_rest_catalog",
 "org.apache.iceberg.spark.SparkCatalog") \
    .config("spark.sql.catalog.s3_rest_catalog.type", "rest") \
    .config("spark.sql.catalog.s3_rest_catalog.uri", "https://
s3tables.Region.amazonaws.com/iceberg") \
    .config("spark.sql.catalog.s3_rest_catalog.warehouse",
 "arn:aws:s3tables:Region:111122223333:s3tablescatalog/amzn-s3-demo-table-
bucket") \
    .config("spark.sql.catalog.s3_rest_catalog.rest.sigv4-enabled", "true") \
    .config("spark.sql.catalog.s3_rest_catalog.rest.signing-name", "s3tables") \
    .config("spark.sql.catalog.s3_rest_catalog.rest.signing-region", "Region") \
    .config('spark.sql.catalog.s3_rest_catalog.io-
impl','org.apache.iceberg.aws.s3.S3FileIO') \
    .config('spark.sql.catalog.s3_rest_catalog.rest-metrics-reporting-
enabled','false') \
    .getOrCreate()
```

### 使用交互式 Amazon Glue 会话

如果您将交互式笔记本会话与 Amazon Glue 5.0 结合使用，请在执行代码之前，在单元格中使用 %%configure 魔法指定相同的配置。将占位符值 替换为您自己的表存储桶的信息。

```
%%configure
{
    "conf": {
        "spark.sql.extensions":
 "org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions",
        "spark.sql.defaultCatalog": "s3_rest_catalog",
        "spark.sql.catalog.s3_rest_catalog":
 "org.apache.iceberg.spark.SparkCatalog",
        "spark.sql.catalog.s3_rest_catalog.type": "rest",
        "spark.sql.catalog.s3_rest_catalog.uri": "https://
s3tables.Region.amazonaws.com/iceberg",
        "spark.sql.catalog.s3_rest_catalog.warehouse":
 "arn:aws:s3tables:Region:111122223333:s3tablescatalog/amzn-s3-demo-table-
bucket",
        "spark.sql.catalog.s3_rest_catalog.rest.sigv4-enabled": "true",
        "spark.sql.catalog.s3_rest_catalog.rest.signing-name": "s3tables",
        "spark.sql.catalog.s3_rest_catalog.rest.signing-region": "Region",
```

```
        "spark.sql.catalog.s3_rest_catalog.io-impl":
 "org.apache.iceberg.aws.s3.S3FileIO",
        "spark.sql.catalog.s3_rest_catalog.rest-metrics-reporting-enabled":
 "false"
    }
}
```

### Amazon S3 Tables Catalog for Apache Iceberg

作为使用适用于 Apache Iceberg 的 Amazon S3 表类数据存储服务目录连接到表的先决条件，您必须先下载最新的目录 jar 并将其上传到 S3 存储桶。然后，在创建作业时，将指向客户端目录 JAR 的路径添加为一个特殊参数。有关 Amazon Glue 中作业参数的更多信息，请参阅《Amazon Glue 开发人员指南》中的 Amazon Glue 作业中使用的特殊参数。

可以通过作业中的 Spark 会话或交互式会话中的 Amazon Glue Studio 魔法来配置与表存储桶的连接。要使用以下示例，请将####替换为您自己的表存储桶的信息。

#### 使用 PySpark 脚本

在 PySpark 脚本中使用以下代码段，以便将 Amazon Glue 作业配置为使用 JAR 连接到表存储桶。将占位符值 替换为您自己的表存储桶的信息。

```
spark = SparkSession.builder.appName("glue-s3-tables") \
    .config("spark.sql.extensions",
 "org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions") \
    .config("spark.sql.defaultCatalog", "s3tablesbucket") \
    .config("spark.sql.catalog.s3tablesbucket",
 "org.apache.iceberg.spark.SparkCatalog") \
    .config("spark.sql.catalog.s3tablesbucket.catalog-impl",
 "software.amazon.s3tables.iceberg.S3TablesCatalog") \
    .config("spark.sql.catalog.s3tablesbucket.warehouse",
 "arn:aws:s3tables:Region:111122223333:bucket/amzn-s3-demo-table-bucket") \
    .getOrCreate()
```

#### 使用交互式 Amazon Glue 会话

如果您将交互式笔记本会话与 Amazon Glue 5.0 结合使用，请在执行代码之前，在单元格中使用 %%configure 魔法指定相同的配置。将占位符值 替换为您自己的表存储桶的信息。

```
%%configure
{
```

```
    "conf": {
    "spark.sql.extensions":
 "org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions",
    "spark.sql.defaultCatalog": "s3tablesbucket",
    "spark.sql.catalog.s3tablesbucket": "org.apache.iceberg.spark.SparkCatalog",
    "spark.sql.catalog.s3tablesbucket.catalog-impl":
 "software.amazon.s3tables.iceberg.S3TablesCatalog",
    "spark.sql.catalog.s3tablesbucket.warehouse":
 "arn:aws:s3tables:Region:111122223333:bucket/amzn-s3-demo-table-bucket"
    },
    "extra-jars": "s3://amzn-s3-demo-bucket/jars/s3-tables-catalog-for-iceberg-
runtime-0.1.5.jar"
}
```

示例脚本

以下示例 PySpark 脚本可用于测试通过 Amazon Glue 作业来查询 S3 表。这些脚本连接到表存储桶，然后运行查询来执行以下操作：创建新的命名空间、创建示例表、向表中插入数据以及返回表数据。要使用这些脚本，请将####替换为您自己的表存储桶的信息。

根据 S3 表类数据存储服务访问方法从以下脚本中进行选择。

S3 Tables integration with Amazon analytics services

```
from pyspark.sql import SparkSession

spark = SparkSession.builder.appName("SparkIcebergSQL") \
    .config("spark.sql.extensions",
 "org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions") \
    .config("spark.sql.defaultCatalog","s3tables")
    .config("spark.sql.catalog.s3tables", "org.apache.iceberg.spark.SparkCatalog") \
    .config("spark.sql.catalog.s3tables.catalog-impl",
 "org.apache.iceberg.aws.glue.GlueCatalog") \
    .config("spark.sql.catalog.s3tables.glue.id",
 "111122223333:s3tablescatalog/amzn-s3-demo-table-bucket") \
    .config("spark.sql.catalog.s3tables.warehouse", "s3://amzn-s3-demo-table-bucket/
bucket/amzn-s3-demo-table-bucket") \
    .getOrCreate()

namespace = "new_namespace"
table = "new_table"
```

```
spark.sql("SHOW DATABASES").show()

spark.sql(f"DESCRIBE NAMESPACE {namespace}").show()

spark.sql(f"""
    CREATE TABLE IF NOT EXISTS {namespace}.{table} (
       id INT,
       name STRING,
       value INT
    )
""")

spark.sql(f"""
    INSERT INTO {namespace}.{table}
    VALUES
       (1, 'ABC', 100),
       (2, 'XYZ', 200)
""")

spark.sql(f"SELECT * FROM {namespace}.{table} LIMIT 10").show()
```

### Amazon S3 Tables Iceberg REST endpoint

```
from pyspark.sql import SparkSession

spark = SparkSession.builder.appName("glue-s3-tables-rest") \
    .config("spark.sql.extensions",
 "org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions") \
    .config("spark.sql.defaultCatalog", "s3_rest_catalog") \
    .config("spark.sql.catalog.s3_rest_catalog",
 "org.apache.iceberg.spark.SparkCatalog") \
    .config("spark.sql.catalog.s3_rest_catalog.type", "rest") \
    .config("spark.sql.catalog.s3_rest_catalog.uri", "https://
s3tables.Region.amazonaws.com/iceberg") \
    .config("spark.sql.catalog.s3_rest_catalog.warehouse",
 "arn:aws:s3tables:Region:111122223333:bucket/amzn-s3-demo-table-bucket") \
    .config("spark.sql.catalog.s3_rest_catalog.rest.sigv4-enabled", "true") \
    .config("spark.sql.catalog.s3_rest_catalog.rest.signing-name", "s3tables") \
    .config("spark.sql.catalog.s3_rest_catalog.rest.signing-region", "Region") \
    .config('spark.sql.catalog.s3_rest_catalog.io-
impl','org.apache.iceberg.aws.s3.S3FileIO') \
    .config('spark.sql.catalog.s3_rest_catalog.rest-metrics-reporting-
enabled','false') \
```

```
    .getOrCreate()

namespace = "s3_tables_rest_namespace"
table = "new_table_s3_rest"

spark.sql("SHOW DATABASES").show()

spark.sql(f"DESCRIBE NAMESPACE {namespace}").show()

spark.sql(f"""
    CREATE TABLE IF NOT EXISTS {namespace}.{table} (
       id INT,
       name STRING,
       value INT
    )
""")

spark.sql(f"""
    INSERT INTO {namespace}.{table}
    VALUES
       (1, 'ABC', 100),
       (2, 'XYZ', 200)
""")

spark.sql(f"SELECT * FROM {namespace}.{table} LIMIT 10").show()
```

### Amazon S3 Tables Catalog for Apache Iceberg

```
from pyspark.sql import SparkSession

#Spark session configurations
spark = SparkSession.builder.appName("glue-s3-tables") \
    .config("spark.sql.extensions",
 "org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions") \
    .config("spark.sql.defaultCatalog", "s3tablesbucket") \
    .config("spark.sql.catalog.s3tablesbucket",
 "org.apache.iceberg.spark.SparkCatalog") \
    .config("spark.sql.catalog.s3tablesbucket.catalog-impl",
 "software.amazon.s3tables.iceberg.S3TablesCatalog") \
    .config("spark.sql.catalog.s3tablesbucket.warehouse",
 "arn:aws:s3tables:Region:111122223333:bucket/amzn-s3-demo-table-bucket") \
```

```
    .getOrCreate()

#Script
namespace = "new_namespace"
table = "new_table"

spark.sql(f"CREATE NAMESPACE IF NOT EXISTS s3tablesbucket.{namespace}")
spark.sql(f"DESCRIBE NAMESPACE {namespace}").show()

spark.sql(f"""
    CREATE TABLE IF NOT EXISTS {namespace}.{table} (
       id INT,
       name STRING,
       value INT
    )
""")

spark.sql(f"""
    INSERT INTO {namespace}.{table}
    VALUES
       (1, 'ABC', 100),
       (2, 'XYZ', 200)
""")

spark.sql(f"SELECT * FROM {namespace}.{table} LIMIT 10").show()
```

## 创建用于查询表的 Amazon Glue 作业

以下过程显示了如何设置连接到 S3 表存储桶的 Amazon Glue 作业。您可以使用 Amazon CLI 或将控制台与 Amazon Glue Studio 脚本编辑器结合使用来完成此操作。有关更多信息，请参阅《Amazon Glue 用户指南》中的在 Amazon Glue 中编写任务。

### 使用 Amazon Glue Studio 脚本编辑器

以下过程介绍了如何使用 Amazon Glue Studio 脚本编辑器来创建用于查询 S3 表的 ETL 任务。

#### 先决条件

- 先决条件
- 创建用于连接到表存储桶的脚本

1. 通过 https://console.aws.amazon.com/glue/ 打开 Amazon Glue 控制台。
2. 在导航窗格中，选择 ETL 任务。
3. 选择脚本编辑器，然后选择上传脚本并上传您创建的用于查询 S3 表的 PySpark 脚本。
4. 选择任务详细信息选项卡，然后对于基本属性输入以下内容。
   - 对于名称，输入任务的名称。
   - 对于 IAM 角色，选择您为 Amazon Glue 创建的角色。
5. （可选）如果您使用适用于 Apache Iceberg 的 Amazon S3 表类数据存储服务目录访问方法，请展开高级属性，对于从属 JAR 路径，输入您作为先决条件上传到 S3 存储桶的客户端目录 jar 的 S3 URI。例如，s3://*amzn-s3-demo-bucket1*/*jars*/s3-tables-catalog-for-iceberg-runtime-*0.1.5*.jar
6. 选择保存以创建任务。
7. 选择运行以启动任务，然后在运行选项卡下查看任务状态。

使用 Amazon CLI

以下过程介绍了如何使用 Amazon CLI 来创建用于查询 S3 表的 ETL 任务。要使用这些命令，请将*###*替换为您自己的值。

先决条件

- 先决条件
- 创建用于连接到表存储桶的脚本并将其上传到 S3 存储桶。

1. 创建 Amazon Glue 任务。

```
aws glue create-job \
--name etl-tables-job \
--role arn:aws:iam::111122223333:role/AWSGlueServiceRole \
--command '{
    "Name": "glueetl",
    "ScriptLocation": "s3://amzn-s3-demo-bucket1/scripts/glue-etl-query.py",
    "PythonVersion": "3"
}' \
--default-arguments '{
    "--job-language": "python",
    "--class": "GlueApp"
}' \
```

```
--glue-version "5.0"
```

> **Note**
>
> （可选）如果您使用适用于 Apache Iceberg 的 Amazon S3 表类数据存储服务目录访问方法，请使用 `--extra-jars` 参数将客户端目录 JAR 添加到 `--default-arguments` 中。添加参数时，将*#####*替换为您自己的信息。
>
> ```
> "--extra-jars": "s3://amzn-s3-demo-bucket/jar-path/s3-tables-catalog-for-iceberg-runtime-0.1.5.jar"
> ```

2. 启动任务。

```
aws glue start-job-run \
--job-name etl-tables-job
```

3. 要查看任务状态，请复制上一个命令中的运行 ID，然后将其输入到以下命令中。

```
aws glue get-job-run --job-name etl-tables-job \
--run-id jr_ec9a8a302e71f8483060f87b6c309601ea9ee9c1ffc2db56706dfcceb3d0e1ad
```

# S3 表类数据存储服务 Amazon Web Services 区域、端点和服务配额

以下各节包括 S3 表类数据存储服务支持的 Amazon Web Services 区域和服务配额。

主题

- S3 表类数据存储服务 Amazon Web Services 区域和端点
- S3 表类数据存储服务配额

## S3 表类数据存储服务 Amazon Web Services 区域和端点

S3 表类数据存储服务目前在以下 Amazon Web Services 区域中可用。要通过编程方式连接到 Amazon 服务，您需要使用端点。有关更多信息，请参阅Amazon服务端点。有关更多 Amazon S3 端点信息，请参阅 Amazon S3 endpoints。

| 区域名称 | 区域 | 端点 | 协议 | 签名版本支持 |
| --- | --- | --- | --- | --- |
| 非洲（开普敦） | af-south-1 | s3tables.af-south-1.amazonaws.com | HTTPS | 4 |
| 亚太地区（香港） | ap-east-1 | s3tables.ap-east-1.amazonaws.com | HTTPS | 4 |
| 亚太地区（东京） | ap-northeast-1 | s3tables.ap-northeast-1.amazonaws.com | HTTPS | 4 |
| 亚太地区（首尔） | ap-northeast-2 | s3tables.ap-northeast-2.amazonaws.com | HTTPS | 4 |
| 亚太地区（大阪） | ap-northeast-3 | s3tables.ap-northeast-3.amazonaws.com | HTTPS | 4 |
| 亚太地区（孟买） | ap-south-1 | s3tables.ap-south-1.amazonaws.com | HTTPS | 4 |
| 亚太地区（海得拉巴） | ap-south-2 | s3tables.ap-south-2.amazonaws.com | HTTPS | 4 |

| 区域名称 | 区域 | 端点 | 协议 | 签名版本支持 |
| --- | --- | --- | --- | --- |
| 亚太地区（新加坡） | ap-southeast-1 | s3tables.ap-southeast-1.amazonaws.com | HTTPS | 4 |
| 亚太地区（悉尼） | ap-southeast-2 | s3tables.ap-southeast-2.amazonaws.com | HTTPS | 4 |
| 亚太地区（雅加达） | ap-southeast-3 | s3tables.ap-southeast-3.amazonaws.com | HTTPS | 4 |
| 亚太地区（墨尔本） | ap-southeast-4 | s3tables.ap-southeast-4.amazonaws.com | HTTPS | 4 |
| 亚太地区（马来西亚） | ap-southeast-5 | s3tables.ap-southeast-5.amazonaws.com | HTTPS | 4 |
| 加拿大（中部） | ca-central-1 | s3tables.ca-central-1.amazonaws.com | HTTPS | 4 |
| 加拿大西部（卡尔加里） | ca-west-1 | s3tables.ca-west-1.amazonaws.com | HTTPS | 4 |

| 区域名称 | 区域 | 端点 | 协议 | 签名版本支持 |
|---|---|---|---|---|
| 欧洲地区（法兰克福） | eu-central-1 | s3tables.eu-central-1.amazonaws.com | HTTPS | 4 |
| 欧洲（苏黎世） | eu-central-2 | s3tables.eu-central-2.amazonaws.com | HTTPS | 4 |
| 欧洲地区（斯德哥尔摩） | eu-north-1 | s3tables.eu-north-1.amazonaws.com | HTTPS | 4 |
| 欧洲地区（米兰） | eu-south-1 | s3tables.eu-south-1.amazonaws.com | HTTPS | 4 |
| 欧洲（西班牙） | eu-south-2 | s3tables.eu-south-2.amazonaws.com | HTTPS | 4 |
| 欧洲地区（爱尔兰） | eu-west-1 | s3tables.eu-west-1.amazonaws.com | HTTPS | 4 |
| 欧洲地区（伦敦） | eu-west-2 | s3tables.eu-west-2.amazonaws.com | HTTPS | 4 |

| 区域名称 | 区域 | 端点 | 协议 | 签名版本支持 |
|---|---|---|---|---|
| 欧洲地区（巴黎） | eu-west-3 | s3tables.eu-west-3.amazonaws.com | HTTPS | 4 |
| 以色列（特拉维夫） | il-central-1 | s3tables.il-central-1.amazonaws.com | HTTPS | 4 |
| 中东（阿联酋） | me-central-1 | s3tables.me-central-1.amazonaws.com | HTTPS | 4 |
| 中东（巴林） | me-south-1 | s3tables.me-south-1.amazonaws.com | HTTPS | 4 |
| 南美洲（圣保罗） | sa-east-1 | s3tables.sa-east-1.amazonaws.com | HTTPS | 4 |
| 美国东部（弗吉尼亚州北部） | us-east-1 | s3tables.us-east-1.amazonaws.com | HTTPS | 4 |
| 美国东部（俄亥俄州） | us-east-2 | s3tables.us-east-2.amazonaws.com | HTTPS | 4 |

| 区域名称 | 区域 | 端点 | 协议 | 签名版本支持 |
| --- | --- | --- | --- | --- |
| 美国西部（加利福尼亚北部） | us-west-1 | `s3tables.us-west-1.amazonaws.com` | HTTPS | 4 |
| 美国西部（俄勒冈州） | us-west-2 | `s3tables.us-west-2.amazonaws.com` | HTTPS | 4 |

## S3 表类数据存储服务配额

配额（也称为限制）是 Amazon Web Services 账户的服务资源或操作的最大数量。以下是 S3 表类数据存储服务资源的配额。有关 Amazon S3 配额的更多信息，请参阅 Amazon S3 quotas。

| 名称 | 默认值 | 可调整 | 描述 |
| --- | --- | --- | --- |
| 表存储桶 | 10 | 要请求提高配额，请联系 Amazon Web Services 支持。 | 您可以在账户中为每个 Amazon Web Services 区域创建的 Amazon S3 表存储桶的数量。 |
| 命名空间 | 10000 | 要请求提高配额，请联系 Amazon Web Services 支持。 | 可以在每个表存储桶中创建的 Amazon S3 表命名空间的数量。 |
| 表 | 10000 | 要请求提高配额，请联系 Amazon Web Services 支持。 | 可以在每个表存储桶中创建的 Amazon S3 表类数据存储服务的数量。 |

# S3 表类数据存储服务的安全性

Amazon S3 提供了各种安全功能和工具。以下是 S3 表类数据存储服务支持的这些功能和工具的列表。正确应用这些工具有助于确保资源受到保护，且只有目标用户才能访问这些资源。

基于身份的策略

基于身份的策略附加到 IAM 用户、组或角色。您可以使用基于身份的策略，来向 IAM 身份授予对表存储桶或表的访问权限。默认情况下，用户和角色不拥有创建和修改表和表存储桶的权限。他们也无法通过 S3 控制台、Amazon CLI 或 Amazon S3 REST API 执行任务。您可以在您的账户中创建 IAM 用户、组和角色，并为其附加访问策略。然和，您可以授予对资源的访问权限。要创建和访问表存储桶和表，IAM 管理员必须向 Amazon Identity and Access Management（IAM）角色或用户授予必要的权限。有关更多信息，请参阅 S3 表类数据存储服务的访问管理。

基于资源的策略

基于资源的策略附加到某个资源。您可以为表存储桶和表创建基于资源的策略。您可以使用表存储桶策略来控制表存储桶和命名空间级的 API 访问权限。还可以使用表存储桶策略来控制对存储桶中多个表的表级 API 权限。根据策略定义，附加到存储桶的权限可以应用于存储桶中的所有表或特定表。还可以使用表策略来授予对存储桶中各个表的表级 API 访问权限。

当 S3 表类数据存储服务收到执行表存储桶操作或表操作的请求时，它首先验证请求者是否拥有必要的权限。它对所有相关访问策略、用户策略和基于资源的策略（IAM 用户策略、IAM 角色策略、表存储桶策略和表策略）进行评估，以决定是否对该请求进行授权。通过表存储桶策略和表策略，您可以对资源的访问权限进行个性化设置，以确保只有您已批准的身份才能访问您的资源并对其执行操作。有关更多信息，请参阅 S3 表类数据存储服务的访问管理。

S3 表类数据存储服务的 Amazon Organizations 服务控制策略（SCP）。

可以在服务控制策略（SCP）中使用 Amazon S3 表类数据存储服务来管理组织中用户的权限。与 IAM 和资源策略类似，所有表和存储桶级操作都作为 `s3tables` 命名空间的一部分在策略中引用。有关更多信息，请参阅《Amazon Organizations 用户指南》中的服务控制策略（SCP）。

主题

- 使用加密保护 S3 表数据
- S3 表类数据存储服务的访问管理
- S3 表类数据存储服务的 VPC 连接
- S3 表类数据存储服务的安全注意事项和限制

# 使用加密保护 S3 表数据

## 在表存储桶中使用具有 Amazon KMS 密钥的服务器端加密（SSE-KMS）

主题


- SSE-KMS 存储桶如何用于表和表存储桶
- 对表和表存储桶强制使用 SSE-KMS 并确定其范围
- 监控和审计表和表存储桶的 SSE-KMS 加密
- S3 表类数据存储服务 SSE-KMS 加密的权限要求
- 在表存储桶中指定具有 Amazon KMS 密钥的服务器端加密（SSE-KMS）


表存储桶具有默认加密配置，该配置通过使用具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）来自动加密表。此加密适用于 S3 表存储桶中的所有表，而您无需支付任何费用。

如果您需要对加密密钥进行更多控制，例如管理密钥轮换和访问策略授予，则可以将表存储桶配置为使用具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）。Amazon KMS 中的安全控制可帮助您满足与加密相关的合规性要求。有关 SSE-KMS 的更多信息，请参阅 使用具有 Amazon KMS 密钥的服务器端加密（SSE-KMS）。

SSE-KMS 存储桶如何用于表和表存储桶

表存储桶中的 SSE-KMS 与通用存储桶中的 SSE-KMS 在以下几个方面有所不同：

- 您可以为表存储桶和各个表指定加密设置。
- 您只能将客户自主管理型密钥与 SSE-KMS 结合使用。不支持 Amazon 托管式密钥。
- 您必须向某些角色和 Amazon 服务主体授予访问 Amazon KMS 密钥的权限。有关更多信息，请参阅 S3 表类数据存储服务 SSE-KMS 加密的权限要求。这包括向以下主体授予访问权限：
  - S3 维护主体：用于对加密的表执行表维护
  - S3 表类数据存储服务集成角色：用于在 Amazon 分析服务中处理加密的表
  - 客户端访问角色：用于从 Apache Iceberg 客户端直接访问加密的表
  - S3 元数据主体：用于更新加密的 S3 元数据表
- 加密的表使用表级别密钥，此类密钥可最大限度地减少向 Amazon KMS 发出的请求数量，从而提高处理 SSE-KMS 加密表的成本效益。

表存储桶的 SSE-KMS 加密

创建表存储桶时，可以选择 SSE-KMS 作为默认加密类型，并选择将用于加密的特定 KMS 密钥。在该存储桶中创建的任何表都将自动从其表存储桶继承这些加密设置。您可以随时使用 Amazon CLI、S3 API 或 Amazon SDK 来修改或移除表存储桶上的默认加密设置。当您修改表存储桶上的加密设置时，这些设置仅适用于在该存储桶中创建的新表。而不更改先前存在的表的加密设置。有关更多信息，请参阅 为表存储桶指定加密。

表的 SSE-KMS 加密

您还可以选择使用不同的 KMS 密钥来加密单个表，而不管存储桶的默认加密配置如何。要为单个表设置加密，必须在创建表时指定所需的加密密钥。如果要更改现有表的加密，则需要使用所需密钥创建一个表，并将数据从旧表复制到新表。有关更多信息，请参阅 为表指定加密。

使用 Amazon KMS 加密时，S3 表类数据存储服务会自动创建唯一的表级别数据密钥，用于加密与每个表关联的新对象。这些密钥在有限的时段内使用，最大限度地减少了在加密操作期间对额外 Amazon KMS 请求的需求，并降低了加密成本。这类似于 SSE-KMS 的 S3 存储桶密钥。

对表和表存储桶强制使用 SSE-KMS 并确定其范围

您可以使用 S3 表类数据存储服务基于资源的策略、KMS 密钥策略、基于 IAM 身份的策略或这些策略的任意组合，来强制对 S3 表和表存储桶使用 SSE-KMS。有关表的身份和资源策略的更多信息，请参阅 S3 表类数据存储服务的访问管理。有关编写密钥策略的信息，请参阅《Amazon Key Management Service Developer Guide》中的 Key policies。以下示例说明如何使用策略来强制执行 SSE-KMS。

使用表存储桶策略强制对所有表使用 SSE-KMS

这是表存储桶策略的示例，该策略禁止用户在特定的表存储桶中创建表，除非他们使用特定 Amazon KMS 密钥对表进行加密。要使用此策略，请将#######替换为您自己的信息：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceKMSEncryption",
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3tables:CreateTable"
      ],
      "Resource": [
```

```
        "<table-bucket-arn>/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "s3tables:sseAlgorithm": "aws:kms",
          "s3tables:kmsKeyArn": "<kms-key-arn>"
        }
      }
    }
  ]
}
```

要求用户将 SSE-KMS 加密与 IAM 策略结合使用

此 IAM 身份策略要求用户在创建或配置 S3 表类数据存储服务资源时使用特定的 Amazon KMS 密钥进行加密。要使用此策略，请将*#######*替换为您自己的信息：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RequireKMSKeyOnTables",
      "Action": [
          "s3tables:CreateTableBucket",
          "s3tables:PutTableBucketEncryption",
          "s3tables:CreateTable"
      ]
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
            "s3tables:sseAlgorithm": "aws:kms",
            "s3tables:kmsKeyArn": "<key_arn>"
        }
      }
    }
  ]
}
```

使用 KMS 密钥策略将密钥的使用限制为特定的表存储桶

此示例 KMS 密钥策略仅让特定用户将密钥用于特定表存储桶中的加密操作。这种类型的策略对于在跨账户场景中限制对密钥的访问非常有用。要使用此策略，请将*#######*替换为您自己的信息：

```
{
  "Version": "2012-10-17",
  "Id": "Id",
  "Statement": [
    {
      "Sid": "AllowPermissionsToKMS",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:EncryptionContext:aws:s3:arn": "<table-bucket-arn>/*"
        }
      }
    }
  ]
}
```

监控和审计表和表存储桶的 SSE-KMS 加密

要审计为 SSE-KMS 加密数据使用 Amazon KMS 密钥的情况，您可以使用 Amazon CloudTrail 日志。您可以深入了解自己的加密操作，例如 GenerateDataKey 和 Decrypt。CloudTrail 支持多种属性值来筛选您的搜索，包括事件名称、用户名和事件源。

可以使用 CloudTrail 事件跟踪 Amazon S3 表和表存储桶的加密配置请求。CloudTrail 日志中使用以下 API 事件名称：

- s3tables:PutTableBucketEncryption
- s3tables:GetTableBucketEncryption
- s3tables:DeleteTableBucketEncryption
- s3tables:GetTableEncryption
- s3tables:CreateTable
- s3tables:CreateTableBucket

> **Note**
>
> 表存储桶不支持 EventBridge。

### S3 表类数据存储服务 SSE-KMS 加密的权限要求

当您对 S3 表存储桶中的表使用具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）时，您需要为账户中的不同身份授予权限。您的访问身份和 S3 表类数据存储服务维护主体至少需要具有访问您的密钥的权限，所需的其它权限取决于您的应用场景。

#### 所需权限

要访问使用 KMS 密钥加密的表，您需要对该密钥具有以下权限：

- `kms:GenerateDataKey`
- `kms:Decrypt`

> **Important**
>
> 要对表使用 SSE-KMS，Amazon S3 表类数据存储服务维护服务主体 (`maintenance.s3tables.amazonaws.com`) 需要对密钥具有 `kms:GenerateDataKey` 和 `kms:Decrypt` 权限。

#### 其他权限

根据您的应用场景，需要以下附加权限：

- Amazon 分析服务集成的权限：如果您在 Amazon 分析服务中使用由 SSE-KMS 加密的表，则集成角色需要具有使用 KMS 密钥的权限。
- 直接访问的权限：如果您通过诸如 Amazon S3 表类数据存储服务 Iceberg REST 端点或适用于 Apache Iceberg 的 Amazon S3 表类数据存储服务目录之类的方法直接使用由 SSE-KMS 加密的表，则需要向客户端使用的 IAM 角色授予访问您的密钥的权限。
- S3 元数据表的权限：如果您对 S3 元数据表使用 SSE-KMS 加密，则需要向 S3 元数据服务主体 (`metadata.s3.amazonaws.com`) 提供对 KMS 密钥的访问权限。这可让 S3 元数据更新加密的表，这样它们就能够反映您的最新数据更改。

> **Note**
>
> 对于跨账户 KMS 密钥，您的 IAM 角色在密钥策略中同时需要密钥访问权限和显式授权。有关 KMS 密钥的跨账户权限的更多信息，请参阅《Amazon Key Management Service Service Developer Guide》中的 Allowing external Amazon accounts to use a KMS key。

主题

- 向 S3 表类数据存储服务维护服务主体授予对 KMS 密钥的权限
- 向 IAM 主体授予在集成的 Amazon 分析服务中使用加密表的权限
- 向 IAM 主体授予直接使用加密表的权限
- 向 S3 元数据服务主体授予使用您的 KMS 密钥的权限

向 S3 表类数据存储服务维护服务主体授予对 KMS 密钥的权限

需要此权限才能创建通过 SSE-KMS 加密的表，并支持对加密的表进行自动表维护，例如压缩、快照管理和未引用文件移除。

> **Note**
>
> 每当您发出请求来创建通过 SSE-KMS 加密的表时，S3 表类数据存储服务都会进行检查，以确保 `maintenance.s3tables.amazonaws.com` 主体有权访问您的 KMS 密钥。要执行此检查，需要在表存储桶中临时创建一个零字节对象，而未引用文件移除维护操作将自动移除该对象。如果您为加密指定的 KMS 密钥没有维护访问权限，则 createTable 操作将失败。

要授予对通过 SSE-KMS 加密的表的维护访问权限，您可以使用以下示例密钥策略。在此策略中，向 `maintenance.s3tables.amazonaws.com` 服务主体授予使用特定 KMS 密钥对特定表存储桶中的表进行加密和解密的权限。要使用此策略，请将`#######`替换为您自己的信息：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnableKeyUsage",
            "Effect": "Allow",
            "Principal": {
```

```
                "Service": "maintenance.s3tables.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "<kms-key-arn>",
            "Condition": {
                "StringLike": {
                    "kms:EncryptionContext:aws:s3:arn":"<table-or-table-bucket-arn>/*"
                }
            }
        }
    ]
}
```

向 IAM 主体授予在集成的 Amazon 分析服务中使用加密表的权限

要在 Amazon 分析服务中使用 S3 表，可以将表存储桶与 Amazon SageMaker 智能湖仓集成。这种集成支持 Amazon 分析服务自动发现和访问表数据。有关集成的更多信息，请参阅将 Amazon S3 表类数据存储服务与 Amazon 分析服务结合使用。

当您在这些服务中使用通过 SSE-KMS 加密的表时，您使用的角色需要拥有使用 Amazon KMS 密钥进行加密操作的权限。您可以将这些权限应用于在集成期间创建的 `S3TablesRoleForLakeFormation` 角色或您自己的 IAM 角色。

以下内联 IAM 策略示例可用于向 `S3TablesRoleForLakeFormation` 服务角色授予使用您账户中的特定 KMS 密钥进行加密操作的权限。要使用此策略，请将`######`替换为您自己的信息。

```
{
  "Sid": "AllowTableRoleAccess",
  "Effect": "Allow",
  "Principal": {
 "AWS": "arn:aws:iam::111122223333:role/service-role/S3TablesRoleForLakeFormation"
  },
  "Action": [
      "kms:GenerateDataKey",
      "kms:Decrypt"
  ],
  "Resource": "<kms-key-arn>"
}
```

向 IAM 主体授予直接使用加密表的权限

当您通过第三方或直接访问方法处理加密表时，必须向您使用的角色授予对 KMS 密钥的访问权限。以下示例说明如何通过 IAM 策略或 KMS 密钥策略授予访问权限。

IAM policy

将此内联策略附加到您的 IAM 角色，以支持访问 KMS 密钥。要使用此策略，请将######替换为您自己的 KMS 密钥 arn。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
        "Effect": "Allow",
        "Action": [
            "kms:Decrypt",
            "kms:GenerateDataKey"
         ],
        "Resource": "<kms-key-arn>"
        }
    ]
}
```

KMS key policy

将此内联策略附加到 KMS 密钥，以让指定的 Amazon KMS 角色使用该密钥。要使用此策略，请将######替换为您的 IAM 角色。

```
{
    "Sid": "Allow use of the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": [
            "arn:aws:iam::<catalog-account-id>:role/<role-name>"
        ]
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey",
    ],
    "Resource": "*"
```

```
}
```

向 S3 元数据服务主体授予使用您的 KMS 密钥的权限

要支持 Amazon S3 更新通过 SSE-KMS 加密的元数据表并对这些元数据表执行维护，您可以使用以下示例密钥策略。在此策略中，您可以让 `metadata.s3.amazonaws.com` 和 `maintenance.s3tables.amazonaws.com` 服务主体使用特定密钥对特定表存储桶中的表进行加密和解密。要使用此策略，请将*#######*替换为您自己的信息：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnableKeyUsage",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "maintenance.s3tables.amazonaws.com",
                    "metadata.s3.amazonaws.com"
                ]
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "<kms-key-arn>",
            "Condition": {
                "StringLike ": {
                    "kms:EncryptionContext:aws:s3:arn": "<table-or-table-bucket-arn>/*"
                }
            }
        }
    ]
}
```

在表存储桶中指定具有 Amazon KMS 密钥的服务器端加密（SSE-KMS）

默认情况下，所有 Amazon S3 表存储桶都配置了加密，所有在表存储桶中创建的新表都会自动静态加密。具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）是每个表存储桶的默认加密配置。如果您要指定不同的加密类型，可以使用具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）。

可以在 CreateTableBucket 或 CreateTable 请求中指定 SSE-KMS 加密，也可以在 PutTableBucketEncryption 请求中设置表存储桶中的默认加密配置。

> **Important**
>
> 要支持对通过 SSE-KMS 加密的表和表存储桶进行自动维护，您必须向 maintenance.s3tables.amazonaws.com 服务主体授予使用 KMS 密钥的权限。有关更多信息，请参阅 S3 表类数据存储服务 SSE-KMS 加密的权限要求。

### 为表存储桶指定加密

在创建新的表存储桶时，您可以指定 SSE-KMS 作为默认加密类型，有关示例，请参阅创建表存储桶。创建表存储桶后，您可以使用 REST API 操作、Amazon SDK 和 Amazon Command Line Interface（Amazon CLI）来指定将 SSE-KMS 用作默认加密设置。

> **Note**
>
> 当您将 SSE-KMS 指定为默认加密类型时，用于加密的密钥必须支持访问 S3 表类数据存储服务维护服务主体。如果维护服务主体没有访问权限，您将无法在该表存储桶中创建表。有关更多信息，请参阅 向 S3 表类数据存储服务维护服务主体授予对 KMS 密钥的权限 。

#### 使用 Amazon CLI

要使用以下示例 Amazon CLI 命令，请将*#######*替换为您自己的信息。

```
aws s3tables put-table-bucket-encryption \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-bucket; \
    --encryption-configuration '{
        "sseAlgorithm": "aws:kms",
        "kmsKeyArn": "arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }' \
    --region us-east-1
```

您可以使用 DeleteTableBucketEncryption API 操作移除表存储桶的默认加密设置。移除加密设置后，在表存储桶中创建的新表将使用默认的 SSE-S3 加密。

### 为表指定加密

在使用查询引擎、REST API 操作、Amazon SDK 和 Amazon Command Line Interface（Amazon CLI）创建新表时，可以对该表应用 SSE-KMS 加密。您在创建表时指定的加密设置优先于表存储桶的默认加密设置。

> **Note**
>
> 对表使用 SSE-KMS 加密时，用于加密的密钥必须支持 S3 表类数据存储服务维护服务主体访问该表。如果维护服务主体没有访问权限，您将无法创建表。有关更多信息，请参阅 向 S3 表类数据存储服务维护服务主体授予对 KMS 密钥的权限 。

#### 所需权限

创建加密表需要以下权限

- `s3tables:CreateTable`
- `s3tables:PutTableEncryption`

#### 使用 Amazon CLI

以下 Amazon CLI 示例使用基本架构创建一个新表，并使用客户自主管理型 Amazon KMS 密钥对其进行加密。要使用该命令，请将*#######* 替换为您自己的信息。

```
aws s3tables create-table \
  --table-bucket-arn "arn:aws:s3tables:Region:ownerAccountId:bucket/amzn-s3-demo-table-bucket" \
  --namespace "mydataset" \
  --name "orders" \
  --format "ICEBERG" \
  --encryption-configuration '{
    "sseAlgorithm": "aws:kms",
    "kmsKeyArn":
 "arn:aws:kms:Region:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  }' \
  --metadata '{
    "iceberg": {
      "schema": {
        "fields": [
```

```
          {
            "name": "order_id",
            "type": "string",
            "required": true
          },
          {
            "name": "order_date",
            "type": "timestamp",
            "required": true
          },
          {
            "name": "total_amount",
            "type": "decimal(10,2)",
            "required": true
          }
        ]
      }
    }
  }'
```

数据保护指在数据传输（数据发往和离开 Amazon S3 时）和处于静态（数据存储在 Amazon S3 数据中心的磁盘上时）期间保护数据。S3 表类数据存储服务始终通过 HTTPS 使用传输层安全性（1.2 及更高版本）来保护传输中数据。为保护 S3 表存储桶中的静态数据，您具有以下选项：

具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）

默认情况下，所有 Amazon S3 表存储桶都配置了加密。服务器端加密的默认选项是使用 Amazon S3 托管式密钥（SSE-S3）。这种加密对您来说是免费的，并且适用于 S3 表存储桶中的所有表，除非您指定了另一种加密形式。每个对象都使用唯一的密钥来进行加密。作为额外的保护措施，SSE-S3 使用定期轮换的根密钥加密密钥本身。SSE-S3 使用可用的最强数据块密码之一 [即 256 位高级加密标准（AES-256）] 来加密您的数据。

具有 Amazon KMS 密钥的服务器端加密（SSE-KMS）

可以选择将表存储桶或表配置为使用具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）。Amazon KMS 中的安全控制可帮助您满足与加密相关的合规性要求。SSE-KMS 可让您通过执行以下操作来更好地控制加密密钥：

- 创建、查看、编辑、监控、启用或禁用、轮换以及安排删除 KMS 密钥。
- 定义控制如何使用和谁可以使用 KMS 密钥的策略。
- 在 Amazon CloudTrail 中跟踪密钥使用情况，以验证 KMS 密钥是否得到正确使用。

S3 表类数据存储服务支持在 SSE-KMS 中使用客户自主管理型密钥来加密表。不支持 Amazon 托管式密钥。有关对 S3 表和表存储桶使用 SSE-KMS 的更多信息，请参阅在表存储桶中使用具有 Amazon KMS 密钥的服务器端加密（SSE-KMS）。

## S3 表类数据存储服务的访问管理

在 S3 表类数据存储服务中，资源包括表存储桶及其包含的表。默认情况下，创建资源的 Amazon Web Services 账户的根用户（资源拥有者）和该账户中具有必要权限的 Amazon Identity and Access Management（IAM）用户可以访问他们创建的资源。资源拥有者指定还有谁可以访问该资源以及支持他们对该资源执行哪些操作。Amazon S3 具有各种访问管理工具，您可以使用这些工具向其他人授予对您的 S3 资源的访问权限。以下主题概述了 S3 表类数据存储服务的资源、IAM 操作和条件键。它们还提供了 S3 表类数据存储服务的基于资源和基于身份的策略的示例。

主题


- 资源
- S3 表类数据存储服务的操作
- S3 表类数据存储服务的条件键
- S3 表类数据存储服务的基于 IAM 身份的策略
- S3 表类数据存储服务的基于资源的策略
- 适用于 S3 表类数据存储服务的 Amazon 托管式策略
- 使用 SQL 语义授予访问权限


### 资源

S3 表类数据存储服务资源包括表存储桶及其包含的表。

- 表存储桶：表存储桶专为表而设计，与通用 S3 存储桶中自行管理的表相比，可提供更高的每秒事务数（TPS）和更好的查询吞吐量。表存储桶具有与 Amazon S3 通用存储桶相同的耐久性、可用性、可扩展性和性能特征。
- 表 - 表存储桶中的表以 Apache Iceberg 格式存储。您可以在支持 Iceberg 的查询引擎中使用标准 SQL 查询这些表。

表和表存储桶的 Amazon 资源名称（ARN）包含 `s3tables` 命名空间、Amazon Web Services 区域、Amazon Web Services 账户 ID 和存储桶名称。要访问表和表存储桶并对其执行操作，必须使用以下 ARN 格式：

- 表格 ARN 格式：

  arn:aws:s3tables:*us-west-2*:*111122223333*:bucket/*amzn-s3-demo-bucket*/table/*demo-tableID*

## S3 表类数据存储服务的操作

在基于身份的策略或基于资源的策略中，您可以定义对于特定 IAM 主体支持或拒绝哪些 S3 表类数据存储服务操作。表操作对应于存储桶和表级 API 操作。所有操作都是唯一 IAM 命名空间的一部分：s3tables。

当您在策略中使用一项操作时，通常会允许或拒绝使用具有相同名称的 API 操作。但在某些情况下，单个操作可控制对多个 API 操作的访问。例如，s3tables:GetTableData 操作包括对于 GetObject、ListParts 和 ListMultiparts API 操作的权限。

以下是表存储桶支持的操作。您可以在 IAM 策略或资源策略的 Action 元素中指定以下操作。

| 操作 | 描述 | 访问级别 | 跨账户访问 |
| --- | --- | --- | --- |
| s3tables:CreateTableBucket | 授予创建表存储桶的权限 | Write | 否 |
| s3tables:GetTableBucket | 授予检索表存储桶 ARN、表存储桶名称和创建日期的权限。 | Write | 是 |
| s3tables:ListTableBuckets | 授予列出此账户中所有表存储桶的权限 | Read | 否 |
| s3tables:CreateNamespace | 授予在表存储桶中创建命名空间的权限 | Read | 是 |

| 操作 | 描述 | 访问级别 | 跨账户访问 |
| --- | --- | --- | --- |
| s3tables:GetNamespace | 授予检索命名空间详细信息的权限 | Read | 是 |
| s3tables:ListNamespaces | 授予列出表存储桶上所有命名空间的权限。 | Read | 是 |
| s3tables:DeleteNamespace | 授予删除表存储桶中命名空间的权限 | Write | 是 |
| s3tables:DeleteTableBucket | 授予删除存储桶的权限 | Write | 是 |
| s3tables:PutTableBucketPolicy | 授予添加或替换存储桶策略的权限 | Permissions Management | 否 |
| s3tables:GetTableBucketPolicy | 授予检索存储桶策略的权限 | Read | 否 |
| s3tables:DeleteTableBucketPolicy | 授予删除存储桶策略的权限 | Permissions Management | 否 |
| s3tables:GetTableBucketMaintenanceConfiguration | 授予检索表存储桶的维护配置的权限 | Read | 是 |

| 操作 | 描述 | 访问级别 | 跨账户访问 |
| --- | --- | --- | --- |
| s3tables:PutTableBucketMaintenanceConfiguration | 授予添加或替换表存储桶的维护配置的权限 | Write | 是 |
| s3tables:PutTableBucketEncryption | 授予添加或替换表存储桶的加密配置的权限 | Write | 否 |
| s3tables:GetTableBucketEncryption | 授予检索表存储桶的加密配置的权限 | Read | 否 |
| s3tables:DeleteTableBucketEncryption | 授予删除表存储桶的加密配置的权限 | Write | 否 |

表支持以下操作：

| 操作 | 描述 | 访问级别 | 跨账户访问 |
| --- | --- | --- | --- |
| s3tables:GetTableMaintenanceConfiguration | 授予检索表的维护配置的权限 | Read | 是 |
| s3tables:PutTableMaintenanc | 授予添加或替换表的维护配置的权限 | Write | 是 |

| 操作 | 描述 | 访问级别 | 跨账户访问 |
| --- | --- | --- | --- |
| eConfigur ation | | | |
| s3tables: PutTableP olicy | 授予添加或替换表策略的权限 | Permissions Management | 否 |
| s3tables: GetTableP olicy | 授予检索表策略的权限 | Read | 否 |
| s3tables: DeleteTab lePolicy | 授予删除表策略的权限 | Permissions management | 否 |
| s3tables: CreateTable | 授予在表存储桶中创建表的权限 | Write | 是 |
| s3tables: GetTable | 授予检索表信息的权限 | Read | 是 |
| s3tables: GetTableM etadataLo cation | 授予检索表根指针（元数据文件）的权限 | Read | 是 |
| s3tables: ListTables | 授予列出表存储桶中的所有表的权限 | Read | 是 |
| s3tables: RenameTable | 授予更改表名称的权限 | Write | 是 |

| 操作 | 描述 | 访问级别 | 跨账户访问 |
| --- | --- | --- | --- |
| s3tables:UpdateTableMetadataLocation | 授予更新表根指针（元数据文件）的权限 | Write | 是 |
| s3tables:GetTableData | 授予读取存储在表存储桶中的表元数据和数据对象的权限 | Read | 是 |
| s3tables:PutTableData | 授予写入存储在表存储桶中的表元数据和数据对象的权限 | Write | 是 |
| s3tables:GetTableEncryption | 授予检索表的加密设置的权限 | Write | 否 |
| s3tables:PutTableEncryption | 授予将加密添加到表的权限 | Write | 否 |

为了执行表级读取和写入操作，S3 表类数据存储服务支持如 GetObject 和 PutObject 等 Amazon S3 API 操作。下表提供了对象级操作的列表。在授予对表的读写权限时，您可以使用以下操作。

| 操作 | S3 对象 API | | |
| --- | --- | --- | --- |
| s3tables:GetTableData | GetObject，ListParts， | | |

| 操作 | S3 对象 API | | |
| --- | --- | --- | --- |
| | HeadObject | | |
| s3tables:PutTableData | PutObject，CreateMultipartUpload，CompleteMultipartUpload，UploadPart，AbortMultipartUpload | | |

例如，如果用户拥有 GetTableData 权限，则他们可以读取与该表关联的所有文件，例如其元数据文件、清单、清单列表文件和 parquet 数据文件。

## S3 表类数据存储服务的条件键

S3 表类数据存储服务支持 Amazon 全局条件上下文条件键。

此外，S3 表类数据存储服务定义以下可以在访问策略中使用的条件键。

| 条件键 | 描述 | 类型 | |
| --- | --- | --- | --- |
| s3tables:tableName | 按表存储桶中表的名称筛选访问权限。<br><br>您可以使用 s3tables:tableName 条件键来编 | String | |

| 条件键 | 描述 | 类型 | |
| --- | --- | --- | --- |
| | 写 IAM 或表存储桶策略，以限制用户或应用程序仅可访问符合此名称条件的表。<br><br>请务必注意，如果您使用 `s3tables:tableName` 条件键来控制访问权限，则表名称的更改可能会影响这些策略。<br>示例值：`"s3tables:tableName":"department*"` | | |

| 条件键 | 描述 | 类型 | |
|---|---|---|---|
| s3tables:namespace | 按在表存储桶中创建的命名空间筛选访问权限。<br><br>您可以使用 s3tables:namespace 条件键编写 IAM、表或表存储桶策略，以限制用户或应用程序对作为特定命名空间一部分的表的访问权限。示例值："s3tables:namespace":"hr"<br><br>请务必注意，如果您使用 s3tables:namespace 条件键来控制访问权限，那么命名空间的更改可能会影响这些策略。 | String | |

| 条件键 | 描述 | 类型 | |
|---|---|---|---|
| s3tables:SSEAlgorithm | 按用于加密表的服务器端加密算法筛选访问权限。<br><br>您可以使用 s3tables:SSEAlgorithm 条件键编写 IAM、表或表存储桶策略，以限制用户或应用程序只能访问使用特定加密类型加密的表。示例值："s3tables:SSEAlgorithm":"aws:kms"<br><br>请务必注意，如果您使用 s3tables:SSEAlgorithm 条件键来控制访问权限，那么加密的更改可能会影响这些策略。 | String | |

| 条件键 | 描述 | 类型 | |
|---|---|---|---|
| s3tables:KMSKeyArn | 按用于加密表的密钥的 Amazon KMS 密钥 ARN 筛选访问权限<br><br>您可以使用 s3tables:KMSKeyArn 条件键来编写 IAM、表或表存储桶策略，以限制用户或应用程序只能访问使用特定 KMS 密钥加密的表。<br><br>请务必注意，如果您使用 s3tables:KMSKeyArn 条件键来控制访问权限，则更改 KMS 密钥可能会影响这些策略。 | ARN | |

## S3 表类数据存储服务的基于 IAM 身份的策略

默认情况下，用户和角色不拥有创建或修改表和表存储桶的权限。他们也无法通过 s3 控制台、Amazon Command Line Interface（Amazon CLI）或 Amazon S3 REST API 执行任务。要创建和访问表存储桶和表，Amazon Identity and Access Management（IAM）管理员必须向 IAM 角色或用户授予必要的权限。要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅 IAM 用户指南中的 创建 IAM 策略。

以下主题包括基于 IAM 身份的策略示例。要使用以下示例策略，请将####### 替换为您自己的信息。

主题


- 示例 1：支持创建和使用表存储桶的访问权限
- 示例 2：支持在表存储桶中创建和使用表的访问权限


示例 1：支持创建和使用表存储桶的访问权限

.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AllowBucketActions",
        "Effect": "Allow",
        "Action": [
            "s3tables:CreateTableBucket",
            "s3tables:PutTableBucketPolicy",
            "s3tables:GetTableBucketPolicy",
            "s3tables:ListTableBuckets",
            "s3tables:GetTableBucket"
        ],

        "Resource": "arn:aws:s3tables:region:account_id:bucket/*"
    }]
}
```

示例 2：支持在表存储桶中创建和使用表的访问权限

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Sid": "AllowBucketActions",
             "Effect": "Allow",
             "Action": [
                 "s3tables:CreateTable",
                 "s3tables:PutTableData",
                 "s3tables:GetTableData",
                 "s3tables:GetTableMetadataLocation",
                 "s3tables:UpdateTableMetadataLocation",
                 "s3tables:GetNamespace",
```

```
                "s3tables:CreateNamespace"
            ],

            "Resource": [
              "arn:aws:s3tables:region:account_id:bucket/amzn-s3-demo-bucket",
              "arn:aws:s3tables:region:account_id:bucket/amzn-s3-demo-bucket/table/*"
            ]
        }
    ]
}
```

## S3 表类数据存储服务的基于资源的策略

S3 表类数据存储服务提供了基于资源的策略，用于管理对表存储桶和表的访问权限：表存储桶策略和表策略。可以使用表存储桶策略在表存储桶、命名空间或表级授予 API 访问权限。附加到表存储桶的权限可以应用于存储桶中的所有表，也可以应用于存储桶中的特定表，具体取决于策略定义。可以使用表策略在表级授予权限。

当 S3 表类数据存储服务收到请求时，它首先验证请求者是否拥有必要的权限。它对所有相关访问策略、用户策略和基于资源的策略（IAM 用户策略、IAM 角色策略、表存储桶策略和表策略）进行评估，以决定是否对该请求进行授权。例如，如果表存储桶策略授予用户对存储桶中的表执行所有操作（包括 DeleteTable）的权限，但单个表的表策略拒绝所有用户执行 DeleteTable 操作，则该用户无法删除该表。

以下主题包括表和表存储桶策略的示例。要使用这些策略，请将*###### 替换为您自己的信息。

> **Note**
>
> - 每个授予修改表的权限的策略都应包括供 GetTableMetadataLocation 访问表根文件的权限。有关更多信息，请参阅 GetTableMetadataLocation。
> - 每次对表执行写入或删除活动时，都要在访问策略中包含对 UpdateTableMetadataLocation 的权限。
> - 我们建议使用表存储桶策略来管理对存储桶级操作的访问权限，并使用表策略来管理对表级操作的访问权限。如果您想在多个表中定义相同的权限集，那么我们建议使用表存储桶策略。

主题

- 示例 1：表存储桶策略支持对账户中的存储桶执行 PutBucketMaintenanceConfiguration 的访问权限

- 示例 2：支持对存储在 hr 命名空间中的表进行读取（SELECT）访问的表存储桶策略
- 示例 3：支持用户删除表的表策略

示例 1：表存储桶策略支持对账户中的存储桶执行 **PutBucketMaintenanceConfiguration** 的访问权限

以下示例表存储桶策略通过支持访问 PutBucketMaintenanceConfiguration，可让 IAM data steward 删除账户中所有存储桶的未引用对象。

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Effect": "Allow",
             "Principal": {
               "AWS": "arn:aws:iam::account_id:role/datasteward"
             },
             "Action": ["s3tables:PutTableBucketMaintenanceConfiguration"],
             "Resource":"arn:aws:s3tables:region:account_id:bucket/*"
     }]
 }
```

示例 2：支持对存储在 **hr** 命名空间中的表进行读取（SELECT）访问的表存储桶策略

以下示例表存储桶策略支持 Jane（来自 Amazon Web Services 账户 ID 123456789012 的用户）访问存储在表存储桶的 hr 命名空间中的表。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/Jane"
            },
            "Action": [
                "s3tables:GetTableData",
                "s3tables:GetTableMetadataLocation"
            ],
            "Resource": "arn:aws:s3tables:region:account_id:bucket/amzn-s3-demo-table-
bucket/table/*",
```

```
            "Condition": {
                "StringLike": {"s3tables:namespace": "hr"}
            }
        }
    ]
}
```

示例 3：支持用户删除表的表策略

以下示例表策略支持 IAM 角色 `data steward` 删除表。

```
{
     "Version": "2012-10-17",
     "Id": "DeleteTable",
     "Statement": [
      {
       "Effect": "Allow",
       "Principal": {
         "AWS": "arn:aws:iam::account_id:role/datasteward"
        },
        "Action": [
           "s3tables:DeleteTable",
           "s3tables:UpdateTableMetadataLocation",
           "s3tables:PutTableData",
           "s3tables:GetTableMetadataLocation"

        ],
        "Resource":"arn:aws:s3tables:region:account_id:bucket/amzn-s3-demo-bucket1/
table/tableUUID"
     }]
}
```

## 适用于 S3 表类数据存储服务的 Amazon 托管式策略

Amazon 托管式策略是由 Amazon 创建和管理的独立策略。Amazon 托管式策略旨在为许多常见使用场景提供权限，以便您可以开始为用户、组和角色分配权限。

请记住，Amazon 托管策略可能不会为您的特定使用场景授予最低权限，因为它们可供所有 Amazon 客户使用。我们建议通过定义特定于您的使用场景的客户管理型策略来进一步减少权限。

您无法更改 Amazon 托管策略中定义的权限。如果 Amazon 更新在 Amazon 托管策略中定义的权限，则更新会影响该策略所附加到的所有主体身份（用户、组和角色）。当新的 Amazon Web Services 服务 启动或新的 API 操作可用于现有服务时，Amazon 最有可能更新 Amazon 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 Amazon 托管式策略。

Amazon 托管策略：AmazonS3TablesFullAccess

您可以将 AmazonTablesS3FullAccess 策略附加到 IAM 身份。此策略授予支持完全访问 Amazon S3 表类数据存储服务的权限。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "s3tables:*"
   ],
   "Resource": "*"
  }
 ]
}
```

Amazon 托管策略：AmazonS3TablesReadOnlyAccess

您可以将 AmazonS3TablesReadOnlyAccess 策略附加到 IAM 身份。此策略授予支持对 Amazon S3 表类数据存储服务进行只读访问的权限。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "s3tables:Get*",
    "s3tables:List*"
   ],
   "Resource": "*"
  }
 ]
}
```

Amazon S3 表类数据存储服务对 Amazon 托管式策略的更新

查看有关自 Amazon S3 表类数据存储服务开始跟踪更改以来，对 S3 表类数据存储服务的 Amazon 托管式策略的更新的详细信息。

| 更改 | 描述 | 日期 |
| --- | --- | --- |
| Amazon S3 表类数据存储服务添加了 AmazonTablesS3FullAccess 。 | S3 表类数据存储服务添加了一个名为 AmazonTablesS3FullAccess 的新 Amazon 托管式策略。此策略授予支持完全访问 Amazon S3 表类数据存储服务的权限。 | 2024 年 12 月 3 日 |
| Amazon S3 表类数据存储服务添加了 AmazonS3TablesReadOnlyAccess 。 | S3 表类数据存储服务添加了一个名为 AmazonS3TablesReadOnlyAccess 的新 Amazon 托管式策略。此策略授予支持对 Amazon S3 表类数据存储服务进行只读访问的权限。 | 2024 年 12 月 3 日 |
| Amazon S3 表类数据存储服务开始了跟踪更改。 | Amazon S3 表类数据存储服务为其 Amazon 托管式策略开始了跟踪更改。 | 2024 年 12 月 3 日 |

## 使用 SQL 语义授予访问权限

可以通过在表和表存储桶策略中使用 SQL 语义来授予对表的权限。可以使用的 SQL 语义的示例为 CREATE、INSERT、DELETE、UPDATE 和 ALTER。下表提供了与 SQL 语义关联的 API 操作的列表，您可以使用这些操作向用户授予权限。

S3 表类数据存储服务部分支持使用 SQL 语义的权限。例如，CreateTable API 仅在表存储桶中创建一个空表。您需要额外的权限（例如 UpdateTableMetadata、PutTableData 和 GetTableMetadataLocation），才能设置表架构。这些额外权限还意味着您还授予用户在表中插入行的权限。如果您希望纯粹基于 SQL 语义来管理访问权限，那么我们建议您使用 Amazon Lake Formation 或任何与 S3 表类数据存储服务集成的第三方解决方案。

| 表级活动 | IAM 操作 | | |
| --- | --- | --- | --- |
| SELECT | s3tables:GetTableData , s3tables:GetTableMetadataLocation | | |
| CREATE | s3tables:CreateTable , s3tables:UpdateTableMetadataLocation , s3tables:PutTableData , s3tables:GetTableMetadataLocation , | | |
| INSERT | s3tables:UpdateTableMetadataLocation , s3tables:PutTableData , s3tables:GetTableM | | |

| 表级活动 | IAM 操作 | | |
| --- | --- | --- | --- |
| | etadataLocation | | |
| UPDATE | s3tables:UpdateTableMetadataLocation , s3tables:PutTableData , s3tables:GetTableMetadataLocation | | |
| ALTER,RENAME | s3tables:UpdateTableMetadataLocation , s3tables:PutTableData , s3tables:GetTableMetadataLocation , s3tables:RenameTable | | |

| 表级活动 | IAM 操作 | | |
| --- | --- | --- | --- |
| DELETE,DROP | s3tables:DeleteTable , s3tables:UpdateTableMetadataLocation , s3tables:PutTableData , s3tables:GetTableMetadataLocation | | |

## S3 表类数据存储服务的 VPC 连接

S3 表类数据存储服务中的所有表均采用 Apache Iceberg 格式，并由两种类型的 S3 对象组成。这两种类型的对象是存储数据的数据文件，以及跟踪有关不同时间点的数据文件信息的元数据文件。所有表存储桶、命名空间和表操作（例如 `CreateNamespace`、`CreateTable` 等）均通过 S3 表类数据存储服务端点 (`s3tables.region.amazonaws.com`) 路由，而读取或写入数据和元数据文件的所有对象级操作都将继续通过 S3 服务端点 (`s3.region.amazonaws.com`) 路由。

为访问 S3 表类数据存储服务，Amazon S3 通过使用 Amazon PrivateLink 支持两种类型的 VPC 端点：网关端点和接口端点。网关端点是您在路由表中指定的网关，用于通过 Amazon 网络从 VPC 访问 S3。接口端点通过私有 IP 地址，使用 VPC 对等连接或 Amazon Transit Gateway 将请求从您的 VPC 内、本地或其它 Amazon Web Services 区域中的 VPC 路由到 Amazon S3，从而扩展网关端点的功能。

要从 VPC 访问 S3 表类数据存储服务，我们建议创建两个 VPC 端点（一个用于 S3，另一个用于 S3 表类数据存储服务）。可以创建网关或接口端点来将文件（对象）级操作路由到 S3，并创建接口端点来将存储桶和表级操作路由到 S3 表。可以使用 S3 为文件级请求创建和使用 VPC 端点。有关更多信息，请参阅《Amazon PrivateLink 用户指南》中的 Gateway endpoints。

要了解有关使用 Amazon PrivateLink 为 S3 表类数据存储服务创建和使用端点的更多信息，请参阅以下主题。要创建 VPC 接口端点，请参阅《Amazon PrivateLink 指南》中的创建 VPC 端点。

主题

- 为 S3 表类数据存储服务创建 VPC 端点
- 使用 Amazon CLI 通过端点访问表存储桶和表
- 使用查询引擎时配置 VPC 网络
- 在 VPC 网络中限制对 S3 表类数据存储服务的访问权限

## 为 S3 表类数据存储服务创建 VPC 端点

当您创建 VPC 端点时，S3 表类数据存储服务会生成两种类型的特定于端点的 DNS 名称：区域和可用区。

- 区域 DNS 名称采用以下格式：`VPCendpointID.s3tables.AWSregion.vpce.amazonaws.com`。例如，对于 VPC 端点 ID `vpce-1a2b3c4d`，生成的 DNS 名称将类似于 `vpce-1a2b3c4d-5e6f.s3tables.us-east-1.vpce.amazonaws.com`
- 可用区 DNS 名称采用以下格式：`VPCendpointID-AvailabilityZone.s3tables.AWSregion.vpce.amazonaws.com`。例如，对于 VPC 端点 ID `vpce-1a2b3c4d-5e6f.`，生成的 DNS 名称将类似于 `vpce-1a2b3c4d-5e6f-us-east-1a.s3tables.us-east-1.vpce.amazonaws.com`

  可用区 DNS 名称包括您的可用区。如果您的架构隔离了可用区，则可以使用可用区 DNS 名称。可以从 S3 公有 DNS 域解析端点特定的 S3 DNS 名称。

还可以使用私有 DNS 选项来简化通过 VPC 端点路由 S3 流量的过程，并协助您充分利用应用程序可用的最低成本网络路径。私有 DNS 将 S3 表类数据存储服务的公有端点（例如 `s3tables.region.amazonaws.com`）映射到 VPC 中的私有 IP。可以使用私有 DNS 选项来路由区域 S3 流量，而无需更新 S3 客户端以使用接口端点的端点特定的 DNS 名称。

> **Note**
>
> 适用于 Amazon S3 的 Amazon PrivateLink 不支持使用 Amazon S3 双堆栈端点。有关更多信息，请参阅《Amazon S3 API 参考》中的 Using Amazon S3 dual-stack endpoints。

## 使用 Amazon CLI 通过端点访问表存储桶和表

可以使用 Amazon Command Line Interface（Amazon CLI）通过接口端点访问表存储桶和表。使用 Amazon CLI，aws s3 命令通过 Amazon S3 端点路由流量。aws s3tables Amazon CLI 命令使用 Amazon S3 表类数据存储服务端点。

s3tables VPC 端点的示例为 vpce-0123456afghjipljw-nmopsqea.s3tables.region.vpce.amazonaws.com

s3tables VPC 端点不包含存储桶名称。可以使用 aws s3tables Amazon CLI 命令访问 s3tables VPC 端点。

s3 VPC 端点的示例为 amzn-s3-demo-bucket.vpce-0123456afghjipljw-nmopsqea.s3.region.vpce.amazonaws.com

可以使用 aws s3 Amazon CLI 命令访问 s3 VPC 端点。

使用 Amazon CLI

要使用 Amazon CLI 通过接口端点访问表存储桶和表，请使用 -region 和 --endpoint-url 参数。要执行表存储桶和表级操作，请使用 S3 表类数据存储服务端点 URL。要执行对象级操作，请使用 Amazon S3 端点 URL。

在以下示例中，请将####### 替换为您自己的信息。

示例 1：使用端点 URL 列出账户中的表存储桶

```
aws s3tables list-table-buckets --endpoint https://vpce-0123456afghjipljb-aac.s3tables.us-east-1.vpce.amazonaws.com –region us-east-1
```

示例 2：使用端点 URL 列出存储桶中的表

```
aws s3tables list-tables --table-bucket-arn arn:aws:s3tables:us-east-1:123456789301:bucket/amzn-s3-demo-bucket --endpoint
 https://vpce-0123456afghjipljb-aac.s3tables.us-east-1.vpce.amazonaws.com --region us-east-1
```

## 使用查询引擎时配置 VPC 网络

使用查询引擎时，请使用以下步骤配置 VPC 网络。

1. 要开始使用，您可以创建或更新 VPC。有关更多信息，请参阅创建 VPC。

2. 对于路由到 S3 表类数据存储服务的表和表存储桶级操作，请创建一个新的接口端点。有关更多信息，请参阅使用接口 VPC 端点访问 Amazon 服务。
3. 对于路由到 Amazon S3 的所有对象级操作，请创建网关端点或接口端点。有关网关端点的更多信息，请参阅 Create a gateway endpoint。
4. 接下来，配置数据资源并启动 Amazon EMR 集群。有关更多信息，请参阅 Getting started with Amazon EMR。
5. 然后，可以通过从 VPC 端点中选择 DNS 名称，来提交带有额外配置的 Spark 应用程序。例如 `spark.sql.catalog.ice_catalog.s3tables.endpoint` 和 `https://interface-endpoint.s3tables.us-east-1.vpce.amazonaws.com`。有关更多信息，请参阅 Submit work to your Amazon EMR cluster。

### 在 VPC 网络中限制对 S3 表类数据存储服务的访问权限

与基于资源的策略类似，可以向 VPC 端点附加端点策略，来控制对表和表存储桶的访问权限。在以下示例中，接口端点策略限制为仅可访问特定的表存储桶。

```
{
    "Version": "2012-10-17",
    "Id": "Policy141511512309",
    "Statement": [{
        "Sid": "Access-to-specific-bucket-only",
        "Principal": "*",
        "Action": "s3tables:*",
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3tables:region:account_id:bucket/amzn-s3-demo-bucket",
            "arn:aws:s3tables:region:account_id:bucket/amzn-s3-demo-bucket/*"
        ]
    }]
}
```

## S3 表类数据存储服务的安全注意事项和限制

以下列表描述了 S3 表类数据存储服务不支持或限制哪些安全和访问控制特性和功能。

- 不支持公有访问策略。用户无法修改存储桶或表策略来支持公有访问。
- 不支持用于访问与表关联的对象的预签名 URL。
- 表存储桶和表不支持标签。因此，对于基于属性的访问控制和基于标签的分配的支持不可用。

- 不支持通过 HTTP 发出的请求。对于通过 HTTP 发出的任何请求，Amazon S3 都会自动以 HTTP 重定向作为响应，从而将请求升级到 HTTPS。
- 使用 REST API 向接入点发出请求时，必须使用 Amazon 签名版本 4。
- 通过互联网协议版本 6（IPv6）发出的请求仅适用于通过表存储端点执行对象级操作，而不适用于表级和存储桶级操作。
- 表存储桶和表访问策略的大小限制为 20 KB。

# 使用 Amazon CloudTrail 对 S3 表类数据存储服务进行日志记录

Amazon S3 与 Amazon CloudTrail 集成，后者是一项提供由用户、角色或 Amazon 服务所采取操作的记录的服务。CloudTrail 将 Amazon S3 的所有 API 调用作为事件捕获。借助通过 CloudTrail 收集的信息，您可以确定向 Amazon S3 发出哪些请求、发出请求的 IP 地址、请求的发出时间以及其它详细信息。当 Amazon S3 中发生受支持的事件活动时，该活动将记录在 CloudTrail 事件中。可以使用 Amazon CloudTrail 跟踪来记录 S3 表类数据存储服务的管理事件和数据事件。有关更多信息，请参阅《Amazon CloudTrail User Guide》中的 Amazon S3 CloudTrail events 和 What is Amazon CloudTrail?

## S3 表类数据存储服务的 CloudTrail 管理事件

管理事件提供有关对在您 Amazon 账户内的资源上执行的管理操作的信息。

默认情况下，CloudTrail 会记录 S3 表类数据存储服务的管理事件。S3 表类数据存储服务的 CloudTrail 管理事件的 `eventsource` 为 `s3tables.amazonaws.com`。当您设置 Amazon 账户时，CloudTrail 管理事件默认处于启用状态。以下管理事件记录到 CloudTrail。

- `CreateNamespace`
- `CreateTable`
- `CreateTableBucket`
- `DeleteNamespace`
- `DeleteTable`
- `DeleteTableBucket`
- `DeleteTableBucketPolicy`
- `DeleteTablePolicy`
- `GetNamespace`
- `GetTable`

- GetTableBucket
- GetTableBucketMaintenanceConfiguration
- GetTableBucketPolicy
- GetTableMaintenanceConfiguration
- GetTableMaintenanceJobStatus
- GetTableMetadataLocation
- GetTablePolicy
- ListNamespaces
- ListTableBuckets
- ListTables
- PutTableBucketMaintenanceConfiguration
- PutTableMaintenanceConfiguration
- PutBucketPolicy
- PutTablePolicy
- RenameTable
- UpdateTableMetadataLocation

有关 CloudTrail 管理事件的更多信息，请参阅《Amazon CloudTrail User Guide》中的 Logging management events。

## S3 表类数据存储服务的 CloudTrail 数据事件

数据事件提供对资源或在资源中执行的资源操作的信息。默认情况下，CloudTrail 跟踪不记录数据事件，但您可以将跟踪配置为记录数据事件。

在 CloudTrail 中记录跟踪的数据事件时，您将选择或指定资源类型。S3 表类数据存储服务有两种资源类型：`AWS::S3Tables::Table` 和 `AWS::S3Tables::TableBucket`。

以下数据事件记录到 CloudTrail。

- AbortMultipartUpload
- CompleteMultipartUpload
- CreateMultipartUpload
- GetObject

- HeadObject
- ListParts
- PutObject
- UploadPart

有关 CloudTrail 数据事件的更多信息，请参阅《Amazon CloudTrail User Guide》中的 Logging data events。

有关 S3 表类数据存储服务的 CloudTrail 事件的更多信息，请参阅以下主题：

主题

- S3 表类数据存储服务的 Amazon CloudTrail 数据事件日志文件示例

## S3 表类数据存储服务的 Amazon CloudTrail 数据事件日志文件示例

Amazon CloudTrail 日志文件包括有关所请求 API 操作的信息、操作的日期和时间和请求参数等。本主题为 S3 表类数据存储服务的 CloudTrail 数据事件提供示例日志文件。

主题

- 示例 - GetObject 数据事件的 CloudTrail 日志文件
- 示例 - PutObject 数据事件的 CloudTrail 日志文件

### 示例 - **GetObject** 数据事件的 CloudTrail 日志文件

下面的示例显示了一个 CloudTrail 日志文件示例，该示例演示了 GetObject API 操作。

```
    {
        "eventVersion": "1.11",
        "userIdentity": {
          "type": "IAMUser",
          "principalId": "123456789012",
          "arn": "arn": "arn:aws:iam::111122223333:user/"myUserName",
          "accountId": "111122223333",
          "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
          "userName":"myUserName"
        },
        "eventTime": "2024-11-22T17:12:25Z",
        "eventSource": "s3tables.amazonaws.com",
```

```
        "eventName": "GetObject",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "192.0.2.0",
        "userAgent": "[aws-cli/2.18.5]",
        "requestParameters": {
            "Host": "tableWarehouseLocation.s3.us-east-1.amazonaws.com",
            "key": "product-info.json"
        },
        "responseElements":  null,
        "additionalEventData": {
            "SignatureVersion": "SigV4",
            "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
            "bytesTransferredIn": 0,
            "AuthenticationMethod": "AuthHeader",
            "xAmzId2": "q6xhNJYmhg",
            "bytesTransferredOut": 28441,

          },
          "requestID": "07D681123BD12AED",
          "eventID": "f2b287f3-0df1-1234-a2f4-c4bdfed47657",
          "readOnly": true,
          "resources": [{
              "accountId": "111122223333",
              "type": "AWS::S3Tables::TableBucket",
               "ARN": "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
bucket1"
           }, {
              "accountId": "111122223333",
              "type": "AWS::S3Tables::Table",
              "ARN": "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
bucket/table/111aa1111-22bb-33cc-44dd-5555eee66ffff"

           }],
           "eventType": "AwsApiCall",
           "managementEvent": false,
           "recipientAccountId": "444455556666",
           "eventCategory": "Data",
           "tlsDetails": {
             "tlsVersion": "TLSv1.2",
             "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256"
             "clientProvidedHostHeader": "tableWarehouseLocation.s3.us-
east-1.amazonaws.com"
          }
```

```
    }
```

## 示例 - **PutObject** 数据事件的 CloudTrail 日志文件

下面的示例显示了一个 CloudTrail 日志文件示例，该示例演示了 PutObject API 操作。

```
{
        "eventVersion": "1.11",
        "userIdentity": {
          "type": "IAMUser",
          "principalId": "123456789012",
          "arn": "arn": "arn:aws:iam::444455556666:user/"myUserName",
          "accountId": "444455556666",
          "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
          "userName":"myUserName"
        },
        "eventTime": "2024-11-22T17:12:25Z",
        "eventSource": "s3tables.amazonaws.com",
        "eventName": "PutObject",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "192.0.2.0",
        "userAgent": "[aws-cli/2.18.5]",
        "requestParameters": {
            "Host": "tableWarehouseLocation.s3.us-east-1.amazonaws.com",
            "key": "product-info.json"
        },
        "responseElements":  {
            "x-amz-server-side-encryption": "AES256",
            "x-amz-version-id": "13zAFMdccAjt3MWd6ehxgCCCDRdkAKDw"
        },
        "additionalEventData": {
            "SignatureVersion": "SigV4",
            "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
            "bytesTransferredIn": 28441,
            "AuthenticationMethod": "AuthHeader",
            "xAmzId2": "q6xhCJYmhg",
            "bytesTransferredOut": 0,

          },
          "requestID": "28d2faaf-1234-4649-997d-EXAMPLE72818",
          "eventID": "694d604a-d190-1234-0dd1-EXAMPLEe20c1",
          "readOnly": false,
          "resources": [{
```

```
              "accountId": "444455556666",
              "type": "AWS::S3Tables::TableBucket",
               "ARN": "arn:aws:s3tables:us-east-1444455556666:bucket/amzn-s3-demo-
bucket1"
           }, {
              "accountId": "444455556666",
              "type":  "type": "AWS::S3Tables::Table",
              "ARN": "arn:aws:s3tables:us-east-1:444455556666:bucket/amzn-s3-demo-
bucket1/table/b89ec883-b1d9-4b37-9cd7-b86f590123f4"
           }],
           "eventType": "AwsApiCall",
           "managementEvent": false,
           "recipientAccountId": "111122223333",
           "eventCategory": "Data",
           "tlsDetails": {
             "tlsVersion": "TLSv1.2",
             "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256"
             "clientProvidedHostHeader": "tableWarehouseLocation.s3.us-
east-1.amazonaws.com"
            }
         }
```

# Amazon S3 中的访问控制

在 Amazon 中，资源是您可使用的实体。在 Amazon Simple Storage Service（S3）中，存储桶和对象是最初的 Amazon S3 资源。每个 S3 客户可能都有包含对象的存储桶。当有新功能添加到 S3 时，则会添加额外的资源，但并非每个客户都使用这些特定于功能的资源。有关 Amazon S3 资源的更多信息，请参阅 S3 资源。

默认情况下，所有 Amazon S3 资源都是私有的。此外，默认情况下，创建资源的 Amazon Web Services 账户的根用户（资源拥有者）和该账户中具有必要权限的 IAM 用户可以访问他们创建的资源。资源拥有者决定还有谁可以访问该资源以及允许其他人对该资源执行哪些操作。S3 有各种访问管理工具，您可以使用这些工具向其他人授予对您的 S3 资源的访问权限。

以下各节概述了 S3 资源、可用的 S3 访问管理工具以及每种访问管理工具的最佳使用案例。这些章节中的列表力求全面，旨在包括所有 S3 资源、访问管理工具和常见的访问管理使用案例。同时，这些章节设计成目录，可引导您找到所需的技术细节。如果您对以下某些主题有很好的理解，则可以跳到适用于您的章节。

有关按 S3 资源类型对 S3 API 操作的权限的更多信息，请参阅 Amazon S3 API 操作所需的权限。

主题


- S3 资源
- 身份
- 访问管理工具
- 操作
- 访问管理使用案例
- 访问管理故障排除


## S3 资源

原始 Amazon S3 资源是存储桶及其中包含的对象。随着向 S3 添加新功能，也会添加新的资源。以下是 S3 资源及相应功能的完整列表。

| 资源类型 | Amazon S3 功能 | 描述 |
| --- | --- | --- |
| bucket | 核心功能 | 存储桶是对象的容器。要将对象存储在 S3 中，请创建存储桶，然后将一个或多个对象上传到该存储桶。有关更多信息，请参阅 创建、配置和使用 Amazon S3 通用存储桶。 |
| object | | 对象可以是一个文件和描述该文件的任何元数据。当对象位于存储桶中时，您可以将其打开、下载并移动它。有关更多信息，请参阅 使用 Amazon S3 中的对象。 |
| accesspoint | 访问点 | 接入点是附加到存储桶的命名网络端点，您可以使用这些存储桶执行 Amazon S3 object 操作（如 GetObject 和 PutObject ）。每个接入点都有不同的权限、网络控制和自定义的接入点策略，该策略与附加到底层存储桶的存储桶策略结合使用。您可以将任何接入点配置为仅接受来自虚拟私有云（VPC）的请求，或者为每个接入点配置自定义屏蔽公共访问权限设置。有关更多信息，请参阅 通过接入点管理对通用存储桶中共享数据集的访问。 |
| objectlambdaaccesspoint | | 对象 Lambda 接入点是也与 Lambda 函数相关联的存储桶的接入点。借助对象 Lambda 接入点，您可以将自己的代码添加到 Amazon S3 GET、LIST 和 HEAD 请求中，以便在数据返回到应用程序时修改和处理数据。有关更多信息，请参阅 创建对象 Lambda 接入点。 |
| multiregionaccesspoint | | 多区域接入点提供了一个全局端点，应用程序可以使用该端点来满足来自位于多个 Amazon 区域的 Amazon S3 存储桶的请求。您可以使用多区域接入点通过单个区域中使用的相同架构构建多区域应用程序，然后在世界任何地方运行这些应用程序。向多区域接入点全局端点发出的应用程序请求自动通过 Amazon 全局网络路由到距离最近的 Amazon S3 存储桶，而不是通过拥挤的公共互联网发送请求。有关更多信息，请参阅 使用多区域接入点管理多区域流量。 |
| job | S3 批量操作 | 任务是 S3 批量操作功能的资源。您可以使用 S3 批量操作对您指定的 Amazon S3 对象列表执行大规模批量操作。Amazon S3 跟踪批量操作任务的进度，发送通知，并存储所有操 |

| 资源类型 | Amazon S3 功能 | 描述 |
| --- | --- | --- |
| | | 作的详细完成报告，从而提供完全托管式、可审计的无服务器体验。有关更多信息，请参阅 使用批量操作批量执行对象操作。 |
| storagelensconfiguration | S3 Storage Lens 存储统计管理工具 | S3 Storage Lens 存储分析功能配置负责收集组织范围的存储指标和跨账户的用户数据。S3 Storage Lens 存储分析功能为管理员提供了组织中数百甚至数千个账户的对象存储使用情况和活动的单一视图，并提供了可在多个聚合级别生成见解的详细信息。有关更多信息，请参阅 使用 Amazon S3 Storage Lens 存储统计管理工具评估您的存储活动和使用情况。 |
| storagelensgroup | | S3 Storage Lens 组使用基于对象元数据的自定义筛选条件来聚合指标。S3 Storage Lens 组可协助您调查数据的特征，例如按龄期划分的对象分布、最常见的文件类型等。有关更多信息，请参阅 使用 S3 Storage Lens 组筛选和汇总指标。 |
| accessgrantsinstance | S3 访问权限管控 | S3 Access Grants 实例是您创建的 S3 授权的容器。借助 S3 Access Grants，您可以为您账户中的 IAM 身份、其它账户（跨账户）中的 IAM 身份以及从公司目录中添加到 Amazon IAM Identity Center 的目录身份创建对于您的 Amazon S3 数据的授权。有关 S3 Access Grants 的更多信息，请参阅使用 S3 Access Grants 管理访问权限。 |
| accessgrantslocation | | Access Grants 位置是存储桶、存储桶内的前缀或您在 S3 Access Grants 实例中注册的对象。您必须在 S3 Access Grants 实例中注册位置，然后才能创建对该位置的授权。然后，借助 S3 Access Grants，您可以为您账户中的 IAM 身份、其它账户（跨账户）中的 IAM 身份以及从公司目录中添加到 Amazon IAM Identity Center 的目录身份授予对存储桶、前缀或对象的访问权限。有关 S3 Access Grants 的更多信息，请参阅使用 S3 Access Grants 管理访问权限。 |

| 资源类型 | Amazon S3 功能 | 描述 |
| --- | --- | --- |
| accessgrant | | 访问授权是对您的 Amazon S3 数据的单独授权。借助 S3 Access Grants，您可以为您账户中的 IAM 身份、其它账户（跨账户）中的 IAM 身份以及从公司目录中添加到 Amazon IAM Identity Center 的目录身份创建对于您的 Amazon S3 数据的授权。有关 S3 Access Grants 的更多信息，请参阅使用 S3 Access Grants 管理访问权限。 |

存储桶

Amazon S3 存储桶有两种类型：通用型存储桶 和目录存储桶。

- 通用存储桶是最初的 S3 存储桶类型，建议用于大多数使用案例和访问模式。通用存储桶还允许跨所有存储类（S3 Express One Zone 除外）存储对象。有关 S3 存储类的更多信息，请参阅了解和管理 Amazon S3 存储类。
- 目录存储桶使用 S3 Express 单区存储类，如果您的应用程序注重性能，并且受益于个位数毫秒的 PUT 和 GET 延迟，则建议使用该存储类。有关更多信息，请参阅使用目录存储桶、S3 Express One Zone和使用 IAM 对区域端点 API 操作进行授权。

对 S3 资源进行分类

Amazon S3 提供了对您的 S3 资源进行分类和整理的功能。对资源进行分类不仅对整理资源很有用，还可以根据资源类别设置访问管理规则。特别是，前缀和标记是设置访问管理权限时可以使用的两个存储整理功能。

> **Note**
>
> 以下信息适用于通用型存储桶。目录存储桶不支持标记，并且有前缀限制。有关更多信息，请参阅 使用 IAM 对区域端点 API 操作进行授权。

- 前缀 – Amazon S3 中的前缀是对象键名称开头的一个字符串，用于整理存储在 S3 存储桶中的对象。您可以使用分隔符 [例如正斜杠（/）] 来表示对象键名称中前缀的结尾。例如，您可能有以 engineering/ 前缀开头的对象键名称或以 marketing/campaigns/ 前缀开头的对象键名称。

在前缀末尾使用分隔符（例如正斜杠字符 /）可以模拟文件夹和文件命名约定。但是，在 S3 中，前缀是对象键名称的一部分。在通用型 S3 存储桶中，没有实际的文件夹层次结构。

Amazon S3 支持使用对象的前缀对于对象进行整理和分组。您还可以通过对象的前缀管理对于对象的访问权限。例如，您可以将访问权限限制为仅限名称以特定前缀开头的对象。

有关更多信息，请参阅 使用前缀组织对象。S3 控制台使用文件夹 的概念，在通用型存储桶中，文件夹本质上是附加在对象键名称之前的前缀。有关更多信息，请参阅 使用文件夹在 Amazon S3 控制台中整理对象。

- 标签 – 每个标签都是您分配给资源的键值对。例如，您可以使用标签 `topicCategory=engineering` 标记某些资源。您可以使用标记来协助进行成本分配、分类和整理以及访问控制。存储桶标记仅用于成本分配。您可以标记对象、Storage Lens 存储分析功能、任务和 S3 Access Grants，以便进行整理或实施访问控制。在 S3 Access Grants 中，您还可以使用标记进行成本分配。举个使用标签控制资源访问权限的示例，您只能共享具有特定标签或标签组合的对象。

  有关更多信息，请参阅《IAM 用户指南》中的使用资源标签控制对 Amazon 资源的访问。

## 身份

在 Amazon S3 中，资源拥有者是创建资源（例如存储桶或对象）的身份。默认情况下，只有创建资源的账户的根用户和该账户中具有所需权限的 IAM 身份才能访问 S3 资源。资源拥有者可以向其它身份授予对其 S3 资源的访问权限。

不拥有资源的身份可以请求访问该资源。对资源的请求已经过身份验证或未经过身份验证。经过身份验证的请求必须包含可验证请求发送者身份的签名值，但未经身份验证的请求不需要签名。我们建议您仅向经过身份验证的用户授予访问权限。有关请求身份验证的更多信息，请参阅《Amazon S3 API 参考》中的 Making requests。

> **Important**
>
> 我们建议不要使用 Amazon Web Services 账户根用户凭证发起经过身份验证的请求。而应创建一个 IAM 角色并授予该角色完全访问权限。我们将具有此角色的用户称为管理员用户。您可以使用分配给管理员角色的用户凭证而不是 Amazon Web Services 账户 根用户凭证来与 Amazon 交互和执行任务，例如创建存储桶、创建用户以及授予权限。有关更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon Web Services 账户 根用户凭证和 IAM 用户凭证，并参阅《IAM 用户指南》中的 IAM 中的安全最佳实践。

在 Amazon S3 中访问您的数据的身份可以是以下身份之一：

Amazon Web Services 账户拥有者

创建资源的 Amazon Web Services 账户。例如，创建存储桶的账户。此账户是该资源的拥有者。有关更多信息，请参阅 Amazon 账户根用户。

与 Amazon Web Services 账户拥有者同属一个账户的 IAM 身份

在为需要 S3 访问权限的新团队成员设置账户时，Amazon Web Services 账户拥有者可以使用 Amazon Identity and Access Management（IAM）来创建用户、组和角色。然后，Amazon Web Services 账户拥有者可以与这些 IAM 身份共享资源。账户拥有者还可以指定要向 IAM 身份授予的权限，这些权限允许或拒绝可以对共享资源执行的操作。

IAM 身份提供了增强的功能，包括要求用户在访问共享资源之前先输入登录凭证的功能。通过使用 IAM 身份，您可以实施一种形式的 IAM 多重身份验证（MFA）来支持强大的身份基础。IAM 最佳实践是创建用于访问管理的角色，而不是向每个单独用户授予权限。您可以将各个用户分配给相应的角色。有关更多信息，请参阅 IAM 安全最佳实践。

其它 Amazon 账户拥有者及其 IAM 身份（跨账户存取）

Amazon Web Services 账户拥有者还可以向其它 Amazon 账户拥有者或属于其它 Amazon 账户的 IAM 身份授予对资源的访问权限。

> **Note**
>
> 权限委托 – 如果某个 Amazon Web Services 账户拥有一项资源，则该账户可以将这些权限授予其它 Amazon Web Services 账户。然后，这个账户就可以将这些权限或其子集委托给同一账户中的用户。这称为 权限委托。但从另一账户接收权限的账户不能“跨账户”向其它 Amazon Web Services 账户委托这些权限。

匿名用户（公共访问权限）

Amazon Web Services 账户拥有者可以公开资源。从技术上讲，公开某资源会与匿名用户 共享该资源。除非您更改此设置，否则默认情况下，自 2023 年 4 月以来创建的存储桶会屏蔽所有公共访问权限。我们建议您将存储桶设置为屏蔽公共访问权限，并且仅向经过身份验证的用户授予访问权限。有关屏蔽公共访问权限的更多信息，请参阅阻止对您的 Amazon S3 存储的公有访问。

Amazon Web Services 服务

资源拥有者可以向其它 Amazon 服务授予对 Amazon S3 资源的访问权限。例如，您可以向 Amazon CloudTrail 服务授予将日志文件写入存储桶的 `s3:PutObject` 权限。有关更多信息，请参阅向 Amazon 服务提供访问权限。

公司目录身份

资源拥有者可以使用 S3 Access Grants 向公司目录中的用户或角色授予对 S3 资源的访问权限。有关将公司目录添加到 Amazon IAM Identity Center 的更多信息，请参阅 What is IAM Identity Center?

## 存储桶拥有者或资源拥有者

用于创建存储桶和上传对象的 Amazon Web Services 账户拥有这些资源。存储桶拥有者可以向其他 Amazon Web Services 账户（或其他账户中的用户）授予上传对象的跨账户权限。

当存储桶拥有者允许其它账户向存储桶上传对象时，默认情况下，该存储桶拥有者拥有上传到其存储桶的所有对象。但是，如果强制存储桶拥有者 和存储桶拥有者优先 存储桶设置都处于关闭状态，则上传对象的 Amazon Web Services 账户将拥有这些对象，而存储桶拥有者对其它账户拥有的对象没有权限，但以下情况除外：

- 账单由存储桶拥有者支付。存储桶拥有者可以拒绝对任何对象的访问，或删除存储桶中的任何对象，而无论它们的拥有者是谁。
- 存储桶拥有者可以归档任何对象或还原归档的对象，而无论它们的拥有者是谁。归档是指用于存储对象的存储类。有关更多信息，请参阅 管理对象的生命周期。

# 访问管理工具

Amazon S3 提供了各种安全功能和工具。以下是这些功能和工具的完整列表。您并不需要所有这些访问管理工具，但必须使用一个或多个工具来授予对您的 Amazon S3 资源的访问权限。正确应用这些工具有助于确保只有目标用户才能访问您的资源。

最常用的访问管理工具是访问策略。访问策略可以是附加到 Amazon 资源的基于资源的策略，例如存储桶的存储桶策略。访问策略也可以是附加到 Amazon Identity and Access Management（IAM）身份（如 IAM 用户、组或角色）的基于身份的策略。编写访问策略来向 Amazon Web Services 账户和 IAM 用户、组和角色授予对资源执行操作的权限。例如，您可以向另一个 Amazon Web Services 账户授予 `PUT Object` 权限，以使该账户可以向您的存储桶上传对象。

访问策略描述了谁可以访问哪些内容。当 Amazon S3 收到请求时，它必须评估所有访问策略，来决定是授权还是拒绝该请求。有关 Amazon S3 如何评估这些策略的更多信息，请参阅 Amazon S3 如何对请求授权。

以下是 Amazon S3 中提供的访问管理工具。

## 存储桶策略

Amazon S3 存储桶策略是采用 JSON 格式的 Amazon Identity and Access Management（IAM）基于资源的策略，该策略附加到特定的存储桶。使用存储桶策略来向其它 Amazon Web Services 账户或 IAM 身份授予对相应存储桶及其中对象的权限。使用存储桶策略可以满足许多 S3 访问管理使用案例的要求。通过存储桶策略，您可以对存储桶访问权限进行个性化设置，以协助确保只有您已批准的身份才能访问资源并在其中执行操作。有关更多信息，请参阅 Amazon S3 的存储桶策略。

下面是一个示例存储桶策略。您可以使用 JSON 文件来表示存储桶策略。此示例策略向 IAM 角色授予对存储桶中所有对象的读取权限。该策略包含一条名为 `BucketLevelReadPermissions` 的语句，该语句允许对名为 `amzn-s3-demo-bucket1` 的存储桶中的对象执行 `s3:GetObject` 操作（读取权限）。通过将 IAM 角色指定为 `Principal`，此策略向具有该角色的任何 IAM 用户授予访问权限。要使用此示例策略，请将 *`user input placeholders`* 替换为您自己的信息。

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid":"BucketLevelReadPermissions",
      "Effect":"Allow",
      "Principal": {
     "AWS": "arn:aws:iam::123456789101:role/s3-role"
      },
      "Action":["s3:GetObject"],
      "Resource":["arn:aws:s3:::amzn-s3-demo-bucket1/*"]
    }]
  }
```

> **Note**
>
> 创建策略时，请避免在 `Principal` 元素中使用通配符（`*`），因为使用通配符将允许任何人访问您的 Amazon S3 资源。而是应显式列出允许访问存储桶的用户或组，或者使用策略中的条件子句列出必须满足的条件。此外，在适用的情况下，向用户或组授予特定的权限，而不是包含通配符来让用户或组执行操作。

## 基于身份的策略

基于身份的策略或 IAM 用户策略是一种 Amazon Identity and Access Management（IAM）策略。基于身份的策略是采用 JSON 格式的策略，该策略附加到您的 Amazon 账户中的 IAM 用户、组或角色。您可以使用基于身份的策略，来向 IAM 身份授予对您的存储桶或对象的访问权限。您可以在您的账户中创建 IAM 用户、组和角色，并为其附加访问策略。然后，您可以授予对 Amazon 资源（包括 Amazon S3 资源）的访问权限。有关更多信息，请参阅 Amazon S3 基于身份的策略。

下面是基于身份的策略的示例。此示例策略允许关联的 IAM 角色对存储桶及其中的对象执行六种不同的 Amazon S3 操作（权限）。如果您将此策略附加到您账户中的 IAM 角色，并将该角色分配给您的某些 IAM 用户，则具有此角色的用户将能够对在策略中指定的资源（存储桶）执行这些操作。要使用此示例策略，请将 *user input placeholders* 替换为您自己的信息。

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Sid": "AssignARoleActions",
    "Effect": "Allow",
    "Action": [
   "s3:PutObject",
   "s3:GetObject",
   "s3:ListBucket",
   "s3:DeleteObject",
   "s3:GetBucketLocation"
    ],
    "Resource": [
   "arn:aws:s3:::amzn-s3-demo-bucket1/*",
   "arn:aws:s3:::amzn-s3-demo-bucket1"
    ]
    },
  {
    "Sid": "AssignARoleActions2",
    "Effect": "Allow",
    "Action": "s3:ListAllMyBuckets",
    "Resource": "*"
  }
  ]
}
```

### S3 访问权限管控

使用 S3 Access Grants 为企业身份目录（例如 Active Directory）中的身份以及 Amazon Identity and Access Management（IAM）身份创建对您的 Amazon S3 数据的访问授权。S3 Access Grants 可协助您大规模管理数据权限。此外，S3 Access Grants 还会记录最终用户身份以及用于访问 Amazon CloudTrail 中 S3 数据的应用程序。这提供了详细的审计历史记录，细至与 S3 存储桶中数据的所有访问权限对应的最终用户身份。有关更多信息，请参阅 使用 S3 Access Grants 管理访问权限。

### 访问点

对于使用 S3 上的共享数据集的应用程序，Amazon S3 接入点可简化大规模管理数据访问的事宜。接入点是附加到存储桶的命名网络端点。您可以使用接入点来大规模执行 S3 对象操作，例如上传和检索对象。一个存储桶最多可附加 10000 个接入点，对于每个接入点，您可以强制实施不同的权限和网络控制，从而让您可以详细控制对于 S3 对象的访问权限。S3 接入点可以与同一个账户或其它可信账户中的存储桶相关联。接入点策略是与底层存储桶策略一起进行评估的基于资源的策略。有关更多信息，请参阅 通过接入点管理对通用存储桶中共享数据集的访问。

### 访问控制列表 (ACL)

ACL 是用于确定被授权者和所授予权限的授权列表。ACL 向其它 Amazon Web Services 账户授予基本的读取或写入权限。ACL 使用特定于 Amazon S3 的 XML 架构。ACL 是一种 Amazon Identity and Access Management（IAM）策略。对象 ACL 用于管理对于对象的访问权限，而存储桶 ACL 用于管理对存储桶的访问权限。使用存储桶策略，整个存储桶只有单个策略，但可以为每个对象指定对象 ACL。我们建议您将 ACL 保持为关闭状态，除非有必须单独控制每个对象的访问权限的特殊情况。有关 ACL 的更多信息，请参阅 为您的存储桶控制对象所有权和禁用 ACL。。

> **Warning**
>
> Amazon S3 中的大多数现代使用案例不需要使用 ACL。

下面是一个示例存储桶 ACL。ACL 中的授权显示一个具有完全控制权限的存储桶拥有者。

```
<?xml version="1.0" encoding="UTF-8"?>
 <AccessControlPolicy xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Owner>
   <ID>Owner-Canonical-User-ID</ID>
   <DisplayName>owner-display-name</DisplayName>
  </Owner>
```

```
 <AccessControlList>
  <Grant>
   <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="Canonical
 User">
    <ID>Owner-Canonical-User-ID</ID>
    <DisplayName>display-name</DisplayName>
   </Grantee>
   <Permission>FULL_CONTROL</Permission>
  </Grant>
 </AccessControlList>
</AccessControlPolicy>
```

## 对象所有权

要管理对于对象的访问权限，您必须是该对象的拥有者。您可以使用对象所有权存储桶级别设置，来控制上传到存储桶的对象的所有权。此外，使用对象所有权来开启 ACL。默认情况下，对象所有权设为强制存储桶拥有者设置，并且所有 ACL 均处于关闭状态。关闭 ACL 后，存储桶拥有者拥有存储桶中的所有对象，并独占管理对数据的访问权限。为了管理访问权限，存储桶拥有者使用策略或其它访问管理工具（ACL 除外）。有关更多信息，请参阅 为您的存储桶控制对象所有权和禁用 ACL。。

对象所有权有三个设置，您可以使用它们来控制上传到存储桶的对象的所有权并开启 ACL：

ACL 已关闭

- 强制存储桶拥有者（默认）– ACL 已关闭，存储桶拥有者自动拥有并完全控制存储桶中的每个对象。ACL 不影响对 S3 存储桶中数据的权限。存储桶专门使用策略来定义访问控制。

ACL 已开启

- Bucket owner preferred（首选存储桶拥有者）— 存储桶拥有者拥有并完全控制其他账户使用 `bucket-owner-full-control` 标准 ACL 写入存储桶的新对象。
- 对象编写者— 该 Amazon Web Services 账户上传对象拥有该对象，对其拥有完全控制权，并且可以通过 ACL 授予其他用户访问该对象的权限。

其他最佳实践

考虑使用以下存储桶设置和工具来协助保护传输中数据和静态数据，这两者对于保持数据的完整性和可访问性至关重要：

- 屏蔽公共访问权限 - 请勿关闭默认的存储桶级别设置屏蔽公共访问权限。默认情况下，此设置会屏蔽对您的数据的公共访问权限。有关屏蔽公共访问权限的更多信息，请参阅阻止对您的 Amazon S3 存储的公有访问。
- S3 版本控制 – 为确保数据完整性，您可以实现 S3 版本控制存储桶设置，此设置在您进行更新时对于对象进行版本控制，而不是覆盖它们。如果需要，您可以使用 S3 版本控制功能来保留、检索和还原以前的版本。有关 S3 版本控制的信息，请参阅使用 S3 版本控制保留对象的多个版本。
- S3 对象锁定 – S3 对象锁定是您可以实施来实现数据完整性的另一个设置。此功能可以实现一次写入多次读取（WORM）模式，从而以不可变的方式存储对象。有关对象锁定的信息，请参阅使用对象锁定以锁定对象。
- 对象加密 – Amazon S3 提供了多种对象加密选项，用于保护传输中数据和静态数据。服务器端加密会在将对象保存到数据中心的磁盘上之前为对象加密，然后在下载对象时对数据进行解密。如果您验证了您的请求并且您拥有访问权限，则您访问加密对象或未加密对象的方式就没有区别。有关更多信息，请参阅 使用服务器端加密保护数据。默认情况下，S3 会加密新上传的对象。有关更多信息，请参阅 为 Amazon S3 存储桶设置默认服务器端加密行为。客户端加密是在将数据发送到 Amazon S3 之前加密数据的行为。有关更多信息，请参阅 使用客户端加密保护数据。
- 签名方法 – 签名版本 4 是将身份验证信息添加到通过 HTTP 发送的 Amazon 请求的过程。出于安全考虑，大多数 Amazon 请求都必须使用访问密钥（包括访问密钥 ID 和秘密访问密钥）进行签名。这两个密钥通常称为您的安全凭证。有关更多信息，请参阅对请求进行身份验证（Amazon Signature Version 4）和 Signature Version 4 签名过程。

## 操作

有关 S3 权限和条件键的完整列表，请参阅《服务授权参考》中的 Actions, resources, and condition keys for Amazon S3。

有关按 S3 资源类型对 S3 API 操作的权限的更多信息，请参阅 Amazon S3 API 操作所需的权限。

### 操作

Amazon S3 的 Amazon Identity and Access Management（IAM）操作是可以对 S3 存储桶或对象执行的可能操作。您可以向身份授予这些操作，以便这些身份可以对您的 S3 资源执行操作。S3 操作的示例为 `s3:GetObject`（读取存储桶中的对象）和 `s3:PutObject`（将对象写入存储桶）。

### 条件键

除操作外，IAM 条件键限制为仅在满足条件时才授予访问权限。条件键是可选的。

> **Note**
>
> 在基于资源的访问策略（例如存储桶策略）或基于身份的策略中，您可以指定以下内容：
>
> - 策略语句的 `Action` 元素中的一个操作或一系列操作。
> - 在策略语句的 `Effect` 元素中，您可以指定 `Allow` 来授予列出的操作，也可以指定 `Deny` 来阻止列出的操作。为进一步保持最低权限的做法，访问策略的 `Effect` 元素中的 `Deny` 语句应尽可能宽泛，而 `Allow` 语句应尽可能受限。与 `s3:*` 操作配对的 `Deny` 效果是为策略条件语句中包含的身份实现选择加入最佳实践的另一个好方法。
> - 策略语句的 `Condition` 元素中的条件键。

# 访问管理使用案例

Amazon S3 为资源拥有者提供了各种用于授予访问权限的工具。您使用的 S3 访问管理工具取决于您要共享的 S3 资源、您要授予访问权限的身份以及您想要允许或拒绝的操作。您可能希望使用一种 S3 访问管理工具或组合使用多种 S3 访问管理工具，来管理对 S3 资源的访问权限。

大多数情况下，您可以使用访问策略来管理权限。访问策略可以是基于资源的策略，此策略附加到资源（例如存储桶）或其它 Amazon S3 资源（S3 资源）。访问策略也可以是基于身份的策略，该策略附加到您账户中的 Amazon Identity and Access Management（IAM）用户、组或角色。您可能会发现存储桶策略更适合您的使用案例。有关更多信息，请参阅 Amazon S3 的存储桶策略。或者，使用 Amazon Identity and Access Management（IAM），您可以在您的 Amazon Web Services 账户中创建 IAM 用户、组和角色，并通过基于身份的策略管理它们对存储桶和对象的访问权限。有关更多信息，请参阅 Amazon S3 基于身份的策略。

为了协助您浏览这些访问管理选项，以下是常见的 Amazon S3 客户使用案例和对于每个 S3 访问管理工具的建议。

## Amazon Web Services 账户拥有者希望仅与同一账户内的用户共享存储桶

所有访问管理工具都可以满足这个基本使用案例的要求。对于此使用案例，我们建议使用以下访问管理工具：

- 存储桶策略 – 如果您要授予对一个存储桶或少量存储桶的访问权限，或者如果不同存储桶之间的存储桶访问权限相似，请使用存储桶策略。使用存储桶策略，您可以为每个存储桶管理一个策略。有关更多信息，请参阅 Amazon S3 的存储桶策略。

- 基于身份的策略 – 如果您有大量的存储桶，每个存储桶的访问权限不同，并且只有几个用户角色需要管理，则可以对用户、组或角色使用 IAM 策略。如果您要管理用户对其它 Amazon 资源以及 Amazon S3 资源的访问权限，IAM 策略也是一个不错的选择。有关更多信息，请参阅 示例 1：存储桶拥有者向其用户授予存储桶权限。
- S3 Access Grants – 您可以使用 S3 Access Grants 来授予对 S3 存储桶、前缀或对象的访问权限。S3 Access Grants 允许您大规模指定不同的对象级别权限，而存储桶策略的大小限制为 20 KB。有关更多信息，请参阅 开始使用 S3 Access Grants。
- 接入点 – 您可以使用接入点，接入点是附加到存储桶的命名网络端点。一个存储桶最多可附加 10000 个接入点，对于每个接入点，您可以强制实施不同的权限和网络控制，从而让您可以详细控制对于 S3 对象的访问权限。有关更多信息，请参阅 通过接入点管理对通用存储桶中共享数据集的访问。

## Amazon Web Services 账户拥有者想要与其它 Amazon 账户（跨账户）的用户共享存储桶或对象

要向其它 Amazon Web Services 账户授予权限，您必须使用存储桶策略或以下建议的访问管理工具之一。您不能对此使用案例使用基于身份的访问策略。有关授予跨账户存取权限的更多信息，请参阅如何提供对 Amazon S3 存储桶中对象的跨账户存取权限？

对于此使用案例，我们建议使用以下访问管理工具：

- 存储桶策略 - 使用存储桶策略，您可以为每个存储桶管理一个策略。有关更多信息，请参阅 Amazon S3 的存储桶策略。
- S3 Access Grants – 您可以使用 S3 Access Grants 来授予对 S3 存储桶、前缀或对象的跨账户权限。您可以使用 S3 Access Grants 大规模指定不同的对象级别权限，而存储桶策略的大小限制为 20 KB。有关更多信息，请参阅 开始使用 S3 Access Grants。
- 接入点 – 您可以使用接入点，接入点是附加到存储桶的命名网络端点。一个存储桶最多可附加 10000 个接入点，对于每个接入点，您可以强制实施不同的权限和网络控制，从而让您可以详细控制对于 S3 对象的访问权限。有关更多信息，请参阅 通过接入点管理对通用存储桶中共享数据集的访问。

## Amazon Web Services 账户拥有者或存储桶拥有者必须授予对象级别或前缀级别的权限，这些权限因对象或前缀而异

例如，在存储桶策略中，您可以授予对存储桶中共享特定 key name prefix 或具有特定标签的对象的访问权限。您可以授予对以键名称前缀 `logs/` 开头的对象的读取权限。但是，如果您的访问权限因对象

而异，那么使用存储桶策略授予对各个对象的权限可能不太实际，特别是由于存储桶策略的大小限制为 20 KB。

对于此使用案例，我们建议使用以下访问管理工具：

- S3 Access Grants – 您可以使用 S3 Access Grants 来管理对象级别或前缀级别的权限。与存储桶策略不同，您可以使用 S3 Access Grants 大规模指定不同的对象级别权限。存储桶策略的大小限制为 20 KB。有关更多信息，请参阅 开始使用 S3 Access Grants。
- 接入点 - 您可以使用接入点来管理对象级别或前缀级别的权限。接入点是附加到存储桶的命名网络端点。一个存储桶最多可附加 10000 个接入点，对于每个接入点，您可以强制实施不同的权限和网络控制，从而让您可以详细控制对于 S3 对象的访问权限。有关更多信息，请参阅 通过接入点管理对通用存储桶中共享数据集的访问。
- ACL – 我们建议不要使用访问控制列表（ACL），特别是因为 ACL 限制为每个对象 100 个授权。但是，如果您选择开启 ACL，请在存储桶设置中，将对象所有权 设置为存储桶拥有者优先 且 ACL 已启用。有了这个设置，用 `bucket-owner-full-control` 标准的 ACL 编写的新对象将自动归存储桶拥有者而不是对象编写者所有。然后，您可以使用对象 ACL（一个采用 XML 格式的访问策略）来向其他用户授予对于对象的访问权限。有关更多信息，请参阅 访问控制列表 (ACL) 概述。

## Amazon Web Services 账户拥有者或存储桶拥有者希望将存储桶访问权限限制为仅限特定的账户 ID

对于此使用案例，我们建议使用以下访问管理工具：

- 存储桶策略 - 使用存储桶策略，您可以为每个存储桶管理一个策略。有关更多信息，请参阅 Amazon S3 的存储桶策略。
- 接入点 – 接入点是附加到存储桶的命名网络端点。一个存储桶最多可附加 10000 个接入点，对于每个接入点，您可以强制实施不同的权限和网络控制，从而让您可以详细控制对于 S3 对象的访问权限。有关更多信息，请参阅 通过接入点管理对通用存储桶中共享数据集的访问。

## Amazon Web Services 账户拥有者或存储桶拥有者希望每个访问其数据的用户或应用程序都使用不同的端点

对于此使用案例，我们建议使用以下访问管理工具：

- 接入点 – 接入点是附加到存储桶的命名网络端点。一个存储桶最多可附加 10000 个接入点，对于每个接入点，您可以强制实施不同的权限和网络控制，从而让您可以详细控制对于 S3 对象的访问权

限。每个接入点强制实施自定义接入点策略，该策略与附加到底层存储桶的存储桶策略结合使用。有关更多信息，请参阅 通过接入点管理对通用存储桶中共享数据集的访问。

## Amazon Web Services 账户拥有者或存储桶拥有者必须管理从 S3 的虚拟私有云（VPC）端点进行的访问

Amazon S3 的虚拟私有云（VPC）端点是 VPC 内仅允许连接到 S3 的逻辑实体。对于此使用案例，我们建议使用以下访问管理工具：

- VPC 中的存储桶设置 – 您可以使用存储桶策略来控制允许谁访问您的存储桶，以及他们可以访问哪些 VPC 端点。有关更多信息，请参阅 使用存储桶策略控制从 VPC 端点的访问。
- 接入点 - 如果您选择设置接入点，则可以使用接入点策略。您可以将任何接入点配置为仅接受来自 Virtual Private Cloud（VPC）的请求，以限制专用网络的 Amazon S3 数据访问。您还可以为每个接入点配置自定义屏蔽公共访问权限设置。有关更多信息，请参阅 通过接入点管理对通用存储桶中共享数据集的访问。

## Amazon Web Services 账户拥有者或存储桶拥有者必须公开静态网站

使用 S3，您可以托管静态网站，并允许任何人查看该网站的内容（托管在 S3 存储桶中）。

对于此使用案例，我们建议使用以下访问管理工具：

- Amazon CloudFront – 该解决方案允许您面向公众托管 Amazon S3 静态网站，同时还继续屏蔽对存储桶内容的所有公共访问权限。如果要将所有四个“S3 屏蔽公共访问权限”设置保持为启用状态并托管 S3 静态网站，则可以使用 Amazon CloudFront 来源访问控制（OAC）。Amazon CloudFront 提供了设置安全静态网站所需的功能。此外，不使用此解决方案的 Amazon S3 静态网站只能支持 HTTP 端点。CloudFront 使用 Amazon S3 的持久存储，同时提供额外的安全标头，如 HTTPS。HTTPS 通过加密正常 HTTP 请求并防范常见的网络攻击来增强安全性。

  有关更多信息，请参阅《Amazon CloudFront 开发人员指南》中的安全静态网站入门。
- 让 Amazon S3 存储桶可供公开访问 – 您可以配置存储桶来用作公开访问的静态网站。

> **Warning**
>
> 我们建议不要使用这种方法。相反，我们建议您将 Amazon S3 静态网站用作 Amazon CloudFront 的一部分。有关更多信息，请参阅前一个选项或参阅安全静态网站入门。

要在没有 Amazon CloudFront 的情况下创建 Amazon S3 静态网站，首先必须关闭所有屏蔽公共访问权限设置。在为静态网站编写存储桶策略时，请确保仅允许 `s3:GetObject` 操作，而非 `ListObject` 或 `PutObject` 权限。这有助于确保用户无法查看存储桶中的所有对象或添加其自己的内容。有关更多信息，请参阅 设置访问网站的权限。

## Amazon Web Services 账户拥有者或存储桶拥有者想要公开存储桶的内容

创建新的 Amazon S3 存储桶时，屏蔽公共访问权限 设置默认处于启用状态。有关屏蔽公共访问权限的更多信息，请参阅阻止对您的 Amazon S3 存储的公有访问。

我们建议不要对存储桶允许公共访问权限。但是，如果您必须针对特定使用案例允许公共访问权限，我们建议您为此使用案例使用以下访问管理工具：

- 禁用屏蔽公共访问权限设置 - 存储桶拥有者可以允许向存储桶发送未经身份验证的请求。例如，当存储桶具有公有存储桶策略或存储桶 ACL 授予公共访问权限时，允许未经身份验证的 PUT Object 请求。所有未经身份验证的请求均由其他任意 Amazon 用户发出，甚至是由未经身份验证的匿名用户发出。此用户在 ACL 中由特定的规范用户 ID `65a011a29cdf8ec533ec3d1ccaae921c` 表示。如果将对象上传到 `WRITE` 或 `FULL_CONTROL`，这会专门向“所有用户”组或匿名用户授予访问权限。有关公有存储桶策略和公有访问控制列表（ACL）的更多信息，请参阅 “公有”的含义。

## Amazon Web Services 账户拥有者或存储桶拥有者已超过访问策略大小限制

存储桶策略和基于身份的策略都有 20 KB 的大小限制。如果您的访问权限要求很复杂，则可能会超过此大小限制。

对于此使用案例，我们建议使用以下访问管理工具：

- 接入点 – 如果接入点适用于您的使用案例，请使用接入点。对于接入点，每个存储桶都有多个命名网络端点，每个端点都有自己的接入点策略，该策略与底层存储桶策略结合使用。但是，接入点只能对于对象执行操作，而不能对存储桶执行操作，并且不支持跨区域复制。有关更多信息，请参阅 通过接入点管理对通用存储桶中共享数据集的访问。
- S3 Access Grants – 使用 S3 Access Grants，这支持大量授权来授予对存储桶、前缀或对象的访问权限。有关更多信息，请参阅 开始使用 S3 Access Grants。

## Amazon Web Services 账户拥有者或管理员角色想要直接向公司目录中的用户或组授予存储桶、前缀或对象访问权限

您可以将公司目录添加到 Amazon IAM Identity Center，而不必通过 Amazon Identity and Access Management（IAM）管理用户、组和角色。有关更多信息，请参阅 What is IAM Identity Center?

将公司目录添加到 Amazon IAM Identity Center 后，我们建议您使用以下访问管理工具，向公司目录身份授予对 S3 资源的访问权限：

- S3 Access Grants – 使用 S3 Access Grants，这支持向公司目录中的用户或角色授予访问权限。有关更多信息，请参阅 开始使用 S3 Access Grants。

## Amazon Web Services 账户拥有者或存储桶拥有者想要向 Amazon CloudFront 服务授予访问权限，以便将 CloudFront 日志写入 S3 存储桶

对于此使用案例，我们建议使用以下访问管理工具：

- 存储桶 ACL – 存储桶 ACL 的唯一建议使用案例是向某些 Amazon Web Services 服务（如 Amazon CloudFront `awslogsdelivery` 账户）授予权限。当您创建或更新分配并开启 CloudFront 日志记录时，CloudFront 会更新存储桶（ACL）来向 `awslogsdelivery` 账户授予 `FULL_CONTROL` 权限，从而将日志写入您的存储桶。有关更多信息，请参阅 Amazon CloudFront Developer Guide（Amazon CloudFront 开发人员指南）中的 Permissions required to configure standard logging and to access your log files（配置标准日志和访问日志文件所需的权限）。如果存储日志的存储桶对于 S3 对象所有权使用强制存储桶拥有者设置来关闭 ACL，则 CloudFront 无法将日志写入存储桶。有关更多信息，请参阅 为您的存储桶控制对象所有权和禁用 ACL。。

## 作为存储桶拥有者，您希望对其他用户添加到存储桶中的对象保持完全控制权

您可以使用存储桶策略、接入点或 S3 Access Grants，来向其它账户授予将对象上传到您的存储桶的访问权限。如果您已授予对存储桶的跨账户存取权限，则可以确保上传到存储桶的任何对象均保持在您的完全控制之下。

对于此使用案例，我们建议使用以下访问管理工具：

- 对象所有权 - 将存储桶级别的设置对象所有权 保留为默认的强制存储桶拥有者 设置。

# 访问管理故障排除

以下资源有助于您排查 S3 访问管理方面的任何问题：

排查拒绝访问（403 禁止）错误

如果您遇到拒绝访问问题，请检查账户级别和存储桶级别的设置。此外，请检查您用于授予访问权限的访问管理功能，来确保策略、设置或配置正确无误。有关 Amazon S3 中拒绝访问（403 禁止）错误的常见原因的更多信息，请参阅排查 Amazon S3 中的拒绝访问（403 Forbidden）错误。

适用于 S3 的 IAM Access Analyzer

如果您不想公开您的任何资源，或者您想限制对资源的公共访问权限，则可以使用适用于 S3 的 IAM Access Analyzer。在 Amazon S3 控制台上，使用适用于 S3 的 IAM Access Analyzer 来查看具有存储桶访问控制列表（ACL）、存储桶策略或授予公共或共享访问权限的接入点策略的所有存储桶。如果存在已配置为允许互联网上的任何人或其他 Amazon Web Services 账户（包括组织外部的 Amazon Web Services 账户）访问的存储桶，适用于 S3 的 IAM Access Analyzer 会向您发出提醒。您会收到每个公共存储桶或共享存储桶的结果，其中报告了公共或共享访问的来源和级别。

在适用于 S3 的 IAM Access Analyzer 中，只需一个操作，即可屏蔽对存储桶的所有公共访问权限。我们建议您屏蔽所有对存储桶的公共访问权限，除非您需要公共访问权限才能支持特定使用案例。在屏蔽所有公共访问权限之前，确保您的应用程序在没有公共访问权限的情况下可以继续正常工作。有关更多信息，请参阅 阻止对您的 Amazon S3 存储的公有访问。

您还可以查看存储桶级别的权限设置，来配置详细的访问级别。对于需要公共或共享访问的特定和经验证的使用案例，您可以通过对存储桶的结果进行归档来确认和记录存储桶保持公开或共享的意图。您可以随时重新访问和修改这些存储桶配置。您还可以将结果下载为 CSV 格式的报告以供审计使用。

Amazon S3 控制台上提供适用于 S3 的 IAM Access Analyzer，无需额外费用。适用于 S3 的 IAM Access Analyzer 由 Amazon Identity and Access Management（IAM）IAM Access Analyzer 提供支持。要在 Amazon S3 控制台上使用适用于 S3 的 IAM Access Analyzer，您必须访问 IAM 控制台，然后在 IAM Access Analyzer 中为每个单独区域创建账户级别分析器。

有关适用于 S3 的 IAM Access Analyzer 的更多信息，请参阅使用适用于 S3 的 IAM Access Analyzer 查看存储桶访问权限。

日志记录和监控

监控是维护 Amazon S3 解决方案的可靠性、可用性和性能的重要组成部分，以便您可以更轻松地调试访问故障。日志记录有助于您深入了解用户收到的任何错误，以及何时发出了什么样的请求。Amazon 提供了几种用于监控 Amazon S3 资源的工具，如下所示：

- Amazon CloudTrail
- Amazon S3 访问日志
- Amazon Trusted Advisor
- Amazon CloudWatch

有关更多信息，请参阅 Amazon S3 中的日志记录和监控。

# Amazon S3 的身份和访问管理

Amazon Identity and Access Management（IAM）是一项 Amazon Web Services 服务，可以帮助管理员安全地控制对 Amazon 资源的访问。IAM 管理员控制谁可以通过身份验证（登录）和授权（具有权限）使用 Amazon S3 资源。IAM 是一项无需额外费用即可使用的 Amazon Web Services 服务。

有关按 S3 资源类型对 S3 API 操作的权限的更多信息，请参阅 Amazon S3 API 操作所需的权限。

> **Note**
>
> 有关将 Amazon S3 Express One Zone 存储类与目录存储桶配合使用的更多信息，请参阅 S3 Express One Zone 和使用目录存储桶。

主题


- 受众
- 使用身份进行身份验证
- 使用策略管理访问
- Amazon S3 如何与 IAM 配合使用
- Amazon S3 如何对请求授权
- Amazon S3 API 操作所需的权限
- Amazon S3 中的策略和权限
- Amazon S3 的存储桶策略
- Amazon S3 基于身份的策略
- 演练：使用策略管理针对 Amazon S3 资源的访问权限
- 将服务相关角色用于 Amazon S3 Storage Lens 存储统计管理工具

- Amazon S3 身份和访问问题排查
- Amazon 适用于 Amazon S3 的托管策略

## 受众

如何使用 Amazon Identity and Access Management（IAM）因您在 Amazon S3 中执行的操作而异。

服务用户：如果您使用 Amazon S3 服务来完成任务，管理员会为您提供所需的凭证和权限。随着您使用更多 Amazon S3 功能来完成任务，您可能需要额外权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问 Amazon S3 中的功能，请参阅Amazon S3 身份和访问问题排查。

服务管理员：如果您在公司负责管理 Amazon S3 资源，您可能对 Amazon S3 具有完全访问权限。您有责任确定您的服务用户应访问哪些 Amazon S3 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要了解有关您的公司如何将 IAM 与 Amazon S3 搭配使用的更多信息，请参阅Amazon S3 如何与 IAM 配合使用。

IAM 管理员：如果您是 IAM 管理员，您可能希望了解如何编写策略以管理对 Amazon S3 的访问的详细信息。要查看您可在 IAM 中使用的 Amazon S3 基于身份的策略示例，请参阅Amazon S3 基于身份的策略。

## 使用身份进行身份验证

身份验证是您使用身份凭证登录 Amazon 的方法。您必须作为 Amazon Web Services 账户根用户、IAM 用户或通过代入 IAM 角色进行身份验证（登录到 Amazon）。

如果您以编程方式访问 Amazon，则 Amazon 将提供软件开发工具包（SDK）和命令行界面（CLI），以便使用您的凭证以加密方式签署您的请求。如果您不使用 Amazon 工具，则必须自行对请求签名。有关使用推荐的方法自行签署请求的更多信息，请参阅《IAM 用户指南》中的用于签署 API 请求的 Amazon 签名版本 4。

无论使用何种身份验证方法，您都可能需要提供其他安全信息。例如，Amazon 建议您使用多重身份验证（MFA）来提高账户的安全性。要了解更多信息，请参阅《IAM 用户指南》中的 IAM 中的 Amazon 多重身份验证。

### Amazon Web Services 账户根用户

当您创建 Amazon Web Services 账户时，最初使用的是一个对账户中所有 Amazon Web Services 服务和资源拥有完全访问权限的登录身份。此身份称为 Amazon Web Services 账户根用户，使用您创建

账户时所用的电子邮件地址和密码登录，即可获得该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅 IAM 用户指南中的需要根用户凭证的任务。

## 联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）结合使用联合身份验证和身份提供程序，以使用临时凭证来访问 Amazon Web Services 服务。

联合身份是来自企业用户目录、Web 身份提供程序、Amazon Directory Service、的用户，或任何使用通过身份源提供的凭证来访问 Amazon Web Services 服务的用户。当联合身份访问 Amazon Web Services 账户时，他们代入角色，而角色提供临时凭证。

## IAM 用户和群组

IAM 用户是 Amazon Web Services 账户内对某个人员或应用程序具有特定权限的一个身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的用例，应在需要时更新访问密钥。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅《IAM 用户指南》中的 IAM 用户的使用案例。

## IAM 角色

IAM 角色是 Amazon Web Services 账户中具有特定权限的身份。它类似于 IAM 用户，但与特定人员不关联。要在 Amazon Web Services Management Console中临时代入 IAM 角色，可以从用户切换到 IAM 角色（控制台）。您可以调用 Amazon CLI 或 Amazon API 操作或使用自定义网址以代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的代入角色的方法。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 联合用户访问：要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关用于联合身份验证的角色的信息，请参阅《IAM 用户指南》中的针对第三方身份提供商创建角色（联合身份验证）。

- 临时 IAM 用户权限：IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取：您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些 Amazon Web Services 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅 IAM 用户指南中的 IAM 中的跨账户资源访问。
- 跨服务访问：某些 Amazon Web Services 服务使用其他 Amazon Web Services 服务中的特征。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 Simple Storage Service（Amazon S3）中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话（FAS）：当您使用 IAM 用户或角色在 Amazon 中执行操作时，您将被视为主体。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用主体调用 Amazon Web Services 服务的权限，结合请求的 Amazon Web Services 服务，向下游服务发出请求。只有在服务收到需要与其他 Amazon Web Services 服务或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两项操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。
  - 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 Amazon Web Services 服务委派权限的角色。
  - 服务相关角色：服务相关角色是与 Amazon Web Services 服务 关联的一种服务角色。服务可以代入代表您执行操作的角色。服务相关角色显示在您的 Amazon Web Services 账户 中，并由该服务拥有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 Amazon EC2 上运行的应用程序：您可以使用 IAM 角色管理在 EC2 实例上运行并发出 Amazon CLI 或 Amazon API 请求的应用程序的临时凭证。这优先于在 EC2 实例中存储访问密钥。要将 Amazon 角色分配给 EC2 实例并使其对该实例的所有应用程序可用，您可以创建一个附加到实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM 角色向在 Amazon EC2 实例上运行的应用程序授予权限。

## 使用策略管理访问

您将创建策略并将其附加到 Amazon 身份或资源，以控制 Amazon 中的访问。策略是 Amazon 中的对象；在与身份或资源相关联时，策略定义它们的权限。在主体（用户、根用户或角色会话）发出请求时，Amazon 将评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略在 Amazon 中存储为 JSON 文档。有关 JSON 策略文档的结构和内容的更多信息，请参阅 IAM 用户指南中的 JSON 策略概览。

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

IAM 策略定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设您有一个允许 `iam:GetRole` 操作的策略。具有该策略的用户可以从 Amazon Web Services Management Console、Amazon CLI 或 Amazon API 获取角色信息。

### 基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户托管策略定义自定义 IAM 权限。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管策略是可以附加到 Amazon Web Services 账户 中的多个用户、组和角色的独立策略。托管式策略包括 Amazon 托管式策略和客户托管策略。要了解如何在托管策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管策略与内联策略之间进行选择。

### 基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。主体可以包括账户、用户、角色、联合用户或 Amazon Web Services 服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用来自 IAM 的 Amazon 托管式策略。

### 访问控制列表（ACL）

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，但它们不使用 JSON 策略文档格式。

Amazon S3、Amazon WAF 和 VPC 是支持 ACL 的服务示例。要了解有关 ACL 的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的访问控制列表（ACL）概览。

### 其他策略类型

Amazon 支持额外的、不太常用的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界：权限边界是一个高级特征，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅IAM 用户指南中的 IAM 实体的权限边界。
- 服务控制策略（SCP）– SCP 是 JSON 策略，指定了组织或组织单元（OU）在 Amazon Organizations 中的最大权限。Amazon Organizations 服务可以分组和集中管理您的企业拥有的多个 Amazon Web Services 账户 账户。如果在组织内启用了所有特征，则可对任意或全部账户应用服务控制策略（SCP）。SCP 限制成员账户中实体（包括每个 Amazon Web Services 账户根用户）的权限。有关组织和 SCP 的更多信息，请参阅《Amazon Organizations 用户指南》中的服务控制策略。
- 资源控制策略（RCP）– RCP 是 JSON 策略，您可以使用它们设置账户中资源的最大可用权限，而无需更新附加到您拥有的每个资源的 IAM 策略。RCP 限制了成员账户中资源的权限，并可能影响身份（包括 Amazon Web Services 账户根用户）的有效权限，无论这些身份是否属于您的组织。有关 Organizations 和 RCP（包括支持 RCP 的 Amazon Web Services 服务列表）的更多信息，请参阅《Amazon Organizations User Guide》中的 Resource control policies (RCPs)。
- 会话策略：会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅 IAM 用户指南中的会话策略。

### 多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解 Amazon 如何确定在涉及多种策略类型时是否允许请求，请参阅IAM 用户指南中的策略评估逻辑。

## Amazon S3 如何与 IAM 配合使用

在使用 IAM 管理对 Amazon S3 的访问权限之前，您应该了解哪些 IAM 功能可用于 Amazon S3。

可以与 Amazon S3 配合使用的 IAM 功能

| IAM 特征 | Amazon S3 支持 |
| --- | --- |
| 基于身份的策略 | 是 |
| 基于资源的策略 | 是 |
| 策略操作 | 是 |
| 策略资源 | 是 |
| 策略条件键（特定于服务） | 是 |
| ACL | 是 |
| ABAC（策略中的标签） | 部分 |
| 临时凭证 | 是 |
| 转发访问会话（FAS） | 是 |
| 服务角色 | 是 |
| 服务相关角色 | 部分 |

要深入了解 Amazon S3 和其它 Amazon 服务如何与大多数 IAM 功能配合使用，请参阅《IAM 用户指南》中的使用 IAM 的 Amazon 服务。

有关按 S3 资源类型对 S3 API 操作的权限的更多信息，请参阅 Amazon S3 API 操作所需的权限。

## Amazon S3 基于身份的策略

支持基于身份的策略：是

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户管理型策略定义自定义 IAM 权限。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

### Amazon S3 基于身份的策略示例

要查看 Amazon S3 基于身份的策略的示例，请参阅 Amazon S3 基于身份的策略。

## Amazon S3 内基于资源的策略

支持基于资源的策略：是

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。主体可以包括账户、用户、角色、联合用户或 Amazon Web Services 服务。

要启用跨账户访问，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当主体和资源处于不同的 Amazon Web Services 账户 中时，则信任账户中的 IAM 管理员还必须授予主体实体（用户或角色）对资源的访问权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

Amazon S3 服务支持存储桶策略、接入点策略和访问授权：

- 存储桶策略是附加到 Amazon S3 存储桶的基于资源的策略。存储桶策略定义了哪些主体可以对该存储桶执行操作。
- 接入点策略是与底层存储桶策略一起进行评估的基于资源的策略。
- Access Grants 提供了一个简化模型，用于按前缀、存储桶或对象定义对 Amazon S3 中数据的访问权限。有关 S3 Access Grants 的信息，请参阅使用 S3 Access Grants 管理访问权限。

#### 存储桶策略的主体

`Principal` 元素用于指定被允许或拒绝访问资源的用户、账户、服务或其它实体。下面是指定 `Principal` 的示例。有关更多信息，请参阅 IAM 用户指南中的主体。

#### 向 Amazon Web Services 账户授予权限

要向 Amazon Web Services 账户授予权限，则使用以下格式标识此账户。

```
"AWS":"account-ARN"
```

示例如下。

```
"Principal":{"AWS":"arn:aws:iam::AccountIDWithoutHyphens:root"}
```

```
"Principal":{"AWS":
["arn:aws:iam::AccountID1WithoutHyphens:root","arn:aws:iam::AccountID2WithoutHyphens:root"]}
```

向 IAM 用户授予权限

要向您的账户中的 IAM 用户授予权限，您必须提供 "AWS":"*user-ARN*" 名称值对。

```
"Principal":{"AWS":"arn:aws:iam::account-number-without-hyphens:user/username"}
```

有关提供分步说明的详细示例，请参阅 示例 1：存储桶拥有者向其用户授予存储桶权限 和 示例 3：存储桶拥有者授予不属于自己的对象的权限。

> **Note**
>
> 如果您在更新存储桶策略后删除了 IAM 身份，则存储桶策略将在主体元素中显示唯一标识符，而不是 ARN。这些唯一 ID 从不会重复使用，因此，您可以安全地从所有策略语句中删除具有唯一标识符的主体。有关唯一标识符的更多信息，请参阅《IAM 用户指南》中的 IAM 标识符。

授予匿名权限

> **Warning**
>
> 在授予对您的 Amazon S3 存储桶的匿名访问权限时应谨慎。如果您授予匿名访问权限，那么世界上的任何人都可以访问您的存储桶。我们强烈建议您绝对不要授予对 S3 存储桶的任何类型的匿名写入权限。

要授予每个人权限，也称为匿名访问，请将 Principal 值设置为通配符 ("*")。例如，如果您将存储桶配置为网站，您将需要使该存储桶中的所有对象都可公开访问。

```
"Principal":"*"
```

```
"Principal":{"Amazon":"*"}
```

在基于资源的策略中使用具有 Allow 效果的 "Principal": "*" 允许任何人访问您的资源，即便未登录 Amazon。

在基于资源的策略中使用具有 Allow 效果的 "Principal" : { "Amazon" : "*" } 允许任何根用户、IAM 用户、代入角色会话或联合身份用户在同一分区的任何账户中访问您的资源。

对于匿名用户，这两种方法是等效的。有关更多信息，请参阅《IAM 用户指南》中的所有主体。

您不能使用通配符匹配一部分主体名称或 ARN。

> **Important**
>
> 在 Amazon 访问控制策略中，主体“*”和 {"Amazon": "*"} 的行为相同。

限制资源权限

您还可以使用资源策略来限制对 IAM 主体原本可以使用的资源的访问权限。使用 Deny 语句来阻止访问。

如果未使用安全传输协议，则以下示例会阻止访问：

```
{"Effect": "Deny",
 "Principal": "*",
 "Action": "s3:*",
 "Resource": <bucket ARN>,
 "Condition": {
   "Boolean": { "aws:SecureTransport" : "false"}
 }
}
```

使用 "Principal": "*" 以便此限制适用于每个用户，这是本策略的最佳实践，而不是尝试使用此方法仅拒绝特定账户或主体的访问权限。

要求通过 CloudFront URL 进行访问

您可以要求用户仅使用 CloudFront URL 而不是 Amazon S3 URL 访问您的 Amazon S3 内容。为此，请创建 CloudFront 来源访问控制（OAC）。然后，更改 S3 数据的权限。在存储桶策略中，您可以将 CloudFront 设置为主体，如下所示：

```
"Principal":{"Service":"cloudfront.amazonaws.com"}
```

使用策略中的 Condition 元素，仅在请求代表包含 S3 源的 CloudFront 分配时，才允许 CloudFront 访问存储桶。

```
       "Condition": {
          "StringEquals": {
             "AWS:SourceArn":
"arn:aws:cloudfront::111122223333:distribution/CloudFront-distribution-ID"
          }
       }
```

有关需要通过 CloudFront URL 访问 S3 的更多信息，请参阅《Amazon CloudFront 开发人员指南》中的限制对 Amazon Simple Storage Service 源的访问。有关使用 Amazon CloudFront 的安全和隐私优势的更多信息，请参阅配置安全访问和限制对内容的访问。

适用于 Amazon S3 的基于资源的策略示例

- 要查看 Amazon S3 存储桶的策略示例，请参阅Amazon S3 的存储桶策略。
- 要查看接入点的策略示例，请参阅配置 IAM 策略以使用通用存储桶的接入点。

## Amazon S3 的策略操作

支持策略操作：是

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 Action 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 Amazon API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

下图显示了 S3 API 操作和所需策略操作之间不同类型的映射关系。

- 同名一对一映射。例如，要使用 PutBucketPolicy API 操作，需要执行 s3:PutBucketPolicy 策略操作。
- 具有不同名称的一对一映射。例如，要使用 ListObjectsV2 API 操作，需要执行 s3:ListBucket 策略操作。

- 一对多映射。例如，要使用 HeadObject API 操作，则需要执行 s3:GetObject。此外，当您使用 S3 对象锁定并想要获取对象的法定保留状态或保留设置时，还需要执行相应的 s3:GetObjectLegalHold 或 s3:GetObjectRetention 策略操作，然后才能使用 HeadObject API 操作。
- 多对一映射。例如，要使用 ListObjectsV2 或 HeadBucket API 操作，需要执行 s3:ListBucket 策略操作。

要查看在策略中使用的 Amazon S3 操作的列表，请参阅《Service Authorization Reference》中的 Actions defined by Amazon S3。有关 Amazon S3 API 操作的完整列表，请参阅《Amazon Simple Storage Service API Reference》中的 Amazon S3 API Actions。

有关按 S3 资源类型对 S3 API 操作的权限的更多信息，请参阅 Amazon S3 API 操作所需的权限。

Amazon S3 中的策略操作在操作前面使用以下前缀：

```
s3
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
      "s3:action1",
      "s3:action2"
         ]
```

存储桶操作

存储桶操作是在存储桶资源类型上执行的 S3 API 操作。例如：CreateBucket、ListObjectsV2 和 PutBucketPolicy。针对存储桶操作的 S3 策略操作要求存储桶策略或基于 IAM 身份的策略中的 Resource 元素必须是采用以下示例格式的 S3 存储桶类型 Amazon 资源名称 (ARN) 标识符。

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
```

以下存储桶策略向账户 *12345678901* 的用户 *Akua* 授予 s3:ListBucket 权限，来执行 ListObjectsV2 API 操作和列出 S3 存储桶中的对象。

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "Allow Akua to list objects in the bucket",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::12345678901:user/Akua"
            },
            "Action": [
            "s3:ListBucket"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
        }
    ]
}
```

通用存储桶的接入点策略中的存储桶操作

在通用存储桶的接入点策略中授予的权限仅在底层存储桶支持相同的权限时才有效。使用 S3 接入点时，必须将访问控制权从存储桶委托给接入点，或者将接入点策略中的相同权限添加到底层存储桶策略中。有关更多信息，请参阅 配置 IAM 策略以使用通用存储桶的接入点。在接入点策略中，针对存储桶操作的 S3 策略操作要求您对 Resource 元素使用以下格式的接入点 ARN。

```
"Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point"
```

以下接入点策略向账户 *12345678901* 的用户 *Akua* 授予 s3:ListBucket 权限，来通过名为 *example-access-point* 的 S3 接入点执行 ListObjectsV2 API 操作。此权限支持 *Akua* 列出存储桶中与 *example-access-point* 关联的对象。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow Akua to list objects in the bucket through access point",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::12345678901:user/Akua"
            },
            "Action": [
            "s3:ListBucket"
            ],
            "Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-
point"
        }
```

```
    ]
}
```

> **Note**
>
> 并非所有存储桶操作都受通用存储桶的接入点支持。有关更多信息，请参阅 通用存储桶的接入点与 S3 操作的兼容性。

目录存储桶的接入点策略中的存储桶操作

在目录存储桶的接入点策略中授予的权限仅在底层存储桶支持相同的权限时才有效。使用 S3 接入点时，必须将访问控制权从存储桶委托给接入点，或者将接入点策略中的相同权限添加到底层存储桶策略中。有关更多信息，请参阅 配置 IAM 策略以使用目录存储桶的接入点。在接入点策略中，针对存储桶操作的 S3 策略操作要求您对 Resource 元素使用以下格式的接入点 ARN。

```
"Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point--usw2-az1--xa-s3"
```

以下接入点策略向账户 *12345678901* 的用户 *Akua* 授予 s3:ListBucket 权限，来通过名为 *example-access-point--usw2-az1--xa-s3* 的接入点执行 ListObjectsV2 API 操作。此权限支持 *Akua* 列出存储桶中与 *example-access-point--usw2-az1--xa-s3* 关联的对象。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow Akua to list objects in the bucket through access point",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::12345678901:user/Akua"
            },
            "Action": [
            "s3:ListBucket"
            ],
            "Resource": "arn:aws:s3express:us-west-2:123456789012:accesspoint/example-access-point--usw2-az1--xa-s3"
        }
    ]
}
```

> **Note**
>
> 并非所有存储桶操作都受目录存储桶的接入点支持。有关更多信息，请参阅 目录存储桶的接入点的对象操作。

对象操作

对象操作是按对象资源类型执行的 S3 API 操作。例如：GetObject、PutObject 和 DeleteObject。用于对象操作的 S3 策略操作要求策略中的 Resource 元素为采用以下示例格式的 S3 对象 ARN。

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
```

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/*"
```

> **Note**
>
> 对象 ARN 必须在存储桶名称后面包含正斜杠，如前面的示例所示。

以下存储桶策略向账户 *12345678901* 的用户 *Akua* 授予 s3:PutObject 权限。此权限支持 *Akua* 使用 PutObject API 操作将对象上传到名为 *amzn-s3-demo-bucket* 的 S3 存储桶。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow Akua to upload objects",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::12345678901:user/Akua"
            },
            "Action": [
            "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
        }
    ]
}
```

### 接入点策略中的对象操作

使用 S3 接入点控制对对象操作的访问时，可以使用接入点策略。当您使用接入点策略时，用于对象操作的 S3 策略操作要求您对 Resource 元素使用以下格式的接入点 ARN：arn:aws:s3:*region*:*account-id*:accesspoint/*access-point-name*/object/*resource*。对于使用接入点的对象操作，必须在 Resource 元素中整个接入点 ARN 的后面包含 /object/ 值。下面是一些示例。

```
"Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point/object/*"
```

```
"Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point/object/prefix/*"
```

以下接入点策略向账户 *12345678901* 的用户 *Akua* 授予 s3:GetObject 权限。此权限支持 *Akua* 通过名为 *example-access-point* 的接入点，对存储桶中与该接入点关联的所有对象执行 GetObject API 操作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow Akua to get objects through access point",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::12345678901:user/Akua"
            },
            "Action": [
            "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point/object/*"
        }
    ]
}
```

> **Note**
>
> 并非所有对象操作都受接入点支持。有关更多信息，请参阅 通用存储桶的接入点与 S3 操作的兼容性。

### 目录存储桶的接入点策略中的对象操作

使用目录存储桶的接入点来控制对于对象操作的访问权限时，可以使用接入点策略。当您使用接入点策略时，用于对象操作的 S3 策略操作要求您对 Resource 元素使用以下格式的接入点 ARN：arn:aws:s3:*region*:*account-id*:accesspoint/*access-point-name*/object/*resource*。对于使用接入点的对象操作，必须在 Resource 元素中整个接入点 ARN 的后面包含 /object/ 值。下面是一些示例。

```
"Resource": "arn:aws:s3express:us-west-2:123456789012:accesspoint/example-access-point--usw2-az1--xa-s3/object/*"
```

```
"Resource": "arn:aws:s3express:us-west-2:123456789012:accesspoint/example-access-point--usw2-az1--xa-s3/object/prefix/*"
```

以下接入点策略向账户 *12345678901* 的用户 *Akua* 授予 s3:GetObject 权限。此权限支持 *Akua* 通过名为 *example-access-point--usw2-az1--xa-s3* 的接入点，对存储桶中与该接入点关联的所有对象执行 GetObject API 操作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow Akua to get objects through access point",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::12345678901:user/Akua"
            },
            "Action": "s3express:CreateSession","s3:GetObject"
            "Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point--usw2-az1--xa-s3/object/*"
        }
    ]
}
```

> **Note**
>
> 并非所有对象操作都受目录存储桶的接入点支持。有关更多信息，请参阅 目录存储桶的接入点的对象操作。

通用存储桶的接入点操作

接入点操作是在 accesspoint 资源类型上执行的 S3 API 操作。例如：CreateAccessPoint、DeleteAccessPoint 和 GetAccessPointPolicy。用于接入点操作的 S3 策略操作只能在基于 IAM 身份的策略中使用，不能用于存储桶策略或接入点策略。接入点操作要求 Resource 元素为采用以下示例格式的接入点 ARN。

```
"Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point"
```

以下基于 IAM 身份的策略授予 s3:GetAccessPointPolicy 权限，来对名为 *example-access-point* 的 S3 接入点执行 GetAccessPointPolicy API 操作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Grant permission to retrieve the access point policy of access
 point example-access-point",
            "Effect": "Allow",
            "Action": [
            "s3:GetAccessPointPolicy"
            ],
            "Resource": "arn:aws:s3:*:123456789012:accesspoint/example-access-point"
        }
    ]
}
```

使用接入点时，要控制对存储桶操作的访问权限，请参阅通用存储桶的接入点策略中的存储桶操作；要控制对对象操作的访问权限，请参阅接入点策略中的对象操作。有关如何配置接入点策略的更多信息，请参阅配置 IAM 策略以使用通用存储桶的接入点。

目录存储桶的接入点操作

目录存储桶的接入点操作是在 accesspoint 资源类型上执行的 S3 API 操作。例如：CreateAccessPoint、DeleteAccessPoint 和 GetAccessPointPolicy。用于接入点操作的 S3 策略操作只能在基于 IAM 身份的策略中使用，不能用于存储桶策略或接入点策略。目录存储桶的接入点操作要求 Resource 元素为采用以下示例格式的接入点 ARN。

```
"Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point--usw2-
az1--xa-s3"
```

以下基于 IAM 身份的策略授予 s3express:GetAccessPointPolicy 权限，来对名为 *example-access-point--usw2-az1--xa-s3* 的接入点执行 GetAccessPointPolicy API 操作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Grant permission to retrieve the access point policy of access
 point example-access-point--usw2-az1--xa-s3",
            "Effect": "Allow",
            "Action": [
            "s3express:CreateSession","s3express:GetAccessPointPolicy"
            ],
            "Resource": "arn:aws:s3:*:123456789012:accesspoint/example-access-point--
usw2-az1--xa-s3"
        }
    ]
}
```

以下基于 IAM 身份的策略授予为目录存储桶创建接入点的 s3express:CreateAccessPoint 权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Grant CreateAccessPoint.",
            "Principal": "*",
            "Action": "s3express:CreateSession",
            "s3express:CreateAccessPoint""Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

以下基于 IAM 身份的策略授予为目录存储桶的接入点创建接入点范围的 s3express:PutAccessPointScope 权限。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Grant PutAccessPointScope",
            "Principal": "*",
            "Action": "s3express:CreateSession",
            "s3express:CreateAccessPoint",
            "S3Express:PutAccessPointScope""Effect": "Allow",
            "Resource": "*",
        }
    ]
}
```

当使用目录存储桶的接入点来控制对存储桶操作的访问权限时，请参阅目录存储桶的接入点策略中的存储桶操作；要控制对对象操作的访问权限，请参阅目录存储桶的接入点策略中的对象操作。有关如何配置目录存储桶的接入点策略的更多信息，请参阅配置 IAM 策略以使用目录存储桶的接入点。

对象 Lambda 接入点操作

借助 Amazon S3 对象 Lambda，您可以将自己的代码添加到 Amazon S3 GET、LIST 和 HEAD 请求中，以便在数据返回到应用程序时修改和处理数据。您可以通过 Object Lambda 接入点发出请求，与通过其它接入点发出请求的工作方式相同。有关更多信息，请参阅 使用 S3 对象 Lambda 转换对象。

有关如何为对象 Lambda 接入点操作配置策略的更多信息，请参阅为对象 Lambda 接入点配置 IAM 策略。

多区域接入点操作

多区域接入点提供了一个全局端点，应用程序可以使用该端点来满足来自位于多个 Amazon Web Services 区域中的 S3 存储桶的请求。您可以使用多区域接入点通过单个区域中使用的相同架构来构建多区域应用程序，然后在世界任何地方运行这些应用程序。有关更多信息，请参阅 使用多区域接入点管理多区域流量。

有关如何为多区域接入点操作配置策略的更多信息，请参阅多区域接入点策略示例。

批处理作业操作

（批量操作）任务操作是在任务资源类型上运行的 S3 API 操作。例如，DescribeJob 和 CreateJob。用于作业操作的 S3 策略操作只能在基于 IAM 身份的策略中使用，不能用于存储桶策略。此外，作业操作要求基于 IAM 身份的策略中的 Resource 元素必须是采用以下示例格式的 job ARN。

```
"Resource": "arn:aws:s3:*:123456789012:job/*"
```

以下基于 IAM 身份的策略授予 s3:DescribeJob 权限，来对名为 *example-job* 的 S3 批量操作任务执行 DescribeJob API 操作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow describing the Batch operation job example-job",
            "Effect": "Allow",
            "Action": [
            "s3:DescribeJob"
            ],
            "Resource": "arn:aws:s3:*:123456789012:job/example-job"
        }
    ]
}
```

S3 Storage Lens 存储分析功能配置操作

有关如何配置 S3 Storage Lens 存储分析功能配置操作的更多信息，请参阅设置 Amazon S3 Storage Lens 存储统计管理工具权限。

账户操作

账户操作是在账户级别执行的 S3 API 操作。例如，GetPublicAccessBlock（用于账户）。账户不是 Amazon S3 定义的资源类型。用于账户操作的 S3 策略操作只能在基于 IAM 身份的策略中使用，不能用于存储桶策略。此外，账户操作要求基于 IAM 身份的策略中的 Resource 元素必须是 "*"。

以下基于 IAM 身份的策略授予 s3:GetAccountPublicAccessBlock 权限，来执行账户级 GetPublicAccessBlock API 操作和检索账户级公共访问权限屏蔽设置。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"Allow retrieving the account-level Public Access Block settings",
         "Effect":"Allow",
         "Action":[
            "s3:GetAccountPublicAccessBlock"
```

```
         ],
         "Resource":[
            "*"
         ]
      }
   ]
}
```

Amazon S3 的策略示例

- 要查看 Amazon S3 基于身份的策略的示例，请参阅 Amazon S3 基于身份的策略。
- 要查看 Amazon S3 基于资源的策略示例，请参阅Amazon S3 的存储桶策略和配置 IAM 策略以使用通用存储桶的接入点。

## Amazon S3 的策略资源

支持策略资源：是

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

`Resource` JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 `Resource` 或 `NotResource` 元素。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符（*）指示语句应用于所有资源。

```
"Resource": "*"
```

某些 Amazon S3 API 操作支持多个资源。例如，`s3:GetObject` 访问 *`example-resource-1`* 和 *`example-resource-2`*，因此主体必须具有访问这两项资源的权限。要在单个语句中指定多个资源，请使用逗号分隔 ARN，如下面的示例所示。

```
"Resource": [
      "example-resource-1",
      "example-resource-2"
```

Amazon S3 中的资源包括存储桶、对象、接入点或任务。在策略中，使用存储桶、对象、接入点或任务的 Amazon 资源名称（ARN）来识别资源。

有关 Amazon S3 资源类型及其 ARN 的列表，请参阅《Service Authorization Reference》中的 Resources defined by Amazon S3。要了解您可以使用哪些操作指定每个资源的 ARN，请参阅 Actions defined by Amazon S3。

有关按 S3 资源类型对 S3 API 操作的权限的更多信息，请参阅 Amazon S3 API 操作所需的权限。

资源 ARN 中的通配符

可以将通配符用作资源 ARN 的一部分。可以在任何 ARN 分段（用冒号分隔的部分）中使用通配符（* 和 ?）。星号 (*) 表示 0 个或多个字符的任意组合，问号 (?) 表示任何单个字符。您可以在每个分段中使用多个 * 或 ? 字符。但是，通配符不能跨分段。

- 以下 ARN 在此 ARN 的 `relative-ID` 部分中使用 * 通配符，来标识 *amzn-s3-demo-bucket* 存储桶中的所有对象。

```
arn:aws:s3:::amzn-s3-demo-bucket/*
```

- 以下 ARN 使用 * 来表示所有 S3 存储桶和对象。

```
arn:aws:s3:::*
```

- 以下 ARN 在 `relative-ID` 部分中同时使用通配符 * 和 ?。此 ARN 标识存储桶（例如 *amzn-s3-demo-example1bucket*、*amzn-s3-demo-example2bucket*、*amzn-s3-demo-example3bucket* 等）中的所有对象。

```
arn:aws:s3:::amzn-s3-demo-example?bucket/*
```

资源 ARN 的策略变量

您可以在 Amazon S3 ARN 中使用策略变量。在策略评估时，这些预定义变量会被它们的相应值替换。假设您将存储桶组织成一个文件夹集合，每个用户拥有一个文件夹。文件夹名称与用户名相同。要为他们的文件夹授予用户权限，您可以在资源 ARN 中指定策略变量：

```
arn:aws:s3:::bucket_name/developers/${aws:username}/
```

在运行时，如果评估策略，资源 ARN 中的 `${aws:username}` 变量将替换为发出请求的人员的用户名。

Amazon S3 的策略示例

- 要查看 Amazon S3 基于身份的策略的示例，请参阅 Amazon S3 基于身份的策略。
- 要查看 Amazon S3 基于资源的策略示例，请参阅Amazon S3 的存储桶策略和配置 IAM 策略以使用通用存储桶的接入点。

## Amazon S3 的策略条件键

支持特定于服务的策略条件键：是

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 Condition 元素（或 Condition 块）中，可以指定语句生效的条件。Condition 元素是可选的。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 Amazon 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则 Amazon 使用逻辑 OR 运算来评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM 策略元素：变量和标签。

Amazon 支持全局条件键和特定于服务的条件键。要查看所有 Amazon 全局条件键，请参阅《IAM 用户指南》中的 Amazon 全局条件上下文键。

每个 Amazon S3 条件键均映射到可设置条件的 API 所允许的相同名称请求标头。特定于 Amazon S3 的条件键指定同名请求标头的行为。例如，条件键 s3:VersionId 用于对 s3:GetObjectVersion
权限授予条件权限，它定义您在 GET Object 请求中设置的查询参数 versionId 的行为。

要查看 Amazon S3 条件键的列表，请参阅《Service Authorization Reference》中的 Condition keys for Amazon S3。要了解您可以对哪些操作和资源使用条件键，请参阅 Actions defined by Amazon S3。

示例：将对象上传限制为具有特定存储类的对象

假设账户 A（由账户 ID *123456789012* 表示）拥有一个存储桶。账户 A 管理员想要限制 *Dave*（账户 A 中的一位用户），以便仅当对象存储在 STANDARD_IA 存储类中时，*Dave* 才能将对象上传到存

储桶。要将对象上传限制到特定的存储类，账户 A 管理员可以使用 s3:x-amz-storage-class 条件键，如以下示例存储桶策略所示。

```
{
                "Version": "2012-10-17",
                "Statement": [
                  {
                    "Sid": "statement1",
                    "Effect": "Allow",
                    "Principal": {
                      "AWS": "arn:aws:iam::123456789012:user/Dave"
                    },
                    "Action": "s3:PutObject",
                    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
                    "Condition": {
                      "StringEquals": {
                        "s3:x-amz-storage-class": [
                          "STANDARD_IA"
                        ]
                      }
                    }
                  }
                ]
            }
```

在本例中，Condition 块指定应用于指定的键值对 "s3:x-amz-acl":["public-read"] 的 StringEquals 条件。有一组预定义键可用于表达条件。此示例使用 s3:x-amz-acl 条件键。此条件要求用户在每个 PutObject 请求中包含 x-amz-acl 标头以及值 public-read。

Amazon S3 的策略示例

- 要查看 Amazon S3 基于身份的策略的示例，请参阅 Amazon S3 基于身份的策略。
- 要查看 Amazon S3 基于资源的策略示例，请参阅Amazon S3 的存储桶策略和配置 IAM 策略以使用通用存储桶的接入点。

## Amazon S3 中的 ACL

支持 ACL：是

在 Amazon S3 中，访问控制列表（ACL）控制哪些 Amazon Web Services 账户有权限访问资源。ACL 与基于资源的策略类似，但它们不使用 JSON 策略文档格式。

> **Important**
>
> Amazon S3 中的大多数现代使用案例不再需要使用 ACL。

有关如何使用 ACL 在 Amazon S3 中控制访问的信息，请参阅使用 ACL 管理访问。

## ABAC 与 Amazon S3

支持 ABAC（策略中的标签）：部分支持

基于属性的访问控制（ABAC）是一种授权策略，该策略基于属性来定义权限。在 Amazon 中，这些属性称为标签。您可以将标签附加到 IAM 实体（用户或角色）以及 Amazon 资源。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

要基于标签控制访问，您需要使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件键在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为部分。

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权定义权限。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问权限控制（ABAC）。

要查看基于身份的策略（用于根据标签来限制对 S3 分批操作的访问）的示例，请参阅使用任务标签控制批量操作的权限。

ABAC 和对象标签

在 ABAC 策略中，对象使用 `s3:` 标签而不是 `aws:` 标签。要根据对象标签控制对于对象的访问，需要在策略的 Condition 元素中使用以下标签提供标签信息：

- `s3:ExistingObjectTag/tag-key`
- `s3:RequestObjectTagKeys`
- `s3:RequestObjectTag/tag-key`

有关使用对象标签控制访问的信息，包括权限策略示例，请参阅标签和访问控制策略。

## 将临时凭证用于 Amazon S3

支持临时凭证：是

某些 Amazon Web Services 服务 在您使用临时凭证登录时无法正常工作。有关更多信息，包括 Amazon Web Services 服务 与临时凭证配合使用，请参阅 IAM 用户指南中的使用 IAM 的 Amazon Web Services 服务。

如果您不使用用户名和密码而用其他方法登录到 Amazon Web Services Management Console，可使用临时凭证。例如，当您使用贵公司的单点登录（SSO）链接访问 Amazon 时，该过程将自动创建临时凭证。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的从用户切换到 IAM 角色（控制台）。

您可以使用 Amazon CLI 或者 Amazon API 创建临时凭证。之后，您可以使用这些临时凭证访问 Amazon。Amazon 建议您动态生成临时凭证，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 中的临时安全凭证。

## Amazon S3 的转发访问会话

支持转发访问会话（FAS）：是

当您使用 IAM 用户或角色在 Amazon 中执行操作时，您将被视为主体。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用主体调用 Amazon Web Services 服务的权限，结合请求的 Amazon Web Services 服务，向下游服务发出请求。只有在服务收到需要与其他 Amazon Web Services 服务或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两项操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

- 当使用 SSE-KMS 加密对象时，Amazon S3 使用 FAS 调用 Amazon KMS 以解密该对象。有关更多信息，请参阅 使用具有 Amazon KMS 密钥的服务器端加密（SSE-KMS）。
- S3 Access Grants 还使用 FAS。在您为特定身份创建针对 S3 数据的访问授权后，被授权者会向 S3 Access Grants 申请临时凭证。S3 Access Grants 会从 Amazon STS 获取请求者的临时凭证，然后将该凭证发送给请求者。有关更多信息，请参阅 通过 S3 Access Grants 请求访问 Amazon S3 数据。

## Amazon S3 的服务角色

支持服务角色：是

服务角色是由一项服务担任、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 Amazon Web Services 服务委派权限的角色。

> **Warning**
>
> 更改服务角色的权限可能会破坏 Amazon S3 的功能。仅当 Amazon S3 提供相关指导时才编辑服务角色。

## Amazon S3 的服务相关角色

支持服务相关角色：部分支持

服务相关角色是一种与 Amazon Web Services 服务 相关的服务角色。服务可以代入代表您执行操作的角色。服务相关角色显示在您的 Amazon Web Services 账户 中，并由该服务拥有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

Amazon S3 支持针对 Amazon S3 Storage Lens 存储统计管理工具的服务相关角色。有关创建或管理 Amazon S3 服务相关角色的详细信息，请参阅将服务相关角色用于 Amazon S3 Storage Lens 存储统计管理工具。

作为主体的 Amazon S3 服务

| 策略中的服务名称 | S3 功能 | 更多信息 |
| --- | --- | --- |
| `s3.amazonaws.com` | S3 复制 | 设置实时复制概述 |
| `s3.amazonaws.com` | S3 事件通知 | Amazon S3 事件通知 |
| `s3.amazonaws.com` | S3 清单 | 使用 S3 清单对数据进行编目和分析 |
| `access-grants.s3.amazonaws.com` | S3 访问权限管控 | 注册位置 |
| `batchoperations.s3.amazonaws.com` | S3 批量操作 | 授予批处理操作的权限 |

| 策略中的服务名称 | S3 功能 | 更多信息 |
| --- | --- | --- |
| `logging.s3.amazonaws.com` | S3 服务器访问日志记录 | 启用 Amazon S3 服务器访问日志记录 |
| `storage-lens.s3.amazonaws.com` | S3 Storage Lens 存储统计管理工具 | 使用数据导出查看 Amazon S3 Storage Lens 存储统计管理工具指标 |

# Amazon S3 如何对请求授权

当 Amazon S3 收到请求（例如，存储桶或对象操作）时，它首先验证请求者是否拥有必要的权限。Amazon S3 对所有相关访问策略、用户策略和基于资源的策略（存储桶策略、存储桶访问控制列表（ACL）、对象 ACL）进行评估，以决定是否对该请求进行授权。

> **Note**
>
> 如果 Amazon S3 权限检查未能找到有效的权限，将返回拒绝访问（403 禁止）错误。有关更多信息，请参阅排查 Amazon S3 中的拒绝访问（403 Forbidden）错误。

为了确定请求者是否拥有执行特定操作的权限，Amazon S3 会在收到请求时按顺序执行以下操作：

1. 在运行时将所有相关访问策略（用户策略、存储桶策略、ACL）转换为一组策略以进行评估。
2. 通过以下步骤评估生成的策略集。在每个步骤中，Amazon S3 都会基于特定上下文机构来评估上下文中的策略子集。
   a. 用户上下文 – 在用户上下文中，用户所属的父账户是上下文机构。

      Amazon S3 对父账户拥有的策略子集进行评估。该子集包括父账户附加到该用户的用户策略。如果父账户也拥有请求中的资源（存储桶或对象），则 Amazon S3 还会同时评估相应资源策略（存储桶策略、存储桶 ACL 和对象 ACL）。

      用户必须从父账户获得执行该操作的权限。

      只有在 Amazon Web Services 账户中的用户发出请求的情况下，此步骤才适用。如果请求是使用 Amazon Web Services 账户 的根用户凭证发出的，则 Amazon S3 跳过此步骤。

   b. 存储桶上下文 – 在存储桶上下文中，Amazon S3 评估拥有该存储桶的 Amazon Web Services 账户 所拥有的策略。

      如果请求是针对存储桶操作发出的，则请求者必须拥有来自存储桶拥有者的权限。如果请求是针对对象发出的，则 Amazon S3 会评估由存储桶拥有者拥有的所有策略，以检查存储桶拥有者是否未显式拒绝对该对象的访问。如果设置了显式拒绝，则 Amazon S3 不对请求授权。

   c. 对象上下文 – 如果请求是针对对象发出的，则 Amazon S3 对由对象拥有者拥有的策略子集进行评估。

以下是说明 Amazon S3 如何授权请求的一些示例场景。

Example – 请求者是 IAM 主体

如果请求者是 IAM 主体，则 Amazon S3 必须确定主体所属的父 Amazon Web Services 账户是否为主体授予了所需的权限以执行该操作。此外，如果请求是要执行存储桶操作（例如，请求列出存储桶内容），则 Amazon S3 必须验证存储桶拥有者是否已为请求者授予执行该操作的权限。要对资源执行特定的操作，IAM 主体需要来自所属的父 Amazon Web Services 账户以及拥有该资源的 Amazon Web Services 账户的权限。

Example – 请求者是 IAM 主体 - 如果请求针对的是存储桶拥有者未拥有的对象的操作。

如果请求是要针对存储桶拥有者未拥有的对象执行某一操作，则除了确保请求者拥有来自对象拥有者的权限外，Amazon S3 还必须检查存储桶策略，以确保存储桶拥有者未对该对象设置显式拒绝。存储桶拥有者（支付账单者）可以显式拒绝对存储桶中的对象的访问，而不论谁拥有该对象。存储桶拥有者还可以删除存储桶中的任何对象。

默认情况下，当另一个 Amazon Web Services 账户将对象上传到您的 S3 通用存储桶时，该账户（对象写入者）拥有该对象，拥有此对象的访问权限，并可以通过访问控制列表（ACL）授予其他用户访问该对象的权限。您可以使用对象所有权来更改此默认行为，以便禁用 ACL，并且作为存储桶拥有者，您可以自动拥有通用存储桶中的每个对象。因此，数据的访问控制基于策略，例如 IAM 用户策略、S3 存储桶策略、虚拟私有云（VPC）端点策略和 Amazon Organizations 服务控制策略（SCP）。有关更多信息，请参阅 为您的存储桶控制对象所有权和禁用 ACL。。

有关 Amazon S3 如何评估访问策略以授权或拒绝存储桶操作和对象操作请求的更多信息，请参阅以下主题：

主题

- Amazon S3 如何对存储桶操作请求进行授权
- Amazon S3 如何授权对象操作的请求

## Amazon S3 如何对存储桶操作请求进行授权

当 Amazon S3 收到存储桶操作请求时，Amazon S3 会将所有相关的权限转换为一组策略，以在运行时评估。相关权限包括基于资源的权限（例如，存储桶策略和存储桶访问控制列表）和用户策略（如果请求来自 IAM 主体）。然后，Amazon S3 将通过一系列步骤根据特定上下文（用户上下文或存储桶上下文）来评估生成的策略集：

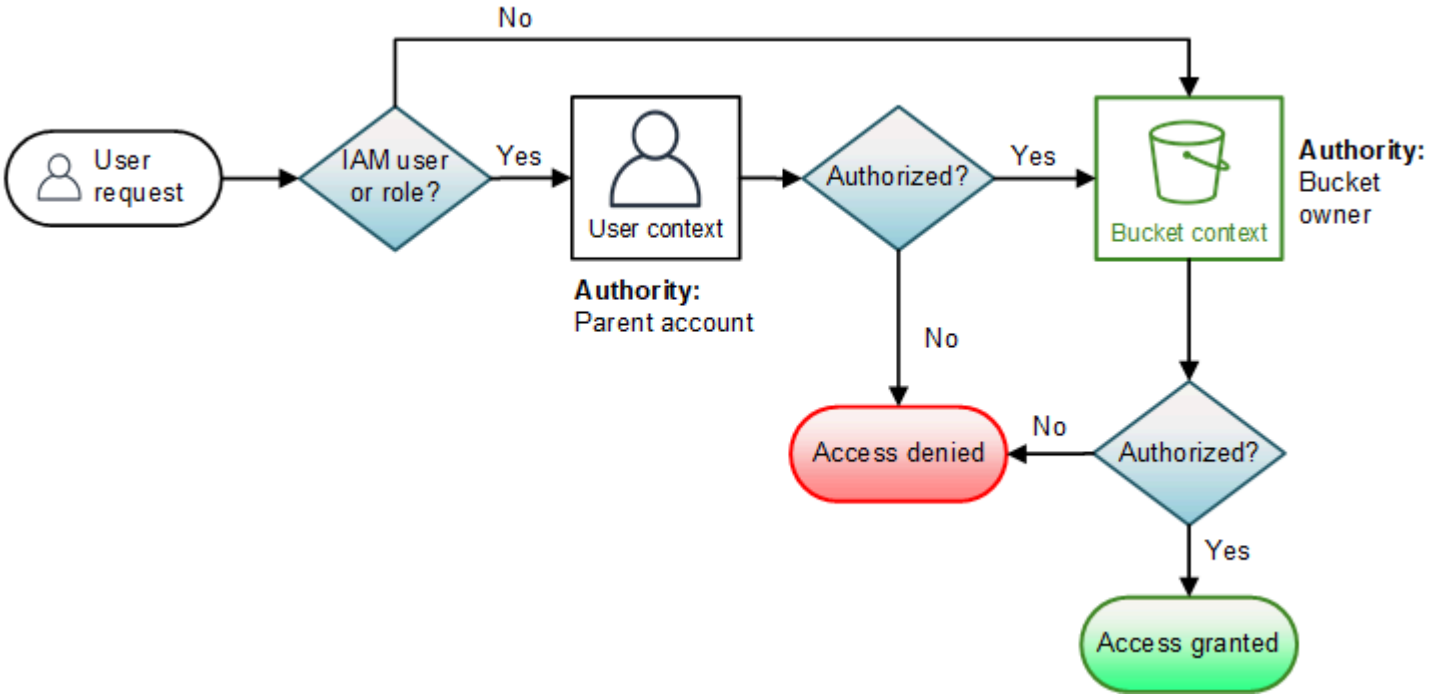
1. 用户上下文 – 如果请求者是 IAM 主体，则主体必须具有来自所属的父 Amazon Web Services 账户 的权限。在此步骤中，Amazon S3 将评估由父账户 (也称为上下文机构) 拥有的一个策略子集。

该策略子集包括父账户附加到主体的用户策略。如果父账户也拥有请求中的资源（在本例中为存储桶），则 Amazon S3 还会同时评估相应资源策略（存储桶策略和存储桶 ACL）。无论何时发出存储桶操作请求，服务器访问日志都会记录请求者的规范 ID。有关更多信息，请参阅 使用服务器访问日志记录来记录请求。

2. 存储桶上下文 – 请求者必须拥有来自存储桶拥有者的权限才能执行特定存储桶操作。在此步骤中，Amazon S3 对由拥有该存储桶的 Amazon Web Services 账户拥有的策略子集进行评估。

   存储桶拥有者可通过使用存储桶策略或存储桶 ACL 来授予权限。如果拥有存储桶的 Amazon Web Services 账户也是 IAM 主体的父账户，则该账户可以在用户策略中配置存储桶权限。

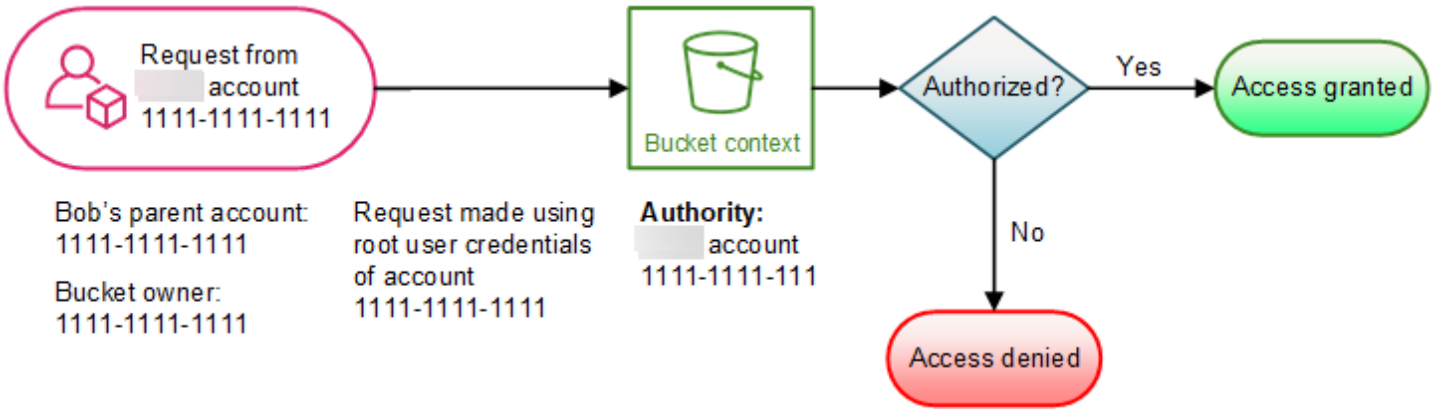
下面是基于上下文对存储桶操作进行评估的图解说明。




下面的示例演示了评估逻辑。

示例 1：由存储桶拥有者请求的存储桶操作

在此示例中，存储桶拥有者使用 Amazon Web Services 账户 的根用户凭证发送存储桶操作请求。

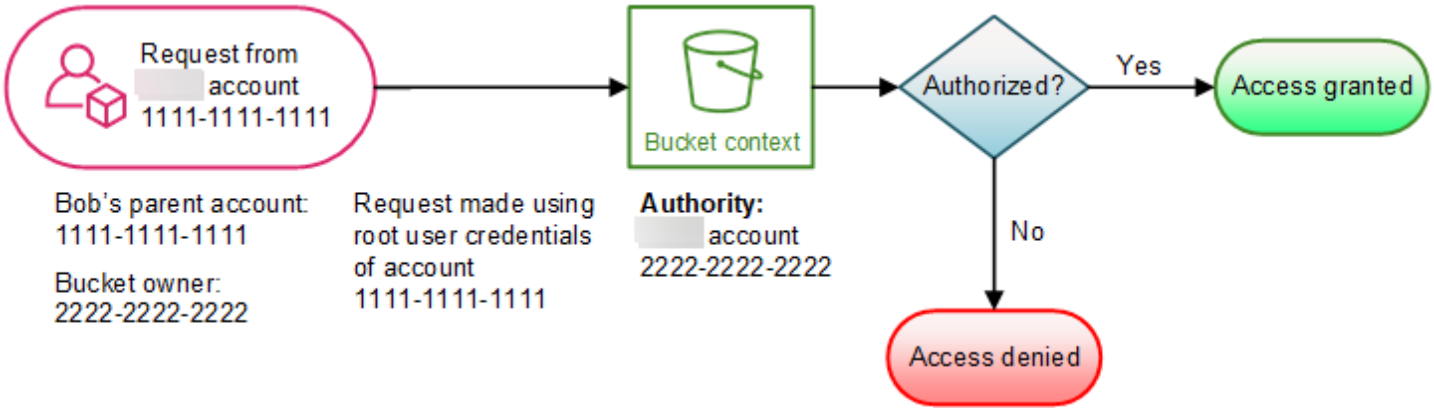



Amazon S3 通过以下方式执行上下文评估：

1. 由于请求是通过使用 Amazon Web Services 账户 的根用户凭证发出的，因此不评估用户上下文。
2. 在存储桶上下文中，Amazon S3 检查存储桶策略以确定请求者是否拥有执行该操作的权限。Amazon S3 对该请求进行授权。

示例 2：由不是存储桶拥有者的 Amazon Web Services 账户请求的存储桶操作

在此示例中，使用 Amazon Web Services 账户 1111-1111-1111 的根用户凭证发出请求，请求执行由 Amazon Web Services 账户 2222-2222-2222 拥有的存储桶操作。该请求不涉及任何 IAM 用户。

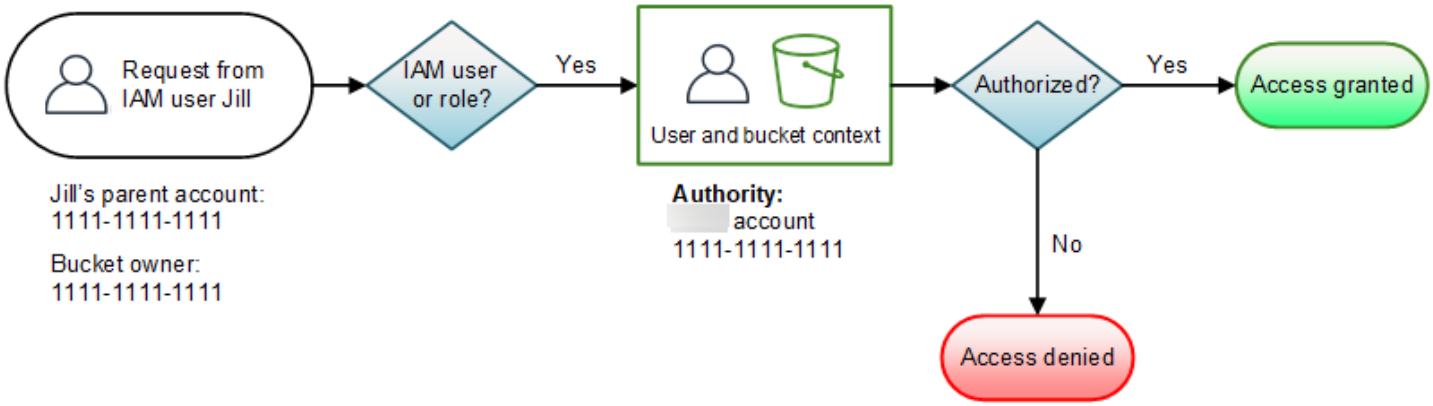



在此示例中，Amazon S3 通过以下方式评估上下文：

1. 由于请求是通过使用 Amazon Web Services 账户 的根用户凭证发出的，因此不评估用户上下文。
2. 在存储桶上下文中，Amazon S3 检查存储桶策略。如果存储桶拥有者（Amazon Web Services 账户 2222-2222-2222）尚未授权 Amazon Web Services 账户 1111-1111-1111 执行请求的操作，则 Amazon S3 拒绝该请求。否则，Amazon S3 授权该请求并执行该操作。

示例 3：IAM 主体请求的存储桶操作，其父 Amazon Web Services 账户也是存储桶拥有者

在此示例中，请求由 Amazon Web Services 账户 1111-1111-1111 中的 IAM 用户 Jill 发送，该账户同时也拥有该存储桶。



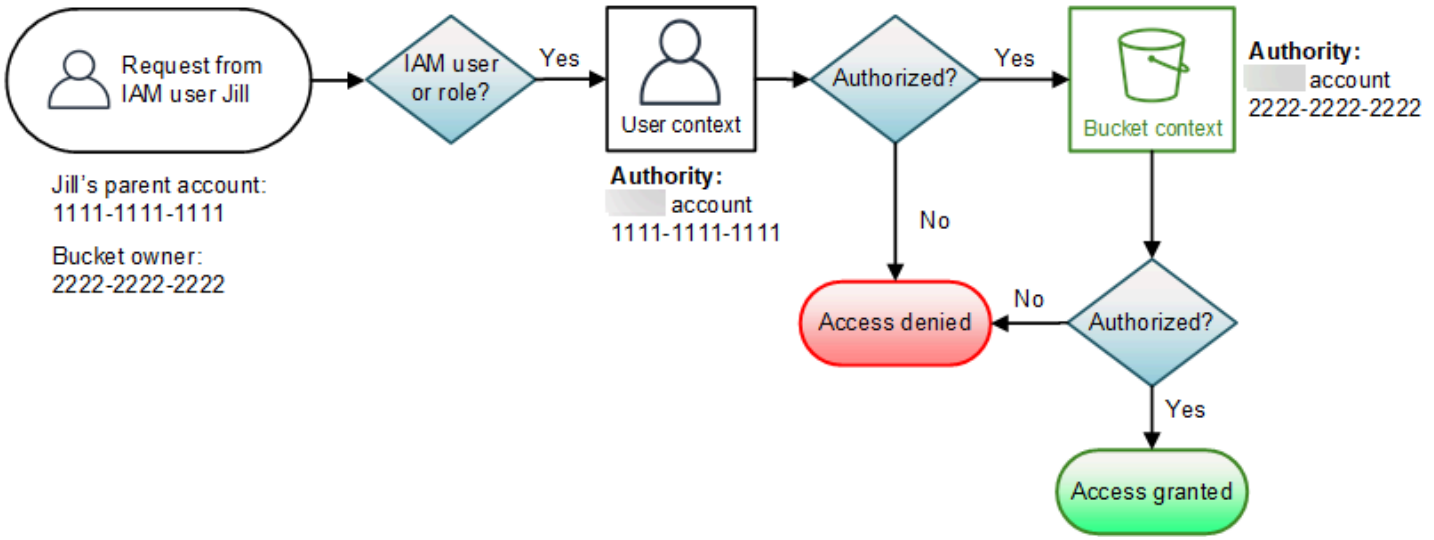

Amazon S3 执行以下上下文评估：

1. 由于请求来自 IAM 主体，因此，在用户上下文中，Amazon S3 评估属于父 Amazon Web Services 账户的所有策略以确定 Jill 是否有权执行该操作。

   在该示例中，主体所属的父 Amazon Web Services 账户 1111-1111-1111 也是存储桶拥有者。因此，除用户策略外，Amazon S3 还要评估同一上下文中的存储桶策略和存储桶 ACL，因为它们属于同一账户。
2. 由于 Amazon S3 已将存储桶策略和存储桶 ACL 作为用户上下文的一部分进行了评估，因此它不会评估存储桶上下文。

示例 4：IAM 主体请求的存储桶操作，其父 Amazon Web Services 账户不是存储桶拥有者

在此示例中，请求是由父 Amazon Web Services 账户是 1111-1111-1111 的 IAM 用户 Jill 发送的，但存储桶由另一个 Amazon Web Services 账户 2222-2222-2222 拥有。




Jill 将需要来自父 Amazon Web Services 账户和存储桶拥有者双方的权限。Amazon S3 通过以下方式评估上下文：

1. 由于请求来自 IAM 主体，因此，Amazon S3 查看账户编写的策略以验证 Jill 是否具有所需的权限，从而对用户上下文进行评估。如果 Jill 拥有权限，则 Amazon S3 会进一步评估存储桶上下文。如果 Jill 没有权限，则会拒绝该请求。
2. 在存储桶上下文中，Amazon S3 验证存储桶拥有者 2222-2222-2222 是否已授予 Jill（或她的父 Amazon Web Services 账户）执行所请求的操作的权限。如果其拥有该权限，则 Amazon S3 会授权该请求并执行该操作。否则，Amazon S3 拒绝该请求。

## Amazon S3 如何授权对象操作的请求

当 Amazon S3 接收对象操作的请求时，它会将所有相关权限转换为一组策略在运行时进行评估，这些相关权限包括：基于资源的权限（对象访问控制列表（ACL）、存储桶策略、存储桶 ACL）和 IAM 用户策略。然后它会通过一系列步骤评估生成的策略集。在每个步骤中，它会在三个特定上下文（用户上下文、存储桶上下文和对象上下文）中评估一个策略子集：

1. 用户上下文 – 如果请求者是 IAM 主体，则主体必须具有来自所属的父 Amazon Web Services 账户的权限。在此步骤中，Amazon S3 会评估由父账户 (也称为上下文机构) 拥有的一个策略子集。该策略子集包括父账户附加到主体的用户策略。如果父账户也拥有请求中的资源（存储桶或对象），则 Amazon S3 会同时评估相应资源策略（存储桶策略、存储桶 ACL 和对象 ACL）。

> **Note**
>
> 如果父 Amazon Web Services 账户拥有资源（存储桶或对象），则该账户可以使用用户策略或资源策略为其 IAM 主体授予资源权限。

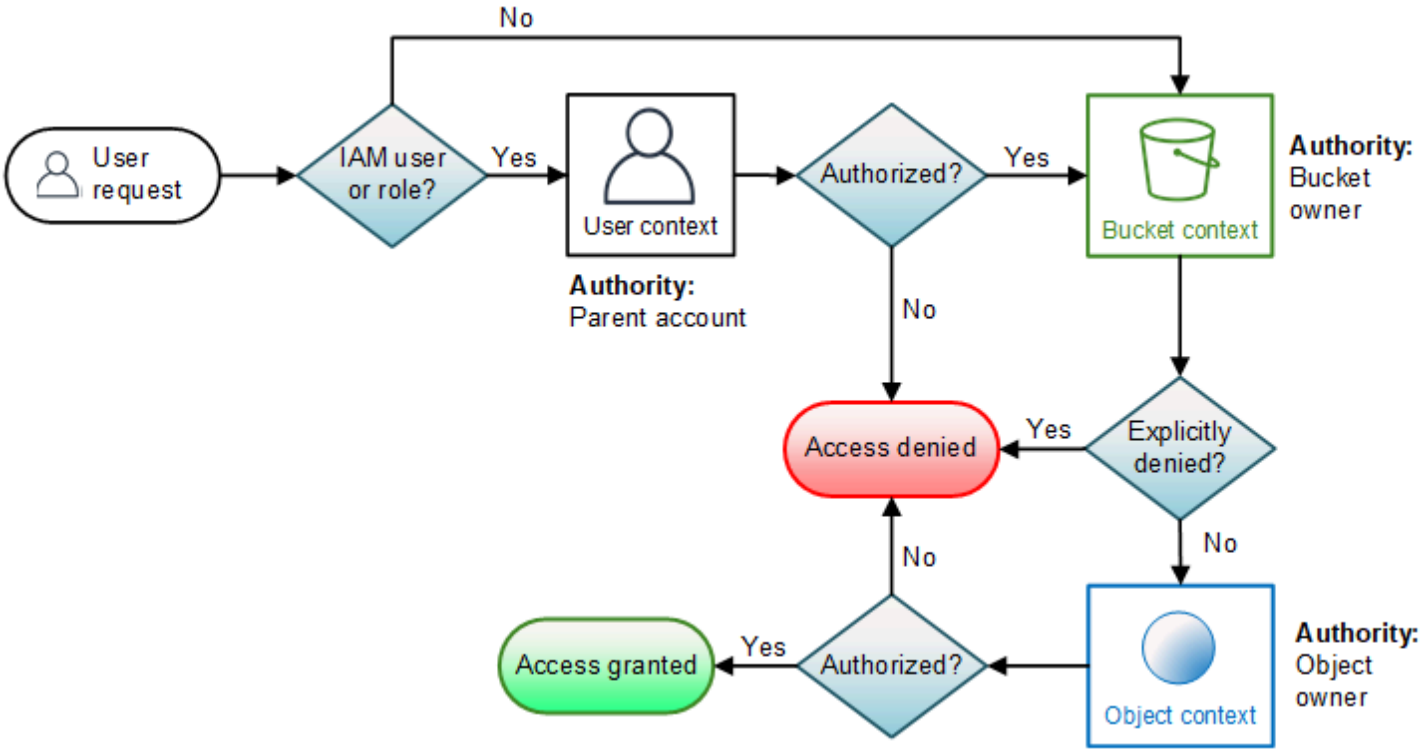
2. 存储桶上下文 – 在此上下文中，Amazon S3 评估拥有该存储桶的 Amazon Web Services 账户所拥有的策略。

   如果拥有请求中的对象的 Amazon Web Services 账户与存储桶拥有者不同，则 Amazon S3 会检查策略，查看存储桶拥有者是否已显式拒绝对该对象的访问。如果对该对象设置了显式拒绝，则 Amazon S3 不对请求授权。

3. 对象上下文 – 请求者必须拥有来自对象拥有者的权限才能执行特定对象操作。在此步骤中，Amazon S3 将评估对象 ACL。

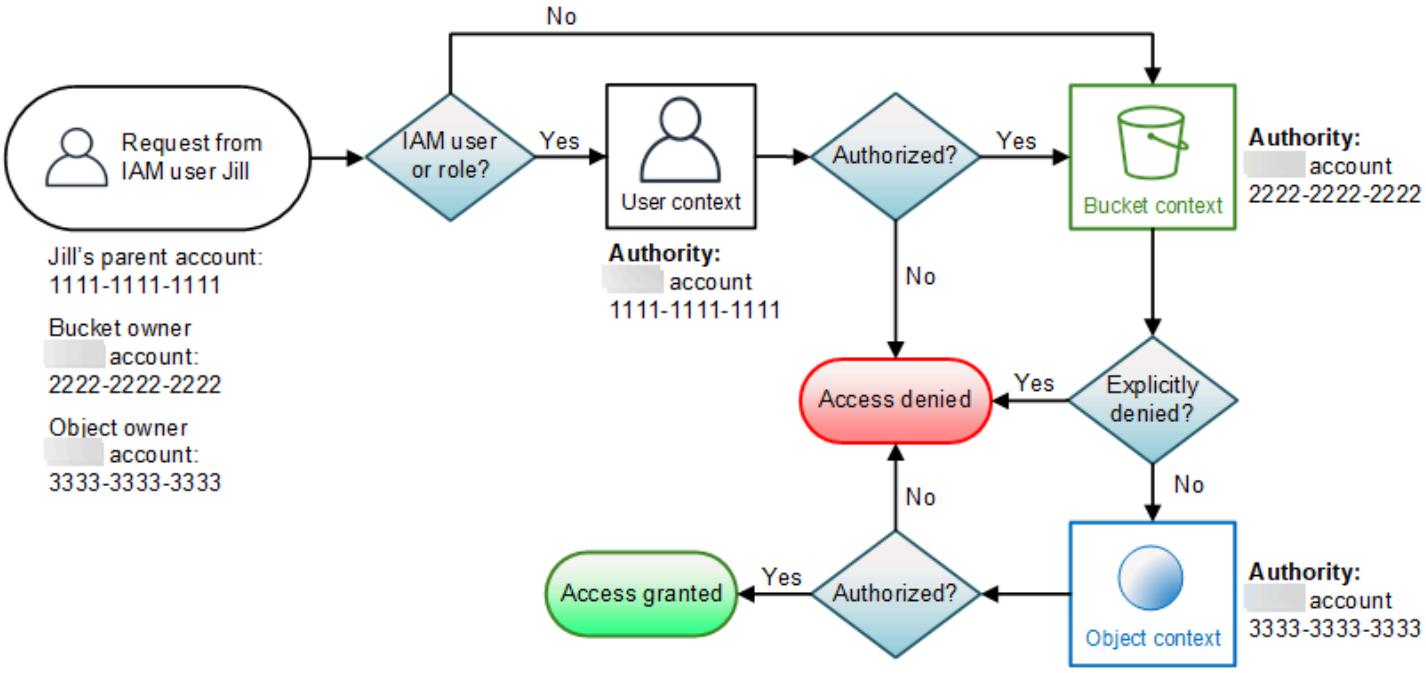
> **Note**
>
> 如果存储桶和对象拥有者相同，则可以在存储桶策略中授予对该对象的访问权限，并会在存储桶上下文中对此进行评估。如果拥有者不同，则对象拥有者必须使用对象 ACL 授予权限。如果拥有对象的 Amazon Web Services 账户 也是 IAM 主体所属的父账户，则该账户可以在用户策略中配置对象权限，将在用户上下文中对其进行评估。有关使用这些备选访问策略的更多信息，请参阅 演练：使用策略管理针对 Amazon S3 资源的访问权限。
> 如果您作为存储桶拥有者想拥有存储桶中的所有对象，并使用存储桶策略或基于 IAM 的策略来管理对这些对象的访问，则可以应用对象所有权的强制存储桶拥有者设置。使用此设置，您作为存储桶拥有者自动拥有并完全控制存储桶中的每个对象。无法编辑存储桶和对象 ACL，也不再考虑访问。有关更多信息，请参阅 为您的存储桶控制对象所有权和禁用 ACL。。

下面是基于上下文来评估对象操作的图解说明。




对象操作请求示例

在此示例中，IAM 用户 Jill（其父 Amazon Web Services 账户是 1111-1111-1111）针对 Amazon Web Services 账户 3333-3333-3333 拥有的对象发送对象操作请求（例如，`GetObject`），该对象位于由 Amazon Web Services 账户 2222-2222-2222 拥有的存储桶中。



Jill 需要从父 Amazon Web Services 账户、存储桶拥有者和对象拥有者获得权限。Amazon S3 通过以下方式评估上下文：

1. 由于请求来自 IAM 主体，因此，Amazon S3 评估用户上下文以验证父 Amazon Web Services 账户 1111-1111-1111 是否为 Jill 授予了权限以执行请求的操作。如果她拥有该权限，则 Amazon S3 评估存储桶上下文。否则，Amazon S3 拒绝该请求。
2. 在存储桶上下文中，存储桶拥有者（Amazon Web Services 账户 2222-2222-2222）是上下文机构。Amazon S3 对存储桶策略进行评估以确定存储桶拥有者是否显式拒绝了 Jill 对该对象的访问。
3. 在对象上下文中，上下文机构是 Amazon Web Services 账户 3333-3333-3333，即对象拥有者。Amazon S3 评估对象 ACL 以确定 Jill 是否拥有访问该对象的权限。如果她拥有该权限，则 Amazon S3 对该请求进行授权。

## Amazon S3 API 操作所需的权限

> **Note**
>
> 本页面介绍面向通用存储桶的 Amazon S3 策略操作。要了解有关面向目录存储桶的 Amazon S3 策略操作的更多信息，请参阅目录存储桶的操作。

要执行 S3 API 操作，必须拥有正确的权限。此页面将 S3 API 操作映射到所需的权限。要授予执行 S3 API 操作的权限，您必须撰写有效的策略（例如 S3 存储桶策略或基于 IAM 身份的策略），并在策略的 `Action` 元素中指定相应的操作。这些操作称为策略操作。并非每个 S3 API 操作都由单个权限（单个策略操作）表示，许多不同的 API 操作需要某些权限（某些策略操作）。

在撰写策略时，必须根据相应的 Amazon S3 策略操作所需的正确资源类型来指定 `Resource` 元素。此页面按资源类型对 S3 API 操作权限进行了分类。有关资源类型的更多信息，请参阅《Service Authorization Reference》中 Resource types defined by Amazon S3。有关策略中使用的 Amazon S3 策略操作、资源和条件键的完整列表，请参阅《Service Authorization Reference》中的 Actions, resources, and condition keys for Amazon S3。有关 Amazon S3 API 操作的完整列表，请参阅《Amazon Simple Storage Service API Reference》中的 Amazon S3 API Actions。

有关如何解决 S3 中的 HTTP `403 Forbidden` 错误的更多信息，请参阅排查 Amazon S3 中的拒绝访问（403 Forbidden）错误。有关与 S3 结合使用的 IAM 功能的更多信息，请参阅 Amazon S3 如何与 IAM 配合使用。有关 S3 安全性最佳实践的更多信息，请参阅 Amazon S3 的安全最佳实践。

主题

- 存储桶操作和权限
- 对象操作和权限
- 通用存储桶的接入点操作和权限
- 对象 Lambda 接入点操作和权限
- 多区域接入点操作和权限
- 批量任务操作和权限
- S3 Storage Lens 存储分析功能配置操作和权限
- S3 Storage Lens 组操作和权限
- S3 访问权限管控实例操作和权限
- S3 访问权限管控位置操作和权限
- S3 访问权限管控授权操作和权限
- 账户操作和权限

## 存储桶操作和权限

存储桶操作是在存储桶资源类型上执行的 S3 API 操作。您必须在存储桶策略或基于 IAM 身份的策略中为存储桶操作指定 S3 策略操作。

在策略中，`Resource` 元素必须为存储桶 Amazon 资源名称（ARN）。有关 `Resource` 元素格式和示例策略的更多信息，请参阅存储桶操作。

> **Note**
>
> 要在接入点策略中授予对存储桶操作的权限，请注意以下几点：
>
> - 在接入点策略中对于存储桶操作授予的权限，仅在底层存储桶支持相同的权限时才有效。使用接入点时，必须将访问控制权从存储桶委托给接入点，或者将接入点策略中的相同权限添加到底层存储桶的策略中。
> - 在授予对存储桶操作的权限的接入点策略中，`Resource` 元素必须是 `accesspoint` ARN。有关 `Resource` 元素格式和示例策略的更多信息，请参阅通用存储桶的接入点策略中的存储桶操作。有关接入点策略的更多信息，请参阅配置 IAM 策略以使用通用存储桶的接入点。
> - 并非所有存储桶操作都受接入点支持。有关更多信息，请参阅 通用存储桶的接入点与 S3 操作的兼容性。

以下是存储桶操作和所需策略操作的映射。

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| CreateBucket | （必需）s3:CreateBucket | 创建新的 s3 存储桶所必需。 |
| | （有条件需要）s3:PutBucketAcl | 如果要在发出 CreateBucket 请求时使用访问控制列表（ACL）来指定对存储桶的权限，则必需。 |
| | （有条件需要）s3:PutBucketObjectLockConfiguration 、s3:PutBucketVersioning | 如果要在创建存储桶时启用对象锁定，则必需。 |
| | （有条件需要）s3:PutBucketOwnershipControls | 如果要在创建存储桶时指定 S3 对象所有权，则必需。 |
| CreateBucketMetadataTableConfiguration | （必需）s3:CreateBucketMetadataTableConfiguration 、s3tables:CreateNamespace 、s3tables:CreateTable 、s3tables:GetTable 、s3tables:PutTablePolicy | 在通用存储桶上创建元数据表配置所必需。<br><br>要在元数据表配置中指定的表存储桶中创建元数据表，您必须具有指定的 s3tables 权限。<br><br>如果您还想将表存储桶与 Amazon 分析服务集成，以便您能够查询元数据表，则需要额外的权限。有关更多信息，请参阅集成 Amazon S3 表类数据存储服务与 Amazon 分析服务。 |
| DeleteBucket | （必需）s3:DeleteBucket | 删除 S3 存储桶所必需。 |

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| DeleteBucketAnalyticsConfiguration | （必需）s3:PutAnalyticsConfiguration | 从 S3 存储桶中删除 S3 分析配置所必需。 |
| DeleteBucketCors | （必需）s3:PutBucketCORS | 删除存储桶的跨源资源共享（CORS）配置所必需。 |
| DeleteBucketEncryption | （必需）s3:PutEncryptionConfiguration | 将 S3 存储桶的默认加密配置重置为具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）所必需。 |
| DeleteBucketIntelligentTieringConfiguration | （必需）s3:PutIntelligentTieringConfiguration | 从 S3 存储桶中删除现有 S3 Intelligent-Tiering 配置所必需。 |
| DeleteBucketInventoryConfiguration | （必需）s3:PutInventoryConfiguration | 从 S3 存储桶中删除 S3 清单配置所必需。 |
| DeleteBucketLifecycle | （必需）s3:PutLifecycleConfiguration | 删除 S3 存储桶的 S3 生命周期配置所必需。 |
| DeleteBucketMetadataTableConfiguration | （必需）s3:DeleteBucketMetadataTableConfiguration | 从通用存储桶中删除元数据表配置所必需。 |
| DeleteBucketMetricsConfiguration | （必需）s3:PutMetricsConfiguration | 从 S3 存储桶中删除 Amazon CloudWatch 请求指标的指标配置所必需。 |
| DeleteBucketOwnershipControls | （必需）s3:PutBucketOwnershipControls | 移除 S3 存储桶的“对象所有权”设置所必需。移除后，“对象所有权”设置变为 Object writer。 |
| DeleteBucketPolicy | （必需）s3:DeleteBucketPolicy | 删除 S3 存储桶的策略所必需。 |

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| DeleteBucketReplication | （必需）s3:PutReplicationConfiguration | 删除 S3 存储桶的复制配置所必需。 |
| DeleteBucketTagging | （必需）s3:PutBucketTagging | 从 S3 存储桶中删除标签所必需。 |
| DeleteBucketWebsite | （必需）s3:DeleteBucketWebsite | 移除 S3 存储桶的网站配置所必需。 |
| DeletePublicAccessBlock（存储桶级） | （必需）s3:PutBucketPublicAccessBlock | 移除 S3 存储桶的屏蔽公共访问权限配置所必需。 |
| GetBucketAccelerateConfiguration | （必需）s3:GetAccelerateConfiguration | 使用加速子资源返回存储桶的 Amazon S3 Transfer Acceleration 状态（已启用或已暂停）所必需。 |
| GetBucketAcl | （必需）s3:GetBucketAcl | 返回 S3 存储桶的访问控制列表（ACL）所必需。 |
| GetBucketAnalyticsConfiguration | （必需）s3:GetAnalyticsConfiguration | 返回 S3 存储桶中由分析配置 ID 标识的分析配置所必需。 |
| GetBucketCors | （必需）s3:GetBucketCORS | 返回 S3 存储桶的跨源资源共享（CORS）配置所必需。 |
| GetBucketEncryption | （必需）s3:GetEncryptionConfiguration | 返回 S3 存储桶的默认加密配置所必需。 |
| GetBucketIntelligentTieringConfiguration | （必需）s3:GetIntelligentTieringConfiguration | 获取 S3 存储桶的 S3 Intelligent-Tiering 配置所必需。 |

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| GetBucketInventoryConfiguration | （必需）s3:GetInventoryConfiguration | 返回存储桶中由清单配置 ID 标识的清单配置所必需。 |
| GetBucketLifecycle | （必需）s3:GetLifecycleConfiguration | 返回存储桶的 S3 生命周期配置所必需。 |
| GetBucketLocation | （必需）s3:GetBucketLocation | 返回 S3 存储桶所在的 Amazon Web Services 区域所必需。 |
| GetBucketLogging | （必需）s3:GetBucketLogging | 返回 S3 存储桶的日志记录状态和用户具有的查看和修改该状态的权限所必需。 |
| GetBucketMetadataTableConfiguration | （必需）s3:GetBucketMetadataTableConfiguration | 检索通用存储桶的元数据表配置所必需。 |
| GetBucketMetricsConfiguration | （必需）s3:GetMetricsConfiguration | 从存储桶中获取由指标配置 ID 指定的指标配置所必需。 |
| GetBucketNotificationConfiguration | （必需）s3:GetBucketNotification | 返回 S3 存储桶的通知配置所必需。 |
| GetBucketOwnershipControls | （必需）s3:GetBucketOwnershipControls | 检索 S3 存储桶的“对象所有权”设置所必需。 |
| GetBucketPolicy | （必需）s3:GetBucketPolicy | 返回 S3 存储桶的策略所必需。 |
| GetBucketPolicyStatus | （必需）s3:GetBucketPolicyStatus | 检索 S3 存储桶的策略状态（指示存储桶是否为公有）所必需。 |

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| GetBucketReplication | （必需）s3:GetReplicationConfiguration | 返回 S3 存储桶的复制配置所必需。 |
| GetBucketRequestPayment | （必需）s3:GetBucketRequestPayment | 返回 S3 存储桶的请求付款配置所必需。 |
| GetBucketVersioning | （必需）s3:GetBucketVersioning | 返回 S3 存储桶的版本控制状态所必需。 |
| GetBucketTagging | （必需）s3:GetBucketTagging | 返回与 S3 存储桶关联的标签集所必需。 |
| GetBucketWebsite | （必需）s3:GetBucketWebsite | 返回 S3 存储桶的网站配置所必需。 |
| GetObjectLockConfiguration | （必需）s3:GetBucketObjectLockConfiguration | 获取 S3 存储桶的对象锁定配置所必需。 |
| GetPublicAccessBlock（存储桶级） | （必需）s3:GetBucketPublicAccessBlock | 检索 S3 存储桶的屏蔽公共访问权限配置所必需。 |
| HeadBucket | （必需）s3:ListBucket | 确定存储桶是否存在以及您是否有权访问该存储桶所必需。 |
| ListBucketAnalyticsConfigurations | （必需）s3:GetAnalyticsConfiguration | 列出 S3 存储桶的分析配置所必需。 |
| ListBucketIntelligentTieringConfigurations | （必需）s3:GetIntelligentTieringConfiguration | 列出 S3 存储桶的 S3 Intelligent-Tiering 配置所必需。 |
| ListBucketInventoryConfigurations | （必需）s3:GetInventoryConfiguration | 返回 S3 存储桶的清单配置列表所必需。 |

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| ListBucketMetricsConfigurations | （必需）s3:GetMetricsConfiguration | 列出 S3 存储桶的指标配置所必需。 |
| ListObjects | （必需）s3:ListBucket | 列出 S3 存储桶中的部分或全部（最多 1000 个）对象所必需。 |
| | （有条件需要）s3:GetObjectAcl | 如果您要显示对象所有者信息，则必需。 |
| ListObjectsV2 | （必需）s3:ListBucket | 列出 S3 存储桶中的部分或全部（最多 1000 个）对象所必需。 |
| | （有条件需要）s3:GetObjectAcl | 如果您要显示对象所有者信息，则必需。 |
| ListObjectVersions | （必需）s3:ListBucketVersions | 获取有关 S3 存储桶中所有对象版本的元数据所必需。 |
| PutBucketAccelerateConfiguration | （必需）s3:PutAccelerateConfiguration | 设置现有存储桶的加速配置所必需。 |
| PutBucketAcl | （必需）s3:PutBucketAcl | 使用访问控制列表（ACL）设置对现有存储桶的权限所必需。 |
| PutBucketAnalyticsConfiguration | （必需）s3:PutAnalyticsConfiguration | 设置 S3 存储桶的分析配置所必需。 |
| PutBucketCors | （必需）s3:PutBucketCORS | 设置 S3 存储桶的跨源资源共享（CORS）配置所必需。 |
| PutBucketEncryption | （必需）s3:PutEncryptionConfiguration | 配置 S3 存储桶的默认加密所必需。 |

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| PutBucketIntelligentTieringConfiguration | （必需）s3:PutIntelligentTieringConfiguration | 将 S3 Intelligent-Tiering 配置放置到 S3 存储桶所必需。 |
| PutBucketInventoryConfiguration | （必需）s3:PutInventoryConfiguration | 将清单配置添加到 S3 存储桶所必需。 |
| PutBucketLifecycle | （必需）s3:PutLifecycleConfiguration | 为 S3 存储桶创建新的 S3 生命周期配置或替换现有生命周期配置所必需。 |
| PutBucketLogging | （必需）s3:PutBucketLogging | 为 S3 存储桶设置日志记录参数并指定谁可以查看和修改日志记录参数的权限所必需。 |
| PutBucketMetricsConfiguration | （必需）s3:PutMetricsConfiguration | 设置或更新 S3 存储桶的 Amazon CloudWatch 请求指标的指标配置所必需。 |
| PutBucketNotificationConfiguration | （必需）s3:PutBucketNotification | 为 S3 存储桶启用指定事件的通知所必需。 |
| PutBucketOwnershipControls | （必需）s3:PutBucketOwnershipControls | 创建或修改 S3 存储桶的“对象所有权”设置所必需。 |
| PutBucketPolicy | （必需）s3:PutBucketPolicy | 将 S3 存储桶策略应用于存储桶所必需。 |
| PutBucketReplication | （必需）s3:PutReplicationConfiguration | 为 S3 存储桶创建新的复制配置或替换现有的复制配置所必需。 |
| PutBucketRequestPayment | （必需）s3:PutBucketRequestPayment | 设置存储桶的请求付款配置所必需。 |

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| PutBucketTagging | （必需）s3:PutBucketTagging | 将一组标签添加到 S3 存储桶所必需。 |
| PutBucketVersioning | （必需）s3:PutBucketVersioning | 设置 S3 存储桶的版本控制状态所必需。 |
| PutBucketWebsite | （必需）s3:PutBucketWebsite | 将存储桶配置为网站并设置网站的配置所必需。 |
| PutObjectLockConfiguration | （必需）s3:PutBucketObjectLockConfiguration | 在 S3 存储桶上放置对象锁定配置所必需。 |
| PutPublicAccessBlock（存储桶级） | （必需）s3:PutBucketPublicAccessBlock | 创建或修改 S3 存储桶的屏蔽公共访问权限配置所必需。 |

## 对象操作和权限

对象操作是对于对象资源类型运行的 S3 API 操作。您必须在基于资源的策略（例如存储桶策略、接入点策略、多区域接入点策略、VPC 端点策略）或基于 IAM 身份的策略中为对象操作指定 S3 策略操作。

在策略中，`Resource` 元素必须是对象 ARN。有关 `Resource` 元素格式和示例策略的更多信息，请参阅对象操作。

> **Note**
>
> - Amazon KMS 策略操作（`kms:GenerateDataKey` 和 `kms:Decrypt`）仅适用于 Amazon KMS 资源类型，并且必须在基于 IAM 身份的策略和基于 Amazon KMS 资源的策略（Amazon KMS 密钥策略）中指定。您无法在基于 S3 资源的策略（例如 S3 存储桶策略）中指定 Amazon KMS 策略操作。
> - 使用接入点控制对于对象操作的访问权限时，可以使用接入点策略。要在接入点策略中授予对于对象操作的权限，请注意以下几点：

- 在授予对于对象操作的权限的接入点策略中，Resource 元素必须是通过接入点访问的对象的 ARN。有关 Resource 元素格式和示例策略的更多信息，请参阅接入点策略中的对象操作。
- 并非所有对象操作都受接入点支持。有关更多信息，请参阅 通用存储桶的接入点与 S3 操作的兼容性。

- 并非所有对象操作都受多区域接入点支持。有关更多信息，请参阅 多区域接入点与 S3 操作的兼容性。

以下是对象操作和所需策略操作的映射。

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| AbortMultipartUpload | （必需）s3:AbortMultipartUpload | 中止分段上传所必需。 |
| CompleteMultipartUpload | （必需）s3:PutObject | 完成分段上传所必需。 |
| | （有条件需要）kms:Decrypt | 如果要为 Amazon KMS 客户自主管理型密钥加密的对象完成分段上传，则必需。 |
| CopyObject | 对于源对象： | 对于源对象： |
| | （必需）s3:GetObject 或 s3:GetObjectVersion | • s3:GetObject ：如果要从源存储桶复制对象而未在请求中指定 versionId ，则必需。<br>• s3:GetObjectVersion ：如果要通过在请求中指定 versionId 来从源存储桶复制对象的特定版本，则必需。 |
| | （有条件需要）kms:Decrypt | 如果要从源存储桶复制 Amazon KMS 客户自主管理型密钥加密的对象，则必需。 |

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| | 对于目标对象： | 对于目标对象： |
| | （必需）s3:PutObject | 将复制的对象放置到目标存储桶中所必需。 |
| | （有条件需要）s3:PutObjectAcl | 如果要在发出 CopyObject 请求时将带有对象访问控制列表（ACL）的已复制对象放置到目标存储桶，则必需。 |
| | （有条件需要）s3:PutObjectTagging | 如果要在发出 CopyObject 请求时将带有对象标记的已复制对象放置到目标存储桶，则必需。 |
| | （有条件需要）kms:GenerateDataKey | 如果要使用 Amazon KMS 客户自主管理型密钥来加密复制的对象并将其放置到目标存储桶，则必需。 |
| | （有条件需要）s3:PutObjectRetention | 如果要为新对象设置对象锁定保留配置，则必需。 |
| | （有条件需要）s3:PutObjectLegalHold | 如果要对新对象实施对象锁定法定保留，则必需。 |
| CreateMultipartUpload | （必需）s3:PutObject | 创建分段上传所必需。 |
| | （有条件需要）s3:PutObjectAcl | 如果要为上传的对象设置对象访问控制列表（ACL）权限，则必需。 |
| | （有条件需要）s3:PutObjectTagging | 如果要向上传的对象添加对象标记，则必需。 |

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| | （有条件需要）kms:GenerateDataKey | 如果要在启动分段上传时使用 Amazon KMS 客户自主管理型密钥来加密对象，则必需。 |
| | （有条件需要）s3:PutObjectRetention | 如果要为上传的对象设置对象锁定保留配置，则必需。 |
| | （有条件需要）s3:PutObjectLegalHold | 如果要对上传的对象应用对象锁定法定保留，则必需。 |
| DeleteObject | （必需）s3:DeleteObject 或 s3:DeleteObjectVersion | • s3:DeleteObject ：如果要移除对象但未在请求中指定 versionId ，则必需。<br>• s3:DeleteObjectVersion ：如果要通过在请求中指定 versionId 来移除对象的特定版本，则必需。 |
| | （有条件需要）s3:BypassGovernanceRetention | 如果要删除受监管模式保护来进行对象锁定保留的对象，则必需。 |
| DeleteObjects | （必需）s3:DeleteObject 或 s3:DeleteObjectVersion | • s3:DeleteObject ：如果要移除对象但未在请求中指定 versionId ，则必需。<br>• s3:DeleteObjectVersion ：如果要通过在请求中指定 versionId 来移除对象的特定版本，则必需。 |
| | （有条件需要）s3:BypassGovernanceRetention | 如果要删除受监管模式保护来进行对象锁定保留的对象，则必需。 |

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| DeleteObjectTagging | （必需）s3:DeleteObjectTagging 或 s3:DeleteObjectVersionTagging | • s3:DeleteObjectTagging ：如果要移除对象的整个标签集但未在请求中指定 versionId ，则必需。<br>• s3:DeleteObjectVersionTagging ：如果要通过在请求中指定 versionId 来删除特定对象版本的标签，则必需。 |
| GetObject | （必需）s3:GetObject 或 s3:GetObjectVersion | • s3:GetObject ：如果要获取对象但未在请求中指定 versionId ，则必需。<br>• s3:GetObjectVersion ：如果要通过在请求中指定 versionId 来获取对象的特定版本，则必需。 |
| | （有条件需要）kms:Decrypt | 如果要获取和解密 Amazon KMS 客户自主管理型密钥加密的对象，则必需。 |
| | （有条件需要）s3:GetObjectTagging | 如果要在发出 GetObject 请求时获取对象的标签集，则必需。 |
| | （有条件需要）s3:GetObjectLegalHold | 如果要获取对象的当前对象锁定法定保留状态，则必需。 |
| | （有条件需要）s3:GetObjectRetention | 如果要检索对象的对象锁定保留设置，则必需。 |

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| GetObjectAcl | （必需）s3:GetObjectAcl 或 s3:GetObjectVersionAcl | • s3:GetObjectAcl ：如果要获取对象的访问控制列表（ACL）但未在请求中指定 versionId ，则必需。<br>• s3:GetObjectVersionAcl ：如果要通过在请求中指定 versionId 来获取对象的访问控制列表（ACL），则必需。 |
| GetObjectAttributes | （必需）s3:GetObject 或 s3:GetObjectVersion | • s3:GetObject ：如果要检索与对象相关的属性但未在请求中指定 versionId ，则必需。<br>• s3:GetObjectVersion ：如果要通过在请求中指定 versionId 来检索与特定对象版本相关的属性，则必需。 |
| | （有条件需要）kms:Decrypt | 如果要检索与 Amazon KMS 客户自主管理型密钥加密的对象相关的属性，则必需。 |
| GetObjectLegalHold | （必需）s3:GetObjectLegalHold | 获取对象的当前对象锁定法定保留状态所必需。 |
| GetObjectRetention | （必需）s3:GetObjectRetention | 检索对象的对象锁定保留设置所必需。 |

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| GetObjectTagging | （必需）s3:GetObjectTagging 或 s3:GetObjectVersionTagging | • s3:GetObjectTagging ：如果要获取对象的标签集但未在请求中指定 versionId ，则必需。<br>• s3:GetObjectVersionTagging ：如果要通过在请求中指定 versionId 来获取特定对象版本的标签，则必需。 |
| GetObjectTorrent | （必需）s3:GetObject | 返回对象的 torrent 文件所必需。 |
| HeadObject | （必需）s3:GetObject | 从对象检索元数据而不返回对象本身所必需。 |
| | （有条件需要）s3:GetObjectLegalHold | 如果要获取对象的当前对象锁定法定保留状态，则必需。 |
| | （有条件需要）s3:GetObjectRetention | 如果要检索对象的对象锁定保留设置，则必需。 |
| ListMultipartUploads | （必需）s3:ListBucketMultipartUploads | 列出存储桶中正在进行的分段上传所必需。 |
| ListParts | （必需）s3:ListMultipartUploadParts | 列出为特定分段上传已上传的分段所必需。 |
| | （有条件需要）kms:Decrypt | 如果要列出 Amazon KMS 客户自主管理型密钥加密的分段上传的各个分段，则必需。 |
| PutObject | （必需）s3:PutObject | 放置对象所必需。 |

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| | （有条件需要）s3:PutObjectAcl | 如果要在发出 PutObject 请求时放置对象访问控制列表（ACL），则必需。 |
| | （有条件需要）s3:PutObjectTagging | 如果要在发出 PutObject 请求时放置对象标记，则必需。 |
| | （有条件需要）kms:GenerateDataKey | 如果要使用 Amazon KMS 客户自主管理型密钥来加密对象，则必需。 |
| | （有条件需要）s3:PutObjectRetention | 如果要在对象上设置对象锁定保留配置，则必需。 |
| | （有条件需要）s3:PutObjectLegalHold | 如果要将对象锁定法定保留配置应用于指定的对象，则必需。 |
| PutObjectAcl | （必需）s3:PutObjectAcl 或 s3:PutObjectVersionAcl | • s3:PutObjectAcl ：如果要为新对象或现有对象设置访问控制列表（ACL）权限但未在请求中指定 versionId ，则必需。<br>• s3:PutObjectVersionAcl ：如果要通过在请求中指定 versionId 来为新对象或现有对象设置访问控制列表（ACL）权限，则必需。 |
| PutObjectLegalHold | （必需）s3:PutObjectLegalHold | 将对象锁定法定保留配置应用于对象所必需。 |
| PutObjectRetention | （必需）s3:PutObjectRetention | 将对象锁定保留配置应用于对象所必需。 |

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| | （有条件需要）s3:BypassGovernanceRetention | 如果要绕过对象锁定保留配置的监管模式，则必需。 |
| PutObjectTagging | （必需）s3:PutObjectTagging 或 s3:PutObjectVersionTagging | • s3:PutObjectTagging ：如果要为存储桶中已存在的对象设置提供的标签集但未在请求中指定 versionId ，则必需。<br>• s3:PutObjectVersionTagging ：如果要通过在请求中指定 versionId 来为存储桶中已存在的对象设置提供的标签集，则必需。 |
| RestoreObject | （必需）s3:RestoreObject | 还原归档对象的副本所必需。 |
| SelectObjectContent | （必需）s3:GetObject | 基于简单结构化查询语言（SQL）语句筛选 S3 对象的内容所必需。 |
| | （有条件需要）kms:Decrypt | 如果要筛选使用 Amazon KMS 客户自主管理型密钥加密的 S3 对象的内容，则必需。 |
| UploadPart | （必需）s3:PutObject | 在分段上传中上传某个分段所必需。 |
| | （有条件需要）kms:GenerateDataKey | 如果要放置某个上传分段并使用 Amazon KMS 客户自主管理型密钥对其进行加密，则必需。 |
| UploadPartCopy | 对于源对象： | 对于源对象： |

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| | （必需）s3:GetObject 或 s3:GetObjectVersion | • s3:GetObject ：如果要从源存储桶复制对象而未在请求中指定 versionId ，则必需。<br>• s3:GetObjectVersion ：如果要通过在请求中指定 versionId 来从源存储桶复制对象的特定版本，则必需。 |
| | （有条件需要）kms:Decrypt | 如果要从源存储桶复制 Amazon KMS 客户自主管理型密钥加密的对象，则必需。 |
| | 对于目标分段： | 对于目标分段： |
| | （必需）s3:PutObject | 将分段上传的某个分段上传到目标存储桶所必需。 |
| | （有条件需要）kms:GenerateDataKey | 如果要在将某个分段上传到目标存储桶时使用 Amazon KMS 客户自主管理型密钥加密该分段，则必需。 |

## 通用存储桶的接入点操作和权限

接入点操作是在 accesspoint 资源类型上执行的 S3 API 操作。必须在基于 IAM 身份的策略中为接入点操作指定 S3 策略操作，而不是在存储桶策略或接入点策略中指定它们。

在策略中，Resource 元素必须是 accesspoint ARN。有关 Resource 元素格式和示例策略的更多信息，请参阅通用存储桶的接入点操作。

> **Note**
>
> 如果要使用接入点来控制对存储桶或对象操作的访问权限，请注意以下几点：

- 有关使用接入点控制对存储桶操作的访问权限的信息，请参阅通用存储桶的接入点策略中的存储桶操作。
- 有关使用接入点控制对于对象操作的访问权限的信息，请参阅接入点策略中的对象操作。
- 有关如何配置接入点策略的更多信息，请参阅配置 IAM 策略以使用通用存储桶的接入点。

以下是接入点操作和所需策略操作的映射。

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| CreateAccessPoint | （必需）s3:CreateAccessPoint | 创建与 S3 存储桶关联的接入点所必需。 |
| DeleteAccessPoint | （必需）s3:DeleteAccessPoint | 删除接入点所必需。 |
| DeleteAccessPointPolicy | （必需）s3:DeleteAccessPointPolicy | 删除接入点策略所必需。 |
| GetAccessPointPolicy | （必需）s3:GetAccessPointPolicy | 检索接入点策略所必需。 |
| GetAccessPointPolicyStatus | （必需）s3:GetAccessPointPolicyStatus | 检索有关指定的接入点当前是否具有相关策略（即支持公共访问权限）的信息所必需。 |
| PutAccessPointPolicy | （必需）s3:PutAccessPointPolicy | 放置接入点策略所必需。 |

## 对象 Lambda 接入点操作和权限

对象 Lambda 接入点操作是在 objectlambdaaccesspoint 资源类型上运行的 S3 API 操作。有关如何为对象 Lambda 接入点操作配置策略的更多信息，请参阅为对象 Lambda 接入点配置 IAM 策略。

以下是对象 Lambda 接入点操作和所需策略操作的映射。

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| CreateAccessPointForObjectLambda | （必需）s3:CreateAccessPointForObjectLambda | 创建对象 Lambda 接入点所必需。 |
| DeleteAccessPointForObjectLambda | （必需）s3:DeleteAccessPointForObjectLambda | 删除指定的对象 Lambda 接入点所必需。 |
| DeleteAccessPointPolicyForObjectLambda | （必需）s3:DeleteAccessPointPolicyForObjectLambda | 删除指定的对象 Lambda 接入点上的策略所必需。 |
| GetAccessPointConfigurationForObjectLambda | （必需）s3:GetAccessPointConfigurationForObjectLambda | 检索对象 Lambda 接入点的配置所必需。 |
| GetAccessPointForObjectLambda | （必需）s3:GetAccessPointForObjectLambda | 检索有关对象 Lambda 接入点的信息所必需。 |
| GetAccessPointPolicyForObjectLambda | （必需）s3:GetAccessPointPolicyForObjectLambda | 返回与指定对象 Lambda 接入点关联的接入点策略所必需。 |
| GetAccessPointPolicyStatusForObjectLambda | （必需）s3:GetAccessPointPolicyStatusForObjectLambda | 返回特定对象 Lambda 接入点策略的策略状态所必需。 |
| PutAccessPointConfigurationForObjectLambda | （必需）s3:PutAccessPointConfigurationForObjectLambda | 设置对象 Lambda 接入点的配置所必需。 |
| PutAccessPointPolicyForObjectLambda | （必需）s3:PutAccessPointPolicyForObjectLambda | 将访问策略与指定的对象 Lambda 接入点相关联所必需。 |

## 多区域接入点操作和权限

多区域接入点操作是在 multiregionaccesspoint 资源类型上运行的 S3 API 操作。有关如何为多区域接入点操作配置策略的更多信息，请参阅多区域接入点策略示例。

以下是多区域接入点操作和所需策略操作的映射。

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| CreateMultiRegionAccessPoint | （必需）s3:CreateMultiRegionAccessPoint | 创建多区域接入点并将其与 S3 存储桶关联所必需。 |
| DeleteMultiRegionAccessPoint | （必需）s3:DeleteMultiRegionAccessPoint | 删除多区域接入点所必需。 |
| DescribeMultiRegionAccessPointOperation | （必需）s3:DescribeMultiRegionAccessPointOperation | 检索管理多区域接入点的异步请求的状态所必需。 |
| GetMultiRegionAccessPoint | （必需）s3:GetMultiRegionAccessPoint | 返回有关指定多区域接入点的配置信息所必需。 |
| GetMultiRegionAccessPointPolicy | （必需）s3:GetMultiRegionAccessPointPolicy | 返回指定多区域接入点的访问控制策略所必需。 |
| GetMultiRegionAccessPointPolicyStatus | （必需）s3:GetMultiRegionAccessPointPolicyStatus | 返回特定多区域接入点的策略状态，以了解指定的多区域接入点是否具有支持公共访问权限的访问控制策略所必需。 |
| GetMultiRegionAccessPointRoutes | （必需）s3:GetMultiRegionAccessPointRoutes | 返回多区域接入点的路由配置所必需。 |

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| PutMultiRegionAccessPointPolicy | （必需）s3:PutMultiRegionAccessPointPolicy | 更新指定多区域接入点的访问控制策略所必需。 |
| SubmitMultiRegionAccessPointRoutes | （必需）s3:SubmitMultiRegionAccessPointRoutes | 提交多区域接入点的已更新路由配置所必需。 |

## 批量任务操作和权限

（批量操作）任务操作是在 job 资源类型上运行的 S3 API 操作。必须在基于 IAM 身份的策略中为任务操作指定 S3 策略操作，而不是在存储桶策略中指定它们。

在策略中，Resource 元素必须是 job ARN。有关 Resource 元素格式和示例策略的更多信息，请参阅批处理作业操作。

以下是批量任务操作和所需策略操作的映射。

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| DeleteJobTagging | （必需）s3:DeleteJobTagging | 从现有 S3 批量操作任务中移除标签所必需。 |
| DescribeJob | （必需）s3:DescribeJob | 检索批量操作任务的配置参数和状态所必需。 |
| GetJobTagging | （必需）s3:GetJobTagging | 返回现有 S3 批量操作任务的标签集所必需。 |
| PutJobTagging | （必需）s3:PutJobTagging | 在现有 S3 批量操作任务上放置或替换标签所必需。 |
| UpdateJobPriority | （必需）s3:UpdateJobPriority | 更新现有任务的优先级所必需。 |

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| UpdateJobStatus | （必需）s3:UpdateJobStatus | 更新指定任务的状态所必需。 |

## S3 Storage Lens 存储分析功能配置操作和权限

S3 Storage Lens 存储分析功能配置操作是在 storagelensconfiguration 资源类型上运行的 S3 API 操作。有关如何配置 S3 Storage Lens 存储分析功能配置操作的更多信息，请参阅设置 Amazon S3 Storage Lens 存储统计管理工具权限。

以下是 S3 Storage Lens 存储分析功能配置操作和所需策略操作的映射。

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| DeleteStorageLensConfiguration | （必需）s3:DeleteStorageLensConfiguration | 删除 S3 Storage Lens 存储分析功能配置所必需。 |
| DeleteStorageLensConfigurationTagging | （必需）s3:DeleteStorageLensConfigurationTagging | 删除 S3 Storage Lens 存储分析功能配置标签所必需。 |
| GetStorageLensConfiguration | （必需）s3:GetStorageLensConfiguration | 获取 S3 Storage Lens 存储分析功能配置所必需。 |
| GetStorageLensConfigurationTagging | （必需）s3:GetStorageLensConfigurationTagging | 获取 S3 Storage Lens 存储分析功能配置的标签所必需。 |
| PutStorageLensConfigurationTagging | （必需）s3:PutStorageLensConfigurationTagging | 在现有 S3 Storage Lens 存储分析功能配置上放置或替换标签所必需。 |

## S3 Storage Lens 组操作和权限

S3 Storage Lens 组操作是在 `storagelensgroup` 资源类型上运行的 S3 API 操作。有关如何配置 S3 Storage Lens 组权限的更多信息，请参阅 Storage Lens 组权限。

以下是 S3 Storage Lens 组操作和所需策略操作的映射。

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| DeleteStorageLensGroup | （必需）`s3:DeleteStorageLensGroup` | 删除现有 S3 Storage Lens 组所必需。 |
| GetStorageLensGroup | （必需）`s3:GetStorageLensGroup` | 检索 S3 Storage Lens 组配置详细信息所必需。 |
| UpdateStorageLensGroup | （必需）`s3:UpdateStorageLensGroup` | 更新现有 S3 Storage Lens 组所必需。 |
| CreateStorageLensGroup | （必需）`s3:CreateStorageLensGroup` | 创建 Storage Lens 组所必需。 |
| CreateStorageLensGroup, TagResource | （必需）`s3:CreateStorageLensGroup` 、`s3:TagResource` | 使用标签新建 Storage Lens 组所必需。 |
| ListStorageLensGroups | （必需）`s3:ListStorageLensGroups` | 列出主区域中的所有 Storage Lens 组所必需。 |
| ListTagsForResource | （必需）`s3:ListTagsForResource` | 列出已添加到 Storage Lens 组的标签所必需。 |
| TagResource | （必需）`s3:TagResource` | 为现有 Storage Lens 组添加或更新 Storage Lens 组标签所必需。 |
| UntagResource | （必需）`s3:UntagResource` | 从 Storage Lens 组删除标签所必需。 |

## S3 访问权限管控实例操作和权限

S3 访问权限管控实例操作是在 accessgrantsinstance 资源类型上运行的 S3 API 操作。S3 访问权限管控实例是访问权限管控的逻辑容器。有关使用 S3 访问权限管控实例的更多信息，请参阅使用 S3 访问权限管控实例。

以下是 S3 访问权限管控实例配置操作和所需策略操作的映射。

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| AssociateAccessGrantsIdentityCenter | （必需）s3:AssociateAccessGrantsIdentityCenter | 将 Amazon IAM Identity Center 实例与 S3 访问权限管控实例关联，从而使您能够为公司身份目录中的用户和组创建访问权限管控所必需。您还必须拥有以下权限：<br><br>sso:CreateApplication 、sso:PutApplicationGrant 和 sso:PutApplicationAuthenticationMethod 。 |
| CreateAccessGrantsInstance | （必需）s3:CreateAccessGrantsInstance | 创建 S3 访问权限管控实例（accessgrantsinstance 资源）所必需，该实例是各个访问权限管控的容器。<br><br>要将 Amazon IAM Identity Center 实例与 S3 访问权限管控实例关联，您还必须拥有 sso:DescribeInstance 、sso:CreateApplication 、sso:PutApplicationGrant 和 sso:PutApplication |

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| | | AuthenticationMethod 权限。 |
| DeleteAccessGrantsInstance | （必需）s3:DeleteAccessGrantsInstance | 从您账户的 Amazon Web Services 区域中删除 S3 访问权限管控实例（accessgrantsinstance 资源）所必需。 |
| DeleteAccessGrantsInstanceResourcePolicy | （必需）s3:DeleteAccessGrantsInstanceResourcePolicy | 删除 S3 访问权限管控实例的资源策略所必需。 |
| DissociateAccessGrantsIdentityCenter | （必需）s3:DissociateAccessGrantsIdentityCenter | 取消 Amazon IAM Identity Center 实例与 S3 访问权限管控实例的关联所必需。您还必须拥有以下权限：<br><br>sso:DeleteApplication |
| GetAccessGrantsInstance | （必需）s3:GetAccessGrantsInstance | 检索您的账户中 Amazon Web Services 区域的 S3 访问权限管控实例所必需。 |
| GetAccessGrantsInstanceForPrefix | （必需）s3:GetAccessGrantsInstanceForPrefix | 检索包含特定前缀的 S3 访问权限管控实例所必需。 |
| GetAccessGrantsInstanceResourcePolicy | （必需）s3:GetAccessGrantsInstanceResourcePolicy | 返回 S3 访问权限管控实例的资源策略所必需。 |
| ListAccessGrantsInstances | （必需）s3:ListAccessGrantsInstances | 返回您账户中 S3 访问权限管控实例的列表所必需。 |

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| PutAccessGrantsInstanceResourcePolicy | （必需）s3:PutAccessGrantsInstanceResourcePolicy | 更新 S3 访问权限管控实例的资源策略所必需。 |

## S3 访问权限管控位置操作和权限

S3 访问权限管控位置操作是在 accessgrantslocation 资源类型上运行的 S3 API 操作。有关使用 S3 访问权限管控位置的更多信息，请参阅使用 S3 访问权限管控位置。

以下是 S3 访问权限管控位置配置操作和所需策略操作的映射。

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| CreateAccessGrantsLocation | （必需）s3:CreateAccessGrantsLocation | 在 S3 访问权限管控实例中注册位置（创建 accessgrantslocation 资源）所必需。您还必须具有指定 IAM 角色的以下权限：<br><br>iam:PassRole |
| DeleteAccessGrantsLocation | （必需）s3:DeleteAccessGrantsLocation | 从 S3 访问权限管控实例中移除已注册的位置所必需。 |
| GetAccessGrantsLocation | （必需）s3:GetAccessGrantsLocation | 检索在 S3 访问权限管控实例中注册的特定位置的详细信息所必需。 |
| ListAccessGrantsLocations | （必需）s3:ListAccessGrantsLocations | 返回在 S3 访问权限管控实例中注册的位置的列表所必需。 |
| UpdateAccessGrantsLocation | （必需）s3:UpdateAccessGrantsLocation | 更新 S3 访问权限管控实例中的注册位置的 IAM 角色所必需。 |

## S3 访问权限管控授权操作和权限

S3 访问权限管控授权操作是在 accessgrant 资源类型上运行的 S3 API 操作。有关使用 S3 访问权限管控处理单独授权的更多信息，请参阅在 S3 访问权限管控中处理授权。

以下是 S3 访问权限管控授权配置操作和所需策略操作的映射。

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| CreateAccessGrant | （必需）s3:CreateAccessGrant | 在 S3 访问权限管控实例中为用户或组创建单独授权（accessgrant 资源）所必需。您还必须拥有以下权限：<br><br>对于任何目录身份：sso:DescribeInstance 和 sso:DescribeApplication<br><br>对于目录用户：identitystore:DescribeUser |
| DeleteAccessGrant | （必需）s3:DeleteAccessGrant | 从 S3 访问权限管控实例中删除单独访问权限管控（accessgrant 资源）所必需。 |
| GetAccessGrant | （必需）s3:GetAccessGrant | 获取有关 S3 访问权限管控实例中的单独访问权限管控的详细信息所必需。 |
| ListAccessGrants | （必需）s3:ListAccessGrants | 返回 S3 访问权限管控实例中单独访问权限管控的列表所必需。 |
| ListCallerAccessGrants | （必需）s3:ListCallerAccessGrants | 列出通过 S3 访问权限管控授权调用方访问 Amazon S3 数据的访问权限管控所必需。 |

## 账户操作和权限

账户操作是在账户级别执行的 S3 API 操作。账户不是 Amazon S3 定义的资源类型。必须在基于 IAM 身份的策略中为账户操作指定 S3 策略操作，而不是在存储桶策略中指定它们。

在策略中，`Resource` 元素必须是 `"*"`。有关示例策略的更多信息，请参阅账户操作。

以下是账户操作和所需策略操作的映射。

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| CreateJob | （必需）`s3:CreateJob` | 创建新的 S3 批量操作任务所必需。 |
| CreateStorageLensGroup | （必需）`s3:CreateStorageLensGroup` | 创建新的 S3 Storage Lens 组并将其与指定的 Amazon Web Services 账户 ID 关联所必需。 |
| | （有条件需要）`s3:TagResource` | 如果要创建带有 Amazon 资源标签的 S3 Storage Lens 组，则必需。 |
| DeletePublicAccessBlock（账户级） | （必需）`s3:PutAccountPublicAccessBlock` | 从 Amazon Web Services 账户中移除屏蔽公共访问权限配置所必需。 |
| GetAccessPoint | （必需）`s3:GetAccessPoint` | 检索有关指定接入点的配置信息所必需。 |
| GetAccessPointPolicy（账户级） | （必需）`s3:GetAccountPublicAccessBlock` | 检索 Amazon Web Services 账户的屏蔽公共访问权限配置所必需。 |
| ListAccessPoints | （必需）`s3:ListAccessPoints` | 列出 S3 存储桶的由 Amazon Web Services 账户拥有的接入点所必需。 |
| ListAccessPointsForObjectLambda | （必需）`s3:ListAccessPointsForObjectLambda` | 列出对象 Lambda 接入点所必需。 |

| API 操作 | 策略操作 | 策略操作的描述 |
| --- | --- | --- |
| ListBuckets | （必需）s3:ListAllMyBuckets | 返回经过身份验证的请求发送人所拥有的所有存储桶的列表所必需。 |
| ListJobs | （必需）s3:ListJobs | 列出当前任务和最近结束的任务所必需。 |
| ListMultiRegionAccessPoints | （必需）s3:ListMultiRegionAccessPoints | 返回当前与指定 Amazon Web Services 账户关联的多区域接入点的列表所必需。 |
| ListStorageLensConfigurations | （必需）s3:ListStorageLensConfigurations | 获取 Amazon Web Services 账户的 S3 Storage Lens 存储分析功能配置列表所必需。 |
| ListStorageLensGroups | （必需）s3:ListStorageLensGroups | 列出指定主 Amazon Web Services 区域中的所有 S3 Storage Lens 组所必需。 |
| PutPublicAccessBlock（账户级） | （必需）s3:PutAccountPublicAccessBlock | 创建或修改 Amazon Web Services 账户的屏蔽公共访问权限配置所必需。 |
| PutStorageLensConfiguration | （必需）s3:PutStorageLensConfiguration | 放置 S3 Storage Lens 存储分析功能配置所必需。 |

## Amazon S3 中的策略和权限

本页概述 Amazon S3 中的存储桶和用户策略，并介绍 Amazon Identity and Access Management（IAM）策略的基本元素。每个列出的元素都链接到有关该元素以及如何使用它的示例的更多详细信息。

有关 Amazon S3 操作、资源和条件的完整列表，请参阅《Service Authorization Reference》中的 Actions, resources, and condition keys for Amazon S3。

有关按 S3 资源类型对 S3 API 操作的权限的更多信息，请参阅 Amazon S3 API 操作所需的权限。

就其最基本的意义而言，策略包含以下元素：

- Resource – 策略适用的 Amazon S3 存储桶、对象、接入点或任务。使用存储桶、对象、接入点或任务的 Amazon 资源名称（ARN）来识别资源。

  存储桶级操作示例：

  `"Resource": "arn:aws:s3:::bucket_name"`

  对象级操作示例：

  - `"Resource": "arn:aws:s3:::bucket_name/*"` 对应于存储桶中的所有对象。
  - `"Resource": "arn:aws:s3:::bucket_name/prefix/*"` 对应于存储桶中特定前缀下的对象。

  有关更多信息，请参阅 Amazon S3 的策略资源。

- Actions – 对于每个资源，Amazon S3 支持一组操作。您可使用操作关键字标识允许（或拒绝）的资源操作。

  例如，`s3:ListBucket` 权限可让用户使用 Amazon S3 ListObjectsV2 操作。（`s3:ListBucket` 权限是指操作名称不直接映射到操作名称的情况。）有关使用 Simple Storage Service (Amazon S3) 操作的更多信息，请参阅 Amazon S3 的策略操作。有关 Amazon S3 操作的完整列表，请参阅《Amazon Simple Storage Service API 参考》中操作部分。

- Effect – 当用户请求特定操作（可以是 `Allow` 或 `Deny`）时的效果。

  如果没有显式授予（允许）对资源的访问权限，则隐式拒绝访问。您也可显式拒绝对资源的访问。您可以执行此操作以确保用户无法访问资源，即使其他策略授予访问权限也是如此。有关更多信息，请参阅《IAM 用户指南》https://docs.amazonaws.cn/IAM/latest/UserGuide/reference_policies_elements_effect.html中的 IAM JSON 策略元素：效果。

- Principal – 支持在语句中访问操作和资源的账户或用户。在存储桶策略中，主体是作为此权限的接收者的用户、账户、服务或其他实体。有关更多信息，请参阅 存储桶策略的主体。

- Condition – 策略生效时的条件。您可以使用 Amazon 范围内的键和特定于 Amazon S3 的键来指定 Amazon S3 访问策略中的条件。有关更多信息，请参阅 使用条件键的存储桶策略示例。

下面的示例存储桶策略显示了 `Effect`、`Principal`、`Action` 和 `Resource` 元素。此策略可让账户 *123456789012* 中的用户 *Akua* 对 *amzn-s3-demo-bucket1* 存储桶具有 `s3:GetObject`、`s3:GetBucketLocation` 和 `s3:ListBucket` Amazon S3 权限。

```
{
    "Version": "2012-10-17",
    "Id": "ExamplePolicy01",
    "Statement": [
        {
            "Sid": "ExampleStatement01",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/Akua"
            },
            "Action": [
                "s3:GetObject",
                "s3:GetBucketLocation",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket1/*",
                "arn:aws:s3:::amzn-s3-demo-bucket1"
            ]
        }
    ]
}
```

有关完整的策略语言信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限和 IAM JSON 策略参考。

## 授予权限

如果某 Amazon Web Services 账户拥有一项资源，它可以将这些权限授予其他 Amazon Web Services 账户。然后这个账户就可以将这些权限或其子集委托给该账户中的用户。这称为 权限委托。但从另一账户接收权限的账户不能向其它 Amazon Web Services 账户跨账户委托权限。

## Amazon S3 存储桶和对象所有权

存储桶和对象是 Amazon S3 资源。默认情况下，只有资源所有者可以访问这些资源。资源拥有者是指创建资源的 Amazon Web Services 账户。例如：

- 用于创建存储桶和上传对象的 Amazon Web Services 账户拥有这些资源。
- 如果您使用 Amazon Identity and Access Management (IAM) 用户或角色凭证上传对象，则用户或角色所属的 Amazon Web Services 账户将拥有该对象。

- 存储桶拥有者可以向其他 Amazon Web Services 账户（或其他账户中的用户）授予上传对象的跨账户权限。在这种情况下，上传对象的 Amazon Web Services 账户拥有这些对象。存储桶拥有者对其它账户拥有的对象没有权限，以下情况除外：
  - 账单由存储桶拥有者支付。存储桶拥有者可以拒绝对任何对象的访问，或删除存储桶中的任何对象，而无论它们的拥有者是谁。
  - 存储桶拥有者可以归档任何对象或还原归档的对象，而无论它们的拥有者是谁。归档是指用于存储对象的存储类。有关更多信息，请参阅 管理对象的生命周期。

所有权和请求身份验证

存储桶的所有请求已经过身份验证或未经过身份验证。经过身份验证的请求必须包含可验证请求发送者的签名值，而未经身份验证的请求则不然。有关请求身份验证的更多信息，请参阅《Amazon S3 API 参考》中的 Making requests。

存储桶拥有者可以允许未经身份验证的请求。例如，当存储桶具有公有存储桶策略，或存储桶 ACL 特别向 `All Users` 组或匿名用户授予 `WRITE` 或 `FULL_CONTROL` 访问权限时，允许未经身份验证的 PutObject 请求。有关公有存储桶策略和公有访问控制列表（ACL）的更多信息，请参阅 “公有”的含义。

所有未经身份验证的请求均由匿名用户发起。此用户在 ACL 中由特定的规范用户 ID `65a011a29cdf8ec533ec3d1ccaae921c` 表示。如果对象是通过未经身份验证的请求上传到存储桶的，匿名用户拥有对象。默认对象 ACL 向作为对象拥有者的匿名用户授予 `FULL_CONTROL`。因此，Amazon S3 允许未经身份验证的请求检索该对象或修改其 ACL。

为防止匿名用户修改对象，建议您不要实施允许对存储桶进行匿名公有写入的存储桶策略，或不要使用允许存储桶的匿名用户写入权限的 ACL。您可以使用 Amazon S3 屏蔽公共访问权限强制实施这个建议行为。

有关屏蔽公共访问权限的更多信息，请参阅阻止对您的 Amazon S3 存储的公有访问。有关 ACL 的更多信息，请参阅 访问控制列表 (ACL) 概述。

> **Important**
>
> 我们建议不要使用 Amazon Web Services 账户根用户凭证发起经过身份验证的请求。而应创建一个 IAM 角色并授予该角色完全访问权限。我们将具有此角色的用户称为管理员用户。您可以使用分配给管理员角色的用户凭证而不是 Amazon Web Services 账户 根用户凭证来与 Amazon 交互和执行任务，例如创建存储桶、创建用户以及授予权限。有关更多信息，请参阅《IAM 用户指南》中的 Amazon 安全凭证和 IAM 的安全防御最佳实操。

# Amazon S3 的存储桶策略

存储桶策略是基于资源的策略，您可以使用该策略向 Amazon S3 存储桶及其中的对象授予访问权限。只有存储桶拥有者才能将策略与存储桶关联。附加到存储桶的权限适用于存储桶拥有者拥有的存储桶中所有对象。这些权限不适用于其它 Amazon Web Services 账户所拥有的对象。

S3 对象所有权是 Amazon S3 存储桶级别的设置，您可以使用该设置来控制上传到存储桶的对象的所有权并禁用或启用访问控制列表（ACL）。默认情况下，对象所有权设为强制存储桶拥有者设置，并且所有 ACL 均处于禁用状态。存储桶拥有者拥有存储桶中的所有对象，并使用策略专门管理对数据的访问权限。

存储桶策略使用基于 JSON 的 Amazon Identity and Access Management（IAM）策略语言。您可以使用存储桶策略添加或拒绝存储桶中对象的权限。存储桶策略可以基于策略中的元素允许或拒绝请求。这些元素包括请求者、S3 操作、资源以及请求的特征或条件（例如，用于发出请求的 IP 地址）。

例如，您可以创建执行以下操作的存储桶策略：

- 授予其他账户将对象上传到您的 S3 存储桶的跨账户权限
- 确保您（存储桶拥有者）对于上传的对象具有完全控制权限

有关更多信息，请参阅 Amazon S3 存储桶策略的示例。

> **Important**
>
> 您不能使用存储桶策略来防止通过 S3 生命周期规则进行删除或转换。例如，即使您的存储桶策略拒绝所有主体的所有操作，您的 S3 生命周期配置也仍能正常发挥作用。

在本节中，我们通过主题提供了示例，并向您展示了如何在 S3 控制台中添加存储桶策略。有关基于身份的策略的信息，请参阅Amazon S3 基于身份的策略。有关存储桶策略语言的信息，请参阅Amazon S3 中的策略和权限。

有关按 S3 资源类型对 S3 API 操作的权限的更多信息，请参阅 Amazon S3 API 操作所需的权限。

主题

- 使用 Amazon S3 控制台添加存储桶策略

- 使用存储桶策略控制从 VPC 端点的访问
- Amazon S3 存储桶策略的示例
- 使用条件键的存储桶策略示例

## 使用 Amazon S3 控制台添加存储桶策略

您可以使用 Amazon 策略生成器和 Amazon S3 控制台添加新的存储桶策略或编辑现有存储桶策略。存储桶策略是基于资源的 Amazon Identity and Access Management（IAM）策略。将存储桶策略添加到一个存储桶可向其他 Amazon Web Services 账户 或 IAM 用户授予对该存储桶以及其中对象的访问权限。对象权限仅应用于存储桶拥有者创建的对象。有关存储桶策略的更多信息，请参阅 Amazon S3 的身份和访问管理。

确保保存策略之前解决来自 Amazon Identity and Access Management Access Analyzer 的安全警告、错误、一般警告和建议。IAM Access Analyzer 将根据 IAM 策略语法和最佳实践运行策略检查，以验证您的策略。这些检查项生成结果并提供可操作的建议，可帮助您编写可操作且符合安全最佳实践的策略。要了解有关使用 IAM Access Analyzer 验证策略的更多信息，请参阅《IAM 用户指南》中的 IAM Access Analyzer 策略验证。要查看 IAM Access Analyzer 返回的警告、错误和建议的列表，请参阅 IAM Access Analyzer 策略检查引用。

有关对策略错误进行故障排查的指南，请参阅排查 Amazon S3 中的拒绝访问（403 Forbidden）错误。

创建或编辑存储桶策略

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶或目录存储桶。
3. 在存储桶列表中，选择要为其创建或编辑存储桶策略的存储桶的名称。
4. 选择 Permissions（权限）选项卡。
5. 在 Bucket policy（存储桶策略）下，请选择 Edit（编辑）。将出现 Edit bucket policy（编辑存储桶策略）页面。
6. 在 Edit bucket policy（编辑存储桶策略）页面上，执行以下操作之一：
   - 要查看存储桶策略的示例，请选择策略示例。或请参阅《Amazon S3 用户指南》中的 Amazon S3 存储桶策略的示例。
   - 要自动生成策略或编辑策略部分中的 JSON，请选择策略生成器。

如果选择 Policy generator（策略生成器），Amazon 策略生成器将在新窗口中打开。

a. 在 Amazon 策略生成器页面上，对于选择策略类型，选择 S3 存储桶策略。

b. 通过在提供的字段中输入信息来添加语句，然后选择添加语句。对所有您想添加的语句重复执行此步骤。有关这些字段的更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素参考。

> **Note**
>
> 为方便起见，编辑桶策略页面会在策略文本字段上方显示当前桶的桶 ARN（Amazon 资源名称）。您可以复制此 ARN，以便在 Amazon 策略生成器页面上的语句中使用。

c. 添加完语句后，请选择生成策略。

d. 复制生成的策略文本，请选择 Close（关闭），然后返回到 Amazon S3 控制台中的 Edit bucket policy（编辑存储桶策略）页面。

7. 在 Policy（策略）框中，编辑现有策略或从 Amazon 策略生成器粘贴存储桶策略。确保在保存策略之前解决安全警告、错误、一般警告和建议。

> **Note**
>
> 存储桶策略的大小限制为 20 KB。

8. （可选）选择右下角的 Preview external access（预览外部访问），以预览新策略如何影响对资源的公有和跨账户访问。在保存策略之前，您可以检查策略是引入了新的 IAM Access Analyzer 发现结果还是解析了现有的发现结果。如果您没有看到活动的分析器，请在 IAM Access Analyzer 中选择 Go to Access Analyzer（转至 Access Analyzer）以创建账户分析器。有关更多信息，请参阅 IAM 用户指南中的预览访问权限。

9. 请选择 Save changes（保存更改），此操作将让您返回到 Permissions（权限）选项卡。

## 使用存储桶策略控制从 VPC 端点的访问

您可以使用 Amazon S3 存储桶策略控制从特定虚拟私有云（VPC）端点或特定 VPC 对存储桶的访问。本部分包含可用于从 VPC 端点控制 Amazon S3 存储桶访问的示例存储桶策略。要了解如何设置 VPC 端点，请参阅 VPC 用户指南中的 VPC 端点。

您可以使用 VPC 在您定义的虚拟网络内启动 Amazon 资源。使用 VPC 端点可以在您的 VPC 和其它 Amazon Web Services 服务之间创建私有连接。此私有连接不需要通过互联网、虚拟专用网络（VPN）连接、NAT 实例或 Amazon Direct Connect 进行访问。

Amazon S3 的 VPC 端点是 VPC 内的逻辑实体，仅允许连接到 Amazon S3。VPC 端点将请求路由到 Amazon S3 并将响应路由回 VPC。VPC 端点仅更改请求的路由方式。Amazon S3 公有端点和 DNS 名称将继续使用 VPC 端点。有关在 Amazon S3 中使用 VPC 端点的重要信息，请参阅《VPC 用户指南》中的 Gateway endpoints 和 Gateway endpoints for Amazon S3。

Amazon S3 的 VPC 端点提供两种方式来控制对 Amazon S3 数据的访问：

- 您可以控制允许通过特定 VPC 端点访问的请求、用户或组。有关此类型的访问控制的信息，请参阅《VPC 用户指南》中的 Controlling access to VPC endpoints using endpoint policies。
- 可以使用 Amazon S3 存储桶策略控制哪些 VPC 或 VPC 端点有权访问存储桶。有关此类型存储桶策略访问控制的示例，请参阅以下有关限制访问的主题。

主题

- 限制对特定 VPC 端点的访问
- 限制对特定 VPC 的访问

> **Important**
>
> 如本节中所述对 VPC 端点应用 Amazon S3 存储桶策略时，您可能会无意中阻止对存储桶的访问权限。存储桶权限旨在专门限制存储桶访问源自 VPC 端点的连接，而这可能会阻止到存储桶的所有连接。有关如何修复此问题的信息，请参阅《Amazon Web Services 支持 知识中心》中的当 VPC 或 VPC 端点 ID 错误时，如何修复存储桶策略？

## 限制对特定 VPC 端点的访问

下面是限制仅从 ID 为 `awsexamplebucket1` 的 VPC 端点访问特定存储桶 `vpce-1a2b3c4d` 的 Amazon S3 存储桶策略示例。如果未使用指定的端点，则该策略会拒绝对存储桶的所有访问。`aws:SourceVpce` 条件指定端点。`aws:SourceVpce` 条件不需要 VPC 端点资源的 Amazon 资源名称（ARN），而只需要 VPC 端点 ID。有关在策略中使用条件的更多信息，请参阅 使用条件键的存储桶策略示例。

**Important**

- 在使用以下示例策略之前，将 VPC 端点 ID 替换为适合您的使用案例的值。否则，您将无法访问您的存储桶。
- 此策略禁用控制台访问指定的存储桶，因为控制台请求不是来自指定的 VPC 端点。

```
{
   "Version": "2012-10-17",
   "Id": "Policy1415115909152",
   "Statement": [
     {
       "Sid": "Access-to-specific-VPCE-only",
       "Principal": "*",
       "Action": "s3:*",
       "Effect": "Deny",
       "Resource": ["arn:aws:s3:::awsexamplebucket1",
                    "arn:aws:s3:::awsexamplebucket1/*"],
       "Condition": {
         "StringNotEquals": {
           "aws:SourceVpce": "vpce-1a2b3c4d"
         }
       }
     }
   ]
}
```

限制对特定 VPC 的访问

可以使用 aws:SourceVpc 条件来创建用于限制对特定 VPC 的访问的存储桶策略。如果在同一 VPC 中配置了多个 VPC 端点，并且要管理对所有端点的 Amazon S3 存储桶的访问，这一点非常有用。以下是拒绝 VPC vpc-111bbb22 以外的任何人访问 awsexamplebucket1 及其对象的策略示例。如果未使用指定的 VPC，则该策略拒绝对存储桶的所有访问。此语句不授予针对存储桶的访问权限。要授予访问权限，必须添加单独的 Allow 语句。vpc-111bbb22 条件键不需要 VPC 资源 的 ARN，仅需要 VPC ID。

> **Important**
>
> - 在使用以下示例策略之前，将 VPC ID 替换为适合您的使用案例的值。否则，您将无法访问您的存储桶。
> - 此策略禁用控制台访问指定的存储桶，因为控制台请求不是来自指定的 VPC。

```
{
   "Version": "2012-10-17",
   "Id": "Policy1415115909153",
   "Statement": [
     {
       "Sid": "Access-to-specific-VPC-only",
       "Principal": "*",
       "Action": "s3:*",
       "Effect": "Deny",
       "Resource": ["arn:aws:s3:::awsexamplebucket1",
                    "arn:aws:s3:::awsexamplebucket1/*"],
       "Condition": {
         "StringNotEquals": {
           "aws:SourceVpc": "vpc-111bbb22"
         }
       }
     }
   ]
}
```

## Amazon S3 存储桶策略的示例

使用 Amazon S3 存储桶策略，您可以保护对存储桶中对象的访问，这样，只有具有适当权限的用户才能访问它们。您甚至可以阻止没有适当权限的经过身份验证的用户访问您的 Amazon S3 资源。

本节介绍关于存储桶策略的典型使用案例的示例。这些示例策略将 *amzn-s3-demo-bucket* 用作资源值。要测试这些策略，您需要将 *user input placeholders* 替换为您自己的信息（例如存储桶名称）。

要授予或拒绝对一组对象的权限，可以在 Amazon资源名称（ARN）和其他值中使用通配符（*）。例如，您可以控制对以通用前缀或以特定扩展名结尾的对象组的访问，例如 .html。

有关 Amazon Identity and Access Management（IAM）策略语言的更多信息，请参阅Amazon S3 中的策略和权限。

有关按 S3 资源类型对 S3 API 操作的权限的更多信息，请参阅 Amazon S3 API 操作所需的权限。

> **Note**
>
> 使用 Amazon S3 控制台测试权限时，您必须授予控制台所需的其他权限（`s3:ListAllMyBuckets`、`s3:GetBucketLocation` 和 `s3:ListBucket`）。有关向用户授予权限并使用控制台测试这些权限的示例演练，请参阅使用用户策略控制对存储桶的访问。

用于创建存储桶策略的其它资源包括以下内容：

- 有关在创建存储桶策略时可以使用的 IAM 策略操作、资源和条件键的列表，请参阅《Service Authorization Reference》中的 Actions, resources, and condition keys for Amazon S3。
- 有关按 S3 资源类型对 S3 API 操作的权限的更多信息，请参阅 Amazon S3 API 操作所需的权限。
- 有关创建 S3 策略的指南，请参阅使用 Amazon S3 控制台添加存储桶策略。
- 要对策略错误进行故障排查，请参阅排查 Amazon S3 中的拒绝访问（403 Forbidden）错误。

主题


- 向公共匿名用户授予只读权限
- 需要加密
- 使用标准 ACL 管理存储桶
- 使用对象标记管理对象访问权限
- 使用全局条件键管理对象访问权限
- 管理基于 HTTP 或 HTTPS 请求的访问权限
- 管理用户对特定文件夹的访问权限
- 管理访问日志的访问权限
- 管理对 Amazon CloudFront OAI 的访问
- 管理 Amazon S3 Storage Lens 存储统计管理工具的访问权限
- 管理 S3 清单、S3 分析和 S3 清单报告的权限
- 需要 MFA

- 防止用户删除对象

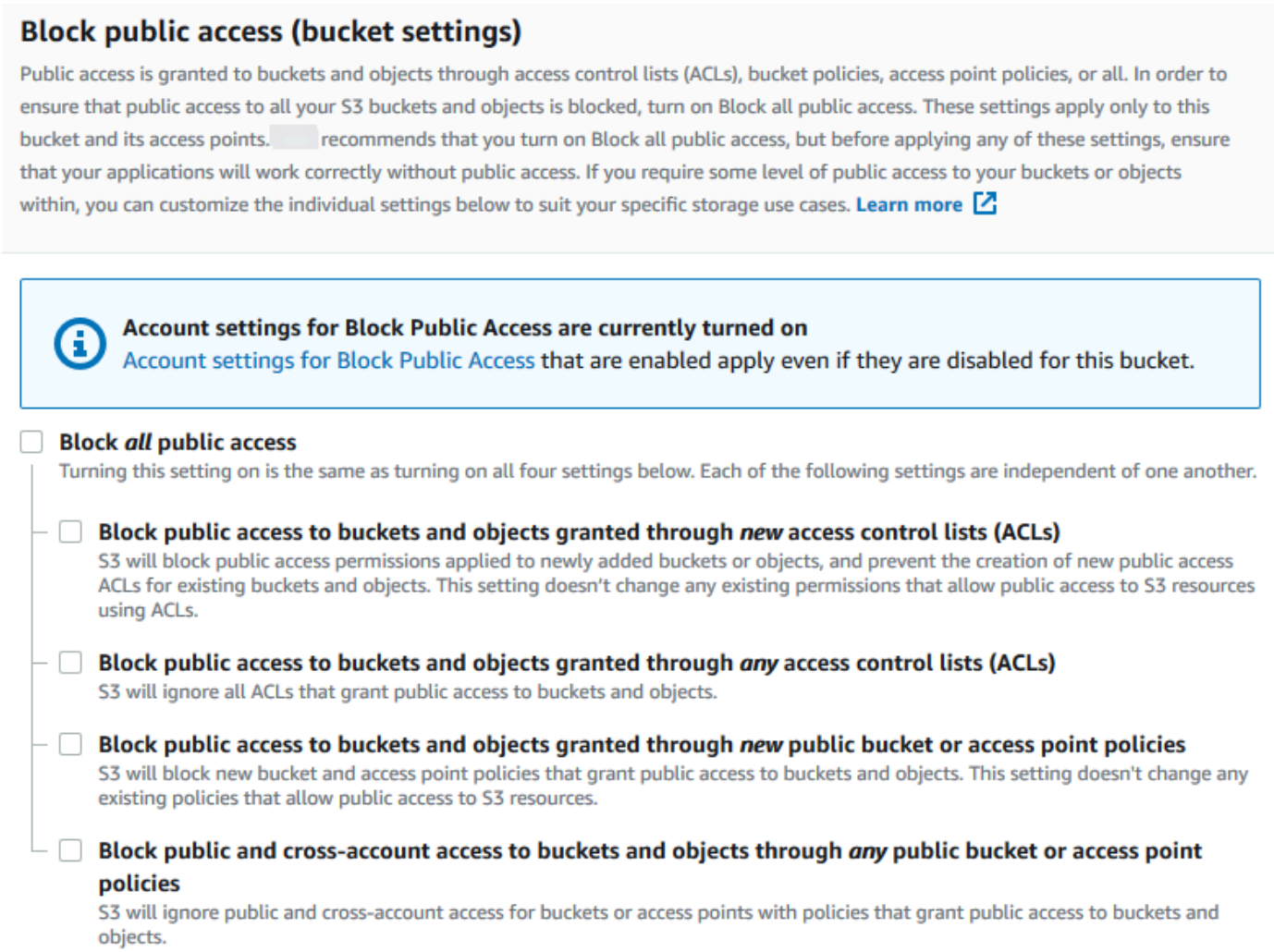
向公共匿名用户授予只读权限

可以使用策略设置向公共匿名用户授予访问权限，如果您要将存储桶配置为静态网站，这将非常有用。向公共匿名用户授予访问权限要求您对存储桶禁用“屏蔽公共访问权限”设置。有关更多信息以及如何执行此操作，请参阅设置访问网站的权限。要了解如何出于相同的目的设置更严格的策略，请参阅 Amazon 知识中心的如何授予对 Amazon S3 存储桶中某些对象的公共读取访问权限？。

默认情况下，Amazon S3 阻止对您的账户和存储桶的公有访问权限。如果要使用存储桶托管静态网站，您可以使用以下步骤编辑您的屏蔽公共访问权限设置。

> **Warning**
>
> 在完成这些步骤之前，请查看阻止对您的 Amazon S3 存储的公有访问，来确保您了解并接受支持公共访问权限所涉及的风险。当您关闭屏蔽公共访问权限设置以使您的存储桶变为公有时，Internet 上的任何人都可以访问您的存储桶。我们建议您阻止对存储桶的所有公有访问。

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 请选择已配置为静态网站的存储桶的名称。
3. 选择权限。
4. 在屏蔽公共访问权限（存储桶设置）下，请选择编辑。
5. 清除阻止所有公有访问，然后选择保存更改。




Amazon S3 关闭了存储桶的屏蔽公共访问权限设置。要创建公有静态网站，可能还必须为您的账户配置屏蔽公共访问权限设置，然后再添加存储桶策略。如果当前已开启账户的屏蔽公共访问权限设置，您将在屏蔽公共访问权限（存储桶设置）下看到一条备注。

需要加密

您可以要求使用具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS），如以下示例所示。

要求对写入存储桶的所有对象使用 SSE-KMS

以下示例策略要求写入存储桶的每个对象都通过使用 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）进行加密。如果对象未使用 SSE-KMS 进行加密，则请求将被拒绝。

```
{
"Version": "2012-10-17",
"Id": "PutObjPolicy",
"Statement": [{
  "Sid": "DenyObjectsThatAreNotSSEKMS",
  "Principal": "*",
  "Effect": "Deny",
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
  "Condition": {
    "Null": {
      "s3:x-amz-server-side-encryption-aws-kms-key-id": "true"
    }
  }
}]
}
```

要求对写入存储桶的所有对象使用具有特定 Amazon KMS key 的 SSE-KMS

如果未使用特定的 KMS 密钥 ID 通过 SSE-KMS 加密任何对象，则以下示例策略会拒绝将此类对象写入存储桶。即使使用每请求标头或存储桶默认加密通过 SSE-KMS 加密对象，但如果尚未使用指定的 KMS 密钥加密对象，则无法将其写入存储桶。确保将本示例中使用的 KMS 密钥 ARN 替换为您自己的 KMS 密钥 ARN。

```
{
"Version": "2012-10-17",
"Id": "PutObjPolicy",
"Statement": [{
  "Sid": "DenyObjectsThatAreNotSSEKMSWithSpecificKey",
  "Principal": "*",
  "Effect": "Deny",
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
  "Condition": {
    "ArnNotEqualsIfExists": {
      "s3:x-amz-server-side-encryption-aws-kms-key-id": "arn:aws:kms:us-
east-2:111122223333:key/01234567-89ab-cdef-0123-456789abcdef"
    }
  }
}]
}
```

使用标准 ACL 管理存储桶

授予多个账户上传对象或设置对象 ACL 以进行公有访问的权限

以下示例策略向多个 Amazon Web Services 账户授予 `s3:PutObject` 和 `s3:PutObjectAcl` 权限。此外，该示例策略还要求针对这些操作的任何请求都必须包含 `public-read` 标准访问控制列表（ACL）。有关更多信息，请参阅Amazon S3 的策略操作和Amazon S3 的策略条件键。

> **Warning**
>
> `public-read` 标准 ACL 允许世界上的任何人查看您存储桶中的对象。在授予对 Amazon S3 存储桶的匿名访问权限或禁用屏蔽公共访问权限设置时，请小心谨慎。如果您授予匿名访问权限，那么世界上的任何人都可以访问您的存储桶。我们建议您永远不要授予对 Amazon S3 存储桶的匿名访问权限，除非您明确需要，如使用静态网站托管时。如果您想为静态网站托管启用屏蔽公共访问权限设置，请参阅教程：在 Amazon S3 上配置静态网站。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AddPublicReadCannedAcl",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:root",
                    "arn:aws:iam::444455556666:root"
                ]
            },
            "Action": [
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": [
                        "public-read"
                    ]
                }
            }
        }
```

```
    ]
}
```

在授予上传对象的跨账户权限的同时，确保存储桶拥有者拥有完全控制权

以下示例说明如何允许另一个 Amazon Web Services 账户将对象上传到存储桶，同时确保您完全控制上传的对象。此策略向特定 Amazon Web Services 账户（*111122223333*）授予上传对象的能力，但仅当该账户在上传时包含 `bucket-owner-full-control` 标准 ACL 时才能上传对象。该策略中的 `StringEquals` 条件指定 `s3:x-amz-acl` 条件键以表示标准 ACL 要求。有关更多信息，请参阅 Amazon S3 的策略条件键。

```
{
   "Version":"2012-10-17",
   "Statement":[
     {
       "Sid":"PolicyForAllowUploadWithACL",
       "Effect":"Allow",
       "Principal":{"AWS":"111122223333"},
       "Action":"s3:PutObject",
       "Resource":"arn:aws:s3:::amzn-s3-demo-bucket/*",
       "Condition": {
         "StringEquals": {"s3:x-amz-acl":"bucket-owner-full-control"}
       }
     }
   ]
}
```

使用对象标记管理对象访问权限

允许用户仅读取具有特定标签键和值的对象

以下权限策略限制用户只能读取具有 `environment: production` 标签键和值的对象。该策略使用 `s3:ExistingObjectTag` 条件键来指定标签键和值。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Principal":{
            "AWS":"arn:aws:iam::111122223333:role/JohnDoe"
         },
         "Effect":"Allow",
```

```
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket/*",
         "Condition":{
            "StringEquals":{
               "s3:ExistingObjectTag/environment":"production"
            }
         }
      }
   ]
}
```

限制用户可以添加哪些对象标签键

以下示例策略将向用户授予执行 s3:PutObjectTagging 操作的权限，这使用户可以将标签添加到现有对象。条件使用 s3:RequestObjectTagKeys 条件键指定允许的标签键，例如 Owner 或 CreationDate。有关更多信息，请参阅《IAM 用户指南》中的创建测试多个键值的条件。

该策略确保在请求中指定的每个标签键都是授权的标签键。条件中的 ForAnyValue 限定符确保请求中必须至少存在指定的值之一。

```
{
   "Version": "2012-10-17",
  "Statement": [
    {"Principal":{"AWS":[
            "arn:aws:iam::111122223333:role/JohnDoe"
         ]
       },
 "Effect": "Allow",
      "Action": [
        "s3:PutObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {"ForAnyValue:StringEquals": {"s3:RequestObjectTagKeys": [
            "Owner",
            "CreationDate"
          ]
        }
      }
```

```
    }
  ]
}
```

在允许用户添加对象标签时需要特定的标签键和值

以下示例策略将向用户授予执行 s3:PutObjectTagging 操作的权限，这使用户可以将标签添加到现有对象。条件要求用户包含值设置为 *X* 的特定标签键（*Project*）。

```
{
   "Version": "2012-10-17",
  "Statement": [
    {"Principal":{"AWS":[
       "arn:aws:iam::111122223333:user/JohnDoe"
         ]
       },
      "Effect": "Allow",
      "Action": [
        "s3:PutObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {"StringEquals": {"s3:RequestObjectTag/Project": "X"
        }
      }
    }
  ]
}
```

允许用户仅添加具有特定对象标签键和值的对象

以下示例策略向用户授予执行 s3:PutObject 操作的权限，以便他们可以向存储桶添加对象。但是，Condition 语句限制了上传的对象上允许的标签键和值。在此示例中，用户只可以将具有特定标签键（*Department*）（值设置为 *Finance*）的对象添加到存储桶。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Principal":{
            "AWS":[
                 "arn:aws:iam::111122223333:user/JohnDoe"
         ]
```

```
        },
        "Effect": "Allow",
        "Action": [
            "s3:PutObject"
        ],
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ],
        "Condition": {
            "StringEquals": {
                "s3:RequestObjectTag/Department": "Finance"
            }
        }
    }]
}
```

使用全局条件键管理对象访问权限

全局条件键是带有 aws 前缀的条件键。Amazon Web Services 服务 可以支持全局条件键或包含服务前缀的服务特定键。您可以使用 JSON 策略的 Condition 元素将请求中的键与您在策略中指定的键值进行比较。

限制只能访问 Amazon S3 服务器访问日志传输

在下面的示例存储桶策略中，aws:SourceArn 全局条件键用于比较资源的 Amazon资源名称（ARN），从而使用在策略中指定的 ARN 发出服务对服务请求。aws:SourceArn 全局条件键用于防止 Amazon S3 服务在服务之间执行事务时被用作混淆代理人。只有 Amazon S3 服务才能将对象添加到 Amazon S3 存储桶。

此示例存储桶策略仅向日志服务主体（logging.s3.amazonaws.com）授予 s3:PutObject 权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowPutObjectS3ServerAccessLogsPolicy",
            "Principal": {
                "Service": "logging.s3.amazonaws.com"
            },
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket-logs/*",
```

```
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111111111111"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:::EXAMPLE-SOURCE-BUCKET"
                }
            }
        },
        {
            "Sid": "RestrictToS3ServerAccessLogs",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket-logs/*",
            "Condition": {
                "ForAllValues:StringNotEquals": {
                    "aws:PrincipalServiceNamesList": "logging.s3.amazonaws.com"
                }
            }
        }
    ]
}
```

仅允许访问您的组织

如果您希望要求访问资源的所有 IAM 主体都来自组织中的 Amazon Web Services 账户（包括 Amazon Organizations 管理账户），则可以使用 `aws:PrincipalOrgID` 全局条件键。

要授予或限制此类访问权限，请在存储桶策略中定义 `aws:PrincipalOrgID` 条件并将值设置为您的组织 ID。组织 ID 用于控制对存储桶的访问权限。当您使用 `aws:PrincipalOrgID` 条件时，存储桶策略中的权限也将应用于添加到组织的所有新账户。

以下是一个基于资源的存储桶策略的示例，您可以使用该策略向组织中的特定 IAM 主体授予对存储桶的直接访问权限。通过向您的存储桶策略添加 `aws:PrincipalOrgID` 全局条件键，主体账户现在必须在您的组织中才能访问资源。即使您在授予访问权限时意外指定了错误的账户，aws:PrincipalOrgID 全局条件键也可以起到额外保护作用。当在策略中使用该全局键时，此策略防止指定组织之外的所有主体访问 S3 存储桶。只有来自所列组织中账户的主体才能获得对资源的访问权限。

```
{
    "Version": "2012-10-17",
    "Statement": [{
```

```
        "Sid": "AllowGetObject",
        "Principal": {
            "AWS": "*"
        },
        "Effect": "Allow",
        "Action": "s3:GetObject",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
        "Condition": {
            "StringEquals": {
                "aws:PrincipalOrgID": ["o-aa111bb222"]
            }
        }
    }]
}
```

管理基于 HTTP 或 HTTPS 请求的访问权限

仅限 HTTPS 请求访问

如果您想防止潜在攻击者操纵网络流量，则可以使用 HTTPS（TLS）以仅允许加密连接，同时限制 HTTP 请求访问您的存储桶。要确定请求是 HTTP 还是 HTTPS，请在 S3 存储桶策略中使用 aws:SecureTransport 全局条件键。aws:SecureTransport 条件键检查请求是不是使用 HTTP 发送的。

如果请求返回 `true`，则该请求是通过 HTTPS 发送的。如果请求返回 `false`，则该请求是通过 HTTP 发送的。然后，您可以根据所需的请求方案允许或拒绝对存储桶的访问。

在以下示例中，存储桶策略明确拒绝 HTTP 请求。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "RestrictToTLSRequestsOnly",
        "Action": "s3:*",
        "Effect": "Deny",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket",
            "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ],
        "Condition": {
            "Bool": {
                "aws:SecureTransport": "false"
            }
```

```
        },
        "Principal": "*"
    }]
}
```

仅限特定 HTTP 引用站点访问

假设您拥有一个网站，其域名为 *www.example.com* 或 *example.com*，并且带有指向存储在名为 *amzn-s3-demo-bucket* 的存储桶中的照片和视频的链接。默认情况下，所有 Amazon S3 资源都是私有的，因此，只有创建资源的 Amazon Web Services 账户才能访问它们。

要允许从您的网站对这些对象进行读取访问，您可以添加一个存储桶策略，以允许 `s3:GetObject` 权限并附带一个条件，即 GET 请求必须源自特定的网页。以下策略通过使用 `StringLike` 条件和 `aws:Referer` 条件键来限制请求。

```
{
  "Version":"2012-10-17",
  "Id":"HTTP referer policy example",
  "Statement":[
    {
      "Sid":"Allow only GET requests originating from www.example.com and
 example.com.",
      "Effect":"Allow",
      "Principal":"*",
      "Action":["s3:GetObject","s3:GetObjectVersion"],
      "Resource":"arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition":{
        "StringLike":{"aws:Referer":["http://www.example.com/*","http://example.com/
*"]}
      }
    }
  ]
}
```

确保您使用的浏览器在请求中包含 HTTP `referer` 标头。

> **Warning**
>
> 我们建议您谨慎使用 `aws:Referer` 条件键。包含公共已知的 HTTP 引用站点标头值是非常危险的。未经授权方可能会使用修改的浏览器或自定义浏览器提供他们选择的任何 `aws:Referer` 值。因此，请勿使用 `aws:Referer` 防止未经授权的各方直接进行 Amazon 请求。

提供 aws:Referer 条件键只是为了允许客户保护其数字内容（如存储在 Amazon S3 中的内容），以免在未经授权的第三方站点上引用。有关更多信息，请参阅 IAM 用户指南中的 aws:Referer。

管理用户对特定文件夹的访问权限

授予用户对特定文件夹的访问权限

假设您正在尝试授予用户对特定文件夹的访问权限。如果 IAM 用户和 S3 存储桶属于同一个 Amazon Web Services 账户，则您可以使用 IAM 策略向用户授予对特定存储桶文件夹的访问权限。使用这种方法，您无需更新存储桶策略即可授予访问权限。您可以将 IAM 策略添加到多个用户可以切换到的 IAM 角色。

如果 IAM 身份和 S3 存储桶属于不同的 Amazon Web Services 账户，则您必须在 IAM 策略和存储桶策略中授予跨账户访问权限。有关授予跨账户访问权限的信息，请参阅存储桶拥有者授予跨账户存储桶权限。

以下示例存储桶策略仅授予 *JohnDoe* 对他的文件夹（home/*JohnDoe*/）的完全控制台访问权限。通过创建 home 文件夹并向您的用户授予相应的权限，您可以让多个用户共享单个存储桶。该策略由三条 Allow 语句组成：

- *AllowRootAndHomeListingOfCompanyBucket*：允许用户（*JohnDoe*）列出 *amzn-s3-demo-bucket* 存储桶的根级别和 home 文件夹中的对象。此语句还允许用户使用控制台根据前缀 home/ 进行搜索。
- *AllowListingOfUserFolder*：允许用户（*JohnDoe*）列出 home/*JohnDoe*/ 文件夹和任何子文件夹中的所有对象。
- *AllowAllS3ActionsInUserFolder*：允许用户通过授予 Read、Write 和 Delete 权限来执行所有 Amazon S3 操作。权限仅限于存储桶拥有者的主文件夹。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRootAndHomeListingOfCompanyBucket",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:user/JohnDoe"
                ]
```

```
            },
            "Effect": "Allow",
            "Action": ["s3:ListBucket"],
            "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket"],
            "Condition": {
                "StringEquals": {
                    "s3:prefix": ["", "home/", "home/JohnDoe"],
                    "s3:delimiter": ["/"]
                }
            }
        },
        {
            "Sid": "AllowListingOfUserFolder",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:user/JohnDoe"
                ]
            },
            "Action": ["s3:ListBucket"],
            "Effect": "Allow",
            "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket"],
            "Condition": {
                "StringLike": {
                    "s3:prefix": ["home/JohnDoe/*"]
                }
            }
        },
        {
            "Sid": "AllowAllS3ActionsInUserFolder",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:user/JohnDoe"
                ]
            },
            "Action": ["s3:*"],
            "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket/home/JohnDoe/*"]
        }
    ]
}
```

管理访问日志的访问权限

授予应用程序负载均衡器访问权限以启用访问日志

在为应用程序负载均衡器启用访问日志时，您必须指定负载均衡器将在其中存储日志的 S3 存储桶的名称。存储桶必须具有附加的策略，用于为弹性负载均衡授予写入存储桶的权限。

在以下示例中，存储桶策略授予弹性负载均衡（ELB）将访问日志写入存储桶的权限：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Principal": {
        "AWS": "arn:aws:iam::elb-account-id:root"
      },
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/111122223333/*"
    }
  ]
}
```

> **Note**
>
> 请务必将 *elb-account-id* 替换为您的 Amazon Web Services 区域的弹性负载均衡的 Amazon Web Services 账户 ID。有关弹性负载均衡区域的列表，请参阅《弹性负载均衡用户指南》中的将策略附加到您的 Amazon S3 存储桶。

如果您的 Amazon Web Services 区域未出现在支持的弹性负载均衡区域列表中，请使用以下策略，该策略授予对指定日志传输服务的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
       "Principal": {
         "Service": "logdelivery.elasticloadbalancing.amazonaws.com"
          },
      "Effect": "Allow",
```

```
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/111122223333/*"
    }
  ]
}
```

然后，确保通过启用您的弹性负载均衡访问日志来配置它们。您可以通过创建测试文件来验证您的存储桶权限。

管理对 Amazon CloudFront OAI 的访问

向 Amazon CloudFront OAI 授予权限

下面的示例存储桶策略授予 CloudFront 来源访问身份（OAI）权限，以获取（读取）S3 存储桶中的所有对象。您可以使用 CloudFront OAI 以允许用户通过 CloudFront 访问存储桶中的对象，但不能直接通过 Amazon S3 访问。有关更多信息，请参阅《Amazon CloudFront 开发人员指南》中的使用来源访问身份限制对 Amazon S3 内容的访问。

下面的策略使用 OAI 的 ID 作为策略的 `Principal`。有关使用 S3 存储桶策略向 CloudFront OAI 授予访问权限的更多信息，请参阅《Amazon CloudFront 开发人员指南》中的从来源访问身份（OAI）迁移到来源访问控制（OAC)。

要使用此示例，请执行以下操作：

- 将 *EH1HDMB1FH2TC* 替换为 OAI 的 ID。要查找 OAI 的 ID，请参阅 CloudFront 控制台中的来源访问身份页面，或者使用 CloudFront API 中的 ListCloudFrontOriginAccessIdentities。
- 将 *amzn-s3-demo-bucket* 替换为您的存储桶的名称。

```
{
    "Version": "2012-10-17",
    "Id": "PolicyForCloudFrontPrivateContent",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access
 Identity EH1HDMB1FH2TC"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
```

```
        }
    ]
}
```

管理 Amazon S3 Storage Lens 存储统计管理工具的访问权限

授予 Amazon S3 Storage Lens 存储统计管理工具的权限

S3 Storage Lens 存储统计管理工具聚合您的指标，并在 Amazon S3 控制台的 Buckets（存储桶）页上的 Account snapshot（账户快照）部分中显示此信息。S3 Storage Lens 存储统计管理工具还提供了一个交互式控制面板，您可以使用它来可视化见解和趋势，标记异常值，并接收有关优化存储成本和应用数据保护最佳实践的建议。控制面板提供深入分析选项，用于在组织、账户、Amazon Web Services 区域、存储类、存储桶、前缀或 Storage Lens 组级别生成和可视化见解。您还可以将采用 CSV 或 Parquet 格式的每日指标导出发送到 S3 存储桶。

S3 Storage Lens 存储统计管理工具可以将聚合的存储使用情况指标导出到 Amazon S3 存储桶中，以便进一步分析。S3 Storage Lens 存储统计管理工具放置其指标导出的存储桶称为目标存储桶。在设置 S3 Storage Lens 存储统计管理工具指标导出时，您必须为目标存储桶制定存储桶策略。有关更多信息，请参阅 使用 Amazon S3 Storage Lens 存储统计管理工具评估您的存储活动和使用情况。

以下示例存储桶策略授予 Amazon S3 向目标存储桶写入对象（PUT 请求）的权限。在设置 S3 Storage Lens 存储统计管理工具指标导出时，您可以对目标存储桶使用类似这样的存储桶策略。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3StorageLensExamplePolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "storage-lens.s3.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-destination-bucket/destination-prefix/
StorageLens/111122223333/*"
            ],
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": "111122223333",
```

```
                    "aws:SourceArn": "arn:aws:s3:region-code:111122223333:storage-
lens/storage-lens-dashboard-configuration-id"
                }
            }
        }
    ]
}
```

在设置 S3 Storage Lens 存储统计管理工具组织级别的指标导出时，对之前存储桶策略的 Resource 语句进行以下修改。

```
"Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/destination-prefix/
StorageLens/your-organization-id/*",
```

管理 S3 清单、S3 分析和 S3 清单报告的权限

向 S3 清单和 S3 分析功能授予权限

S3 清单在存储桶中创建对象列表，而 S3 分析存储类分析导出功能创建分析中使用的数据的输出文件。由清单列出其对象的存储桶称为源存储桶。清单文件或分析导出文件将写入到的存储桶称为目标存储桶。在设置清单或分析导出时，必须为目标存储桶创建存储桶策略。有关更多信息，请参阅使用 S3 清单对数据进行编目和分析和Amazon S3 分析 – 存储类分析。

以下示例存储桶策略向 Amazon S3 授予将源存储桶的账户中的对象写入（PUT 请求）到目标存储桶的权限。您在设置 S3 清单和 S3 分析导出功能时，将对目标存储桶使用像这样的存储桶策略。

```
{
      "Version": "2012-10-17",
      "Statement": [
        {
            "Sid": "InventoryAndAnalyticsExamplePolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
            ],
```

```
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:::DOC-EXAMPLE-SOURCE-BUCKET"
                },
                "StringEquals": {
                    "aws:SourceAccount": "111122223333",
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
            }
        }
    ]
}
```

控制 S3 清单报告配置的创建

使用 S3 清单对数据进行编目和分析创建 S3 存储桶中对象的列表，并为每个对象创建元数据。s3:PutInventoryConfiguration 权限允许用户创建清单配置（其中包含默认情况下提供的所有可用对象元数据字段）并指定存储清单的目标存储桶。对目标存储桶中的对象具有读取权限的用户可以访问清单报告中提供的所有对象元数据字段。有关 S3 清单中提供的元数据字段的更多信息，请参阅 Amazon S3 清单列表。

要限制用户配置 S3 清单报告，请取消该用户的 s3:PutInventoryConfiguration 权限。

S3 清单报告配置中的某些对象元数据字段是可选的，这意味着它们在默认情况下是可用的，但是当您向用户授予 s3:PutInventoryConfiguration 权限时，它们可能会受到限制。您可以使用 s3:InventoryAccessibleOptionalFields 条件键控制用户能否在报告中包含这些可选元数据字段。有关 S3 清单中可用的可选元数据字段的列表，请参阅《Amazon Simple Storage Service API Reference》中的 OptionalFields。

要向用户授予创建带有特定可选元数据字段的清单配置的权限，请使用 s3:InventoryAccessibleOptionalFields 条件键来完善存储桶策略中的条件。

以下策略示例向用户 (*Ana*) 授予有条件地创建清单配置的权限。该策略中的 ForAllValues:StringEquals 条件使用 s3:InventoryAccessibleOptionalFields 条件键来指定两个允许使用的可选元数据字段，即 Size 和 StorageClass。因此，在 *Ana* 创建清单配置时，她只可以包含可选元数据字段 Size 和 StorageClass。

```
{
 "Id": "InventoryConfigPolicy",
 "Version": "2012-10-17",
 "Statement": [{
```

```
   "Sid": "AllowInventoryCreationConditionally",
   "Effect": "Allow",
   "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/Ana"
   },
   "Action":
    "s3:PutInventoryConfiguration",
   "Resource":
    "arn:aws:s3:::DOC-EXAMPLE-SOURCE-BUCKET",
   "Condition": {
    "ForAllValues:StringEquals": {
     "s3:InventoryAccessibleOptionalFields": [
        "Size",
        "StorageClass"
        ]
      }
    }
   }
 ]
}
```

要限制用户配置包含特定可选元数据字段的 S3 清单报告，请向源存储桶的存储桶策略中添加明确的 Deny 声明。以下存储桶策略示例拒绝用户 *Ana* 在源存储桶 *DOC-EXAMPLE-SOURCE-BUCKET* 中创建包含可选 ObjectAccessControlList 或 ObjectOwner 元数据字段的清单配置。用户 *Ana* 仍然可以使用其他可选元数据字段创建清单配置。

```
{
 "Id": "InventoryConfigSomeFields",
 "Version": "2012-10-17",
 "Statement": [{
   "Sid": "AllowInventoryCreation",
   "Effect": "Allow",
   "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/Ana"
   },
   "Action": "s3:PutInventoryConfiguration",
   "Resource":
    "arn:aws:s3:::DOC-EXAMPLE-SOURCE-BUCKET",

  },
  {
   "Sid": "DenyCertainInventoryFieldCreation",
   "Effect": "Deny",
```

```
    "Principal": {
     "AWS": "arn:aws:iam::111122223333:user/Ana"
    },
    "Action": "s3:PutInventoryConfiguration",
    "Resource":
      "arn:aws:s3:::DOC-EXAMPLE-SOURCE-BUCKET",
    "Condition": {
     "ForAnyValue:StringEquals": {
      "s3:InventoryAccessibleOptionalFields": [
         "ObjectOwner",
         "ObjectAccessControlList"
         ]
       }
     }
    }
 ]
}
```

> **Note**
>
> 在存储桶策略中使用 s3:InventoryAccessibleOptionalFields 条件键不会影响基于现有清单配置的清单报告交付。

> **Important**
>
> 我们建议将 ForAllValues 与 Allow 效果一起使用，或将 ForAnyValue 与 Deny 效果一起使用，如前面的示例所示。
>
> 请勿将 ForAllValues 与 Deny 效果一起使用，或将 ForAnyValue 与 Allow 效果一起使用，因为这些组合可能过于严格，并且会阻止删除清单配置。
>
> 要了解有关 ForAllValues 和 ForAnyValue 条件集运算符的更多信息，请参阅《IAM 用户指南》中的多值上下文键。

### 需要 MFA

Amazon S3 支持受 MFA 保护的 API 访问，这是一项可在访问您的 Amazon S3 资源时强制进行多重身份验证（MFA）的特征。多重验证提供了额外的安全级别，可以应用于您的 Amazon 环境。MFA 是一项安全特征，要求用户通过提供有效 MFA 代码来证明实际拥有 MFA 设备。有关更多信息，请参阅 Amazon 多重身份验证。您可以要求对访问 Amazon S3 资源的任何请求使用 MFA。

要强制实施 MFA 要求，请在存储桶策略中使用 aws:MultiFactorAuthAge 条件键。IAM 用户可以使用由 Amazon Security Token Service（Amazon STS）发布的临时凭证访问 Amazon S3 资源。您可以在 Amazon STS 请求时提供 MFA 代码。

当 Amazon S3 收到带多重身份验证的请求时，aws:MultiFactorAuthAge 条件键将提供一个数值，指示临时凭证是在多久以前创建的（以秒为单位）。如果请求中提供的临时凭证不是使用 MFA 设备创建的，则此键值为空（缺失）。您可以在存储桶策略中添加一个条件来检查此值，如下面的示例所示。

如果请求未使用 MFA 进行身份验证，此示例策略将拒绝对 *amzn-s3-demo-bucket* 存储桶中的 */taxdocuments* 文件夹执行任何 Amazon S3 操作。要了解有关 MFA 的更多信息，请参阅 IAM 用户指南中的在 Amazon 中使用多重身份验证 (MFA)。

```
{
    "Version": "2012-10-17",
    "Id": "123",
    "Statement": [
      {
        "Sid": "",
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:*",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/taxdocuments/*",
        "Condition": { "Null": { "aws:MultiFactorAuthAge": true }}
      }
    ]
 }
```

如果 aws:MultiFactorAuthAge 条件键值为空，即指示请求中的临时安全凭证是在没有 MFA 设备的情况下创建的，则 Condition 块中的 Null 条件的计算结果为 true。

下面的存储桶策略是上述存储桶策略的扩展。以下策略包含两个策略语句。一个语句允许将存储桶（*amzn-s3-demo-bucket*）的 s3:GetObject 权限授予所有人。另一个语句通过要求 MFA，进一步限制对 *amzn-s3-demo-bucket/taxdocuments* 文件夹的访问。

```
{
    "Version": "2012-10-17",
    "Id": "123",
    "Statement": [
      {
        "Sid": "",
```

```
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:*",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/taxdocuments/*",
        "Condition": { "Null": { "aws:MultiFactorAuthAge": true } }
      },
      {
        "Sid": "",
        "Effect": "Allow",
        "Principal": "*",
        "Action": ["s3:GetObject"],
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
      }
    ]
}
```

您可以选择使用数值条件来限制 aws:MultiFactorAuthAge 键的有效期。您使用 aws:MultiFactorAuthAge 键指定的期限独立于对请求进行身份验证时使用的临时安全凭证的生存期。

例如，除了要求 MFA 身份验证外，下面的存储桶策略还会查看临时会话是在多久以前创建的。如果 aws:MultiFactorAuthAge 键值指示临时会话是在一个小时 (3600 秒) 之前创建的，则策略将拒绝任何操作。

```
{
    "Version": "2012-10-17",
    "Id": "123",
    "Statement": [
      {
        "Sid": "",
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:*",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/taxdocuments/*",
        "Condition": {"Null": {"aws:MultiFactorAuthAge": true }}
      },
      {
        "Sid": "",
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:*",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/taxdocuments/*",
        "Condition": {"NumericGreaterThan": {"aws:MultiFactorAuthAge": 3600 }}
```

```
      },
      {
        "Sid": "",
        "Effect": "Allow",
        "Principal": "*",
        "Action": ["s3:GetObject"],
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
      }
    ]
}
```

防止用户删除对象

默认状态下，用户没有权限。但在创建策略时，您可能无意间向用户授予了您并不打算授予的权限。为避免这些权限漏洞，可通过添加显式拒绝编写更严格的访问策略。

要显式阻止用户或账户删除对象，您必须在存储桶策略中添加以下操作：s3:DeleteObject、s3:DeleteObjectVersion 和 s3:PutLifecycleConfiguration 权限。所有三个操作均为必需，因为您可通过显式调用 DELETE Object API 操作或配置其生命周期来删除对象（请参阅管理对象的生命周期），以便 Amazon S3 能够在对象生命周期已过时将它们移除。

在以下策略示例中，您显式对用户 *MaryMajor* 拒绝 DELETE Object 权限。显式 Deny 语句始终取代授予的其它任何权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "statement1",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/MaryMajor"
      },
      "Action": [
        "s3:GetObjectVersion",
        "s3:GetBucketAcl"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket1",
    "arn:aws:s3:::amzn-s3-demo-bucket1/*"
      ]
    },
```

```
    {
      "Sid": "statement2",
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/MaryMajor"
      },
      "Action": [
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket1",
     "arn:aws:s3:::amzn-s3-demo-bucket1/*"
      ]
    }
  ]
}
```

## 使用条件键的存储桶策略示例

您可以使用访问策略语言在授予权限时指定条件。可以使用可选 Condition 元素或 Condition 块来指定策略何时生效的条件。

有关使用 Amazon S3 条件键进行对象和存储桶操作的策略，请参阅以下示例。有关条件键的更多信息，请参阅 Amazon S3 的策略条件键。有关您可以在策略中指定的 Amazon S3 操作、条件键和资源的完整列表，请参阅《Service Authorization Reference》中的 Actions, resources, and condition keys for Amazon S3。

有关按 S3 资源类型对 S3 API 操作的权限的更多信息，请参阅 Amazon S3 API 操作所需的权限。

示例：适用于对象操作的 Amazon S3 条件键

以下示例说明如何将特定于 Amazon S3 的条件键用于对象操作。有关您可以在策略中指定的 Amazon S3 操作、条件键和资源的完整列表，请参阅《Service Authorization Reference》中的 Actions, resources, and condition keys for Amazon S3。

有关按 S3 资源类型对 S3 API 操作的权限的更多信息，请参阅 Amazon S3 API 操作所需的权限。

几个示例策略展示如何将条件键与 PUT Object 操作结合使用。PUT Object 操作允许特定于访问控制列表 (ACL) 的标头，可用于授予基于 ACL 的权限。通过使用这些条件键，您可以设置条件，来要求用户上传对象时需具有特定的访问权限。您还可以通过 PutObjectAcl 操作授予基于 ACL 的权限。有关更

多信息，请参阅 Amazon S3 Amazon Simple Storage Service API 参考中的 PutObjectAcl。有关 ACL 的更多信息，请参阅 访问控制列表 (ACL) 概述。

主题


- 示例 1：授予要求使用服务器端加密来存储对象的 s3:PutObject 权限
- 示例 2：授予复制对象的 s3:PutObject 权限，但对复制源有限制
- 示例 3：授予对特定对象版本的访问权限
- 示例 4：基于对象标签授予权限
- 示例 5：限制存储桶拥有者的 Amazon Web Services 账户 ID 的访问
- 示例 6：要求最低 TLS 版本
- 示例 7：从 Deny 语句中排除特定主体
- 示例 8：强制客户端根据对象键名称或 ETag 有条件地上传对象


### 示例 1：授予要求使用服务器端加密来存储对象的 **s3:PutObject** 权限

假设账户 A 拥有一个存储桶。账户管理员想要向账户 A 中的用户 Jane 授予上传对象的权限，条件是 Jane 始终请求具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）。账户 A 管理员可使用所示的 `s3:x-amz-server-side-encryption` 条件键来指定此要求。以下 `Condition` 块中的键值对将 `s3:x-amz-server-side-encryption` 条件键和 SSE-S3 (AES256) 指定为加密类型：

```
"Condition": {
     "StringNotEquals": {
         "s3:x-amz-server-side-encryption": "AES256"
     }}
```

使用 Amazon CLI 测试此权限时，必须使用 `--server-side-encryption` 参数添加所需的加密，如以下示例所示。要使用此示例命令，请将 *`user input placeholders`* 替换为您自己的信息。

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key HappyFace.jpg --body c:
\HappyFace.jpg --server-side-encryption "AES256" --profile AccountAadmin
```

### 示例 2：授予复制对象的 **s3:PutObject** 权限，但对复制源有限制

在 PUT 对象请求中，如果指定了源对象，则请求为复制操作（请参阅 CopyObject）。因此，存储桶拥有者可以为用户授予权限以复制具有源限制的对象，例如：

- 只支持从指定的源存储桶（例如 *amzn-s3-demo-source-bucket*）复制对象。
- 支持从指定的源存储桶复制对象，并仅复制其键名称前缀以特定前缀（如 *public/*）开头的对象（例如 *amzn-s3-demo-source-bucket/public/**）。
- 只支持从源存储桶（例如 *amzn-s3-demo-source-bucket/example.jpg*）复制特定的对象。

以下存储桶策略向用户 (*Dave*) 授予 s3:PutObject 权限。此策略支持该用户仅复制满足以下条件的对象：请求包含 s3:x-amz-copy-source 标头，并且标头值指定 */amzn-s3-demo-source-bucket/public/** 键名称前缀。要使用此示例策略，请将 *user input placeholders* 替换为您自己的信息。

```
{
    "Version": "2012-10-17",
    "Statement": [
       {
            "Sid": "cross-account permission to user in your own account",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/Dave"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
        },
        {
            "Sid": "Deny your user permission to upload object if copy source is not /
bucket/prefix",
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/Dave"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-source-bucket/*",
            "Condition": {
                "StringNotLike": {
                    "s3:x-amz-copy-source": "amzn-s3-demo-source-bucket/public/*"
                }
            }
        }
    ]
}
```

使用 Amazon CLI 测试策略

可使用 Amazon CLI `copy-object` 命令测试此权限。可通过添加 `--copy-source` 参数指定源；键名称前缀必须与策略中允许的前缀相匹配。您需要使用 `--profile` 参数为用户 Dave 提供凭证。有关设置 Amazon CLI 的更多信息，请参阅《Amazon S3 API 参考》中的 Developing with Amazon S3 using the Amazon CLI。

```
aws s3api copy-object --bucket amzn-s3-demo-source-bucket --key HappyFace.jpg
--copy-source amzn-s3-demo-source-bucket/public/PublicHappyFace1.jpg --
profile AccountADave
```

授予仅复制特定对象的权限

上述策略使用 `StringNotLike` 条件。要授予仅复制特定对象的权限，必须将条件从 `StringNotLike` 更改为 `StringNotEquals`，然后指定确切的对象键，如以下示例所示。要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
"Condition": {
       "StringNotEquals": {
           "s3:x-amz-copy-source": "amzn-s3-demo-source-bucket/public/
PublicHappyFace1.jpg"
       }
}
```

示例 3：授予对特定对象版本的访问权限

假设账户 A 拥有启用版本控制的存储桶。该存储桶具有 *HappyFace.jpg* 对象的多个版本。账户 A 管理员现在想要向用户 *Dave* 授予仅获得特定对象版本的权限。账户管理员可以通过有条件地向用户 *Dave* 授予 `s3:GetObjectVersion` 权限来实现这一点，如以下示例所示。Condition 块中的键值对指定 `s3:VersionId` 条件键。在这种情况下，要从指定的启用版本控制的存储桶中检索对象，*Dave* 需要知道确切的对象版本 ID。要使用此示例策略，请将 *user input placeholders* 替换为您自己的信息。

有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 GetObject。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "statement1",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/Dave"
```

```
            },
            "Action": "s3:GetObjectVersion",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/HappyFace.jpg"
        },
        {
            "Sid": "statement2",
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/Dave"
            },
            "Action": "s3:GetObjectVersion",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/HappyFace.jpg",
            "Condition": {
                "StringNotEquals": {
                    "s3:VersionId": "AaaHbAQitwiL_h47_44lRO2DDfLlBO5e"
                }
            }
        }
    ]
}
```

使用 Amazon CLI 测试策略

可以使用 Amazon CLI `get-object` 命令以及 `--version-id` 参数（标识要检索的特定对象版本）来测试此策略中的权限。此命令会检索该对象的指定版本，并将其保存到 *OutputFile.jpg* 文件。

```
aws s3api get-object --bucket amzn-s3-demo-bucket --key HappyFace.jpg OutputFile.jpg --
version-id AaaHbAQitwiL_h47_44lRO2DDfLlBO5e --profile AccountADave
```

示例 4：基于对象标签授予权限

有关如何将对象标记条件键与 Amazon S3 操作结合使用的示例，请参阅标签和访问控制策略。

示例 5：限制存储桶拥有者的 Amazon Web Services 账户 ID 的访问

可以使用 `aws:ResourceAccount` 或 `s3:ResourceAccount` 条件键编写 IAM 或虚拟私有云（VPC）端点策略，以限制用户、角色或应用程序对特定 Amazon Web Services 账户 ID 所拥有的 Amazon S3 存储桶的访问权限。可以使用这些条件键来限制 VPC 内的客户端访问非您拥有的存储桶。

但请注意，有些 Amazon 服务依赖于访问 Amazon 托管式存储桶。因此，在 IAM 策略中使用 `aws:ResourceAccount` 或 `s3:ResourceAccount` 键也可能会影响对这些资源的访问。有关更多信息，请参阅以下资源：

- 《Amazon PrivateLink 指南》中的限制对指定 Amazon Web Services 账户中存储桶的访问
- 《Amazon ECR 指南》中的限制对 Amazon ECR 使用的存储桶的访问
- Amazon 指南中的为 Amazon Systems Manager 托管式 Amazon S3 存储桶提供对 Systems Manager 的所需访问权限

有关 `aws:ResourceAccount` 和 `s3:ResourceAccount` 条件键的更多信息以及演示如何使用它们的示例，请参阅 Amazon 存储博客 中的 Limit access to Amazon S3 buckets owned by specific Amazon Web Services 账户。

示例 6：要求最低 TLS 版本

可以使用 `s3:TlsVersion` 条件键来编写 IAM 策略、虚拟私有云端点（VPCE）策略或存储桶策略，以便根据客户端使用的 TLS 版本，限制用户或应用程序对 Amazon S3 存储桶的访问权限。您可以使用此条件键来编写要求最低 TLS 版本的策略。

Example

以下示例存储桶策略拒绝 由 TLS 版本低于 1.2（例如 1.1 或 1.0）的客户端发出的 `PutObject` 请求。要使用此示例策略，请将 *`user input placeholders`* 替换为您自己的信息。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket1",
                "arn:aws:s3:::amzn-s3-demo-bucket1/*"
            ],
            "Condition": {
                "NumericLessThan": {
                    "s3:TlsVersion": 1.2
                }
            }
        }
    ]
}
```

Example

以下示例存储桶策略支持 由 TLS 版本高于 1.1（例如 1.2、1.3 或更高版本）的客户端发出的 PutObject 请求：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket1",
                "arn:aws:s3:::amzn-s3-demo-bucket1/*"
            ],
            "Condition": {
                "NumericGreaterThan": {
                    "s3:TlsVersion": 1.1
                }
            }
        }
    ]
}
```

示例 7：从 **Deny** 语句中排除特定主体

以下存储桶策略拒绝 s3:GetObject 访问 *amzn-s3-demo-bucket*，但账号为 *123456789012* 的主体除外。要使用此示例策略，请将 *user input placeholders* 替换为您自己的信息。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessFromPrincipalNotInSpecificAccount",
      "Principal": {
        "AWS": "*"
      },
```

```
      "Action": "s3:GetObject",
      "Effect": "Deny",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalAccount": [
            "123456789012"
          ]
        }
      }
    }
  ]
}
```

示例 8：强制客户端根据对象键名称或 ETag 有条件地上传对象

通过有条件写入，可以向 WRITE 请求中添加一个额外的标头，以便为 S3 操作指定前提条件。此标头指定了一个条件，如果不满足该条件，将导致 S3 操作失败。例如，在对象上传期间，可以通过验证存储桶中尚不存在具有相同键名称的对象，来防止覆盖现有数据。也可以在写入对象之前，在 Amazon S3 中检查对象的实体标签（ETag）。

有关使用存储桶策略中的条件强制执行有条件写入的存储桶策略示例，请参阅the section called “强制实施有条件写入”。

示例：适用于存储桶操作的 Amazon S3 条件键

以下示例策略显示了如何将 Amazon S3 特定的条件键用于存储桶操作。

主题


- 示例 1：授予 s3:GetObject 权限，但对 IP 地址指定了条件
- 示例 2：获取存储桶中具有特定前缀的对象列表
- 示例 3：设置最大键数


示例 1：授予 **s3:GetObject** 权限，但对 IP 地址指定了条件

如果请求源自特定的 IP 地址范围（例如 *192.0.2.**），则可以向经过身份验证的用户授予使用 s3:GetObject 操作的权限，除非此 IP 地址是您要排除的 IP 地址（例如 *192.0.2.188*）。在 Condition 块中，IpAddress 和 NotIpAddress 为条件，而每个条件均提供了一个键值对用于评

估。此示例中的两个键值对均使用 aws:SourceIp Amazon 范围内的键。要使用此示例策略，请将 *user input placeholders* 替换为您自己的信息。

> **Note**
>
> 在 Condition 块中指定的 IPAddress 和 NotIpAddress 键值使用 RFC 4632 中描述的 CIDR 表示法。有关更多信息，请参阅 http://www.rfc-editor.org/rfc/rfc4632.txt。

```
{
    "Version": "2012-10-17",
    "Id": "S3PolicyId1",
    "Statement": [
        {
            "Sid": "statement1",
            "Effect": "Allow",
            "Principal": "*",
            "Action":"s3:GetObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition" : {
                "IpAddress" : {
                    "aws:SourceIp": "192.0.2.0/24"
                },
                "NotIpAddress" : {
                    "aws:SourceIp": "192.0.2.188/32"
                }
            }
        }
    ]
}
```

您还可以在 Amazon S3 策略中使用其他 Amazon 范围的条件键。例如，您可以在适用于 VPC 端点的存储桶策略中指定 aws:SourceVpce 和 aws:SourceVpc 条件键。有关特定示例，请参阅使用存储桶策略控制从 VPC 端点的访问。

> **Note**
>
> 对于某些 Amazon 全局条件键，仅支持某些资源类型。因此，请检查 Amazon S3 是否支持您要使用的全局条件键和资源类型，或者是否需要改用 Amazon S3 特定的条件键。有关 Amazon S3 的受支持资源类型和条件键的完整列表，请参阅《Service Authorization Reference》中的 Actions, resources, and condition keys for Amazon S3。

有关按 S3 资源类型对 S3 API 操作的权限的更多信息，请参阅 Amazon S3 API 操作所需的权限。

示例 2：获取存储桶中具有特定前缀的对象列表

可以使用 s3:prefix 条件键将 ListObjectsV2 API 操作的响应限制为具有特定前缀的键名称。如果您是存储桶拥有者，则可以使用此条件键来限定用户仅列出存储桶中特定前缀的内容。如果存储桶中的对象是按键名称前缀整理的，则 s3:prefix 条件键很有用。

Amazon S3 控制台使用键名前缀来显示文件夹概念。只有控制台支持文件夹的概念；Amazon S3 API 仅支持存储桶和对象。例如，如果您有键名称为 *public/object1.jpg* 和 *public/object2.jpg* 的两个对象，则控制台会在 *public* 文件夹下显示这些对象。在 Amazon S3 API 中，这些是带有前缀的对象，而不是文件夹中的对象。有关使用前缀和分隔符筛选访问权限的更多信息，请参阅 使用用户策略控制对存储桶的访问。

在以下场景中，存储桶拥有者和用户所属的父账户相同。因此，存储桶拥有者可以使用存储桶策略或用户策略来授予访问权限。有关可以与 ListObjectsV2 API 操作结合使用的其它条件键的更多信息，请参阅 ListObjectsV2。

> **Note**
>
> 如果该存储桶启用了版本控制，要列出该存储桶中的对象，必须在以下策略中授予 s3:ListBucketVersions 权限，而不是 s3:ListBucket 权限。s3:ListBucketVersions 权限还支持 s3:prefix 条件键。

用户策略

以下用户策略通过一条 Condition 语句来授予 s3:ListBucket 权限（请参阅 ListObjectsV2），该语句要求用户在请求中指定值为 *projects* 的前缀。要使用此示例策略，请将 *user input placeholders* 替换为您自己的信息。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"statement1",
         "Effect":"Allow",
```

```
         "Action": "s3:ListBucket",
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket",
         "Condition" : {
             "StringEquals" : {
                 "s3:prefix": "projects"
             }
          }
       },
      {
         "Sid":"statement2",
         "Effect":"Deny",
         "Action": "s3:ListBucket",
         "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
         "Condition" : {
             "StringNotEquals" : {
                 "s3:prefix": "projects"
             }
          }
       }
    ]
}
```

Condition 语句限制用户只列出带有 *projects* 前缀的对象键。添加的显式 Deny 语句将拒绝用户列出具有其它任何前缀的键，无论该用户可能具有哪些其它权限。例如，通过更新先前的用户策略或通过存储桶策略，该用户可能能够获得列出对象键而无任何限制的权限。由于显式 Deny 语句始终覆盖 Allow 语句，因此，如果用户尝试列出除带有 *projects* 前缀的键以外的其它键，则请求将被拒绝。

存储桶策略

如果将 Principal 元素添加到上述的用户策略，确定用户，则现在您就拥有了存储桶策略，如以下示例所示。要使用此示例策略，请将 *user input placeholders* 替换为您自己的信息。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"statement1",
         "Effect":"Allow",
         "Principal": {
            "AWS": "arn:aws:iam::123456789012:user/bucket-owner"
         },
         "Action":  "s3:ListBucket",
         "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
```

```
         "Condition" : {
             "StringEquals" : {
                 "s3:prefix": "projects"
             }
          }
       },
      {
         "Sid":"statement2",
         "Effect":"Deny",
         "Principal": {
            "AWS": "arn:aws:iam::123456789012:user/bucket-owner"
         },
         "Action": "s3:ListBucket",
         "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
         "Condition" : {
             "StringNotEquals" : {
                 "s3:prefix": "projects"
             }
          }
       }
    ]
}
```

使用 Amazon CLI 测试策略

可使用以下 `list-object` Amazon CLI 命令测试此策略。在该命令中，使用 `--profile` 参数提供用户凭证。有关设置和使用 Amazon CLI 的更多信息，请参阅《Amazon S3 API 参考》中的 Developing with Amazon S3 using the Amazon CLI。

```
aws s3api list-objects --bucket amzn-s3-demo-bucket --prefix projects --
profile AccountA
```

示例 3：设置最大键数

可以使用 `s3:max-keys` 条件键来设置请求者可以在 ListObjectsV2 或 ListObjectVersions 请求中返回的最大键数。默认情况下，这些 API 操作可返回最多 1000 个键。有关可与 `s3:max-keys` 一起使用的数字条件运算符的列表和相关示例，请参阅 IAM 用户指南中的数字条件运算符。

## Amazon S3 基于身份的策略

默认情况下，用户和角色没有创建或修改 Amazon S3 资源的权限。他们也无法使用 Amazon Web Services Management Console、Amazon Command Line Interface (Amazon CLI) 或 Amazon API 执

行任务。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅《IAM 用户指南》中的创建 IAM 策略（控制台）。

有关 Amazon S3 定义的操作和资源类型的详细信息，包括每种资源类型的 ARN 格式，请参阅《Service Authorization Reference》中的 Actions, resources, and condition keys for Amazon S3。

有关按 S3 资源类型对 S3 API 操作的权限的更多信息，请参阅 Amazon S3 API 操作所需的权限。

主题


- 策略最佳实践
- 使用用户策略控制对存储桶的访问
- Amazon S3 基于身份的策略示例


## 策略最佳实践

基于身份的策略确定某个人是否可以创建、访问或删除您账户中的 Amazon S3 资源。这些操作可能会使 Amazon Web Services 账户 产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- Amazon 托管式策略及转向最低权限许可入门 – 要开始向用户和工作负载授予权限，请使用 Amazon 托管式策略来为许多常见使用场景授予权限。您可以在 Amazon Web Services 账户 中找到这些策略。我们建议通过定义特定于您的使用场景的 Amazon 客户托管式策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 Amazon 托管式策略或工作职能的 Amazon 托管式策略。
- 应用最低权限：在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM 策略中的条件进一步限制访问权限：您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果通过特定 Amazon Web Services 服务（例如 Amazon CloudFormation）使用服务操作，您还可以使用条件来授予对服务操作的访问权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言（JSON）和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM Access Analyzer 验证策略。

- 需要多重身份验证（MFA）：如果您所处的场景要求您的 Amazon Web Services 账户 中有 IAM 用户或根用户，请启用 MFA 来提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的使用 MFA 保护 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实践。

## 使用用户策略控制对存储桶的访问

本演练将介绍用户许可在 Amazon S3 中的使用方式。在该示例中，您创建一个具有文件夹的存储桶。然后，在您的 Amazon Web Services 账户 中创建 Amazon Identity and Access Management IAM 用户，并为这些用户授予对 Amazon S3 存储桶以及其中文件夹的增量权限。

主题


- 存储桶和文件夹基础知识
- 演练摘要
- 准备演练
- 步骤 1：创建存储桶
- 步骤 2：创建 IAM 用户和组
- 步骤 3：确认 IAM 用户没有任何权限
- 步骤 4：授予组级权限
- 步骤 5：授予 IAM 用户 Alice 特定的权限
- 步骤 6：授予 IAM 用户 Bob 特定的权限
- 步骤 7：确保 Private 文件夹的安全
- 步骤 8：清除
- 相关资源


### 存储桶和文件夹基础知识

Amazon S3 数据模型是一种扁平结构：您创建一个存储桶，存储桶存储对象。没有子存储桶或子文件夹层次结构，但您可以模拟文件夹层次结构。Amazon S3 控制台等工具可以显示存储桶中这些逻辑文件夹和子文件夹的视图。

控制台显示名为 `companybucket` 的存储桶具有三个文件夹（`Private`、`Development` 和 `Finance`）和一个对象（`s3-dg.pdf`）。控制台使用对象名称 (键) 来创建文件夹和子文件夹的逻辑层次结构。考虑以下示例：

- 在创建 Development 文件夹时，控制台使用 Development/ 键创建一个对象。请注意尾部斜杠 (/) 分隔符。
- 在上传 Projects1.xls 文件夹中名为 Development 的对象时，控制台上传该对象并为其分配 Development/Projects1.xls 键。

  在该键值中，Development 是前缀，/ 是分隔符。Amazon S3 API 在运行时支持前缀和分隔符。例如，您可以使用特定的前缀和分隔符，从存储桶获取所有对象的列表。在控制台上，在打开 Development 文件夹时，控制台列出该文件夹中的对象。在以下示例中，Development 文件夹包含一个对象。

  当控制台列出 Development 存储桶中的 companybucket 文件夹时，它向 Amazon S3 发送一个请求，在请求中指定 Development 前缀和 / 分隔符。控制台的反应方式与计算机文件系统内的文件夹列表的反应方式相似。上一个示例显示，存储桶 companybucket 拥有一个带键值 Development/Projects1.xls 的对象。

控制台使用对象键来推断逻辑层次结构。Amazon S3 没有物理层次结构。Amazon S3 只拥有包含平面文件结构中的对象的存储桶。使用 Amazon S3 API 创建对象时，您可以使用暗指逻辑层次结构的对象键。在创建对象的逻辑层次结构时，您可以管理对单个文件夹的访问，如本演练中所示。

在开始之前，请确保您熟悉根级 存储桶内容概念。假设 companybucket 存储桶具有以下对象：

- Private/privDoc1.txt
- Private/privDoc2.zip
- Development/project1.xls
- Development/project2.xls
- Finance/Tax2011/document1.pdf
- Finance/Tax2011/document2.pdf
- s3-dg.pdf

这些对象键创建一个逻辑层次结构，将 Private、Development 和 Finance 作为根级文件夹并将 s3-dg.pdf 作为根级对象。在 Amazon S3 控制台上选择存储桶名称时，将显示根级项目。控制台将顶级前缀（Private/、Development/ 和 Finance/）显示为根级文件夹。s3-dg.pdf 对象键没有前缀，因此，它显示为根级项目。

### 演练摘要

在本演练中，您创建一个包含三个文件夹（Private、Development 和 Finance）的存储桶。

您拥有两个用户，Alice 和 Bob。您希望 Alice 仅访问 Development 文件夹，并希望 Bob 仅访问 Finance 文件夹。您希望将 Private 文件夹内容保密。在本演练中，您创建 IAM 用户（该示例使用用户名 Alice 和 Bob）并为其授予所需的权限以管理访问。

IAM 还支持创建用户组以及授予适用于组中所有用户的组级许可。这将帮助您更好地管理权限。在该练习中，Alice 和 Bob 需要具有一些相同的权限。因此，您还创建一个名为 Consultants 的组，然后将 Alice 和 Bob 添加到该组中。您先将一个组策略附加到该组以授予权限。然后，您将策略附加到特定用户以添加用户特定的权限。

> **Note**
>
> 本演练将 companybucket 作为存储桶名称，将 Alice 和 Bob 作为 IAM 用户并将 Consultants 作为组名称。由于 Amazon S3 要求存储桶名称全局唯一，因此，您必须将存储桶名称替换为您创建的名称。

### 准备演练

在该示例中，您使用 Amazon Web Services 账户 凭证来创建 IAM 用户。一开始，这些用户没有权限。您逐步为这些用户授予权限以执行特定的 Amazon S3 操作。为了测试这些权限，您使用每个用户的凭证登录到控制台。由于您不停地以 Amazon Web Services 账户拥有者身份授予许可，并以 IAM 用户身份测试这些许可，因此需要登录和注销，每次都要使用不同的凭证。您可以使用一个浏览器执行该测试，但如果使用两个不同的浏览器，则可以加快该过程的速度。使用您的 Amazon Web Services 账户 凭证通过一个浏览器连接到 Amazon Web Services Management Console，并使用 IAM 用户凭证通过另一个浏览器进行连接。

要使用 Amazon Web Services 账户 凭证登录 Amazon Web Services Management Console，请转到 https://console.aws.amazon.com/。IAM 用户无法使用相同的链接登录。IAM 用户必须使用支持 IAM 的登录页面。作为账户所有者，您可以向您的用户提供此链接。

有关 IAM 的更多信息，请参阅 IAM 用户指南中的 Amazon Web Services Management Console 登录页面。

向 IAM 用户提供登录链接的步骤

1. 登录 Amazon Web Services Management Console，单击 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。

2. 在 Navigation (导航) 窗格中，请选择 IAM Dashboard (IAM 控制面板)。
3. 记下 IAM users sign in link: (IAM 用户登录链接：) 下的 URL。向 IAM 用户提供此链接，允许他们使用 IAM 用户名称和密码登录控制台。

步骤 1：创建存储桶

在该步骤中，您使用 Amazon Web Services 账户 凭证登录到 Amazon S3 控制台，创建一个存储桶，在该存储桶中添加文件夹，然后在每个文件夹中上传一个或两个示例文档。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 创建存储桶。

   如需分步指导，请参阅 创建通用存储桶。
3. 将一个文档上传到存储桶。

   该练习假定您在该存储桶的根级别具有 s3-dg.pdf 文档。如果您上传其他文档，请使用其文件名替代 s3-dg.pdf。
4. 将三个名为 Private、Finance 和 Development 的文件夹添加到存储桶中。

   有关创建文件夹的分步说明，请参阅 Amazon Simple Storage Service 用户指南中的 使用文件夹在 Amazon S3 控制台中整理对象>。
5. 将一个或两个文档上传到每个文件夹。

   对于该练习，假设您在每个文件夹中上传了几个文档，从而导致存储桶包含具有以下键的对象：

   - Private/privDoc1.txt
   - Private/privDoc2.zip
   - Development/project1.xls
   - Development/project2.xls
   - Finance/Tax2011/document1.pdf
   - Finance/Tax2011/document2.pdf
   - s3-dg.pdf

   如需分步指导，请参阅 上传对象。

步骤 2：创建 IAM 用户和组

现在使用 IAM 控制台将两个 IAM 用户（Alice 和 Bob）添加到您的 Amazon Web Services 账户。有关分步说明，请参阅《IAM 用户指南》中的在您的 Amazon Web Services 账户中创建 IAM 用户。

还要创建一个名为 Consultants 的管理组。然后，将这两个用户都添加到该组中。有关分步说明，请参阅创建 IAM 用户组。

> **Warning**
>
> 添加用户和组时，请不要为这些用户附加任何授予权限的策略。起初，这些用户没有任何权限。在以下部分中，您逐步授予权限。首先，您必须确保已为这些 IAM 用户分配密码。您使用这些用户凭证测试 Amazon S3 操作，并验证这些权限是否可按预期工作。

有关创建新的 IAM 用户的分步说明，请参阅《IAM 用户指南》中的在您的 Amazon Web Services 账户中创建 IAM 用户。在为本演练创建用户时，请选择 Amazon Web Services Management Console访问并清除编程访问。

有关创建管理组的分步说明，请参阅 IAM 用户指南中的创建第一个 IAM 管理员用户和组。

步骤 3：确认 IAM 用户没有任何权限

如果您使用两个浏览器，现在可以使用第二个浏览器通过 IAM 用户凭证之一登录控制台。

1. 通过使用 IAM 用户登录链接（请参阅向 IAM 用户提供登录链接的步骤），使用任一 IAM 用户凭证登录到 Amazon Web Services Management Console。
2. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。

   验证是否有告知您访问已被拒绝的控制台消息。

现在，您可以开始为用户授予增量权限。首先，您附加一个组策略，以授予两个用户必须具有的权限。

步骤 4：授予组级权限

您希望用户能够执行以下操作：

- 列出父账户拥有的所有存储桶。要执行此操作，Bob 和 Alice 必须拥有执行 s3:ListAllMyBuckets 操作的权限。

- 列出 companybucket 存储桶中的根级项目、文件夹和对象。要执行此操作，Bob 和 Alice 必须拥有在 companybucket 存储桶上执行 s3:ListBucket 操作的权限。

首先，您创建一个授予这些权限的策略，然后将其附加到 Consultants 组。

步骤 4.1：授予列出所有存储桶的权限

在该步骤中，您创建一个托管策略，它为用户授予最低权限，以使他们能够列出父账户拥有的所有存储桶。然后，您将该策略附加到 Consultants 组。在将该托管式策略附加到一个用户或组时，您为该用户或组授予权限以获取父 Amazon Web Services 账户拥有的存储桶列表。

1. 登录 Amazon Web Services Management Console，单击 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。

   > **Note**
   >
   > 由于您要授予用户权限，请使用您的 Amazon Web Services 账户凭证登录，而不是以 IAM 用户身份登录。

2. 创建托管策略。

   a. 在左侧导航窗格中，请选择策略，然后选择创建策略。

   b. 请选择 JSON 选项卡。

   c. 复制以下访问策略，并将其粘贴到策略文本字段中。

   ```
   {
     "Version": "2012-10-17",
     "Statement": [
       {
         "Sid": "AllowGroupToSeeBucketListInTheConsole",
         "Action": ["s3:ListAllMyBuckets"],
         "Effect": "Allow",
         "Resource": ["arn:aws:s3:::*"]
       }
     ]
   }
   ```

   策略是一个 JSON 文档。在文档中，Statement 是一个对象数组，其中每个对象均使用名称/值对的集合来描述权限。之前的策略描述了一个特定的权限。Action 指定访问权限的

类型。在策略中，s3:ListAllMyBuckets 是预定义的 Amazon S3 操作。此操作涵盖了 Amazon S3 GET Service 操作，它可以返回已验证发件人拥有的所有存储桶的列表。Effect 元素值确定是允许还是拒绝特定的权限。

d. 选择 Review Policy（查看策略）。在下一页上，在名称字段中输入 AllowGroupToSeeBucketListInTheConsole，然后选择创建策略。

> **Note**
>
> 摘要条目显示一条消息，以指出该策略不授予任何权限。对于本演练，您可以安全地忽略此消息。

3. 将您创建的 AllowGroupToSeeBucketListInTheConsole 托管策略附加到 Consultants 组。

   有关附加托管式策略的分步说明，请参阅《IAM 用户指南》中的添加和删除 IAM 身份权限。

   您可以将策略文档附加到 IAM 控制台中的 IAM 用户和组。由于您希望两个用户都能够列出存储桶，因此，您将该策略附加到组。

4. 测试权限。

   a. 使用 IAM 用户登录链接（请参阅 向 IAM 用户提供登录链接的步骤），通过任何 IAM 用户凭证登录控制台。

   b. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。

      控制台现在应该会列出所有的存储桶，但不会列出任何存储桶中的对象。

步骤 4.2：允许用户列出存储桶的根级内容

接下来，您允许 Consultants 组中的所有用户列出根级 companybucket 存储桶项目。当用户在 Amazon S3 控制台上选择 company 存储桶时，用户可以看到该存储桶中的根级项目。

> **Note**
>
> 该示例使用 companybucket 以进行说明。您必须使用创建的存储桶的名称。

要了解在您选择存储桶名称时控制台向 Amazon S3 发送的请求、Amazon S3 返回的响应，以及控制台如何解释该响应，请更详细地介绍该过程。

当您选择存储桶名称时，控制台会向 Amazon S3 发送 GET Bucket (List Objects)请求。该请求包括以下参数：

- 将空字符串作为值的 `prefix` 参数。
- 将 `delimiter` 作为值的 `/` 参数。

以下是一个示例请求。

```
GET ?prefix=&delimiter=/ HTTP/1.1
Host: companybucket.s3.amazonaws.com
Date: Wed, 01 Aug  2012 12:00:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:xQE0diMbLRepdf3YB+FIEXAMPLE=
```

Amazon S3 将返回包含以下 `<ListBucketResult/>` 元素的响应。

```
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Name>companybucket</Name>
  <Prefix></Prefix>
  <Delimiter>/</Delimiter>
   ...
  <Contents>
    <Key>s3-dg.pdf</Key>
    ...
  </Contents>
  <CommonPrefixes>
    <Prefix>Development/</Prefix>
  </CommonPrefixes>
  <CommonPrefixes>
    <Prefix>Finance/</Prefix>
  </CommonPrefixes>
  <CommonPrefixes>
    <Prefix>Private/</Prefix>
  </CommonPrefixes>
</ListBucketResult>
```

键 `s3-dg.pdf` 对象不包含斜杠 (/) 分隔符，并且 Amazon S3 在 `<Contents>` 元素中返回该键。但是，示例存储桶中的所有其他键都包含 `/` 分隔符。Amazon S3 将组合这些密钥，并在指定的 `<CommonPrefixes>` 分隔符首次出现时，为每个不同前缀值 `Development/`、`Finance/` 和 `Private/`（它们是这些密钥开头的子字符串）返回 `/` 元素。

控制台将解释该结果并将根级项目显示为三个文件夹和一个对象键。

如果 Bob 或 Alice 打开 Development (开发) 文件夹，控制台将向 Amazon S3 发送 GET Bucket (List Objects) 请求，并将 prefix 和 delimiter 参数设置为以下值：

- 具有 prefix 值的 Development/ 参数。
- 具有“delimiter”值的 / 参数。

作为响应，Amazon S3 将返回对象密钥，该密钥以指定的前缀开头。

```
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Name>companybucket</Name>
  <Prefix>Development</Prefix>
  <Delimiter>/</Delimiter>
   ...
  <Contents>
    <Key>Project1.xls</Key>
    ...
  </Contents>
  <Contents>
    <Key>Project2.xls</Key>
    ...
  </Contents>
</ListBucketResult>
```

控制台显示这些对象键。

现在，我们返回以授予用户权限，以便列出根级存储桶项目。要列出存储桶内容，用户需要调用 s3:ListBucket 操作的权限，如下面的策略语句中所述。为了确保他们仅看到根级内容，您添加一个条件以要求用户必须在请求中指定空 prefix，即不允许他们双击任何根级文件夹。最后，您添加一个条件以要求用户请求包含值为“delimiter”的 / 参数，从而要求进行文件夹样式的访问。

```
{
  "Sid": "AllowRootLevelListingOfCompanyBucket",
  "Action": ["s3:ListBucket"],
  "Effect": "Allow",
  "Resource": ["arn:aws:s3:::companybucket"],
  "Condition":{
         "StringEquals":{
             "s3:prefix":[""], "s3:delimiter":["/"]
                       }
              }
}
```

在 Amazon S3 控制台上选择一个存储桶时，控制台先发送 GET Bucket location 请求以查找部署了该存储桶的 Amazon Web Services 区域。然后，控制台使用该存储桶的区域特定端点以发送 GET Bucket (List Objects)请求。因此，如果用户要使用控制台，您必须授予 s3:GetBucketLocation 操作权限，如以下策略语句中所示。

```
{
   "Sid": "RequiredByS3Console",
   "Action": ["s3:GetBucketLocation"],
   "Effect": "Allow",
   "Resource": ["arn:aws:s3:::*"]
}
```

允许用户列出根级存储桶内容的步骤

1. 登录 Amazon Web Services Management Console，单击 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。

   使用 Amazon Web Services 账户凭证，而不是 IAM 用户的凭证登录控制台。

2. 将附加到 Consultants 组的现有 AllowGroupToSeeBucketListInTheConsole 托管策略替换为以下策略，这还会允许执行 s3:ListBucket 操作。记得将策略 Resource 中的 *companybucket* 替换为您的存储桶的名称。

   有关分步说明，请参阅《IAM 用户指南》中的编辑 IAM 策略。在按照分步说明进行操作时，请务必执行将更改应用于策略附加到的所有主体实体的步骤。

   ```
   {
     "Version": "2012-10-17",
     "Statement": [
        {
          "Sid":
    "AllowGroupToSeeBucketListAndAlsoAllowGetBucketLocationRequiredForListBucket",
          "Action": [ "s3:ListAllMyBuckets", "s3:GetBucketLocation" ],
          "Effect": "Allow",
          "Resource": [ "arn:aws:s3:::*"  ]
        },
        {
          "Sid": "AllowRootLevelListingOfCompanyBucket",
          "Action": ["s3:ListBucket"],
          "Effect": "Allow",
          "Resource": ["arn:aws:s3:::companybucket"],
          "Condition":{
   ```

```
            "StringEquals":{
                  "s3:prefix":[""], "s3:delimiter":["/"]
                        }
                  }
     }
  ]
}
```

3. 测试更新的权限。

   a. 使用 IAM 用户登录链接（请参阅向 IAM 用户提供登录链接的步骤）登录 Amazon Web Services Management Console。

      通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。

   b. 请选择您创建的存储桶，控制台将显示根级存储桶项目。如果您选择存储桶中的任何文件夹，则无法看到文件夹内容，因为您尚未授予这些权限。

当用户使用 Amazon S3 控制台时，此测试会成功。在控制台上选择一个存储桶时，控制台实施发送一个请求，其中包含将空字符串作为值的 `prefix` 参数以及将“`delimiter`”作为值的 `/` 参数。

步骤 4.3：组策略总结

您所添加的组策略的实际结果是授予 IAM 用户 Alice 和 Bob 以下最低许可：

- 列出父账户拥有的所有存储桶。
- 查看 `companybucket` 存储桶中的根级项目。

不过，用户仍然只能执行很少的操作。接下来，您授予用户特定的权限，如下所示：

- 允许 Alice 在 `Development` 文件夹中获取和放置对象。
- 允许 Bob 在 `Finance` 文件夹中获取和放置对象。

对于用户特定的权限，您需要将策略附加到特定的用户，而不是附加到组。在以下部分中，您为 Alice 授予权限以在 `Development` 文件夹中工作。您可以重复这些步骤，以便为 Bob 授予类似权限以在 `Finance` 文件夹中工作。

步骤 5：授予 IAM 用户 Alice 特定的权限

现在，您为 Alice 授予额外的权限，以便她可以查看 `Development` 文件夹内容以及在该文件夹中获取和放置对象。

步骤 5.1：授予 IAM 用户 Alice 列出 development 文件夹内容的权限

要让 Alice 列出 `Development` 文件夹内容，您必须将一个策略应用于用户 Alice 以授予对 `s3:ListBucket` 存储桶执行 `companybucket` 操作的权限，但前提是请求包含 `Development/` 前缀。您希望仅将该策略应用于 Alice 用户，因此，您使用一个内联策略。有关内联策略的更多信息，请参阅《IAM 用户指南》中的 托管式策略与内联策略。

1. 登录 Amazon Web Services Management Console，单击 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。

   使用 Amazon Web Services 账户凭证，而不是 IAM 用户的凭证登录控制台。

2. 创建一个内联策略，以便为 Alice 用户授予权限以列出 `Development` 文件夹内容。

   a. 在左侧导航窗格中，请选择用户。

   b. 请选择用户名 Alice。

   c. 在用户详细信息页面上，请选择权限选项卡，然后选择添加内联策略。

   d. 请选择 JSON 选项卡。

   e. 复制以下策略，并将其粘贴到策略文本字段中。

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
      "Sid": "AllowListBucketIfSpecificPrefixIsIncludedInRequest",
      "Action": ["s3:ListBucket"],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::companybucket"],
      "Condition":{  "StringLike":{"s3:prefix":["Development/*"] }
       }
    }
  ]
}
```

   f. 选择 Review Policy（查看策略）。在下一页上，在名称字段中输入一个名称，然后选择创建策略。

3. 测试对 Alice 的权限的更改：

   a. 使用 IAM 用户登录链接（请参阅向 IAM 用户提供登录链接的步骤）登录 Amazon Web Services Management Console。

b. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。

c. 在 Amazon S3 控制台中，验证 Alice 能否查看存储桶中 Development/ 文件夹中的对象列表。

当用户单击 /Development 文件夹以查看其中的对象列表时，Amazon S3 控制台会向 Amazon S3 发送 ListObjects 请求并使用前缀 /Development。由于用户已被授予许可，可以查看使用前缀 Development 和分隔符 / 的对象列表，因此 Amazon S3 将返回使用密钥前缀 Development/ 的对象列表，并且控制台将显示该列表。

步骤 5.2：授予 IAM 用户 Alice 在 development 文件夹中获取和放置对象的权限

要让 Alice 在 Development 文件夹中获取和放置对象，她需要具有调用 s3:GetObject 和 s3:PutObject 操作的权限。以下策略语句授予这些权限，但前提是请求包含值为 prefix 的 Development/ 参数。

```
{
    "Sid":"AllowUserToReadWriteObjectData",
    "Action":["s3:GetObject", "s3:PutObject"],
    "Effect":"Allow",
    "Resource":["arn:aws:s3:::companybucket/Development/*"]
 }
```

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。

   使用 Amazon Web Services 账户凭证，而不是 IAM 用户的凭证登录控制台。

2. 编辑您在上一步中创建的内联策略。

   a. 在左侧导航窗格中，请选择用户。

   b. 请选择 Alice 用户名。

   c. 在用户详细信息页面上，请选择权限选项卡，然后展开内联策略部分。

   d. 在上一步中创建的策略名称旁边，请选择编辑策略。

   e. 复制以下策略，并将其粘贴到策略文本字段中，从而替换现有的策略。

```
{
     "Version": "2012-10-17",
     "Statement":[
```

```
      {
         "Sid":"AllowListBucketIfSpecificPrefixIsIncludedInRequest",
         "Action":["s3:ListBucket"],
         "Effect":"Allow",
         "Resource":["arn:aws:s3:::companybucket"],
         "Condition":{
            "StringLike":{"s3:prefix":["Development/*"]
            }
         }
      },
      {
        "Sid":"AllowUserToReadWriteObjectDataInDevelopmentFolder",
        "Action":["s3:GetObject", "s3:PutObject"],
        "Effect":"Allow",
        "Resource":["arn:aws:s3:::companybucket/Development/*"]
      }
   ]
}
```

3. 测试更新的策略：

   a. 使用 IAM 用户登录链接（请参阅向 IAM 用户提供登录链接的步骤）登录 Amazon Web Services Management Console。

   b. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。

   c. 在 Amazon S3 控制台中，验证 Alice 现在能否在 Development 文件夹中添加和下载对象。

步骤 5.3：显式拒绝 IAM 用户 Alice 对存储桶中其他任何文件夹的权限

用户 Alice 现在可以列出 companybucket 存储桶中的根级内容。她还可以在 Development 文件夹中获取和放置对象。如果您确实想要严格控制访问权限，可以显式拒绝 Alice 对存储桶中其他任何文件夹的访问。若存在任何其他策略（存储桶策略或 ACL），而且它们授予了 Alice 访问存储桶中任何其他文件夹的权限，此显式拒绝将覆盖这些权限。

您可以向用户 Alice 策略添加以下声明：要求 Alice 发送到 Amazon S3 的所有请求均包含 prefix 参数，该参数的值可为 Development/* 或空字符串。

```
{
   "Sid": "ExplicitlyDenyAnyRequestsForAllOtherFoldersExceptDevelopment",
   "Action": ["s3:ListBucket"],
   "Effect": "Deny",
```

```
   "Resource": ["arn:aws:s3:::companybucket"],
   "Condition":{  "StringNotLike": {"s3:prefix":["Development/*",""] },
                  "Null"         : {"s3:prefix":false }
    }
}
```

在 Condition 块中具有两个条件表达式。这些条件表达式的结果将使用逻辑 AND 合并在一起。如果两种条件均为真，组合条件的结果才为真。由于该策略中的 Effect 为 Deny，因此，在 Condition 计算结果为 true 时，用户无法执行指定的 Action。

- Null 条件表达式确保来自 Alice 的请求包含 prefix 参数。

  prefix 参数要求类似文件夹的访问权限。如果您发送的请求没有包含 prefix 参数，Amazon S3 将返回所有的对象密钥。

  如果请求包含具有空值的 prefix 参数，则表达式的计算结果为 true，因此，整个 Condition 的计算结果为 true。您必须允许将空字符串作为 prefix 参数的值。在前面讨论的内容中，回顾了采用与前面讨论中控制台相同的方式，通过允许空字符串使 Alice 能够检索根级存储桶项目。有关更多信息，请参阅 步骤 4.2：允许用户列出存储桶的根级内容。
- StringNotLike 条件表达式确保在指定了 prefix 参数值并且不是 Development/* 时，请求失败。

执行上一节中的步骤，并再次更新为 Alice 用户创建的内联策略。

复制以下策略，并将其粘贴到策略文本字段中，从而替换现有的策略。

```
{
   "Version": "2012-10-17",
   "Statement":[
      {
         "Sid":"AllowListBucketIfSpecificPrefixIsIncludedInRequest",
         "Action":["s3:ListBucket"],
         "Effect":"Allow",
         "Resource":["arn:aws:s3:::companybucket"],
         "Condition":{
            "StringLike":{"s3:prefix":["Development/*"]
            }
         }
      },
      {
        "Sid":"AllowUserToReadWriteObjectDataInDevelopmentFolder",
```

```
        "Action":["s3:GetObject", "s3:PutObject"],
        "Effect":"Allow",
        "Resource":["arn:aws:s3:::companybucket/Development/*"]
      },
      {
         "Sid": "ExplicitlyDenyAnyRequestsForAllOtherFoldersExceptDevelopment",
         "Action": ["s3:ListBucket"],
         "Effect": "Deny",
         "Resource": ["arn:aws:s3:::companybucket"],
         "Condition":{  "StringNotLike": {"s3:prefix":["Development/*",""] },
                        "Null"         : {"s3:prefix":false }
          }
      }
   ]
}
```

步骤 6：授予 IAM 用户 Bob 特定的权限

现在，您希望为 Bob 授予 Finance 文件夹的权限。执行您之前为 Alice 授予权限时使用的步骤，但将 Development 文件夹替换为 Finance 文件夹。如需分步指导，请参阅 步骤 5：授予 IAM 用户 Alice 特定的权限。

步骤 7：确保 Private 文件夹的安全

在此示例中，您有两个用户。您已授予了所需最低组级权限，仅当确实需要单个用户级别的权限时才授予用户级权限。此方法有助于最大程度地降低管理权限的工作量。随着用户数的增加，管理权限工作将变得极为繁重。例如，您不希望该示例中的任何用户访问 Private 文件夹内容。您如何确保不会意外地为用户授予 Private 文件夹的权限？ 您可以添加一个策略，显式拒绝对该文件夹的访问。显式拒绝将覆盖任何其他权限。

要确保 Private 文件夹保密，您可以将以下两个拒绝语句添加到组策略中：

- 添加以下声明以显式拒绝对 Private 文件夹 (companybucket/Private/*) 中的资源执行任何操作。

```
{
  "Sid": "ExplictDenyAccessToPrivateFolderToEveryoneInTheGroup",
  "Action": ["s3:*"],
  "Effect": "Deny",
  "Resource":["arn:aws:s3:::companybucket/Private/*"]
}
```

- 若请求指定了 `Private/` 前缀，您也可以拒绝列出对象操作所需的权限。在控制台上，如果 Bob 或 Alice 打开 `Private` 文件夹，该策略导致 Amazon S3 返回错误响应。

```
{
  "Sid": "DenyListBucketOnPrivateFolder",
  "Action": ["s3:ListBucket"],
  "Effect": "Deny",
  "Resource": ["arn:aws:s3:::*"],
  "Condition":{
      "StringLike":{"s3:prefix":["Private/"]}
   }
}
```

将 `Consultants` 组策略替换为包含上述拒绝语句的更新策略。在应用更新的策略后，组中的任何用户都无法访问存储桶中的 `Private` 文件夹。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。

   使用 Amazon Web Services 账户凭证，而不是 IAM 用户的凭证登录控制台。

2. 将附加到 `Consultants` 组的现有 `AllowGroupToSeeBucketListInTheConsole` 托管策略替换为以下策略。记得将策略中的 *`companybucket`* 替换为您的存储桶的名称。

   有关说明，请参阅《IAM 用户指南》中的编辑客户托管策略。按照说明操作时，请确保按照指示操作，以便将您的更改应用到策略附加到的所有主体实体。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid":
 "AllowGroupToSeeBucketListAndAlsoAllowGetBucketLocationRequiredForListBucket",
      "Action": ["s3:ListAllMyBuckets", "s3:GetBucketLocation"],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::*"]
    },
    {
      "Sid": "AllowRootLevelListingOfCompanyBucket",
      "Action": ["s3:ListBucket"],
      "Effect": "Allow",
```

```
      "Resource": ["arn:aws:s3:::companybucket"],
      "Condition":{
          "StringEquals":{"s3:prefix":[""]}
       }
    },
    {
      "Sid": "RequireFolderStyleList",
      "Action": ["s3:ListBucket"],
      "Effect": "Deny",
      "Resource": ["arn:aws:s3:::*"],
      "Condition":{
          "StringNotEquals":{"s3:delimiter":"/"}
       }
     },
    {
      "Sid": "ExplictDenyAccessToPrivateFolderToEveryoneInTheGroup",
      "Action": ["s3:*"],
      "Effect": "Deny",
      "Resource":["arn:aws:s3:::companybucket/Private/*"]
    },
    {
      "Sid": "DenyListBucketOnPrivateFolder",
      "Action": ["s3:ListBucket"],
      "Effect": "Deny",
      "Resource": ["arn:aws:s3:::*"],
      "Condition":{
          "StringLike":{"s3:prefix":["Private/"]}
       }
    }
  ]
}
```

步骤 8：清除

要进行清除，请打开 IAM 控制台并移除用户 Alice 和 Bob。有关分步说明，请参阅《IAM 用户指南》中的删除 IAM 用户。

为了确保不再对您收取存储费用，您还应删除为该练习创建的对象和存储桶。

相关资源

- 《IAM 用户指南》中的 管理 IAM policy

# Amazon S3 基于身份的策略示例

本节介绍用于控制对 Amazon S3 的访问权限的几个基于 Amazon Identity and Access Management（IAM）身份的策略示例。有关存储桶策略（基于资源的策略）的示例，请参阅 Amazon S3 的存储桶策略。有关 IAM 策略语言的信息，请参阅Amazon S3 中的策略和权限。

如果以编程方式使用以下示例策略，它们将正常工作。不过，要在 Amazon S3 控制台中使用这些策略，您必须授予控制台所需的额外权限。有关使用策略（例如与 Amazon S3 控制台一起使用的策略）的信息，请参阅 使用用户策略控制对存储桶的访问。

有关按 S3 资源类型对 S3 API 操作的权限的更多信息，请参阅 Amazon S3 API 操作所需的权限。

主题


- 允许 IAM 用户访问某个存储桶
- 允许每个 IAM 用户访问存储桶中的文件夹
- 允许组在 Amazon S3 中拥有共享的文件夹
- 允许所有用户读取存储桶的某个部分中的对象
- 允许合作伙伴将文件放置到存储桶的特定部分中
- 限制对特定 Amazon Web Services 账户中 Amazon S3 存储桶的访问
- 限制企业单位内对 Amazon S3 存储桶的访问
- 限制对企业内 Amazon S3 存储桶的访问
- 为 Amazon Web Services 账户授予检索 PublicAccessBlock 配置的权限
- 将存储桶的创建限制在一个区域


## 允许 IAM 用户访问某个存储桶

在本示例中，您需要授予您的 Amazon Web Services 账户中的 IAM 用户访问一个存储桶 *amzn-s3-demo-bucket1* 的权限，以便该用户能够添加、更新和删除对象。

除了授予该用户 `s3:PutObject`、`s3:GetObject` 和 `s3:DeleteObject` 权限外，此策略还授予 `s3:ListAllMyBuckets`、`s3:GetBucketLocation` 和 `s3:ListBucket` 权限。这些是控制台所需的其他权限。此外，`s3:PutObjectAcl` 和 `s3:GetObjectAcl` 操作需要能够在控制台中复制、剪切和粘贴对象。有关向用户授予权限并使用控制台测试这些权限的示例演练，请参阅 使用用户策略控制对存储桶的访问。

```
{
   "Version":"2012-10-17",
```

```
   "Statement":[
      {
         "Effect":"Allow",
         "Action": "s3:ListAllMyBuckets",
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":["s3:ListBucket","s3:GetBucketLocation"],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1"
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:GetObject",
            "s3:GetObjectAcl",
            "s3:DeleteObject"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/*"
      }
   ]
}
```

允许每个 IAM 用户访问存储桶中的文件夹

在本示例中，您需要两个 IAM 用户（Mary 和 Carlos）具有访问存储桶 *amzn-s3-demo-bucket1* 的权限，以便他们可以添加、更新和删除对象。但是，您想要限制每个用户对存储桶中单个前缀（文件夹）的访问权限。您可以使用与其用户名匹配的名称创建文件夹。

```
amzn-s3-demo-bucket1
   Mary/
   Carlos/
```

要授予每个用户仅可以访问其文件夹的权限，您可以为每个用户编写策略，然后分别附加它。例如，您可以将以下策略附加到用户 Mary，以允许她对 *amzn-s3-demo-bucket1*/*Mary* 文件夹拥有特定的 Amazon S3 权限。

```
{
   "Version":"2012-10-17",
   "Statement":[
```

```
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:GetObject",
            "s3:GetObjectVersion",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/Mary/*"
      }
   ]
}
```

然后，您可以将类似策略附加到用户 Carlos，同时在 Resource 值中指定文件夹 *Carlos*。

您可以编写一个使用策略变量的策略，然后将该策略附加到一个组，而不是将策略附加到单个用户。首先，您必须创建一个组，并将 Mary 和 Carlos 添加到该组中。以下示例策略允许在 *amzn-s3-demo-bucket1*/${aws:username} 文件夹中具有一组 Amazon S3 权限。评估策略后，策略变量 ${aws:username} 将替换为请求者的用户名。例如，如果 Mary 发送了一个请求以放置对象，只有当 Mary 将对象上传到 *amzn-s3-demo-bucket1*/Mary 文件夹后，才允许该操作。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:GetObject",
            "s3:GetObjectVersion",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/${aws:username}/*"
      }
   ]
}
```

> **Note**
>
> 当使用策略变量时，您必须在策略中明确指定版本 2012-10-17。IAM 策略语言的默认版本 2008-10-17 不支持策略变量。

如果需要在 Amazon S3 控制台上测试之前的策略，控制台需要其他权限，如以下策略所示。有关控制台如何使用这些权限的信息，请参阅 使用用户策略控制对存储桶的访问。

```
{
 "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowGroupToSeeBucketListInTheConsole",
      "Action": [
       "s3:ListAllMyBuckets",
       "s3:GetBucketLocation"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Sid": "AllowRootLevelListingOfTheBucket",
      "Action": "s3:ListBucket",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1",
      "Condition":{
            "StringEquals":{
                   "s3:prefix":[""], "s3:delimiter":["/"]
                          }
               }
    },
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Action": "s3:ListBucket",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1",
      "Condition":{  "StringLike":{"s3:prefix":["${aws:username}/*"] }
       }
    },
      {
     "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
```

```
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:GetObject",
            "s3:GetObjectVersion",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/${aws:username}/*"
      }
   ]
}
```

> **Note**
>
> 在 2012-10-17 版本的策略中，策略变量以 $ 开始。如果您的对象键（对象名称）包括 $，则语法中的此更改可能会产生冲突。
> 为避免此冲突，请通过使用 ${$} 指定 $ 字符。例如，要在策略中包括对象键 my$file，请将其指定为 my${$}file。

尽管 IAM 用户名称是友好、用户可读的标识符，但是它们无需全局唯一。例如，如果用户 Carlos 离开了企业，而另一个 Carlos 加入进来，则新 Carlos 可以访问原 Carlos 的信息。

您可以基于 IAM 用户 ID 创建文件夹，而不是使用用户名。每个 IAM 用户 ID 都是唯一的。在这种情况下，您必须修改之前的策略，以使用 ${aws:userid} 策略变量。有关用户标识符的更多信息，请参阅 IAM 用户指南中的 IAM 标识符。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:GetObject",
            "s3:GetObjectVersion",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/home/${aws:userid}/*"
```

```
      }
   ]
}
```

允许非 IAM 用户（移动应用程序用户）访问存储桶中的文件夹

假设您要开发一个移动应用程序，一个将用户数据存储在 S3 存储桶中的游戏。对于每个应用用户，您都需要在您的存储桶中创建一个文件夹。您还需要限制每个用户对其自己的文件夹的访问权限。但是，在有人下载您的应用程序并开始玩此游戏之前，您不能创建文件夹，因为您没有用户 ID。

这种情况下，您可以要求用户使用公共身份提供商 (如 Login with Amazon、Facebook、或 Google) 登录到您的应用程序。在用户通过某个提供商登录到您的应用程序后，他们具有一个用户 ID，可用于在运行时创建用户特定的文件夹。

然后，您可以使用 Amazon Security Token Service 中的 Web 联合身份验证将来自身份提供商的信息与您的应用相集成，为每个用户获取临时安全凭证。然后，您可以创建 IAM 策略，以便允许该应用访问存储桶和执行操作，如创建用户特定文件夹和上传数据。有关 Web 身份联合验证的更多信息，请参阅《IAM 用户指南》中的关于 Web 身份联合验证。

允许组在 Amazon S3 中拥有共享的文件夹

将以下策略附加到组将授予该组中的每个人访问 Amazon S3 中的以下文件夹的权限：*amzn-s3-demo-bucket1*/share/marketing。组成员仅允许访问策略中显示的特定 Amazon S3 权限，仅适用于指定文件夹中的对象。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:GetObject",
            "s3:GetObjectVersion",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/share/marketing/*"
      }
   ]
}
```

允许所有用户读取存储桶的某个部分中的对象

在该示例中，您创建一个名为 *AllUsers* 的组，其中包含 Amazon Web Services 账户拥有的所有 IAM 用户。然后，您将附加向该组提供对 GetObject 和 GetObjectVersion 的访问权限的策略，但仅适用于 *amzn-s3-demo-bucket1*/readonly 文件夹中的对象。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/readonly/*"
      }
   ]
}
```

允许合作伙伴将文件放置到存储桶的特定部分中

在本示例中，您将创建代表合作伙伴公司的名为 *AnyCompany* 的组。您将为需要访问权限的合作伙伴公司中的特定人员或应用程序创建 IAM 用户，然后将该用户放入组中。

然后，您附加策略，此策略向组提供对存储桶中以下文件夹的 PutObject 访问权限：

*amzn-s3-demo-bucket1*/uploads/anycompany

您需要阻止 *AnyCompany* 组对存储桶执行任何其他操作，因此添加了一条语句，除了对 Amazon Web Services 账户中的任何 Amazon S3 资源执行 PutObject 外，该语句显式拒绝执行任何其他 Amazon S3 操作的权限。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"s3:PutObject",
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/uploads/anycompany/*"
      },
```

```
      {
         "Effect":"Deny",
         "Action":"s3:*",
         "NotResource":"arn:aws:s3:::amzn-s3-demo-bucket1/uploads/anycompany/*"
      }
   ]
}
```

限制对特定 Amazon Web Services 账户中 Amazon S3 存储桶的访问

如果您想确保您的 Amazon S3 主体只能访问受信任 Amazon Web Services 账户中的资源，您可以限制访问权限。例如，基于身份的 IAM 策略使用 Deny 影响来阻止对 Amazon S3 操作的访问，除非正在访问的 Amazon S3 资源在账户 *222222222222* 中。为了防止 Amazon Web Services 账户中的 IAM 主体访问账户外的 Amazon S3 对象，请附加以下 IAM 策略：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyS3AccessOutsideMyBoundary",
      "Effect": "Deny",
      "Action": [
        "s3:*"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:ResourceAccount": [
            "222222222222"
          ]
        }
      }
    }
  ]
}
```

> **Note**
>
> 此策略不会取代现有的 IAM 访问控制，因为它不授予任何访问权限。相反，无论通过其他 IAM 策略授予什么权限，此策略都可以作为其他 IAM 权限的额外防护机制。

请确保将策略中的账户 ID *222222222222* 替换为您自己的 Amazon Web Services 账户。要在仍保持此限制的同时将策略应用于多个账户，请将账户 ID 替换为 `aws:PrincipalAccount` 条件键。该条件要求主体和资源必须在同一账户中。

限制企业单位内对 Amazon S3 存储桶的访问

如果在 Amazon Organizations 中设置了企业单位（OU），则可能需要将 Amazon S3 存储桶访问限制为企业的特定部分。在本示例中，我们将使用 `aws:ResourceOrgPaths` 键以限制 Amazon S3 存储桶对企业中 OU 的访问。在本例中，OU ID 为 *ou-acroot-exampleou*。确保用自己的 OU ID 替换自己的策略中的此值。

```
{
   "Version": "2012-10-17",
   "Statement": [
     {
       "Sid": "AllowS3AccessOutsideMyBoundary",
       "Effect": "Allow",
       "Action": [
         "s3:*"
       ],
       "Resource": "*",
       "Condition": {
         "ForAllValues:StringNotLike": {
           "aws:ResourceOrgPaths": [
             "o-acorg/r-acroot/ou-acroot-exampleou/"
           ]
         }
       }
     }
   ]
 }
```

> **Note**
>
> 该策略不授予任何访问权限。相反，此策略充当其他 IAM 权限的后盾，阻止主体访问 OU 定义边界之外的 Amazon S3 对象。

该策略拒绝对 Amazon S3 操作的访问，除非正在访问的 Amazon S3 对象位于您企业的 *ou-acroot-exampleou* OU 中。IAM 策略条件要求 `aws:ResourceOrgPaths`（多值条件键）包含列出的任何

OU 路径。该策略使用 `ForAllValues:StringNotLike` 运算符将 `aws:ResourceOrgPaths` 的值与列出的 OU 进行比较，而不进行区分大小写的匹配。

限制对企业内 Amazon S3 存储桶的访问

要限制对组织内 Amazon S3 对象的访问，请将 IAM 策略附加到组织的根，并将其应用于组织中的所有账户。如果要求您的 IAM 主体遵守此规则，请使用服务控制策略 (SCP)。如果您选择使用 SCP，请确保先全面测试 SCP，然后将策略附加到企业的根。

在以下示例策略中，将拒绝对 Amazon S3 操作的访问，除非正在访问的 Amazon S3 对象与访问该对象的 IAM 主体位于同一企业中：

```
{
   "Version": "2012-10-17",
   "Statement": [
     {
       "Sid": "DenyS3AccessOutsideMyBoundary",
       "Effect": "Deny",
       "Action": [
         "s3:*"
       ],
       "Resource": "arn:aws:s3:::*/*",
       "Condition": {
         "StringNotEquals": {
           "aws:ResourceOrgID": "${aws:PrincipalOrgID}"
         }
       }
     }
   ]
 }
```

> **Note**
>
> 该策略不授予任何访问权限。相反，此策略充当其他 IAM 权限的后盾，阻止主体访问企业外部的任何 Amazon S3 对象。此策略还适用于在策略生效后创建的 Amazon S3 资源。

本例中的 IAM 策略条件要求 `aws:ResourceOrgID` 和 `aws:PrincipalOrgID` 彼此相等。有了这一要求，提出请求的主体和正在访问的资源必须位于同一企业中。

为 Amazon Web Services 账户授予检索 PublicAccessBlock 配置的权限

以下基于身份的策略示例向用户授予 s3:GetAccountPublicAccessBlock 权限。对于这些权限，请将 Resource 值设置为 "*"。有关资源 ARN 的更多信息，请参阅Amazon S3 的策略资源。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"statement1",
         "Effect":"Allow",
         "Action":[
            "s3:GetAccountPublicAccessBlock"
         ],
         "Resource":[
            "*"
         ]
       }
    ]
}
```

将存储桶的创建限制在一个区域

假定 Amazon Web Services 账户管理员想要授予其用户（Dave）仅在南美洲（圣保罗）区域创建存储桶的权限。账户管理员可附加以下用户策略，授予附带条件的 s3:CreateBucket 权限，如下所示。Condition 块中的键值对指定 s3:LocationConstraint 键，并将 sa-east-1 区域作为值。

> **Note**
>
> 在该示例中，存储桶拥有者为其用户之一授予权限，因此可以使用存储桶策略或用户策略。此示例显示了用户策略。

有关 Amazon S3 区域的列表，请参阅《Amazon Web Services 一般参考》中的区域和端点。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"statement1",
         "Effect":"Allow",
```

```
          "Action": "s3:CreateBucket",
          "Resource": "arn:aws:s3:::*",
          "Condition": {
              "StringLike": {
                  "s3:LocationConstraint": "sa-east-1"
              }
          }
        }
    ]
}
```

添加显式拒绝

前面的策略限制用户只能在 sa-east-1 区域中创建存储桶。但是，别的策略可能授予此用户在其他区域中创建存储桶的权限。例如，如果用户属于某个组，该组可能附加了一个策略，以允许该组中的所有用户在另一个区域中创建存储桶。要确保此用户不会获得在其它任何区域创建存储桶的权限，可在上述策略中添加一个显式拒绝语句。

Deny 语句使用 StringNotLike 条件。也即，如果位置约束不是 sa-east-1，则创建存储桶的请求将被拒绝。显式拒绝不允许用户在其它任何区域创建存储桶，无论该用户获得了哪种其它权限。以下策略包含显式拒绝语句。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"statement1",
         "Effect":"Allow",
         "Action": "s3:CreateBucket",
         "Resource": "arn:aws:s3:::*",
         "Condition": {
             "StringLike": {
                 "s3:LocationConstraint": "sa-east-1"
             }
         }
       },
      {
         "Sid":"statement2",
         "Effect":"Deny",
         "Action": "s3:CreateBucket",
         "Resource": "arn:aws:s3:::*",
         "Condition": {
             "StringNotLike": {
```

```
                "s3:LocationConstraint": "sa-east-1"
            }
         }
      }
   ]
}
```

使用 Amazon CLI 测试策略

可使用以下 `create-bucket` Amazon CLI 命令测试此策略。此示例使用 `bucketconfig.txt` 文件来指定位置约束。记下 Windows 文件路径。您需要更新相应的存储桶名称和路径。必须使用 `--profile` 参数提供用户凭证。有关设置和使用 Amazon CLI 的更多信息，请参阅《Amazon S3 API 参考》中的 Developing with Amazon S3 using the Amazon CLI。

```
aws s3api create-bucket --bucket examplebucket --profile AccountADave --create-bucket-configuration file://c:/Users/someUser/bucketconfig.txt
```

`bucketconfig.txt` 文件指定一些配置，如下所示。

```
{"LocationConstraint": "sa-east-1"}
```

# 演练：使用策略管理针对 Amazon S3 资源的访问权限

本主题提供了以下介绍性示例演练，演示如何授予针对 Amazon S3 资源的访问权限。这些示例使用 Amazon Web Services Management Console 来创建资源（存储桶、对象、用户）并授予它们相应的权限。然后这些示例将向您演示如何使用命令行工具来验证这些权限而不必编写任何代码。我们使用 Amazon Command Line Interface（Amazon CLI）和 Amazon Tools for Windows PowerShell 提供命令。

- 示例 1：存储桶拥有者向其用户授予存储桶权限

  您在您的账户中创建的 IAM 用户默认情况下没有权限。在本练习中，您要授予用户权限来执行存储桶和对象操作。

- 示例 2：存储桶拥有者授予跨账户存储桶权限

  在本练习中，存储桶拥有者账户 A 对另一个 Amazon Web Services 账户（账户 B）授予跨账户权限，然后账户 B 将这些权限委派给其账户中的用户。

- 在对象与存储桶拥有者不同的情况下管理对象权限

  在本例中的示例方案是一个存储桶拥有者向其他人授予对象权限，但并不是该存储桶中所有对象都归该存储桶拥有者所有。存储桶拥有者需要什么权限，以及如何能委派这些权限？

  创建存储桶的 Amazon Web Services 账户称为 存储桶拥有者。该拥有者可以向其他 Amazon Web Services 账户授予上传对象的权限，而创建对象的 Amazon Web Services 账户拥有该对象。存储桶拥有者对其他 Amazon Web Services 账户创建的对象不拥有权限。如果该存储桶拥有者编写了一个存储桶策略来授予针对对象的访问权限，则该策略不适用于其它账户拥有的对象。

  在这种情况下，对象拥有者必须首先使用对象 ACL 向存储桶拥有者授予权限。然后存储桶拥有者才能够如以下示例所示，将这些对象权限委派给其他人、其自己账户中的用户或另一个 Amazon Web Services 账户。

  - 示例 3：存储桶拥有者授予不属于自己的对象的权限

    在本练习中，存储桶拥有者首先从对象拥有者获取权限。然后存储桶拥有者将这些权限委派给自己的账户中的用户。

  - 示例 4：存储桶拥有者针对自己未拥有的对象授予跨账户权限

    在从对象拥有者获得权限后，存储桶拥有者无法将权限委派给其它 Amazon Web Services 账户，因为不支持跨账户委派（请参阅授予权限）。但是，存储桶拥有者可以创建具有执行特定操作（如 get object）的权限的 IAM 角色，并允许其他 Amazon Web Services 账户担任该角色。这样，任

何担任该角色的人都能够访问对象。此示例显示存储桶拥有者如何使用 IAM 角色来启用跨账户委派。

## 在尝试示例演练之前

这些示例使用 Amazon Web Services Management Console 来创建资源和授予权限。为了测试权限，这些示例使用命令行工具 Amazon CLI 和 Amazon Tools for Windows PowerShell，因此您无需编写任何代码。要测试权限，您必须设置其中的一个工具。有关更多信息，请参阅 设置用于演练的工具。

此外，在创建资源时，这些示例并未使用 Amazon Web Services 账户的根用户凭证。而是在这些账户中创建一个管理员用户来执行这些任务。

关于使用管理员用户来创建资源和授予权限

Amazon Identity and Access Management（IAM）建议不要使用 Amazon Web Services 账户 的根用户凭证发起请求。而是应创建 IAM 用户或角色，向他们授予完全访问权限，然后使用其凭证来发出请求。我们将其称为管理员用户或角色。有关更多信息，请转至《Amazon Web Services 一般参考》中的 Amazon Web Services 账户根用户 凭证和 IAM 身份以及《IAM 用户指南》中的 IAM 最佳实践。

本部分中的所有示例演练都使用管理员用户凭证。如果您还未创建您的 Amazon Web Services 账户的管理员用户，此处的主题会向您演示这一过程。

要使用用户凭证登录 Amazon Web Services Management Console，您必须使用 IAM 用户登录 URL。IAM 控制台会为您的 Amazon Web Services 账户提供此 URL。这些主题向您演示如何获取该 URL。

## 设置用于演练的工具

介绍性示例（请参阅 演练：使用策略管理针对 Amazon S3 资源的访问权限）使用 Amazon Web Services Management Console 来创建资源和授予权限。为了测试权限，这些示例使用命令行工具 Amazon Command Line Interface（Amazon CLI）和 Amazon Tools for Windows PowerShell，因此您无需编写任何代码。要测试权限，您必须设置其中的一个工具。

设置 Amazon CLI

1. 下载并配置 Amazon CLI。有关说明，请参阅《Amazon Command Line Interface 用户指南》中的以下主题：

   安装或更新到最新版本的 Amazon Command Line Interface

   开始使用 Amazon Command Line Interface

2. 设置默认的配置文件。

   您将用户凭证存储在 Amazon CLI config 文件中。使用 Amazon Web Services 账户凭证在配置文件中创建默认配置。有关查找和编辑 Amazon CLI 配置文件的说明，请参阅 Configuration and credential file settings。

   ```
   [default]
   aws_access_key_id = access key ID
   aws_secret_access_key = secret access key
   region = us-west-2
   ```

3. 在命令提示符处输入以下命令来验证设置。这两个命令没有显式提供凭证，因此将使用默认配置的凭证。

   - 尝试 help 命令。

     ```
     aws help
     ```

   - 要获取所配置账户的存储桶列表，请使用 aws s3 ls 命令。

     ```
     aws s3 ls
     ```

当您进行演练时，您将创建用户，并且通过创建配置将用户凭证保存在配置文件中，如以下示例所示。这些配置文件的名称为 AccountAadmin 和 AccountBadmin。

```
[profile AccountAadmin]
aws_access_key_id = User AccountAadmin access key ID
aws_secret_access_key = User AccountAadmin secret access key
region = us-west-2

[profile AccountBadmin]
aws_access_key_id = Account B access key ID
aws_secret_access_key = Account B secret access key
region = us-east-1
```

要使用这些用户凭证来运行命令，请添加 --profile 参数来指定配置文件名称。以下 Amazon CLI 命令检索 *examplebucket* 中对象的列表，并指定 AccountBadmin 配置文件。

```
aws s3 ls s3://examplebucket --profile AccountBadmin
```

或者，您也可以从命令提示符处更改 AWS_DEFAULT_PROFILE 环境变量，将一组用户凭证配置为默认的配置文件。完成此操作后，当执行不带 --profile 参数的 Amazon CLI 命令时，Amazon CLI 会将您在环境变量中设置的配置文件用作默认配置文件。

```
$ export AWS_DEFAULT_PROFILE=AccountAadmin
```

要设置 Amazon Tools for Windows PowerShell，请按以下步骤操作：

1. 下载并配置 Amazon Tools for Windows PowerShell。有关说明，请参阅《Amazon Tools for Windows PowerShell User Guide》中的 Installing the Amazon Tools for Windows PowerShell。

   > **Note**
   >
   > 要加载 Amazon Tools for Windows PowerShell 模块，必须启用 PowerShell 脚本执行。有关更多信息，请参阅《Amazon Tools for Windows PowerShell User Guide》中的 Enable Script Execution。

2. 对于这些演练，您需使用 Set-AWSCredentials 命令指定每个会话的 Amazon 凭证。该命令会将凭证保存到持久存储 (-StoreAs 参数)。

   ```
   Set-AWSCredentials -AccessKey AccessKeyID -SecretKey SecretAccessKey -
   storeas string
   ```

3. 验证设置。

   - 要检索可用于 Amazon S3 操作的命令的列表，请运行 Get-Command 命令。

     ```
     Get-Command -module awspowershell -noun s3* -StoredCredentials string
     ```

   - 要检索存储桶中的对象的列表，请运行 Get-S3Object 命令。

     ```
     Get-S3Object -BucketName bucketname -StoredCredentials string
     ```

有关命令列表，请参阅 Amazon Tools for PowerShell Cmdlet Reference。

现在您已经准备就绪，可以尝试进行演练了。访问每个部分开头提供的链接。

# 示例 1：存储桶拥有者向其用户授予存储桶权限

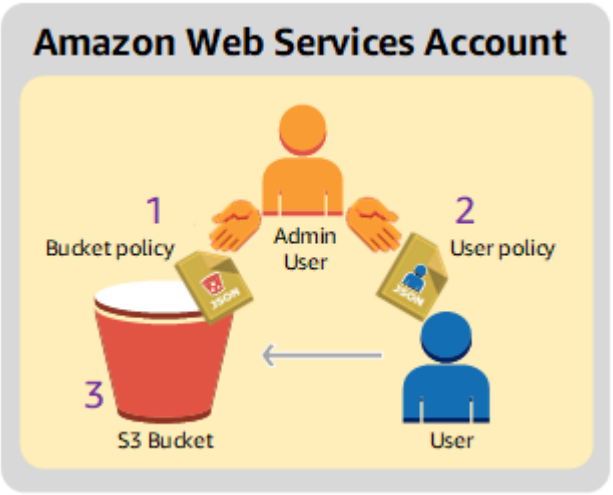
> **Important**
>
> 向 IAM 角色授予权限比向各个用户授予权限更好。有关如何向 IAM 角色授予权限的更多信息，请参阅了解跨账户权限和使用 IAM 角色。

主题


- 准备演练
- 步骤 1：在账户 A 中创建资源并授予权限
- 步骤 2：测试权限


在本演练中，一个 Amazon Web Services 账户拥有存储桶，该账户中包含一个 IAM 用户。默认情况下，该用户没有权限。要让该用户执行任何任务，父账户必须向该用户授予权限。存储桶拥有者和父账户相同。因此，要向用户授予存储桶权限，Amazon Web Services 账户可以使用存储桶策略和/或用户策略。存储桶拥有者将使用存储桶策略授予一些权限，使用用户策略授予其他权限。

以下是演练的步骤概括：




1. 账户管理员创建存储桶策略，向用户授予一组权限。
2. 账户管理员将用户策略附加到用户，授予其他权限。
3. 然后，用户尝试使用通过存储桶策略和用户策略授予的权限。

对于此示例，您需要一个 Amazon Web Services 账户。您将创建一个管理员用户（请参阅 关于使用管理员用户来创建资源和授予权限），而不是使用账户的根用户凭证。我们按下表所示引用 Amazon Web Services 账户和管理员用户：

| 账户 ID | 账户名称 | 账户中的管理员用户 |
| --- | --- | --- |
| *1111-1111-1111* | 账户 A | AccountAadmin |

> **Note**
>
> 本示例中的管理员用户是 AccountAadmin，它代表账户 A，而不是 AccountAdmin。

创建用户和授予权限的所有任务都在 Amazon Web Services Management Console 中完成。为验证权限，演练中使用命令行工具、Amazon Command Line Interface (Amazon CLI) 和 Amazon Tools for Windows PowerShell，因此您无需编写任何代码。

准备演练

1. 确保您有一个 Amazon Web Services 账户并且它的一个用户拥有管理员权限。

   a. 根据需要注册 Amazon Web Services 账户。我们将此账户称为账户 A。

      i. 转到 https://aws.amazon.com/s3，然后单击创建 Amazon 账户。

      ii. 按照屏幕上的说明进行操作。

      账户激活且可用时，Amazon 会通过电子邮件向您发送通知。

   b. 在账户 A 中，创建一个管理员用户 **AccountAadmin**。使用账户 A 凭证登录 IAM 控制台，然后执行以下操作：

      i. 创建用户 **AccountAadmin** 并记下用户安全凭证。

      有关说明，请参阅《IAM 用户指南》中的在您的 Amazon Web Services 账户中创建 IAM 用户。

      ii. 通过附加一个授予完全访问权限的用户策略来向 AccountAadmin 授予管理员权限。

      有关说明，请参阅《IAM 用户指南》中的管理 IAM 策略。

iii. 记下 AccountAadmin 的 IAM 用户登录 URL。您在登录 Amazon Web Services Management Console时需要使用此 URL。有关如何查找登录 URL 的更多信息，请参阅《IAM 用户指南》中的 Sign in to the Amazon Web Services Management Console as an IAM user。记下每个账户的 URL。

2. 设置 Amazon CLI 或 Amazon Tools for Windows PowerShell。请务必保存管理员用户凭证，如下所示：

   - 如果使用 Amazon CLI，请在配置文件中创建配置文件 `AccountAadmin`。
   - 如果使用 Amazon Tools for Windows PowerShell，请确保将用于会话的凭证存储为 `AccountAadmin`。

   有关说明，请参阅设置用于演练的工具。

步骤 1：在账户 A 中创建资源并授予权限

使用账户 A 中用户 `AccountAadmin` 的凭证和专用的 IAM 用户登录 URL 登录 Amazon Web Services Management Console，然后执行以下操作：

1. 创建资源（一个存储桶和一个 IAM 用户）

   a. 在 Amazon S3 控制台中创建一个存储桶。记下创建存储桶的 Amazon Web Services 区域。有关说明，请参阅创建通用存储桶。

   b. 在 IAM 控制台中，执行以下操作：

      i. 创建一个名为 Dave 的用户。

      有关分步说明，请参阅《IAM 用户指南》中的创建 IAM 用户（控制台）。

      ii. 记下 `UserDave` 凭证。

      iii. 记下用户 Dave 的 Amazon 资源名称（ARN）。在 IAM 控制台中，选择该用户，摘要选项卡会提供用户 ARN。

2. 授予权限

   因为存储桶拥有者和用户所属的父账户相同，所以 Amazon Web Services 账户可以使用存储桶策略和/或用户策略向用户授予权限。在此示例中，您同时使用这两种方法。如果对象也由同一个账户拥有，则存储桶拥有者可以在存储桶策略（或 IAM 策略）中授予对象权限。

   a. 在 Amazon S3 控制台中，将以下存储桶策略附加到 *awsexamplebucket1*。

该策略包含两个语句。

- 第一个语句向 Dave 授予存储桶操作权限 s3:GetBucketLocation 和 s3:ListBucket。
- 第二个语句授予 s3:GetObject 权限。因为账户 A 还拥有对象，所以账户管理员能够授予 s3:GetObject 权限。

在 Principal 语句中，Dave 通过其用户 ARN 进行标识。有关策略元素的更多信息，请参阅 Amazon S3 中的策略和权限。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "statement1",
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::AccountA-ID:user/Dave"
         },
         "Action": [
            "s3:GetBucketLocation",
            "s3:ListBucket"
         ],
         "Resource": [
            "arn:aws:s3:::awsexamplebucket1"
         ]
      },
      {
         "Sid": "statement2",
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::AccountA-ID:user/Dave"
         },
         "Action": [
             "s3:GetObject"
         ],
         "Resource": [
            "arn:aws:s3:::awsexamplebucket1/*"
         ]
      }
   ]
```

```
}
```

b. 使用以下策略为用户 Dave 创建一个内联策略。该策略向 Dave 授予 s3:PutObject 权限。您需要通过提供存储桶名称来更新策略。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "PermissionForObjectOperations",
         "Effect": "Allow",
         "Action": [
            "s3:PutObject"
         ],
         "Resource": [
            "arn:aws:s3:::awsexamplebucket1/*"
         ]
      }
   ]
}
```

有关说明，请参阅《IAM 用户指南》中的管理 IAM 策略。请注意，您需要使用账户 A 凭证登录控制台。

步骤 2：测试权限

使用 Dave 的凭证验证权限是否发挥作用。您可以使用以下两个过程之一。

使用 Amazon CLI 测试权限

1. 通过添加以下 UserDaveAccountA 配置文件更新 Amazon CLI 配置文件。有关更多信息，请参阅 设置用于演练的工具。

```
[profile UserDaveAccountA]
aws_access_key_id = access-key
aws_secret_access_key = secret-access-key
region = us-east-1
```

2. 验证 Dave 是否可以执行在用户策略中授权的操作。使用以下 Amazon CLI put-object 命令上传示例对象。

该命令中的 --body 参数指示要上传的源文件。例如，如果文件处于 Windows 计算机上 C: 驱动器的根目录中，则指定 c:\HappyFace.jpg。--key 参数提供对象的键名。

```
aws s3api put-object --bucket awsexamplebucket1 --key HappyFace.jpg --
body HappyFace.jpg --profile UserDaveAccountA
```

运行以下 Amazon CLI 命令以获取对象。

```
aws s3api get-object --bucket awsexamplebucket1 --key HappyFace.jpg OutputFile.jpg
 --profile UserDaveAccountA
```

使用 Amazon Tools for Windows PowerShell 测试权限

1. 将 Dave 的凭证存储为 AccountADave。您随后使用这些凭证对对象执行 PUT 和 GET 操作。

```
set-awscredentials -AccessKey AccessKeyID -SecretKey SecretAccessKey -storeas
 AccountADave
```

2. 通过用户 Dave 的已存储凭证，使用 Amazon Tools for Windows PowerShell Write-S3Object 命令上传示例对象。

```
Write-S3Object -bucketname awsexamplebucket1 -key HappyFace.jpg -file HappyFace.jpg
 -StoredCredentials AccountADave
```

下载之前上传的对象。

```
Read-S3Object -bucketname awsexamplebucket1 -key HappyFace.jpg -file Output.jpg -
StoredCredentials AccountADave
```

# 示例 2：存储桶拥有者授予跨账户存储桶权限

> **Important**
>
> 向 IAM 角色授予权限是比向各个用户授予权限更好的做法。若要了解如何执行此操作，请参阅了解跨账户权限和使用 IAM 角色。

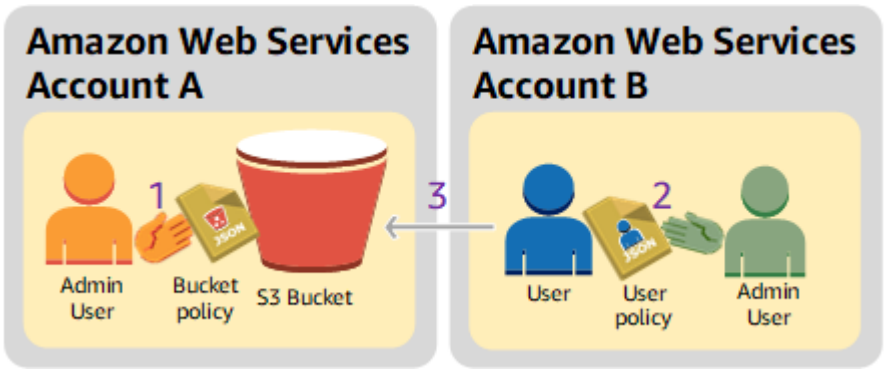
主题


- 准备演练
- 步骤 1：执行账户 A 任务
- 步骤 2：执行账户 B 任务
- 步骤 3：（可选）尝试显式拒绝
- 步骤 4：清除


一个 Amazon Web Services 账户（例如账户 A）可以将访问自身资源（如存储桶和对象）的权限授予另一个 Amazon Web Services 账户（账户 B）。账户 B 随后可以将这些权限委托给其账户中的用户。在此示例情景中，存储桶拥有者向另一个账户授予执行特定存储桶操作的跨账户权限。

> **Note**
>
> 账户 A 还可以使用存储桶策略直接向账户 B 中的用户授予权限。但是，该用户仍需要来自用户所属的父账户（账户 B）的权限，即使账户 B 没有来自账户 A 的权限也是如此。该用户只要同时拥有来自资源拥有者和父账户的权限，便能够访问资源。

下面概括介绍演练步骤：



1. 账户 A 管理员用户附加一个存储桶策略，该策略向账户 B 授予执行特定存储桶操作的跨账户权限。

   请注意，账户 B 中的管理员用户将自动继承这些权限。
2. 账户 B 管理员用户将用户策略附加到用户，委托从账户 A 收到的权限。
3. 账户 B 中的用户随后通过访问账户 A 拥有的存储桶中的对象来验证权限。

对于此示例，您需要两个账户。下表显示我们如何引用这些账户和其中的管理员用户。根据 IAM 准则（请参阅关于使用管理员用户来创建资源和授予权限），我们在本次演练中并不使用根用户凭证。而是在每个账户中创建一个管理员用户，并在创建资源和向他们授予权限时使用这些凭证。

| Amazon Web Services 账户 ID | 账户名称 | 账户中的管理员用户 |
|---|---|---|
| *1111-1111-1111* | 账户 A | AccountAadmin |
| *2222-2222-2222* | 账户 B | AccountBadmin |

创建用户和授予权限的所有任务都在 Amazon Web Services Management Console 中完成。为验证权限，演练中使用命令行工具、Amazon Command Line Interface (CLI) 和 Amazon Tools for Windows PowerShell，因此您无需编写任何代码。

准备演练

1. 确保您有两个 Amazon Web Services 账户并且每个账户都有一个管理员用户，如前面部分的表中所示。

   a. 根据需要注册 Amazon Web Services 账户。

   b. 使用账户 A 凭证登录 IAM 控制台以创建管理员用户：

      i. 创建用户 **`AccountAadmin`** 并记下安全凭证。有关说明，请参阅《IAM 用户指南》中的在您的 Amazon Web Services 账户 中创建 IAM 用户。

      ii. 通过附加一个授予完全访问权限的用户策略来向 AccountAadmin 授予管理员权限。有关说明，请参阅 IAM 用户指南中的使用策略。

   c. 在 IAM 控制台中，记下控制面板上的 IAM 用户登录 URL。账户中的所有用户都必须使用此 URL 登录 Amazon Web Services Management Console。

      有关更多信息，请参阅 IAM 用户指南中的用户如何登录您的账户。

   d. 使用账户 B 凭证重复上一个步骤，然后创建管理员用户 **`AccountBadmin`**。

2. 设置 Amazon Command Line Interface（Amazon CLI）或 Amazon Tools for Windows PowerShell。请务必保存管理员用户凭证，如下所示：

   - 如果使用 Amazon CLI，请在配置文件中创建两个配置文件：AccountAadmin 和 AccountBadmin。
   - 如果使用 Amazon Tools for Windows PowerShell，请确保将用于会话的凭证存储为 AccountAadmin 和 AccountBadmin。

   有关说明，请参阅 设置用于演练的工具。

3. 保存管理员用户凭证，也称为配置文件。您可以对输入的每个命令使用配置文件名称而不是指定凭证。有关更多信息，请参阅 设置用于演练的工具。

   a. 在 Amazon CLI 凭证文件中为两个账户中的每个管理员用户 AccountAadmin 和 AccountBadmin 添加配置文件。

   ```
   [AccountAadmin]
   aws_access_key_id = access-key-ID
   aws_secret_access_key = secret-access-key
   region = us-east-1

   [AccountBadmin]
   aws_access_key_id = access-key-ID
   aws_secret_access_key = secret-access-key
   region = us-east-1
   ```

   b. 如果使用的是 Amazon Tools for Windows PowerShell，请运行以下命令。

   ```
   set-awscredentials -AccessKey AcctA-access-key-ID -SecretKey AcctA-secret-
   access-key -storeas AccountAadmin
   set-awscredentials -AccessKey AcctB-access-key-ID -SecretKey AcctB-secret-
   access-key -storeas AccountBadmin
   ```

步骤 1：执行账户 A 任务

步骤 1.1：登录到 Amazon Web Services Management Console

首先使用账户 A 的 IAM 用户登录 URL，以 AccountAadmin 用户身份登录 Amazon Web Services Management Console。此用户将创建一个存储桶并向其附加一个策略。

步骤 1.2：创建存储桶

1. 在 Amazon S3 控制台中创建一个存储桶。此练习假设该存储桶在美国东部（弗吉尼亚州北部）Amazon Web Services 区域中创建，命名为 *amzn-s3-demo-bucket*。

   有关说明，请参阅 创建通用存储桶。

2. 向存储桶上传示例对象。

   有关说明，请转到 步骤 2：将对象上传到存储桶。

步骤 1.3：附加一个存储桶策略，向账户 B 授予跨账户权限

该存储桶策略向账户 B 授予 s3:GetLifecycleConfiguration 和 s3:ListBucket 权限。假设您仍使用 AccountAadmin 用户凭证登录控制台。

1. 将以下存储桶策略附加到 *amzn-s3-demo-bucket*。该策略向账户 B 授予 s3:GetLifecycleConfiguration 和 s3:ListBucket 操作的权限。

   有关说明，请参阅使用 Amazon S3 控制台添加存储桶策略。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Example permissions",
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::AccountB-ID:root"
         },
         "Action": [
            "s3:GetLifecycleConfiguration",
            "s3:ListBucket"
         ],
         "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket"
         ]
      }
   ]
}
```

2. 验证账户 B（及其管理员用户）是否可以执行这些操作。

- 使用 Amazon CLI 进行验证

```
aws s3 ls s3://amzn-s3-demo-bucket --profile AccountBadmin
aws s3api get-bucket-lifecycle-configuration --bucket amzn-s3-demo-bucket --
profile AccountBadmin
```

- 使用 Amazon Tools for Windows PowerShell 进行验证

```
get-s3object -BucketName amzn-s3-demo-bucket -StoredCredentials AccountBadmin
get-s3bucketlifecycleconfiguration -BucketName amzn-s3-demo-bucket -
StoredCredentials AccountBadmin
```

步骤 2：执行账户 B 任务

现在账户 B 管理员创建用户 Dave，并委派从账户 A 收到的权限。

步骤 2.1：登录到 Amazon Web Services Management Console

首先使用账户 B 的 IAM 用户登录 URL，以 AccountBadmin 用户身份登录 Amazon Web Services Management Console。

步骤 2.2：在账户 B 中创建用户 Dave

在 IAM 控制台中，创建用户 **Dave**。

有关说明，请参阅 IAM 用户指南中的创建 IAM 用户（控制台）。

步骤 2.3：向用户 Dave 授予权限

使用以下策略为用户 Dave 创建一个内联策略。您需要通过提供存储桶名称来更新策略。

假设您使用 AccountBadmin 用户凭证登录控制台。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Example",
         "Effect": "Allow",
         "Action": [
```

```
            "s3:ListBucket"
         ],
         "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket"
         ]
      }
   ]
}
```

有关说明，请参阅《IAM 用户指南》中的管理 IAM 策略。

步骤 2.4：测试权限

现在，账户 B 中的 Dave 可以列出账户 A 拥有的 *amzn-s3-demo-bucket* 的内容。您可以使用以下过程之一验证权限。

使用 Amazon CLI 测试权限

1. 将 UserDave 配置文件添加到 Amazon CLI 配置文件。有关配置文件的更多信息，请参阅设置用于演练的工具。

   ```
   [profile UserDave]
   aws_access_key_id = access-key
   aws_secret_access_key = secret-access-key
   region = us-east-1
   ```

2. 在命令提示符处，输入以下 Amazon CLI 命令，验证 Dave 现在是否可以从账户 A 拥有的 *amzn-s3-demo-bucket* 获取对象列表。请注意，该命令指定了 UserDave 配置文件。

   ```
   aws s3 ls s3://amzn-s3-demo-bucket --profile UserDave
   ```

   Dave 没有任何其它权限。因此，如果他尝试任何其它操作（例如，下面的 get-bucket-lifecycle 配置操作），则 Amazon S3 会返回权限被拒绝的消息。

   ```
   aws s3api get-bucket-lifecycle-configuration --bucket amzn-s3-demo-bucket --profile
    UserDave
   ```

使用 Amazon Tools for Windows PowerShell 测试权限

1. 将 Dave 的凭证存储为 AccountBDave。

```
set-awscredentials -AccessKey AccessKeyID -SecretKey SecretAccessKey -storeas
 AccountBDave
```

2. 尝试列出存储桶的命令。

```
get-s3object -BucketName amzn-s3-demo-bucket -StoredCredentials AccountBDave
```

Dave 没有任何其它权限。因此，如果他尝试任何其它操作（例如，下面的 get-s3bucketlifecycleconfiguration 操作），则 Amazon S3 会返回权限被拒绝的消息。

```
get-s3bucketlifecycleconfiguration -BucketName amzn-s3-demo-bucket -
StoredCredentials AccountBDave
```

步骤 3：（可选）尝试显式拒绝

您可以使用访问控制列表（ACL）、存储桶策略或用户策略授予权限。但是，如果通过存储桶策略或用户策略设置了显式拒绝，则显式拒绝优先于任何其它权限。为进行测试，请更新存储桶策略，对账户 B 显式拒绝 s3:ListBucket 权限。该策略还授予了 s3:ListBucket 权限。但是，显式拒绝处于优先地位，因此账户 B 或账户 B 中的用户无法列出 *amzn-s3-demo-bucket* 中的对象。

1. 使用账户 A 中的用户 AccountAadmin 的凭证，将存储桶策略替换为以下内容。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Example permissions",
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::AccountB-ID:root"
         },
         "Action": [
            "s3:GetLifecycleConfiguration",
            "s3:ListBucket"
         ],
         "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket"
         ]
      },
```

```
      {
         "Sid": "Deny permission",
         "Effect": "Deny",
         "Principal": {
            "AWS": "arn:aws:iam::AccountB-ID:root"
         },
         "Action": [
            "s3:ListBucket"
         ],
         "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket"
         ]
      }
   ]
}
```

2. 现在，如果您尝试使用 AccountBadmin 凭证获取存储桶列表，则您的访问会被拒绝。

   - 使用 Amazon CLI，运行以下命令：

     ```
     aws s3 ls s3://amzn-s3-demo-bucket --profile AccountBadmin
     ```

   - 使用 Amazon Tools for Windows PowerShell，运行以下命令：

     ```
     get-s3object -BucketName amzn-s3-demo-bucket -StoredCredentials AccountBDave
     ```

步骤 4：清除

1. 完成测试之后，您可以执行以下操作来进行清理：

   - 使用账户 A 凭证登录 Amazon Web Services Management Console（Amazon Web Services Management Console），执行以下操作：

     - 在 Amazon S3 控制台中，删除附加到 *amzn-s3-demo-bucket* 的存储桶策略。在存储桶 Properties（属性）中，删除 Permissions（权限）部分中的策略。
     - 如果该存储桶是为此练习而创建的，请在 Amazon S3 控制台中删除对象，然后删除存储桶。
     - 在 IAM 控制台中，移除 AccountAadmin 用户。

2. 使用账户 B 凭证登录 IAM 控制台。删除用户 AccountBadmin。有关分步说明，请参阅《IAM 用户指南》中的删除 IAM 用户。

# 示例 3：存储桶拥有者授予不属于自己的对象的权限

> **Important**
>
> 向 IAM 角色授予权限是比向各个用户授予权限更好的做法。若要了解如何执行此操作，请参阅了解跨账户权限和使用 IAM 角色。

主题


- 步骤 0：准备演练
- 步骤 1：执行账户 A 任务
- 步骤 2：执行账户 B 任务
- 步骤 3：测试权限
- 步骤 4：清除


此示例的情况是，存储桶拥有者要授予对象访问权限，但该存储桶拥有者并未拥有该存储桶中的所有对象。在此示例中，存储桶拥有者想要向其账户中的用户授予权限。

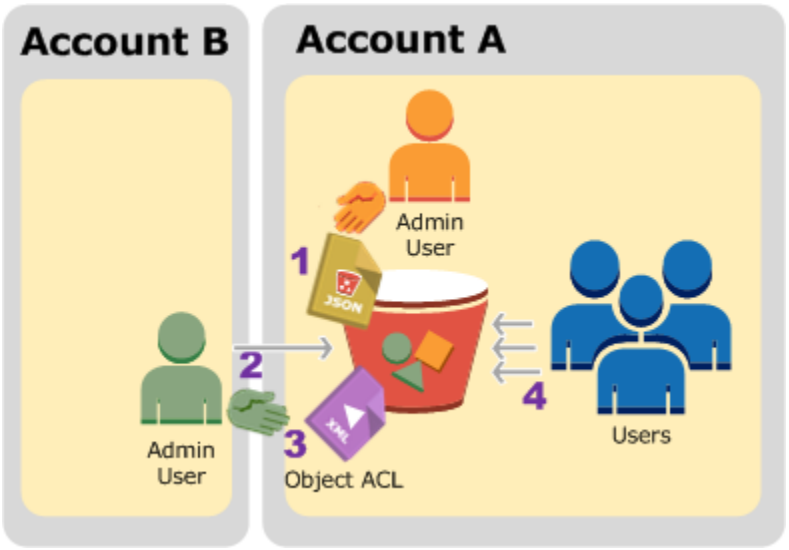
存储桶拥有者可让其他 Amazon Web Services 账户上传对象。默认情况下，存储桶拥有者不拥有 Amazon Web Services 账户 写入存储桶的对象。对象归将它们写入 S3 存储桶的账户所有。如果存储桶拥有者未拥有存储桶中的对象，对象拥有者必须首先使用对象访问控制列表（ACL）授予存储桶拥有者权限。然后，存储桶拥有者可以授予他们未拥有的对象的权限。有关更多信息，请参阅 Amazon S3 存储桶和对象所有权。

如果存储桶拥有者对存储桶的 S3 对象所有权应用了强制存储桶拥有者设置，则存储桶拥有者将拥有存储桶中的所有对象，包括另一个 Amazon Web Services 账户 所编写的对象。此方法将解决存储桶拥有者未拥有对象的问题。然后，您可以将权限委派给自己账户中的用户或其他 Amazon Web Services 账户。

> **Note**
>
> S3 对象所有权是 Amazon S3 存储桶级别的设置，您可以使用该设置来控制上传到存储桶的对象的所有权和禁用或启用 ACL。默认情况下，对象所有权设为强制存储桶拥有者设置，并且所有 ACL 均处于禁用状态。禁用 ACL 后，存储桶拥有者拥有存储桶中的所有对象，并使用访问管理策略来专门管理对这些对象的访问权限。
>
> Amazon S3 中的大多数现代使用案例不再需要使用 ACL。我们建议您将 ACL 保持为禁用状态，除非有需要单独控制每个对象的访问权限的特殊情况。禁用 ACL 后，您可以使用策略来控

制对存储桶中所有对象的访问权限，无论是谁将对象上传到您的存储桶。有关更多信息，请参阅 为您的存储桶控制对象所有权和禁用 ACL。。

在此示例中，我们假设存储桶拥有者尚未应用对象所有权的强制存储桶拥有者设置。存储桶拥有者向其账户中的用户委派权限。下面概括介绍演练步骤：




1. 账户 A 管理员用户使用两条语句来附加存储桶策略。
   - 向账户 B 授予跨账户上传对象的权限。
   - 允许用户使用自己的账户访问存储桶中的对象。
2. 账户 B 管理员用户将对象上传至账户 A 拥有的存储桶。
3. 账户 B 管理员将更新对象 ACL，在其中添加授权，以向存储桶拥有者授予对于该对象的完全控制权限。
4. 账户 A 中的用户将通过访问存储桶中的对象（而不管谁拥有它们）来验证权限。

对于此示例，您需要两个账户。下表显示我们如何引用这些账户和这些账户中的管理员用户。根据建议的 IAM 指南，在本演练中，请不要使用账户根用户凭证。有关更多信息，请参阅 关于使用管理员用户来创建资源和授予权限。而是在每个账户中创建一个管理员，在创建资源和向他们授予权限时使用这些凭证。

| Amazon Web Services 账户 ID | 账户名称 | 账户中的管理员 |
| --- | --- | --- |
| *1111-1111-1111* | 账户 A | AccountAadmin |

| Amazon Web Services 账户 ID | 账户名称 | 账户中的管理员 |
| --- | --- | --- |
| *2222-2222-2222* | 账户 B | AccountBadmin |

创建用户和授予权限的所有任务都在 Amazon Web Services Management Console 中完成。为验证权限，演练中使用命令行工具、Amazon Command Line Interface (Amazon CLI) 和 Amazon Tools for Windows PowerShell，因此您无需编写任何代码。

步骤 0：准备演练

1. 确保您有两个 Amazon Web Services 账户，并且每个账户都有一个管理员，如前面部分的表中所示。

   a. 根据需要注册 Amazon Web Services 账户。

   b. 使用账户 A 凭证登录 IAM 控制台，然后执行以下操作以创建管理员用户：

      - 创建用户 **AccountAadmin** 并记下该用户的安全凭证。有关添加用户的更多信息，请参阅 IAM 用户指南中的在您的 Amazon Web Services 账户中创建 IAM 用户。
      - 通过附加一个授予完全访问权限的用户策略来向 AccountAadmin 授予管理员权限。有关说明，请参阅《IAM 用户指南》中的管理 IAM 策略。
      - 在 IAM 控制台的控制面板中，记下 IAM 用户登录 URL。此账户中的用户必须在登录 Amazon Web Services Management Console 时使用此 URL。有关更多信息，请参阅 IAM 用户指南中的用户如何登录您的账户。

   c. 使用账户 B 凭证重复上一个步骤，然后创建管理员用户 **AccountBadmin**。

2. 设置 Amazon CLI 或 Tools for Windows PowerShell。请务必保存管理员凭证，如下所示：

   - 如果使用 Amazon CLI，请在配置文件中创建两个配置文件：`AccountAadmin` 和 `AccountBadmin`。
   - 如果使用 Tools for Windows PowerShell，请确保将用于会话的凭证存储为 `AccountAadmin` 和 `AccountBadmin`。

   有关说明，请参阅 设置用于演练的工具。

步骤 1：执行账户 A 任务

对账户 A 执行以下步骤：

步骤 1.1：登录到控制台

使用账户 A 的 IAM 用户登录 URL，以 **AccountAadmin** 用户身份登录 Amazon Web Services Management Console。此用户将创建一个存储桶并向其附加一个策略。

步骤 1.2：创建存储桶和用户，并添加一条授予用户权限的存储桶策略

1. 在 Amazon S3 控制台中创建一个存储桶。此练习假设该存储桶在美国东部（弗吉尼亚州北部）Amazon Web Services 区域创建，名称为 *amzn-s3-demo-bucket1*。

   有关说明，请参阅创建通用存储桶。

2. 在 IAM 控制台中，创建用户 **Dave**。

   有关分步说明，请参阅《IAM 用户指南》中的创建 IAM 用户（控制台）。

3. 记下用户 Dave 的凭证。

4. 在 Amazon S3 控制台中，将以下存储桶策略附加到 *amzn-s3-demo-bucket1* 存储桶。有关说明，请参阅使用 Amazon S3 控制台添加存储桶策略。按照这些步骤添加存储桶策略。有关如何查找账户 ID 的信息，请参阅查找您的 Amazon Web Services 账户 ID。

   该策略将向账户 B 授予 s3:PutObject 和 s3:ListBucket 权限。该策略还为用户 Dave 授予了 s3:GetObject 权限。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Statement1",
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::AccountB-ID:root"
         },
         "Action": [
            "s3:PutObject",
            "s3:ListBucket"
         ],
         "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "arn:aws:s3:::amzn-s3-demo-bucket1"
         ]
      },
      {
```

```
            "Sid": "Statement3",
            "Effect": "Allow",
            "Principal": {
               "AWS": "arn:aws:iam::AccountA-ID:user/Dave"
            },
            "Action": [
               "s3:GetObject"
            ],
            "Resource": [
               "arn:aws:s3:::amzn-s3-demo-bucket1/*"
            ]
         }
      ]
}
```

步骤 2：执行账户 B 任务

现在账户 B 有权对账户 A 的存储桶执行操作，账户 B 管理员将执行以下操作：

- 将对象上传到账户 A 的存储桶。
- 在对象 ACL 中添加授权，向账户 A（存储桶拥有者）授予完全控制权限。

使用 Amazon CLI

1. 使用 `put-object` Amazon CLI 命令，上传对象。该命令中的 `--body` 参数指示要上传的源文件。例如，如果该文件在 Windows 计算机上的 `C:` 驱动器中，您应指定 `c:\HappyFace.jpg`。`--key` 参数提供对象的键名。

   ```
   aws s3api put-object --bucket amzn-s3-demo-bucket1 --key HappyFace.jpg --body
    HappyFace.jpg --profile AccountBadmin
   ```

2. 在对象 ACL 中添加一个授权，向存储桶拥有者授予对于对象的完全控制权。有关如何查找规范用户 ID 的信息，请参阅《Amazon 账户管理参考指南》中的 Find the canonical user ID for your Amazon Web Services 账户。

   ```
   aws s3api put-object-acl --bucket amzn-s3-demo-bucket1 --key HappyFace.jpg --grant-
   full-control id="AccountA-CanonicalUserID" --profile AccountBadmin
   ```

使用 Tools for Windows PowerShell

1. 使用 `Write-S3Object` 命令，上传对象。

```
Write-S3Object -BucketName amzn-s3-demo-bucket1 -key HappyFace.jpg -file
 HappyFace.jpg -StoredCredentials AccountBadmin
```

2. 在对象 ACL 中添加一个授权，向存储桶拥有者授予对于对象的完全控制权。

```
Set-S3ACL -BucketName amzn-s3-demo-bucket1 -Key HappyFace.jpg -CannedACLName
 "bucket-owner-full-control" -StoredCreden
```

步骤 3：测试权限

现在验证账户 A 中的用户 Dave 是否能够访问账户 B 拥有的对象。

使用 Amazon CLI

1. 将用户 Dave 的凭证添加到 Amazon CLI 配置文件，并创建新的配置文件 `UserDaveAccountA`。有关更多信息，请参阅 设置用于演练的工具。

```
[profile UserDaveAccountA]
aws_access_key_id = access-key
aws_secret_access_key = secret-access-key
region = us-east-1
```

2. 运行 `get-object` CLI 命令，下载 `HappyFace.jpg`，并将它保存在本地。您可以通过添加参数 `--profile` 为用户 Dave 提供凭证。

```
aws s3api get-object --bucket amzn-s3-demo-bucket1 --key
 HappyFace.jpg Outputfile.jpg --profile UserDaveAccountA
```

使用 Tools for Windows PowerShell

1. 将用户 Dave 的 Amazon 凭证以 `UserDaveAccountA` 的身份保存到持久存储。

```
Set-AWSCredentials -AccessKey UserDave-AccessKey -SecretKey UserDave-
SecretAccessKey -storeas UserDaveAccountA
```

2. 运行 Read-S3Object 命令，下载 HappyFace.jpg 对象，并将它保存在本地。您可以通过添加参数 -StoredCredentials 为用户 Dave 提供凭证。

```
Read-S3Object -BucketName amzn-s3-demo-bucket1 -Key HappyFace.jpg -file
 HappyFace.jpg  -StoredCredentials UserDaveAccountA
```

步骤 4：清除

1. 完成测试之后，您可以执行以下操作来进行清理：
   - 使用账户 A 凭证登录 Amazon Web Services Management Console，并执行以下操作：
     - 在 Amazon S3 控制台中，移除附加到 *amzn-s3-demo-bucket1* 的存储桶策略。在存储桶 Properties（属性）中，删除 Permissions（权限）部分中的策略。
     - 如果该存储桶是为此练习而创建的，请在 Amazon S3 控制台中删除对象，然后删除存储桶。
     - 在 IAM 控制台中，移除 AccountAadmin 用户。有关分步说明，请参阅《IAM 用户指南》中的删除 IAM 用户。
2. 使用账户 B 凭证登录 Amazon Web Services Management Console。在 IAM 控制台中，删除用户 AccountBadmin。

## 示例 4：存储桶拥有者针对自己未拥有的对象授予跨账户权限

主题


- 了解跨账户权限和使用 IAM 角色
- 步骤 0：准备演练
- 步骤 1：执行账户 A 任务
- 步骤 2：执行账户 B 任务
- 步骤 3：执行账户 C 任务
- 步骤 4：清除
- 相关资源


在此示例场景中，您拥有一个存储桶，并且启用了其他 Amazon Web Services 账户以上传对象。如果您已经为存储桶的 S3 对象所有权应用了强制存储桶拥有者设置，那么您将拥有存储桶中的所有对象，

包括另一个 Amazon Web Services 账户 所编写的对象。此方法将解决存储桶拥有者未拥有对象的问题。然后，您可以将权限委派给自己账户中的用户或其他 Amazon Web Services 账户。假设尚未启用 S3 对象所有权的强制存储桶拥有者设置。也就是说，您的存储桶中可以有其他 Amazon Web Services 账户所拥有的对象。

现在，假设作为存储桶拥有者，您需要向另一个账户中的用户授予对象（无论拥有者是谁）的跨账户权限。例如，该用户可以是需要访问对象元数据的账单应用程序。存在两个核心问题：

- 存储桶拥有者对其他 Amazon Web Services 账户创建的对象不拥有权限。因此，存储桶拥有者若要针对自己未拥有的对象授予权限，必须先由对象拥有者向存储桶拥有者授予权限。对象拥有者是创建对象版本的 Amazon Web Services 账户。然后，存储桶拥有者才能委托这些权限。
- 存储桶拥有者账户可以向其账户中的用户委派权限（请参阅示例 3：存储桶拥有者授予不属于自己的对象的权限）。但是，存储桶拥有者账户无法将权限委派给其它 Amazon Web Services 账户，因为不支持跨账户委派。

在这种情况下，存储桶拥有者可以创建具有对象访问权限的 Amazon Identity and Access Management（IAM）角色，然后存储桶拥有者可以向另一个 Amazon Web Services 账户授予临时担任该角色的权限，使它可以访问存储桶中的对象。

> **Note**
>
> S3 对象所有权是 Amazon S3 存储桶级别的设置，您可以使用该设置来控制上传到存储桶的对象的所有权和禁用或启用 ACL。默认情况下，对象所有权设为强制存储桶拥有者设置，并且所有 ACL 均处于禁用状态。禁用 ACL 后，存储桶拥有者拥有存储桶中的所有对象，并使用访问管理策略来专门管理对这些对象的访问权限。
>
> Amazon S3 中的大多数现代使用案例不再需要使用 ACL。我们建议您将 ACL 保持为禁用状态，除非有需要单独控制每个对象的访问权限的特殊情况。禁用 ACL 后，您可以使用策略来控制对存储桶中所有对象的访问权限，无论是谁将对象上传到您的存储桶。有关更多信息，请参阅 为您的存储桶控制对象所有权和禁用 ACL。。

了解跨账户权限和使用 IAM 角色

IAM 角色可实现多种资源委托访问权限方案，跨账户访问是重要方案之一。在此示例中，存储桶拥有者（账户 A）使用一个 IAM 角色临时将跨账户对象访问权限委派给另一个 Amazon Web Services 账户（账户 C）中的用户。您创建的每个 IAM 角色都附加了以下两个策略：

- 一个信任策略，用于标识可以担任角色的其他 Amazon Web Services 账户。

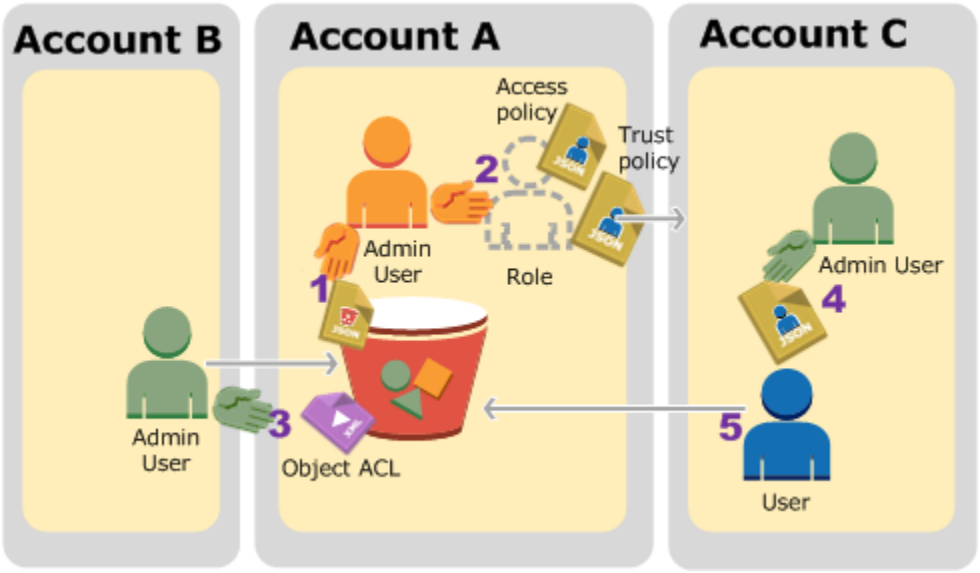
- 一个访问策略，用于定义在某个用户担任角色时允许的权限，例如 `s3:GetObject`。有关可以在策略中指定的权限的列表，请参阅 Amazon S3 的策略操作。

然后，信任策略中标识的 Amazon Web Services 账户向其用户授予担任角色的权限。该用户即可执行以下操作以访问对象：

- 担任角色，然后在响应中获取临时安全凭证。
- 使用临时安全凭证访问存储桶中的对象。

有关 IAM 角色的更多信息，请参阅《IAM 用户指南》中的 IAM 角色。

下面概括介绍演练步骤：




1. 账户 A 管理员用户附加一个存储桶策略，向账户 B 授予上传对象的条件权限。
2. 账户 A 管理员创建一个 IAM 角色，与账户 C 建立信任，以便该账户中的用户可以访问账户 A。附加到该角色的访问策略限制账户 C 中的用户访问账户 A 时可以执行的操作。
3. 账户 B 管理员将一个对象上传到账户 A 拥有的存储桶，从而向存储桶拥有者授予完全控制权限。
4. 账户 C 管理员创建一个用户，附加一个用户策略允许该用户担任该角色。
5. 账户 C 中的用户首先担任角色，这会向该用户返回临时安全凭证。该用户随后使用这些临时凭证访问存储桶中的对象。

对于此示例，您需要三个账户。下表显示我们如何引用这些账户和这些账户中的管理员用户。根据 IAM 准则（请参阅关于使用管理员用户来创建资源和授予权限），我们在本演练中并不使用 Amazon

Web Services 账户根用户 凭证。而是在每个账户中创建一个管理员用户，并在创建资源和向他们授予权限时使用这些凭证。

| Amazon Web Services 账户 ID | 账户名称 | 账户中的管理员用户 |
|---|---|---|
| *1111-1111-1111* | 账户 A | AccountAadmin |
| *2222-2222-2222* | 账户 B | AccountBadmin |
| *3333-3333-3333* | 账户 C | AccountCadmin |

步骤 0：准备演练

> **Note**
>
> 在演练这些步骤时，您可能需要打开文本编辑器，记下某些信息。具体而言，您需要账户 ID、规范用户 ID、供每个账户连接到控制台的 IAM 用户登录 URL，以及 IAM 用户和角色的 Amazon 资源名称（ARN）。

1. 确保您有三个 Amazon Web Services 账户并且每个账户都有一个管理员用户，如前面部分的表中所示。

   a. 根据需要注册 Amazon Web Services 账户。我们将这些账户称为账户 A、账户 B 和账户 C。

   b. 使用账户 A 凭证登录 IAM 控制台，然后执行以下操作以创建管理员用户：

      - 创建用户 **`AccountAadmin`** 并记下其安全凭证。有关添加用户的更多信息，请参阅 IAM 用户指南中的在您的 Amazon Web Services 账户中创建 IAM 用户。
      - 通过附加一个授予完全访问权限的用户策略来向 AccountAadmin 授予管理员权限。有关说明，请参阅《IAM 用户指南》中的管理 IAM 策略。
      - 在 IAM 控制台的控制面板中，记下 IAM 用户登录 URL。此账户中的用户必须在登录 Amazon Web Services Management Console 时使用此 URL。有关更多信息，请参阅《IAM 用户指南》中的 Sign in to the Amazon Web Services Management Console as an IAM user。

   c. 重复上述步骤，在账户 B 和账户 C 中创建管理员用户。

2. 对于账户 C，请记下规范用户 ID。

在账户 A 中创建 IAM 角色时，信任策略通过指定账户 ID 向账户 C 授予担任该角色的权限。您可以查找账户信息，如下所示：

a. 使用 Amazon Web Services 账户 ID 或账户别名、您的 IAM 用户名和密码登录 Amazon S3 控制台。

b. 请选择 Amazon S3 存储桶的名称以查看有关该存储桶的详细信息。

c. 请选择 Permissions (权限) 选项卡，然后选择 Access Control List (访问控制列表)。

d. 在 Access for your Amazon Web Services 账户 (您的 Amazon 账户的访问权限) 部分，Account (账户) 列中是长标识符，例如 `c1daexampleaaf850ea79cf0430f33d72579fd1611c97f7ded193374c0b163b6`。这是您的规范用户 ID。

3. 创建存储桶策略时，您需要以下信息。记下以下值：

- 账户 A 的规范用户 ID – 账户 A 管理员向账户 B 管理员授予条件上传对象权限时，条件指定必须获取对象完全控制权的账户 A 用户的规范用户 ID。

> **Note**
>
> 规范用户 ID 是 Amazon S3 独有的概念。它是 64 字符模糊版本的账户 ID。

- 账户 B 管理员的用户 ARN：您可以在 IAM 控制台中找到用户 ARN。您必须选择该用户并在摘要选项卡中找到该用户的 ARN。

  在存储桶策略中，向 `AccountBadmin` 授予上传对象的权限，使用 ARN 指定用户。下面是一个示例 ARN 值：

```
arn:aws:iam::AccountB-ID:user/AccountBadmin
```

4. 设置 Amazon Command Line Interface (CLI) 或 Amazon Tools for Windows PowerShell。请务必保存管理员用户凭证，如下所示：

- 如果使用 Amazon CLI，请在配置文件中创建配置文件：`AccountAadmin` 和 `AccountBadmin`。
- 如果使用 Amazon Tools for Windows PowerShell，请确保将用于会话的凭证存储为 `AccountAadmin` 和 `AccountBadmin`。

有关说明，请参阅 设置用于演练的工具。

步骤 1：执行账户 A 任务

在此示例中，账户 A 是存储桶拥有者。因此，账户 A 中的用户 AccountAadmin 将执行以下操作：

- 创建存储桶。
- 附加存储桶策略，向账户 B 管理员授予上传对象的权限。
- 创建 IAM 角色，授予账户 C 代入该角色的权限，使其能够访问存储桶中的对象。

步骤 1.1：登录到 Amazon Web Services Management Console

首先使用账户 A 的 IAM 用户登录 URL，以 **AccountAadmin** 用户身份登录 Amazon Web Services Management Console。此用户将创建一个存储桶并向其附加一个策略。

步骤 1.2：创建存储桶并附加存储桶策略

在 Amazon S3 控制台中，执行以下操作：

1. 创建存储桶。此练习假设存储桶名称是 *amzn-s3-demo-bucket1*。

   有关说明，请参阅 创建通用存储桶。
2. 附加以下存储桶策略。该策略向账户 B 管理员授予上传对象的条件权限。

   请通过为 *amzn-s3-demo-bucket1*、*AccountB-ID* 和 *CanonicalUserId-of-AWSaccountA-BucketOwner* 提供自己的值来更新策略。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "111",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::AccountB-ID:user/AccountBadmin"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*"
        },
        {
            "Sid": "112",
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::AccountB-ID:user/AccountBadmin"
```

```
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-grant-full-control": "id=CanonicalUserId-of-
AWSaccountA-BucketOwner"
                }
            }
        }
    ]
}
```

步骤 1.3：在账户 A 中创建一个 IAM 角色以允许账户 C 进行跨账户访问

在 IAM 控制台中创建一个 IAM 角色（**examplerole**），授予账户 C 担任该角色的权限。请务必仍以账户 A 管理员身份登录，因为该角色必须在账户 A 中创建。

1. 创建角色之前，准备好定义角色所需权限的托管策略。您可在以后的步骤中将此策略附加到角色。

   a. 在左侧导航窗格中，请选择策略，然后选择创建策略。

   b. 在 Create Your Own Policy 旁，选择 Select。

   c. 在 Policy Name (策略名称) 字段中输入 **access-accountA-bucket**。

   d. 复制下面的访问策略，然后将其粘贴到 Policy Document (策略文档) 字段中。该访问策略授予该角色 s3:GetObject 权限，这样，账户 C 用户在担任该角色时只能执行 s3:GetObject 操作。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*"
    }
  ]
}
```

   e. 选择创建策略。

      新策略会显示在托管策略列表中。

2. 在左侧的导航窗格中，选择角色，然后选择创建角色。
3. 在选择角色类型下，选择用于跨账户访问的角色，然后单击提供在您的 Amazon Web Services 账户之间进行相互访问的权限旁边的选择按钮。
4. 输入账户 C 的账户 ID。

   对于此演练，您不必要求用户经过多重身份验证（MFA）来承担角色，因此请不要选择该选项。
5. 选择下一步，设置与该角色关联的权限。
6. 选中您创建的 access-accountA-bucket 策略旁边的复选框，然后选择下一步。

   “Review (审核)”页面随即出现，使您可以在创建角色之前确认其设置。此页面上有一项极为重要，需要注意，即您可发送给需要使用此角色的用户的链接。使用该链接的用户会直接转到已填写“账户 ID”和“角色名称 ”字段的切换角色页面。稍后您可以在任何跨账户角色的角色摘要页面上看到此链接。
7. 输入 `examplerole` 作为角色名称，然后单击下一步。
8. 检查角色后，选择创建角色。

   `examplerole` 角色显示在角色列表中。
9. 选择角色名称 `examplerole`。
10. 选择 Trust Relationships (信任关系) 选项卡。
11. 选择显示策略文档并验证所示信任策略是否与以下策略相符。

    以下信任策略通过允许账户 C 执行 `sts:AssumeRole` 操作，与它建立信任。有关更多信息，请参阅 Amazon Security Token Service API 参考中的 AssumeRole。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::AccountC-ID:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

12. 记下您创建的 examplerole 角色的 Amazon 资源名称（ARN）。

    稍后在以下步骤中，您附加一个用户策略以允许 IAM 用户担任此角色，并通过 ARN 值标识角色。

步骤 2：执行账户 B 任务

账户 A 拥有的示例存储桶需要由其它账户拥有的对象。在此步骤中，账户 B 管理员使用命令行工具上传对象。

- 使用 put-object Amazon CLI 命令，将对象上传到 *amzn-s3-demo-bucket1*。

  ```
  aws s3api put-object --bucket amzn-s3-demo-bucket1 --key HappyFace.jpg --
  body HappyFace.jpg --grant-full-control id="canonicalUserId-ofTheBucketOwner" --
  profile AccountBadmin
  ```

  请注意以下几点：

  - --Profile 参数指定 AccountBadmin 配置文件，因此该对象由账户 B 拥有。
  - 参数 grant-full-control 根据存储桶策略的要求向存储桶拥有者授予对象的完全控制权限。
  - --body 参数标识要上传的源文件。例如，如果该文件在 Windows 计算机上的 C: 驱动器中，您应指定 c:\HappyFace.jpg。

步骤 3：执行账户 C 任务

在前面的步骤中，账户 A 已创建一个角色 examplerole，与账户 C 建立了信任。该角色使账户 C 中的用户可以访问账户 A。在此步骤中，账户 C 管理员创建一个用户（Dave），向他委派从账户 A 收到的 sts:AssumeRole 权限。此方法让 Dave 可以担任 examplerole 并临时获取对账户 A 的访问权限。账户 A 附加到该角色的访问策略将限制 Dave 在访问账户 A 时可以执行的操作，具体而言，就是获取 *amzn-s3-demo-bucket1* 中的对象。

步骤 3.1：在账户 C 中创建一个用户并向其委派担任 examplerole 的权限

1. 首先使用账户 C 的 IAM 用户登录 URL，以 **AccountCadmin** 用户身份登录 Amazon Web Services Management Console。

2. 在 IAM 控制台中，创建用户 Dave。

有关分步说明，请参阅《IAM 用户指南》中的创建 IAM 用户（Amazon Web Services Management Console）。

3. 记下 Dave 的凭证。Dave 需要这些凭证才能担任 `examplerole` 角色。
4. 为 IAM 用户 Dave 创建一个内联策略，向 Dave 委派担任账户 A 中的 `examplerole` 角色的 `sts:AssumeRole` 权限。

   a. 在左侧导航窗格中，请选择用户。

   b. 请选择用户名 Dave。

   c. 在用户详细信息页面上，选择 Permissions (权限) 选项卡，然后展开 Inline Policies (内联策略) 部分。

   d. 请选择 click here (单击此处) (或 Create User Policy (创建用户策略))。

   e. 选择 Custom Policy，然后选择 Select。

   f. 在 Policy Name (策略名称) 字段中为策略输入一个名称。

   g. 将以下策略复制到 Policy Document (策略文档) 字段中。

      您必须提供 *AccountA-ID* 来更新策略。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["sts:AssumeRole"],
      "Resource": "arn:aws:iam::AccountA-ID:role/examplerole"
    }
  ]
}
```

   h. 选择应用策略。

5. 通过添加另一个配置文件 `AccountCDave` 将 Dave 的凭证保存到 Amazon CLI 的配置文件。

```
[profile AccountCDave]
aws_access_key_id = UserDaveAccessKeyID
aws_secret_access_key = UserDaveSecretAccessKey
region = us-west-2
```

步骤 3.2：担任角色（examplerole）并访问对象

现在 Dave 可以访问账户 A 拥有的存储桶中的对象，如下所示：

- Dave 首先使用自己的凭证担任 examplerole。这会返回临时凭证。
- Dave 随后使用临时凭证访问账户 A 的存储桶中的对象。

1. 在命令提示符处，使用 AccountCDave 配置文件运行下面的 Amazon CLI assume-role 命令。

   您必须通过提供 *AccountA-ID*（其中定义了 examplerole）在命令中更新 ARN 值。

   ```
   aws sts assume-role --role-arn arn:aws:iam::AccountA-ID:role/examplerole --profile
    AccountCDave --role-session-name test
   ```

   在响应中，Amazon Security Token Service（Amazon STS）返回临时安全凭证（访问密钥 ID、秘密访问密钥和会话令牌）。
2. 将临时安全凭证保存在 Amazon CLI 配置文件中的 TempCred 配置文件下。

   ```
   [profile TempCred]
   aws_access_key_id = temp-access-key-ID
   aws_secret_access_key = temp-secret-access-key
   aws_session_token = session-token
   region = us-west-2
   ```
3. 在命令提示符处，使用临时凭证运行以下 Amazon CLI 命令以访问对象。例如，该命令指定 head-object API 以检索 HappyFace.jpg 对象的对象元数据。

   ```
   aws s3api get-object --bucket amzn-s3-demo-bucket1 --
   key HappyFace.jpg SaveFileAs.jpg --profile TempCred
   ```

   因为附加到 examplerole 的访问策略允许执行这些操作，所以 Amazon S3 会处理请求。您可以对存储桶中的任何其他对象尝试任何其他操作。

   如果您尝试任何其它操作（例如 get-object-acl），则系统会拒绝权限，因为不允许角色执行该操作。

   ```
   aws s3api get-object-acl --bucket amzn-s3-demo-bucket1 --key HappyFace.jpg --
   profile TempCred
   ```

我们使用用户 Dave 担任角色，并使用临时凭证访问对象。它还可以是账户 C 中访问 *amzn-s3-demo-bucket1* 中的对象的应用程序。应用程序可以获取临时安全凭证，账户 C 可以向应用程序委托担任 `examplerole` 的权限。

步骤 4：清除

1. 完成测试之后，您可以执行以下操作来进行清理：
   - 使用账户 A 凭证登录 Amazon Web Services Management Console，并执行以下操作：
     - 在 Amazon S3 控制台中，移除附加到 *amzn-s3-demo-bucket1* 的存储桶策略。在存储桶 Properties（属性）中，删除 Permissions（权限）部分中的策略。
     - 如果该存储桶是为此练习而创建的，请在 Amazon S3 控制台中删除对象，然后删除存储桶。
     - 在 IAM 控制台中，删除您在账户 A 中创建的 `examplerole`。有关分步说明，请参阅《IAM 用户指南》中的删除 IAM 用户。
     - 在 IAM 控制台中，移除 AccountAadmin 用户。
2. 使用账户 B 凭证登录 IAM 控制台。删除用户 AccountBadmin。
3. 使用账户 C 凭证登录 IAM 控制台。删除 AccountCadmin 和用户 Dave。

相关资源

有关本演练的更多信息，请参阅《IAM 用户指南》中的以下资源：

- 创建向 IAM 用户委派权限的角色
- 教程：使用 IAM 角色委派跨 Amazon Web Services 账户的访问权限
- 管理 IAM 策略

## 将服务相关角色用于 Amazon S3 Storage Lens 存储统计管理工具

要使用 Amazon S3 Storage Lens 存储统计管理工具来收集和聚合 Amazon Organizations 中所有账户的指标，您必须首先确保 S3 Storage Lens 存储统计管理工具具有由企业中的管理账户启用的可信访问权限。S3 Storage Lens 存储统计管理工具将创建一个服务相关角色，使其能够获取属于您组织的 Amazon Web Services 账户的列表。在创建或更新 S3 Storage Lens 存储统计管理工具控制面板或配置时，S3 Storage Lens 存储统计管理工具使用此账户列表来收集所有成员账户中 S3 资源的指标。

Amazon S3 Storage Lens 存储统计管理工具使用 Amazon Identity and Access Management（IAM）服务相关角色。服务相关角色是一种与 S3 Storage Lens 存储统计管理工具直接关联的独特类型的 IAM 角色。服务相关角色由 S3 Storage Lens 存储统计管理工具预定义，具有服务代表您调用其它 Amazon Web Services 服务所需的所有权限。

服务相关角色可让您更轻松地设置 S3 Storage Lens 存储统计管理工具，因为您不必手动添加必要的权限。S3 Storage Lens 存储统计管理工具定义了其服务相关角色的权限，除非另外定义，否则只有 S3 Storage Lens 存储统计管理工具可以代入该角色。定义的权限包括信任策略和权限策略，以及不能附加到任何其他 IAM 实体的权限策略。

只有在先删除相关资源后，才能删除此服务相关角色。这将保护您的 S3 Storage Lens 存储统计管理工具资源，因为您不会无意中删除对资源的访问权限。

有关支持服务相关角色的其他服务的信息，请参阅与 IAM 配合使用的 Amazon 服务，并查找 Service-Linked Role（服务相关角色）列为 Yes（是）的服务。请选择 Yes 与查看该服务的服务相关角色文档的链接。

## Amazon S3 Storage Lens 存储统计管理工具的服务相关角色权限

S3 Storage Lens 存储统计管理工具使用名为 AWSServiceRoleForS3StorageLens 的服务相关角色 – 这支持访问 S3 Storage Lens 存储统计管理工具使用或管理的 Amazon 服务和资源。这允许 S3 Storage Lens 存储统计管理工具代表您访问 Amazon Organizations 资源。

S3 Storage Lens 存储统计管理工具服务相关角色信任组织存储上的以下服务：

- `storage-lens.s3.amazonaws.com`

角色权限策略允许 S3 Storage Lens 存储统计管理工具完成以下操作：

- `organizations:DescribeOrganization`

  `organizations:ListAccounts`

  `organizations:ListAWSServiceAccessForOrganization`

  `organizations:ListDelegatedAdministrators`

您必须配置权限以允许 IAM 实体（例如，用户、组或角色）创建、编辑或删除服务相关角色。有关更多信息，请参阅 IAM 用户指南中的服务相关角色权限。

## 为 S3 Storage Lens 存储统计管理工具创建服务相关角色

您无需手动创建服务相关角色。当您在登录 Amazon Organizations 管理或委托管理员账户时完成以下任务之一后，S3 Storage Lens 存储统计管理工具将为您创建服务相关角色：

- 在 Amazon S3 控制台中为您的组织创建 S3 Storage Lens 存储统计管理工具控制面板配置。
- 使用 REST API、Amazon CLI 和 SDK 为您的企业 PUT S3 Storage Lens 存储统计管理工具配置。

> **Note**
>
> S3 Storage Lens 存储统计管理工具最多将为每个组织支持五名委派管理员。

如果删除此服务相关角色，则上述操作将根据需要重新创建该角色。

S3 Storage Lens 存储统计管理工具服务相关角色的示例策略

Example S3 Storage Lens 存储统计管理工具服务相关角色的权限策略

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AwsOrgsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListDelegatedAdministrators"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

## 为 Amazon S3 Storage Lens 存储统计管理工具编辑服务相关角色

S3 Storage Lens 存储统计管理工具不允许您编辑 AWSServiceRoleForS3StorageLens 服务相关角色。在创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。不过，您可以使用 IAM 编辑角色的说明。有关更多信息，请参阅 IAM 用户指南中的编辑服务相关角色。

## 删除 Amazon S3 Storage Lens 存储统计管理工具的服务相关角色

如果您不再使用服务相关角色，我们建议您删除该角色。这样您就没有未被主动监控或维护的未使用实体。但是，您必须先清除服务相关角色的资源，然后才能手动删除它。

> **Note**
>
> 如果在您试图删除资源时 Amazon S3 Storage Lens 存储统计管理工具服务正在使用该角色，则删除操作可能会失败。如果发生这种情况，则请等待几分钟后重试。

要删除 AWSServiceRoleForS3StorageLens，您必须使用 Amazon Organizations 管理或委派管理员账户删除所有 Amazon Web Services 区域中存在的所有组织级别 S3 Storage Lens 存储统计管理工具配置。

这些资源是组织级 S3 Storage Lens 存储统计管理工具配置。使用 S3 Storage Lens 存储统计管理工具清理资源，然后使用 IAM 控制台、CLI、REST API 或 Amazon SDK 删除角色。

在 REST API、Amazon CLI 和 SDK 中，可以在组织创建 S3 Storage Lens 存储统计管理工具配置的所有区域中使用 `ListStorageLensConfigurations` 发现 S3 Storage Lens 存储统计管理工具配置。使用操作 `DeleteStorageLensConfiguration` 删除这些配置，以便随后可以删除角色。

> **Note**
>
> 要删除服务相关角色，您必须在存在这些配置的所有区域中删除所有组织级 S3 Storage Lens 配置。

删除 AWSServiceRoleForS3StorageLens SLR 使用的 Amazon S3 Storage Lens 存储统计管理工具资源

1. 要获取您的组织级别配置的列表，您必须在具有 S3 Storage Lens 存储统计管理工具配置的每个区域中使用 `ListStorageLensConfigurations`。此列表也可以从 Amazon S3 控制台获取。

2. 通过调用 `DeleteStorageLensConfiguration` API 调用或通过使用 Amazon S3 控制台从适当的区域端点中删除这些配置。

使用 IAM 手动删除服务相关角色

删除配置后，可以从 IAM 控制台中，或通过调用 IAM API `DeleteServiceLinkedRole`，或使用 Amazon CLI 或 Amazon SDK 删除 AWSServiceRoleForS3StorageLens SLR。有关更多信息，请参阅 IAM 用户指南中的删除服务相关角色。

### S3 Storage Lens 存储统计管理工具服务相关角色的受支持区域

S3 Storage Lens 存储统计管理工具支持在提供服务相关角色的所有 Amazon Web Services 区域中使用该服务。有关更多信息，请参阅 Amazon S3 区域和端点。

## Amazon S3 身份和访问问题排查

可以使用以下信息，协助您诊断和修复在使用 Amazon S3 和 IAM 时可能遇到的常见问题。

主题

- 我收到了拒绝访问错误
- 我无权在 Amazon S3 中执行操作
- 我无权执行 iam:PassRole
- 我希望允许我的 Amazon Web Services 账户以外的人访问我的 Amazon S3 资源
- 排查 Amazon S3 中的拒绝访问（403 Forbidden）错误

### 我收到了拒绝访问错误

确认无论是在存储桶策略还是基于身份的策略中，都没有针对您尝试向其授予权限的请求者使用显式 `Deny` 语句。

有关排查拒绝访问错误的详细信息，请参阅排查 Amazon S3 中的拒绝访问（403 Forbidden）错误。

### 我无权在 Amazon S3 中执行操作

如果您收到错误提示，指明您无权执行某个操作，则必须更新策略以允许执行该操作。

当 `mateojackson` IAM 用户尝试使用控制台查看有关虚构 *`my-example-widget`* 资源的详细信息，但不拥有虚构 `s3:`*`GetWidget`* 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 s3:GetWidget on resource: my-example-widget
```

在此情况下，必须更新 mateojackson 用户的策略，以允许使用 s3:*GetWidget* 操作访问 *my-example-widget* 资源。

如果您需要帮助，请联系 Amazon 管理员。您的管理员是提供登录凭证的人。

## 我无权执行 iam:PassRole

如果您收到一个错误，表明您无权执行 iam:PassRole 操作，则必须更新策略以允许您将角色传递给 Amazon S3。

有些 Amazon Web Services 服务 允许将现有角色传递到该服务，而不是创建新服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为 marymajor 的 IAM 用户尝试使用控制台在 Amazon S3 中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 iam:PassRole 操作。

如果您需要帮助，请联系 Amazon 管理员。您的管理员是提供登录凭证的人。

## 我希望允许我的 Amazon Web Services 账户以外的人访问我的 Amazon S3 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以代入角色。对于支持基于资源的策略或访问控制列表（ACL）的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解 Amazon S3 是否支持这些功能，请参阅Amazon S3 如何与 IAM 配合使用。
- 要了解如何为您拥有的 Amazon Web Services 账户中的资源提供访问权限，请参阅《IAM 用户指南》中的为您拥有的另一个 Amazon Web Services 账户中的 IAM 用户提供访问权限。
- 要了解如何为第三方 Amazon Web Services 账户 提供您的资源的访问权限，请参阅《IAM 用户指南》中的为第三方拥有的 Amazon Web Services 账户 提供访问权限。

- 要了解如何通过身份联合验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（身份联合验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

## 排查 Amazon S3 中的拒绝访问（403 Forbidden）错误

当 Amazon 显式或隐式拒绝授权请求时，将显示拒绝访问（HTTP 403 Forbidden）错误。

- 当策略包含特定的 Amazon 操作的 Deny 语句时，将发生显式拒绝。
- 当没有适用的 Deny 语句且没有适用的 Allow 语句时，会发生隐式拒绝。

由于 Amazon Identity and Access Management（IAM）策略默认情况下隐式拒绝 IAM 主体，因此该策略必须显式支持主体执行操作。否则，该策略会隐式拒绝访问。有关更多信息，请参阅《IAM 用户指南》中的显式拒绝和隐式拒绝之间的区别。有关确定是支持还是拒绝访问请求的策略评估逻辑的信息，请参阅《IAM 用户指南》中的策略评估逻辑。

有关按 S3 资源类型对 S3 API 操作的权限的更多信息，请参阅 Amazon S3 API 操作所需的权限。

以下主题涵盖了 Amazon S3 中拒绝访问错误的最常见原因。

> **Note**
>
> 对于拒绝访问（HTTP 403 Forbidden）错误，如果请求是在存储桶拥有者的个人 Amazon 账户或存储桶拥有者的 Amazon 组织外部发起的，则 S3 不会向存储桶拥有者收费。

主题

- 拒绝访问消息示例以及如何对其进行故障排除
- 桶策略和 IAM policy
- Amazon S3 ACL 设置
- S3 屏蔽公共访问权限设置
- Amazon S3 加密设置
- S3 对象锁定设置
- VPC 端点策略
- Amazon Organizations 策略

- 接入点设置

> **Note**
>
> 如果您正在尝试对权限问题进行故障排除，请从the section called “拒绝访问消息示例以及如何对其进行故障排除”一节开始，然后转到???一节。另外，请务必遵循the section called “有关检查权限的提示”中的指导。

拒绝访问消息示例以及如何对其进行故障排除

Amazon S3 现在对于对同一 Amazon Web Services 账户内的资源发出的请求，在拒绝访问（HTTP `403 Forbidden`）错误中包含额外的上下文。这个新的上下文包括拒绝访问的策略类型、拒绝的原因，以及有关请求访问该资源的 IAM 用户或角色的信息。

此附加上下文有助于您解决访问问题，确定拒绝访问错误的根本原因，并通过更新相关策略来修复不正确的访问控制。此附加上下文也可以在 Amazon CloudTrail 日志中找到。针对同账号请求的增强拒绝访问错误消息现已在所有 Amazon Web Services 区域推出，包括 Amazon GovCloud (US) Regions和中国区域。

大多数拒绝访问的错误消息都以 `User` *`user-arn`* `is not authorized to perform` *`action`* `on "`*`resource-arn`*`" because` *`context`* 格式显示。在此示例中，*`user-arn`* 是未获得访问权限的用户的 Amazon 资源名称（ARN），*`action`* 是策略拒绝的服务操作，而 *`resource-arn`* 是策略对其执行操作的资源的 ARN。*`context`* 字段表示有关策略类型的其它上下文，用于解释策略拒绝访问的原因。

当策略因其包含 `Deny` 语句而显式拒绝访问时，拒绝访问错误消息中将包含短语 `with an explicit deny in a` *`type`* `policy`。当策略隐式拒绝访问时，拒绝访问错误消息中将包含短语 `because no` *`type`* `policy allows the` *`action`* `action`。

> **Important**
>
> - 仅针对同账号请求才返回增强拒绝访问消息。跨账户请求会返回一条一般 `Access Denied` 消息。
>
>  有关确定是支持还是拒绝跨账户访问请求的策略评估逻辑的信息，请参阅《IAM 用户指南》中的跨账户策略评估逻辑。有关说明如何授予跨账户访问权限的演练，请参阅the section called “授予跨账户权限”。

- 向目录存储桶发出的请求不会返回增强拒绝访问错误消息。目录存储桶请求会返回一条一般 `Access Denied` 消息。
- 如果同一策略类型的多个策略拒绝授权请求，拒绝访问错误消息不指定策略的数量。
- 如果多种策略类型拒绝授权请求，则错误消息仅包含其中一种策略类型。
- 如果由于多种原因而拒绝访问请求，则错误消息仅包含拒绝原因之一。

下面的示例展示了不同类型的拒绝访问错误消息的格式以及如何对每种类型的消息进行故障排除。

由于资源控制策略而拒绝访问 – 显式拒绝

1. 检查资源控制策略（RCP）中的操作是否有 `Deny` 语句。对于以下示例，操作为 `s3:GetObject`。
2. 通过删除 `Deny` 语句来更新 RCP。有关更多信息，请参阅《Amazon Organizations User Guide》中的 Update a resource control policy (RCP)。

```
An error occurred (AccessDenied) when calling the GetObject operation:
User: arn:aws:iam::777788889999:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name"
with an explicit deny in a resource control policy
```

由于服务控制策略而拒绝访问 – 隐式拒绝

1. 检查服务控制策略（SCP）中的操作是否有缺少的 `Allow` 语句。对于以下示例，操作为 `s3:GetObject`。
2. 通过添加 `Allow` 语句来更新 SCP。有关更多信息，请参阅 Amazon Organizations 用户指南中的更新 SCP。

```
User: arn:aws:iam::777788889999:user/MaryMajor is not authorized to perform:
s3:GetObject because no service control policy allows the s3:GetObject action
```

由于服务控制策略而拒绝访问 – 显式拒绝

1. 检查服务控制策略（SCP）中的操作是否有 `Deny` 语句。对于以下示例，操作为 `s3:GetObject`。
2. 通过更改 `Deny` 语句以支持用户获得必要的访问权限，来更新您的 SCP。有关如何执行此操作的示例，请参阅《Amazon Organizations 用户指南》中的 Prevent IAM users and roles from making

specified changes, with an exception for a specified admin role。有关更新 SCP 的更多信息，请参阅《Amazon Organizations 用户指南》中的 Updating an SCP。

```
User: arn:aws:iam::777788889999:user/MaryMajor is not authorized to perform:
s3:GetObject with an explicit deny in a service control policy
```

由于 VPC 端点策略而拒绝访问 – 隐式拒绝

1. 检查虚拟私有云（VPC）端点策略中的操作是否有缺失的 `Allow` 语句。对于以下示例，操作为 `s3:GetObject`。
2. 通过添加 `Allow` 语句来更新 VPC 端点策略。有关更多信息，请参阅《Amazon PrivateLink 指南》中的更新 VPC 端点策略。

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject because no VPC endpoint policy allows the s3:GetObject action
```

由于 VPC 端点策略而拒绝访问 – 显式拒绝

1. 检查虚拟私有云（VPC）端点策略中的操作是否有显式 `Deny` 语句。对于以下示例，操作为 `s3:GetObject`。
2. 通过更改 `Deny` 语句以支持用户获得必要的访问权限，来更新 VPC 端点策略。例如，可以更新 `Deny` 语句来使用 `aws:PrincipalAccount` 条件键和 `StringNotEquals` 条件运算符，从而支持特定的主体进行访问，如the section called “示例 7：从 Deny 语句中排除主体”中所示。有关更新 VPC 端点策略的更多信息，请参阅《Amazon PrivateLink 指南》中的 Update a VPC endpoint policy。

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name" with
an explicit deny in a VPC endpoint policy
```

由于权限边界而拒绝访问 – 隐式拒绝

1. 检查权限边界中的操作是否有缺失的 `Allow` 语句。对于以下示例，操作为 `s3:GetObject`。
2. 通过将 `Allow` 语句添加到 IAM policy 来更新权限边界。有关更多信息，请参阅《IAM 用户指南》中的 IAM 实体的权限边界和编辑 IAM 策略。

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name"
because no permissions boundary allows the s3:GetObject action
```

由于权限边界而拒绝访问 – 显式拒绝

1. 检查权限边界中的操作是否有显式 Deny 语句。对于以下示例，操作为 s3:GetObject。
2. 通过更改 IAM 策略中的 Deny 语句以支持用户获得必要的访问权限，来更新您的权限边界。例如，可以更新 Deny 语句来使用 aws:PrincipalAccount 条件键和 StringNotEquals 条件运算符，从而支持特定的主体进行访问，如《IAM 用户指南》中的 aws:PrincipalAccount 所示。有关更多信息，请参阅《IAM 用户指南》中的 IAM 实体的权限边界和编辑 IAM 策略。

```
User: arn:aws:iam::777788889999:user/MaryMajor is not authorized to perform:
s3:GetObject with an explicit deny in a permissions boundary
```

由于会话策略而拒绝访问 – 隐式拒绝

1. 检查会话策略中的操作是否有缺失的 Allow 语句。对于以下示例，操作为 s3:GetObject。
2. 通过添加 Allow 语句来更新会话策略。有关更多信息，请参阅《IAM 用户指南》中的会话策略和编辑 IAM 策略。

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject because no session policy allows the s3:GetObject action
```

由于会话策略而拒绝访问 – 显式拒绝

1. 检查会话策略中的操作是否有显式 Deny 语句。对于以下示例，操作为 s3:GetObject。
2. 通过更改 Deny 语句以支持用户获得必要的访问权限，来更新您的会话策略。例如，可以更新 Deny 语句来使用 aws:PrincipalAccount 条件键和 StringNotEquals 条件运算符，从而支持特定的主体进行访问，如the section called “示例 7：从 Deny 语句中排除主体”中所示。有关更新会话策略的更多信息，请参阅《IAM 用户指南》中的会话策略和编辑 IAM 策略。

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name" with
an explicit deny in a session policy
```

由于基于资源的策略而拒绝访问 – 隐式拒绝

> **Note**
>
> 基于资源的策略 是指诸如存储桶策略和接入点策略之类的策略。

1. 检查基于资源的策略中的操作是否有缺失的 `Allow` 语句。还要检查 `IgnorePublicAcls` S3 屏蔽公共访问权限设置是否应用于存储桶、接入点或账户级。对于以下示例，操作为 `s3:GetObject`。
2. 通过添加 `Allow` 语句来更新策略。有关更多信息，请参阅《IAM 用户指南》中的基于资源的策略和编辑 IAM 策略。

   您可能还需要调整存储桶、接入点或账户的 `IgnorePublicAcls` 屏蔽公共访问权限设置。有关更多信息，请参阅the section called “由于屏蔽公共访问权限设置而拒绝访问”和the section called “配置存储桶和接入点设置”。

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject because no resource-based policy allows the s3:GetObject action
```

由于基于资源的策略而拒绝访问 – 显式拒绝

> **Note**
>
> 基于资源的策略 是指诸如存储桶策略和接入点策略之类的策略。

1. 检查基于资源的策略中的操作是否有显式 `Deny` 语句。还要检查 `RestrictPublicBuckets` S3 屏蔽公共访问权限设置是否应用于存储桶、接入点或账户级。对于以下示例，操作为 `s3:GetObject`。
2. 通过更改 `Deny` 语句以支持用户获得必要的访问权限，来更新您的策略。例如，可以更新 `Deny` 语句来使用 `aws:PrincipalAccount` 条件键和 `StringNotEquals` 条件运算符，从而支持特定的主体进行访问，如the section called “示例 7：从 Deny 语句中排除主体”中所示。有关更新基于资源的策略的更多信息，请参阅《IAM 用户指南》中的基于资源的策略和编辑 IAM 策略。

   您可能还需要调整存储桶、接入点或账户的 `RestrictPublicBuckets` 屏蔽公共访问权限设置。有关更多信息，请参阅the section called “由于屏蔽公共访问权限设置而拒绝访问”和the section called “配置存储桶和接入点设置”。

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name" with
an explicit deny in a resource-based policy
```

由于基于身份的策略而拒绝访问 – 隐式拒绝

1. 检查附加到身份的基于身份的策略中的操作中是否有缺失的 Allow 语句。对于以下示例，操作为附加到用户 MaryMajor 的 s3:GetObject。
2. 通过添加 Allow 语句来更新策略。有关更多信息，请参阅《IAM 用户指南》中的基于身份的策略和编辑 IAM 策略。

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject because no identity-based policy allows the s3:GetObject action
```

由于基于身份的策略而拒绝访问 – 显式拒绝

1. 检查附加到身份的基于身份的策略中的操作中是否有显式 Deny 语句。对于以下示例，操作为附加到用户 MaryMajor 的 s3:GetObject。
2. 通过更改 Deny 语句以支持用户获得必要的访问权限，来更新您的策略。例如，可以更新 Deny 语句来使用 aws:PrincipalAccount 条件键和 StringNotEquals 条件运算符，从而支持特定的主体进行访问，如《IAM 用户指南》中的 aws:PrincipalAccount 所示。有关更多信息，请参阅《IAM 用户指南》中的基于身份的策略和编辑 IAM 策略。

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name" with
an explicit deny in an identity-based policy
```

由于屏蔽公共访问权限设置而拒绝访问

Amazon S3 屏蔽公共访问权限特征提供接入点、存储桶和账户设置，帮助您管理对 Amazon S3 资源的公有访问。有关 Amazon S3 如何定义“公共”的更多信息，请参阅“公有”的含义。

默认情况下，新存储桶、接入点和对象不允许公有访问。但是，用户可以修改存储桶策略、接入点策略、IAM 用户策略、对象权限或访问控制列表（ACL）来支持公共访问权限。S3 屏蔽公共访问权限设置会覆盖这些策略、权限和 ACL。自 2023 年 4 月起，默认情况下为新存储桶启用所有屏蔽公共访问权限设置。

当 Amazon S3 收到访问存储桶或对象的请求时，它将确定该存储桶或存储桶拥有者的账户是否应用了屏蔽公共访问权限设置。如果请求是通过接入点发出，则 Amazon S3 还会检查接入点的屏蔽公共访问权限设置。如果现有的屏蔽公共访问权限设置禁止请求的访问，则 Amazon S3 将拒绝该请求。

Amazon S3 屏蔽公共访问权限提供四种设置。这些设置彼此独立，可任意组合使用。每个设置都可以应用于访问点、存储桶或整个 Amazon 账户。如果接入点、存储桶或账户的屏蔽公共访问权限设置不同，则 Amazon S3 应用接入点、存储桶和账户设置的最严格组合。

当 Amazon S3 评估屏蔽公共访问权限设置是否禁止某一操作时，它将拒绝违反接入点、存储桶或账户设置的任何请求。

Amazon S3 屏蔽公共访问权限提供的四种设置如下：

- `BlockPublicAcls` – 此设置适用于 `PutBucketAcl`、`PutObjectAcl`、`PutObject`、`CreateBucket`、`CopyObject` 和 `POST Object` 请求。`BlockPublicAcls` 设置会导致以下行为：
  - 如果指定的访问控制列表（ACL）为公有，`PutBucketAcl` 和 `PutObjectAcl` 调用将失败。
  - 如果请求包含公有 ACL，则 `PutObject` 调用失败。
  - 如果将此设置应用于某个账户，则当请求包含公有 ACL 时，`CreateBucket` 调用将失败，并返回 HTTP `400` (`Bad Request`) 响应。

  例如，当对 `CopyObject` 请求的访问因 `BlockPublicAcls` 设置而被拒绝时，您将收到以下消息：

  ```
  An error occurred (AccessDenied) when calling the CopyObject operation:
  User: arn:aws:sts::123456789012:user/MaryMajor is not authorized to
  perform: s3:CopyObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name"
  because public access control lists (ACLs) are blocked by the BlockPublicAcls block
  public access setting.
  ```

- `IgnorePublicAcls` – `IgnorePublicAcls` 设置会使 Amazon S3 忽略存储桶及其包含的任何对象上的所有公有 ACL。如果您的请求的权限仅由公共 ACL 授予，则 `IgnorePublicAcls` 设置会拒绝该请求。

  由 `IgnorePublicAcls` 设置导致的任何拒绝都是隐式的。例如，如果 `IgnorePublicAcls` 因公有 ACL 而拒绝 `GetObject` 请求，您将收到以下消息：

  ```
  User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
  s3:GetObject because no resource-based policy allows the s3:GetObject action
  ```

- `BlockPublicPolicy` – 此设置适用于 `PutBucketPolicy` 和 `PutAccessPointPolicy` 请求。

  为存储桶设置 `BlockPublicPolicy` 将导致 Amazon S3 在指定的存储桶策略支持公共访问权限时拒绝对 `PutBucketPolicy` 的调用。如果指定的策略支持公共访问权限，则此设置也会导致 Amazon S3 针对存储桶的所有相同账户接入点拒绝对 `PutAccessPointPolicy` 的调用。

  如果（为接入点或底层存储桶）指定的策略支持公共访问权限，则为接入点设置 `BlockPublicPolicy` 会导致 Amazon S3 拒绝通过该接入点对 `PutAccessPointPolicy` 和 `PutBucketPolicy` 进行的调用。

  例如，当对 `PutBucketPolicy` 请求的访问因 `BlockPublicPolicy` 设置而被拒绝时，您将收到以下消息：

  ```
  An error occurred (AccessDenied) when calling the PutBucketPolicy operation:
  User: arn:aws:sts::123456789012:user/MaryMajor is not authorized to
  perform: s3:PutBucketPolicy on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-
  name"
  because public policies are blocked by the BlockPublicPolicy block public
  access setting.
  ```

- `RestrictPublicBuckets` – `RestrictPublicBuckets` 设置会将使用公有策略对接入点或存储桶的访问权限限制为仅该存储桶拥有者账户和接入点拥有者账户中的 Amazon Web Services 服务主体和授权用户。此设置会阻止对接入点或存储桶的所有跨账户访问（Amazon Web Services 服务主体的访问除外），但仍支持该账户内的用户管理接入点或存储桶。此设置还拒绝所有匿名（或未签名的）调用。

  由 `RestrictPublicBuckets` 设置导致的任何拒绝都是显式的。例如，如果 `RestrictPublicBuckets` 因公有存储桶或接入点策略而拒绝 `GetObject` 请求，您将收到以下消息：

  ```
  User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
  s3:GetObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name" with
  an explicit deny in a resource-based policy
  ```

有关这些设置的更多信息，请参阅 the section called “屏蔽公共访问权限设置”。要查看和更新这些设置，请参阅the section called “配置屏蔽公共访问权限”。

桶策略和 IAM policy

存储桶级别操作

如果没有存储桶策略，则存储桶会隐式支持来自存储桶拥有者账户中任何 Amazon Identity and Access Management（IAM）身份的请求。桶还隐式拒绝来自任何其他账户的任何其他 IAM 身份的请求以及匿名（未签名）请求。但是，如果没有 IAM 用户策略，则会隐式拒绝请求者（除非他们是 Amazon Web Services 账户根用户）发出任何请求。有关此评估逻辑的更多信息，请参阅《IAM 用户指南》中的确定是允许还是拒绝账户内的请求。

对象级别操作

如果对象归桶拥有者账户拥有，则桶策略和 IAM 用户策略在对象级别操作中的运作方式与在桶级别操作中的运行方式相同。例如，如果没有存储桶策略，则存储桶会隐式支持来自存储桶拥有者账户中任何 IAM 身份的对象请求。桶还隐式拒绝来自任何其他账户的任何其他 IAM 身份的对象请求以及匿名（未签名）请求。但是，如果没有 IAM 用户策略，则会隐式拒绝请求者（除非他们是 Amazon Web Services 账户根用户）发出任何对象请求。

如果对象归外部账户拥有，则只能通过对象访问控制列表（ACL）授予对该对象的访问权限。桶策略和 IAM 用户策略仍可用于拒绝对象请求。

因此，为确保存储桶策略或 IAM 用户策略不会导致拒绝访问（403 禁止）错误，请确保满足以下要求：

- 对于同账户访问，无论是在桶策略还是 IAM 用户策略中，都不得针对您尝试向其授予权限的请求者使用显式 `Deny` 语句。如果您想仅使用桶策略和 IAM 用户策略授予权限，则其中一个策略中必须至少有一条显式 `Allow` 语句。
- 对于跨账户访问，无论是在存储桶策略还是 IAM 用户策略中，都不得针对您尝试向其授予权限的请求者使用显式 `Deny` 语句。要仅使用存储桶策略和 IAM 用户策略授予跨账户权限，请确保请求者的存储桶策略和 IAM 用户策略都包含显式 `Allow` 语句。

> **Note**
>
> 桶策略中的 `Allow` 语句仅适用于由同一桶拥有者账户拥有的对象。但是，无论对象所有权如何，桶策略中的 `Deny` 语句都适用于所有对象。

### 查看或编辑您的桶策略

> **Note**
>
> 要查看或编辑桶策略，您必须拥有 `s3:GetBucketPolicy` 权限。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 从桶列表中，选择要查看或编辑其桶策略的桶的名称。
4. 选择 Permissions（权限）选项卡。
5. 在 Bucket policy（存储桶策略）下，请选择 Edit（编辑）。将出现 Edit bucket policy（编辑存储桶策略）页面。

要使用 Amazon Command Line Interface（Amazon CLI）查看或编辑您的桶策略，请使用 get-bucket-policy 命令。

> **Note**
>
> 如果您因为存储桶策略不正确而被锁定在存储桶之外，sign in to the Amazon Web Services Management Console by using your Amazon Web Services 账户 root user credentials（请使用 Amazon 账户根用户凭证登录 Amazon 管理控制台）。要重新获得对存储桶的访问权限，请务必使用 Amazon Web Services 账户根用户凭证删除不正确的存储桶策略。

### 有关检查权限的提示

要检查请求者是否具有执行 Amazon S3 操作的适当权限，请尝试以下操作：

- 确定请求者。如果是未签名的请求，则它是没有 IAM 用户策略的匿名请求。如果这是使用预签名 URL 的请求，则用户策略会与对请求进行签名的 IAM 用户或角色的策略相同。
- 验证您使用的是正确的 IAM 用户或角色。您可以通过检查 Amazon Web Services Management Console的右上角或使用 aws sts get-caller-identity 命令来验证您的 IAM 用户或角色。
- 检查与 IAM 用户或角色相关的 IAM policy。您可以使用以下方法之一：
  - 使用 IAM policy simulator 测试 IAM policy。
  - 查看不同的 IAM policy 类型。

- 如果需要，编辑您的 IAM 用户策略。
- 查看以下显式拒绝或允许访问的策略示例：
  - 显式允许 IAM 用户策略：IAM：允许和拒绝以编程方式和在控制台中访问多个服务
  - 显式允许桶策略：授予多个账户上传对象或设置对象 ACL 以进行公共访问的权限
  - 显式拒绝 IAM 用户策略：Amazon：根据请求的 Amazon Web Services 区域拒绝访问 Amazon
  - 显式拒绝桶策略：要求对写入桶的所有对象使用 SSE-KMS

Amazon S3 ACL 设置

检查 ACL 设置时，请先查看您的对象所有权设置，以检查桶上是否已启用 ACL。请注意，ACL 权限只能用于授予权限，而不能用于拒绝请求。对于由存储桶策略或 IAM 用户策略中的显式拒绝而被拒绝的请求者，ACL 也不能用于向他们授予访问权限。

对象所有权设置设为强制桶拥有者

如果启用了强制桶拥有者设置，则 ACL 设置不太可能导致拒绝访问（403 禁止）错误，因为此设置会禁用适用于桶和对象的所有 ACL。强制桶拥有者是 Amazon S3 桶的原定设置，并且是推荐设置。

对象所有权设置设为首选桶拥有者或对象写入者

使用首选桶拥有者设置或对象编写者设置时，ACL 权限仍然有效。ACL 有两种：桶 ACL 和对象 ACL。有关这两种类型的 ACL 之间的区别，请参阅 ACL 权限和访问策略权限的映射。

根据被拒绝的请求的操作，检查您的桶或对象的 ACL 权限：

- 如果 Amazon S3 拒绝了 `LIST`、`PUT` 对象、`GetBucketAcl` 或 `PutBucketAcl` 请求，请查看您的桶的 ACL 权限。

  > **Note**
  >
  > 您无法使用存储桶 ACL 设置授予 `GET` 对象权限。

- 如果 Amazon S3 拒绝了对 S3 对象的 `GET` 请求或拒绝了 PutObjectAcl 请求，请查看该对象的 ACL 权限。

  > **Important**
  >
  > 如果拥有该对象的账户与拥有该桶的账户不同，则对该对象的访问权限不受桶策略控制。

排查在跨账户对象所有权期间来自 **GET** 对象请求的拒绝访问（403 禁止）错误

查看桶的对象所有权设置以确定对象拥有者。如果您有权访问对象 ACL，则还可以检查对象拥有者的账户。（要查看对象拥有者的账户，请在 Amazon S3 控制台中查看对象 ACL 设置。）或者，您也可以发出 `GetObjectAcl` 请求，以查找对象拥有者的规范 ID 来验证对象拥有者账户。原定设置情况下，ACL 为对于对象拥有者账户的 `GET` 请求授予显式允许权限。

确认对象拥有者与桶拥有者不同后，根据您的使用案例和访问级别，选择以下方法之一来帮助解决拒绝访问（403 禁止）错误：

- 禁用 ACL（推荐）– 此方法适用于所有对象，可由桶拥有者执行。这种方法自动向桶拥有者授予对桶中每个对象的所有权和完全控制权。在实施此方法之前，请检查禁用 ACL 的先决条件。有关如何将您的桶设置为强制桶拥有者（推荐）模式的信息，请参阅在现有桶上设置对象所有权。

  > **Important**
  >
  > 为防止拒绝访问（403 禁止）错误，请务必在禁用 ACL 之前将 ACL 权限迁移到桶策略。有关更多信息，请参阅从 ACL 权限迁移的桶策略示例。

- 将对象拥有者更改为桶拥有者 - 此方法可以应用于单个对象，但只有对象拥有者（或具有相应权限的用户）才能更改对象的所有权。可能会收取额外的 PUT 费用。（有关更多信息，请参阅 Amazon S3 定价。）此方法向桶拥有者授予对象的完全所有权，允许桶拥有者通过桶策略控制对于对象的访问权限。

  要更改对象的所有权，请执行以下操作之一：

  - 您（桶拥有者）可以将对象复制回桶。
  - 您可以将桶的对象所有权设置更改为首选桶拥有者。如果禁用版本控制，则桶中的对象将被覆盖。如果启用了版本控制，则同一对象的重复版本将出现在桶中，而桶拥有者可以将生命周期规则设置为过期。有关如何更改对象所有权设置的说明，请参阅为现有存储桶设置对象所有权。

    > **Note**
    >
    > 当您将对象所有权设置更新为首选桶拥有者时，该设置仅适用于上传到桶的新对象。

  - 您可以让对象拥有者使用 `bucket-owner-full-control` 标准对象 ACL 再次上传对象。

> **Note**
>
> 对于跨账户上传，您还可以在桶策略中要求使用 `bucket-owner-full-control` 标准对象 ACL。有关桶策略示例，请参阅在授予上传对象的跨账户权限的同时，确保桶拥有者拥有完全控制权。

- 将对象编写者保持为对象拥有者 - 此方法不会更改对象拥有者，但它允许您单独授予对于对象的访问权限。要授予对于对象的访问权限，您必须拥有该对象的 `PutObjectAcl` 权限。然后，要修复“拒绝访问（403 禁止）”错误，请将请求者添加为被授予者，以访问对象的 ACL 中的对象。有关更多信息，请参阅 配置 ACL。

S3 屏蔽公共访问权限设置

如果失败的请求涉及公共访问权限或公共策略，请检查您的账户、存储桶或接入点上的 S3 屏蔽公共访问权限设置。有关排查与 S3 屏蔽公共访问权限设置相关的拒绝访问错误的更多信息，请参阅the section called “由于屏蔽公共访问权限设置而拒绝访问”。

Amazon S3 加密设置

Amazon S3 支持对您的桶进行服务器端加密。服务器端加密是指由接收数据的应用程序或服务在目标位置对数据进行加密。Amazon S3 在将您的数据写入 Amazon 数据中心内的磁盘时会在对象级别加密这些数据，并在您访问这些数据时解密这些数据。

原定设置情况下，Amazon S3 现在应用具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3），作为 Amazon S3 中每个桶的基本加密级别。Amazon S3 还允许您在上传对象时指定服务器端加密方法。

查看您的桶的服务器端加密状态和加密设置

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 从桶列表中，请选择要检查其加密设置的桶。
4. 选择属性选项卡。
5. 向下滚动到原定设置加密部分，并查看加密类型设置。

要使用 Amazon CLI 检查您的加密设置，请使用 get-bucket-encryption 命令。

检查对象的加密状态

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 从桶列表中，请选择包含对象的桶的名称。
4. 从对象列表中，请选择要为其添加或更改加密的对象的名称。

   此时将显示对象的详细信息页面。
5. 向下滚动到服务器端加密设置部分，以查看对象的服务器端加密设置。

要使用 Amazon CLI 检查您的对象加密状态，请使用 head-object 命令。

加密和权限要求

Amazon S3 支持三种类型的服务器端加密：

- 具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）
- 具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）
- 具有客户提供密钥的服务器端加密（SSE-C）

根据您的加密设置，请确保满足以下权限要求：

- SSE-S3 - 不需要额外的权限。
- SSE-KMS（使用客户自主管理型密钥）- 要上传对象，需要针对 Amazon KMS key 的 `kms:GenerateDataKey` 权限。要下载对象和执行对象的分段上传，需要针对 KMS 密钥的 `kms:Decrypt` 权限。
- SSE-KMS（具有 Amazon 托管式密钥）– 请求者必须来自拥有 `aws/s3` KMS 密钥的同一个账户。请求者还必须具有正确的 Amazon S3 权限才能访问该对象。
- SSE-C（具有客户提供的密钥）- 无需其他权限。您可以配置桶策略，以要求和限制具有客户提供的加密密钥的服务器端加密来加密桶中的对象。

如果使用客户自主管理型密钥加密对象，请确保 KMS 密钥策略允许您执行 `kms:GenerateDataKey` 或 `kms:Decrypt` 操作。有关检查 KMS 密钥策略的说明，请参阅《Amazon Key Management Service 开发人员指南》中的查看密钥策略。

S3 对象锁定设置

如果您的桶启用了 S3 对象锁定并且该对象受保留期或法定保留保护，则当您尝试删除该对象时，Amazon S3 会返回拒绝访问（403 禁止）错误。

检查桶是否启用了对象锁定

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 从桶列表中，请选择您想要查看的桶的名称。
4. 选择属性选项卡。
5. 向下滚动到对象锁定部分。验证对象锁定设置是已启用还是已禁用。

要确定该对象是受保留期保护还是受法定保留保护，请查看对象的锁定信息。

如果对象受保留期或法定保留保护，请检查以下各项：

- 如果对象版本受合规性保留模式保护，则无法将其永久删除。来自任何请求者（包括 Amazon Web Services 账户根用户）的永久 DELETE 请求都将导致拒绝访问（403 禁止）错误。另请注意，当您对于受合规性保留模式保护的对象提交 DELETE 请求时，Amazon S3 会为该对象创建删除标记。
- 如果对象版本受监管保留模式保护并且您具有 `s3:BypassGovernanceRetention` 权限，则可以绕过此保护并永久删除该版本。有关更多信息，请参阅绕过监管模式。
- 如果对象版本受法定保留保护，则永久 DELETE 请求可能会导致拒绝访问（403 禁止）错误。要永久删除对象版本，必须解除对于对象版本的法定保留。要解除法定保留，您必须具有 `s3:PutObjectLegalHold` 权限。有关解除法定保留的更多信息，请参阅配置 S3 对象锁定。

VPC 端点策略

如果您使用虚拟私有云（VPC）端点访问 Amazon S3，请确保 VPC 端点策略不会阻止您访问 Amazon S3 资源。原定设置情况下，VPC 端点策略允许向 Amazon S3 发出的所有请求。您还可以配置 VPC 端点策略以限制某些请求。有关如何检查 VPC 端点策略的信息，请参阅以下资源：

- the section called “由于 VPC 端点策略而拒绝访问 – 隐式拒绝”
- the section called “由于 VPC 端点策略而拒绝访问 – 显式拒绝”
- 《Amazon PrivateLink 指南》中的 Control access to VPC endpoints by using endpoint policies。

### Amazon Organizations 策略

如果您的 Amazon Web Services 账户属于某个组织，则 Amazon Organizations 策略可能会阻止您访问 Amazon S3 资源。默认情况下，Amazon Organizations 策略不会阻止向 Amazon S3 发出的任何请求。但是，请确保您的 Amazon Organizations 策略未配置为阻止对 S3 桶进行访问。有关如何查看 Amazon Organizations 策略的说明，请参阅以下资源：

- the section called “由于服务控制策略而拒绝访问 – 隐式拒绝”
- the section called “由于服务控制策略而拒绝访问 – 显式拒绝”
- the section called “由于资源控制策略而拒绝访问 – 显式拒绝”
- 《Amazon Organizations 用户指南》中的 Listing all policies

此外，如果您错误地将成员账户的存储桶策略配置为拒绝所有用户访问您的 S3 存储桶，则可以通过在 IAM 中为该成员账户启动特权会话来解锁存储桶。启动特权会话后，您可以删除配置错误的存储桶策略以重新获得对存储桶的访问权限。有关更多信息，请参阅《Amazon Identity and Access Management User Guide》中的 Perform a privileged task on an Amazon Organizations member account。

### 接入点设置

如果您在通过 Amazon S3 接入点发出请求时收到“拒绝访问（403 禁止）”错误，则可能需要检查以下内容：

- 接入点的配置
- 用于接入点的 IAM 用户策略
- 用于管理或配置跨账户接入点的桶策略

### 接入点配置和策略

- 创建接入点时，可以选择将互联网或 VPC 指定为网络来源。如果网络来源设置为仅限 VPC，Amazon S3 将拒绝向接入点发出的任何并非源自指定 VPC 的请求。要检查接入点的网络来源，请参阅创建限制到虚拟私有云的通用存储桶的接入点。
- 使用接入点，您还可以配置自定义的屏蔽公共访问权限设置，其工作原理与桶或账户级别的屏蔽公共访问权限设置类似。要查看您的自定义屏蔽公共访问权限设置，请参阅管理对通用存储桶的接入点的公共访问权限。
- 要使用接入点向 Amazon S3 发出成功的请求，请确保请求者拥有必要的 IAM 权限。有关更多信息，请参阅 配置 IAM 策略以使用通用存储桶的接入点。

- 如果请求涉及跨账户接入点，请确保桶拥有者已更新桶策略，以授权来自接入点的请求。有关更多信息，请参阅 授予跨账户接入点的权限。

如果在检查了本主题中的所有项目后，拒绝访问（403 禁止）错误仍然存在，请检索您的 Amazon S3 请求 ID 并联系 Amazon Web Services 支持 以获取更多指导。

## Amazon 适用于 Amazon S3 的托管策略

Amazon 托管式策略是由 Amazon 创建和管理的独立策略。Amazon 托管式策略旨在为许多常见使用场景提供权限，以便您可以开始为用户、组和角色分配权限。

请记住，Amazon 托管策略可能不会为您的特定使用场景授予最低权限，因为它们可供所有 Amazon 客户使用。我们建议通过定义特定于您的使用场景的客户管理型策略来进一步减少权限。

您无法更改 Amazon 托管策略中定义的权限。如果 Amazon 更新在 Amazon 托管策略中定义的权限，则更新会影响该策略所附加到的所有主体身份（用户、组和角色）。当新的 Amazon Web Services 服务 启动或新的 API 操作可用于现有服务时，Amazon 最有可能更新 Amazon 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 Amazon 托管式策略。

### Amazon 托管策略：AmazonS3FullAccess

您可以将 `AmazonS3FullAccess` 策略附加到 IAM 身份。 此策略授予允许完全访问 Amazon S3 的权限 。

要查看此策略的权限，请参阅 Amazon Web Services Management Console 中的 AmazonS3FullAccess。

### Amazon 托管策略：AmazonS3ReadOnlyAccess

您可以将 `AmazonS3ReadOnlyAccess` 策略附加到 IAM 身份。 此策略授予允许对 Amazon S3 进行只读访问的权限。

要查看此策略的权限，请参阅 Amazon Web Services Management Console 中的 AmazonS3ReadOnlyAccess。

### Amazon 托管式策略：AmazonS3ObjectLambdaExecutionRolePolicy

提供的 Amazon Lambda 函数在向 S3 对象 Lambda 接入点发出请求时将数据发送到 S3 对象 Lambda 所需的权限。还授予 Lambda 写入 Amazon CloudWatch Logs 的权限。

要查看此策略的权限，请参阅 Amazon Web Services Management Console 中的 AmazonS3ObjectLambdaExecutionRolePolicy。

## Amazon 托管式策略：S3UnlockBucketPolicy

如果您错误地将成员账户的存储桶策略配置为拒绝所有用户访问您的 S3 存储桶，则可以使用此 Amazon 托管式策略（S3UnlockBucketPolicy）来解锁存储桶。有关如何删除拒绝所有主体访问 Amazon S3 存储桶的错误配置存储桶策略的更多信息，请参阅《Amazon Identity and Access Management User Guide》中的 Perform a privileged task on an Amazon Organizations member account。

## Amazon 托管策略的 Amazon S3 更新

查看有关 Amazon S3 的 Amazon 托管策略的更新的详细信息。

| 更改 | 描述 | 日期 |
| --- | --- | --- |
| Amazon S3 添加 S3UnlockBucketPolicy | Amazon S3 添加了一个名为 S3UnlockBucketPolicy 的新 Amazon 托管式策略，用于解锁存储桶，并删除拒绝所有主体访问 Amazon S3 存储桶的配置错误的存储桶策略。 | 2024 年 11 月 1 日 |
| Amazon S3 向 AmazonS3ReadOnlyAccess 添加了描述权限 | Amazon S3 向 AmazonS3ReadOnlyAccess 添加了 s3:Describe* 权限。 | 2023 年 8 月 11 日 |
| Amazon S3 将 S3 对象 Lambda 权限添加到 AmazonS3FullAccess 和 AmazonS3ReadOnlyAccess | Amazon S3 更新 AmazonS3FullAccess 和 AmazonS3ReadOnlyAccess 策略以包括 S3 对象 Lambda 的权限。 | 2021 年 9 月 27 日 |
| Amazon S3 添加 AmazonS3ObjectLambdaExecutionRolePolicy | Amazon S3 添加了一个新的 Amazon 托管策略，称为 AmazonS3ObjectLambdaExecutionRolePolicy ，它提供了 Lambda 函数 | 2021 年 8 月 18 日 |

| 更改 | 描述 | 日期 |
| --- | --- | --- |
| | 权限，以便与 S3 对象 Lambda 交互并写入 CloudWatch Logs。 | |
| Amazon S3 开始跟踪更改 | Amazon S3 为其 Amazon 托管策略开启了跟踪更改。 | 2021 年 8 月 18 日 |

# 通过接入点管理对通用存储桶中共享数据集的访问

通用存储桶的 Amazon S3 接入点简化了在 S3 中存储数据的任何 Amazon 服务或客户应用程序的数据访问。接入点是附加到通用存储桶的命名网络端点，您可以使用这些存储桶来执行 S3 对象操作（如 `GetObject` 和 `PutObject`）。每个接入点都具有不同的权限和网络控制，S3 将它们应用于通过该接入点发出的任何请求。每个接入点强制实施自定义接入点策略，该策略与附加到底层存储桶的存储桶策略结合使用。您可以将任何接入点配置为仅接受来自 Virtual Private Cloud（VPC）的请求，以限制专用网络的 Amazon S3 数据访问。您还可以为每个接入点配置自定义屏蔽公共访问权限设置。

> **Note**
>
> - 您只能使用接入点来执行对象操作。您不能使用接入点执行其他 Amazon S3 操作，例如修改或删除存储桶。有关支持接入点的 S3 操作的完整列表，请参阅通用存储桶的接入点兼容性。
> - 接入点适用于部分服务和特征，但并不适用于全部 Amazon 服务和特征。例如，您不能将跨区域复制配置为通过接入点进行操作。有关与 S3 接入点兼容的 Amazon 服务的完整列表，请参阅通用存储桶的接入点兼容性。

本节中的主题说明如何使用通用存储桶的 Amazon S3 接入点。有关使用通用存储桶的信息，请参阅通用存储桶概述。有关使用对象的信息，请参阅 Amazon S3 对象概述。

主题

- 通用存储桶的接入点命名规则、限制和局限性
- 使用 ARN、接入点别名或虚拟托管类型 URI 来引用通用存储桶的接入点
- 通用存储桶的接入点兼容性
- 配置 IAM 策略以使用通用存储桶的接入点

- 监控和记录通用存储桶的接入点
- 创建通用存储桶的接入点
- 管理通用存储桶的 Amazon S3 接入点
- 使用通用存储桶的 Amazon S3 接入点

# 通用存储桶的接入点命名规则、限制和局限性

通用存储桶的接入点是附加到存储桶的命名网络端点，用于简化数据管理。创建接入点时，您可以选择名称和要在其中创建接入点的 Amazon Web Services 区域。以下主题提供有关接入点命名规则以及限制和局限性的信息。

主题

- 通用存储桶的 Amazon S3 接入点的命名规则
- 通用存储桶的接入点的限制和局限性

## 通用存储桶的 Amazon S3 接入点的命名规则

创建通用存储桶的接入点时，您可以选择接入点名称和要在其中创建接入点的 Amazon Web Services 区域。与通用存储桶不同，接入点名称在 Amazon Web Services 账户或 Amazon Web Services 区域之间不需要是唯一的。同一个 Amazon Web Services 账户可以在不同的 Amazon Web Services 区域中创建名称相同的接入点，或者两个不同的 Amazon Web Services 账户可以使用相同的接入点名称。但是，在单个 Amazon Web Services 区域中，Amazon Web Services 账户 不得具有两个名称完全相同的接入点。

> **Note**
>
> 如果选择公布您的接入点名称，请避免在接入点名称中包含敏感信息。接入点名称将在称为域名系统（DNS）的可公开访问的数据库中得以发布。

接入点名称必须符合 DNS，并且必须满足以下条件：

- 在单个 Amazon Web Services 账户和 Amazon Web Services 区域内必须是唯一的
- 必须以数字或小写字母开头
- 长度必须介于 3-50 个字符之间

- 不能以连字符（-）开头或结尾
- 不能包含下划线 (_)、大写字母、空格或句点 (.)
- 不得以后缀 -s3alias 结尾。此后缀是为接入点别名预留的。有关更多信息，请参阅 通用存储桶的接入点别名。

## 通用存储桶的接入点的限制和局限性

通用存储桶的 Amazon S3 接入点具有以下限制和局限性：

- 通用存储桶的每个接入点仅仅与一个通用存储桶相关联，您必须在创建接入点时指定该存储桶。创建接入点后，您无法将它与另一个存储桶关联。但是，您可以删除接入点，然后创建具有相同名称的另一个接入点并将新的接入点与另一个存储桶关联。
- 创建接入点后，无法更改其 Virtual Private Cloud（VPC）配置。
- 接入点策略的大小限制为 20 KB。
- 每个 Amazon Web Services 区域中的每个 Amazon Web Services 账户最多可以创建 10000 个接入点。如果您需要在单个区域为一个账户使用超过 10000 个接入点，则可以请求增加服务限额。有关服务限额和请求增加限额的更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon 服务限额。
- 您不能将接入点用作 S3 复制的目标。有关复制的更多信息，请参阅 在区域内和跨区域复制对象。
- 您不能使用 S3 接入点别名作为 Amazon S3 控制台中移动操作的源或目标。
- 您只能使用虚拟主机式 URL 为接入点寻址。有关虚拟主机式寻址的更多信息，请参阅访问 Amazon S3 通用存储桶。
- 控制接入点功能（例如，PutAccessPoint 和 GetAccessPointPolicy）的 API 操作不支持跨账户调用。
- 使用 REST API 向接入点发出请求时，必须使用 Amazon 签名版本 4。有关对请求进行身份验证的更多信息，请参阅《Amazon Simple Storage Service API 参考》中的验证请求（Amazon 签名版本 4）。
- 接入点仅支持通过 HTTPS 发出请求。对于通过 HTTP 发出的任何请求，Amazon S3 都会自动以 HTTP 重定向作为响应，从而将请求升级到 HTTPS。
- 接入点不支持匿名访问。
- 除非从存储桶拥有者向您授予权限，否则跨账户接入点不会授予您对数据的访问权限。存储桶拥有者始终保留对数据访问的最终控制权，并且必须更新存储桶策略才能授权来自跨账户接入点的请求。要查看存储桶策略示例，请参阅配置 IAM 策略以使用通用存储桶的接入点。

- 在拥有超过 1000 个接入点的 Amazon Web Services 区域中，您无法在 Amazon S3 控制台中按名称搜索接入点。
- 当您在 Amazon S3 控制台中查看跨账户接入点时，访问列显示未知。Amazon S3 控制台无法确定是否已授予针对关联存储桶和对象的公共访问权限。除非您需要针对特定使用案例进行公共配置，否则我们建议您和存储桶拥有者屏蔽对接入点和存储桶的所有公共访问权限。有关更多信息，请参阅阻止对您的 Amazon S3 存储的公有访问。

## 使用 ARN、接入点别名或虚拟托管类型 URI 来引用通用存储桶的接入点

创建通用存储桶的接入点后，您可以使用这些端点来执行多项操作。在引用通用存储桶的接入点时，可以使用 Amazon 资源名称（ARN）、接入点别名或虚拟托管类型 URI。

主题

- 通用存储桶的接入点 ARN
- 通用存储桶的接入点别名
- 虚拟托管类型 URI

### 通用存储桶的接入点 ARN

接入点具有 Amazon Resource Name（ARN）。通用存储桶的接入点 ARN 与存储桶 ARN 类似，但它们是明确键入的，用于对接入点的 Amazon Web Services 区域和接入点拥有者的 Amazon Web Services 账户 ID 进行编码。有关 ARN 的更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon 资源名称（ARN）。

接入点 ARN 使用以下格式：

```
arn:aws:s3:region:account-id:accesspoint/resource
```

- `arn:aws:s3:us-west-2:123456789012:accesspoint/test` 表示名为 *test* 的接入点，它在区域 *us-west-2* 中由账户 *123456789012* 拥有。
- `arn:aws:s3:us-west-2:123456789012:accesspoint/*` 表示区域 *us-west-2* 中账户 *123456789012* 下的所有接入点。

通过接入点访问的对象的 ARN 使用以下格式：

```
arn:aws:s3:region:account-id:accesspoint/access-point-name/object/resource
```

- arn:aws:s3:*us-west-2*:*123456789012*:accesspoint/*test*/object/*unit-01* 表示对象 *unit-01*，可通过名为 *test* 的接入点（在区域 *us-west-2* 中，由账户 *123456789012* 拥有）进行访问。
- arn:aws:s3:*us-west-2*:*123456789012*:accesspoint/*test*/object/* 表示名为 *test* 的接入点（在区域 *us-west-2* 的账户 *123456789012* 中）的所有对象。
- arn:aws:s3:*us-west-2*:*123456789012*:accesspoint/*test*/object/*unit-01*/*finance*/* 表示名为 *test* 的接入点（在区域 *us-west-2* 的账户 *123456789012* 中）的前缀 *unit-01/finance/* 下的所有对象。

## 通用存储桶的接入点别名

当您创建通用存储桶的接入点时，Amazon S3 会自动生成一个别名，您可以使用该别名来替代 Amazon S3 存储桶名称以进行数据访问。对于接入点数据面板操作，您可以使用此接入点别名，而不是 Amazon 资源名称（ARN）。有关这些操作的列表，请参阅通用存储桶的接入点兼容性。

接入点别名是在与 Amazon S3 存储桶相同的命名空间中创建的。此别名自动生成，无法更改。接入点别名符合有效 Amazon S3 存储桶名称的所有要求，包括以下部分：

*access point prefix*-*metadata*-s3alias

> **Note**
>
> -s3alias 后缀是为接入点别名预留的，不能用于存储桶或接入点名称。有关 Amazon S3 存储桶命名规则的更多信息，请参阅通用存储桶命名规则。

### 通用存储桶的接入点别名用例和限制

采用通用存储桶的接入点时，您可以使用接入点别名，而无需对代码进行大量更改。

当您创建通用存储桶的接入点时，Amazon S3 会自动生成一个接入点别名，如下例所示。要运行此命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control create-access-point --bucket amzn-s3-demo-bucket1 --name my-access-point
 --account-id 111122223333
{
    "AccessPointArn": "arn:aws:s3:region:111122223333:accesspoint/my-access-point",
    "Alias": "my-access-point-aqfqprnstn7aefdfbarligizwgyfouse1a-s3alias"
}
```

在任何数据层面操作中，您都可以使用此接入点别名而不是 Amazon S3 存储桶名称。有关这些操作的列表，请参阅通用存储桶的接入点兼容性。

以下有关 `get-object` 命令的 Amazon CLI 示例使用存储桶的接入点别名来返回有关指定对象的信息。要运行此命令，请将 *`user input placeholders`* 替换为您自己的信息。

```
aws s3api get-object --bucket my-access-point-aqfqprnstn7aefdfbarligizwgyfouse1a-
s3alias --key dir/my_data.rtf my_data.rtf

{
    "AcceptRanges": "bytes",
    "LastModified": "2020-01-08T22:16:28+00:00",
    "ContentLength": 910,
    "ETag": "\"00751974dc146b76404bb7290f8f51bb\"",
    "VersionId": "null",
    "ContentType": "text/rtf",
    "Metadata": {}
}
```

接入点别名限制

- 客户无法配置别名。
- 无法在接入点上删除、修改或禁用别名。
- 在某些数据面板操作中，您可以使用此接入点别名，而不是 Amazon S3 存储桶名称。有关这些操作的列表，请参阅通用存储桶的接入点与 S3 操作的兼容性。
- 您不能将一个接入点别名用于多个 Amazon S3 控制层面操作。有关 Amazon S3 控制层面操作的列表，请参阅《Amazon Simple Storage Service API 参考》中的 Amazon S3 控制。
- 您不能使用 S3 接入点别名作为 Amazon S3 控制台中移动操作的源或目标。
- 别名不能用于 Amazon Identity and Access Management（IAM）策略中。
- 别名不能用作 S3 服务器访问日志的日志记录目标。
- 别名不能用作 Amazon CloudTrail 日志的日志记录目标。
- Amazon SageMaker GroundTruth 不支持接入点别名。

## 虚拟托管类型 URI

通用存储桶的接入点仅支持虚拟托管类型寻址。在虚拟托管类型 URI 中，接入点名称、Amazon Web Services 账户和 Amazon Web Services 区域是 URL 中域名的一部分。有关虚拟托管的更多信息，请参阅通用存储桶的虚拟托管。

接入点的虚拟托管类型 URI 使用以下格式：

```
https://access-point-name-account-id.s3-accesspoint.region.amazonaws.com
```

> **Note**
>
> - 如果您的访问点名称包含破折号 (-) 字符，请在 URL 中包含破折号，然后在账户 ID 之前插入另一个破折号。例如，要使用区域 *us-west-2* 中由账户 *123456789012* 拥有的名为 *finance-docs* 的接入点，相应的 URL 应为 `https://finance-docs-123456789012.s3-accesspoint.us-west-2.amazonaws.com`。
> - S3 接入点不支持通过 HTTP 进行访问。接入点仅支持通过 HTTPS 进行安全访问。

## 通用存储桶的接入点兼容性

您可以使用以下 Amazon S3 API 子集，通过通用存储桶的接入点来访问存储桶。下列所有操作都可以接受接入点 ARN 或接入点别名。

有关使用接入点对于对象执行操作的示例，请参阅使用通用存储桶的 Amazon S3 接入点。

### 通用存储桶的接入点与 S3 操作的兼容性

S3 操作

- AbortMultipartUpload
- CompleteMultipartUpload
- CopyObject（仅限同区域副本）
- CreateMultipartUpload
- DeleteObject
- DeleteObjects
- DeleteObjectTagging
- GetBucketAcl
- GetBucketCors
- GetBucketLocation

- GetBucketNotificationConfiguration
- GetBucketPolicy
- GetObject
- GetObjectAcl
- GetObjectAttributes
- GetObjectLegalHold
- GetObjectRetention
- GetObjectTagging
- HeadBucket
- HeadObject
- ListMultipartUploads
- ListObjects
- ListObjectsV2
- ListObjectVersions
- ListParts
- Presign
- PutObject
- PutObjectAcl
- PutObjectLegalHold
- PutObjectRetention
- PutObjectTagging
- RestoreObject
- UploadPart
- UploadPartCopy（仅限同区域副本）

## 配置 IAM 策略以使用通用存储桶的接入点

通用存储桶的 Amazon S3 接入点支持 Amazon Identity and Access Management（IAM）资源策略，这些策略可让您按资源、用户或其它条件来控制接入点的使用。要使应用程序或用户能够通过接入点访问对象，接入点和底层存储桶都必须允许请求。

> **Important**
>
> 当通过存储桶的名称或 Amazon 资源名称（ARN）直接访问存储桶时，向存储桶添加 S3 接入点不会改变存储桶的行为。针对存储桶的所有现有操作将继续像以前一样运行。您在接入点策略中包括的限制仅适用于通过该接入点发出的请求。

当您使用 IAM 资源策略时，确保在保存策略之前解决来自 Amazon Identity and Access Management Access Analyzer 的安全警告、错误、一般警告和建议。IAM Access Analyzer 将根据 IAM 策略语法和最佳实践运行策略检查，以验证您的策略。这些检查项生成调查结果并提供建议，可帮助您编写可操作且符合安全最佳实践的策略。

要了解有关使用 IAM Access Analyzer 验证策略的更多信息，请参阅《IAM 用户指南》中的 IAM Access Analyzer 策略验证。要查看 IAM Access Analyzer 返回的警告、错误和建议的列表，请参阅 IAM Access Analyzer 策略检查引用。

## 通用存储桶的接入点的策略示例

以下示例演示如何创建 IAM 策略来控制通过通用存储桶的接入点发出的请求。

> **Note**
>
> 在接入点策略中授予的权限仅在底层存储桶也允许相同的访问时才有效。您可以通过两种方式实现这一点：
>
> 1. （推荐）将存储桶的访问控制委派给接入点，如将访问控制委派到接入点中所述。
> 2. 将接入点策略中包含的权限添加到底层存储桶的策略中。示例 1 接入点策略示例说明了如何修改底层存储桶策略以允许必要的访问。

### Example 1 – 接入点策略授予

以下接入点策略通过账户 *123456789012* 中的接入点 *my-access-point* 向账户 *123456789012* 中的 IAM 用户 *Jane* 授予对具有前缀 *Jane/* 的 GET 和 PUT 对象的权限。

```
{
    "Version":"2012-10-17",
    "Statement": [
    {
        "Effect": "Allow",
```

```
        "Principal": {
            "AWS": "arn:aws:iam::123456789012:user/Jane"
        },
        "Action": ["s3:GetObject", "s3:PutObject"],
        "Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/my-access-point/
object/Jane/*"
    }]
}
```

> **Note**
>
> 要使接入点策略有效地向 *Jane* 授予访问权限，底层存储桶也必须对 *Jane* 允许相同的访问权限。可以将存储桶的访问控制委派到接入点，如将访问控制委派到接入点中所述。或者，您也可以将以下策略添加到底层存储桶中，以便向 Jane 授予必要的权限。请注意，接入点策略和存储桶策略的 Resource 条目不同。
>
> ```
> {
>     "Version": "2012-10-17",
>     "Statement": [
>     {
>         "Effect": "Allow",
>         "Principal": {
>             "AWS": "arn:aws:iam::123456789012:user/Jane"
>         },
>         "Action": ["s3:GetObject", "s3:PutObject"],
>         "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/Jane/*"
>     }]
> }
> ```

Example 2 – 带标签条件的接入点策略

以下接入点策略通过账户 *123456789012* 中的接入点 *my-access-point* 向账户 *123456789012* 中的 IAM 用户 *Mateo* 授予对 GET 对象的权限，这些权限具有值设为 *finance* 的标签键 *data*。

```
{
    "Version":"2012-10-17",
    "Statement": [
    {
        "Effect":"Allow",
        "Principal" : {
```

```
            "AWS": "arn:aws:iam::123456789012:user/Mateo"
        },
        "Action":"s3:GetObject",
        "Resource" : "arn:aws:s3:us-west-2:123456789012:accesspoint/my-access-point/
object/*",
        "Condition" : {
            "StringEquals": {
                "s3:ExistingObjectTag/data": "finance"
            }
        }
    }]
}
```

Example 3 – 允许查看存储桶列示内容的接入点策略

以下接入点策略通过账户 *123456789012* 中的接入点 *my-access-point* 授予账户 *123456789012* 中的 IAM 用户 Arnav 查看底层存储桶中包含的对象的权限。

```
{
    "Version":"2012-10-17",
    "Statement": [
    {
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::123456789012:user/Arnav"
        },
        "Action": "s3:ListBucket",
        "Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/my-access-point"
    }]
}
```

Example 4 – 服务控制策略

以下服务控制策略要求使用虚拟私有云（VPC）网络起源创建所有新的接入点。实施此策略时，组织中的用户无法创建可从 Internet 访问的新接入点。

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Effect": "Deny",
        "Action": "s3:CreateAccessPoint",
```

```
        "Resource": "*",
        "Condition": {
            "StringNotEquals": {
                "s3:AccessPointNetworkOrigin": "VPC"
            }
        }
    }]
}
```

Example 5 – 将 S3 操作限制为 VPC 网络起源的存储桶策略

以下存储桶策略限制为只能通过具有 VPC 网络起源的接入点来访问存储桶 *amzn-s3-demo-bucket* 的所有 S3 对象操作。

> **Important**
>
> 在使用类似于此示例所示语句的语句之前，请确保您不需要使用接入点不支持的特征，例如跨区域复制。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": "*",
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:BypassGovernanceRetention",
                "s3:DeleteObject",
                "s3:DeleteObjectTagging",
                "s3:DeleteObjectVersion",
                "s3:DeleteObjectVersionTagging",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectLegalHold",
                "s3:GetObjectRetention",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:GetObjectVersionAcl",
                "s3:GetObjectVersionTagging",
                "s3:ListMultipartUploadParts",
```

```
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectLegalHold",
                "s3:PutObjectRetention",
                "s3:PutObjectTagging",
                "s3:PutObjectVersionAcl",
                "s3:PutObjectVersionTagging",
                "s3:RestoreObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:AccessPointNetworkOrigin": "VPC"
                }
            }
        }
    ]
}
```

## 条件键

通用存储桶的 S3 接入点具有条件键，这些键可在 IAM 策略中用来控制对资源的访问。以下条件键仅代表 IAM 策略的一部分。有关完整策略示例，请参阅通用存储桶的接入点的策略示例、the section called “将访问控制委派到接入点”和the section called “授予跨账户接入点的权限”。

### s3:DataAccessPointArn

此示例显示一个您可以用来匹配接入点 ARN 的字符串。以下示例匹配区域 *us-west-2* 中 Amazon Web Services 账户 *123456789012* 的所有接入点：

```
"Condition" : {
    "StringLike": {
        "s3:DataAccessPointArn": "arn:aws:s3:us-west-2:123456789012:accesspoint/*"
    }
}
```

### s3:DataAccessPointAccount

此示例显示一个字符串运算符，您可以使用它匹配接入点拥有者的账户 ID。以下示例匹配 Amazon Web Services 账户 *123456789012* 拥有的所有接入点。

```
"Condition" : {
```

```
    "StringEquals": {
        "s3:DataAccessPointAccount": "123456789012"
    }
}
```

### s3:AccessPointNetworkOrigin

此示例显示一个字符串运算符，您可以使用它来匹配网络起源（Internet 或 VPC）。以下示例仅匹配起源为 VPC 的接入点。

```
"Condition" : {
    "StringEquals": {
        "s3:AccessPointNetworkOrigin": "VPC"
    }
}
```

有关在 Amazon S3 中使用条件键的更多信息，请参阅《Service Authorization Reference》中的 Actions, resources, and condition keys for Amazon S3。

有关按 S3 资源类型对 S3 API 操作的权限的更多信息，请参阅 Amazon S3 API 操作所需的权限。

## 将访问控制委派到接入点

您可以将存储桶的访问控制委托给存储桶的接入点。以下示例存储桶策略允许对存储桶拥有者账户所拥有的所有接入点进行完全访问。因此，对此存储桶的所有访问都由附加到其接入点的策略控制。我们建议您以这种方式为所有不需要直接访问存储桶的使用案例配置存储桶。

Example 6 – 将访问控制委派给接入点的存储桶策略

```
{
    "Version": "2012-10-17",
    "Statement" : [
    {
        "Effect": "Allow",
        "Principal" : { "AWS": "*" },
        "Action" : "*",
        "Resource" : [ "Bucket ARN", "Bucket ARN/*"],
        "Condition": {
            "StringEquals" : { "s3:DataAccessPointAccount" : "Bucket owner's account
 ID" }
        }
```

```
    }]
}
```

### 授予跨账户接入点的权限

要为另一个账户拥有的存储桶创建接入点，您必须首先通过指定存储桶名称和账户拥有者 ID 来创建接入点。然后，存储桶拥有者必须更新存储桶策略以授权来自接入点的请求。创建接入点与创建 DNS CNAME 类似，因为接入点不提供对存储桶内容的访问权限。所有存储桶访问权限均由存储桶策略控制。以下示例存储桶策略允许从受信任 Amazon Web Services 账户拥有的接入点对存储桶进行 GET 和 LIST 请求。

将 *Bucket ARN* 替换为桶的 ARN。

Example 7 – 将权限委托给其他 Amazon Web Services 账户的存储桶策略

```
{
    "Version": "2012-10-17",
    "Statement" : [
    {
        "Effect": "Allow",
        "Principal" : { "AWS": "*" },
        "Action" : ["s3:GetObject","s3:ListBucket"],
        "Resource" : [ "Bucket ARN", "Bucket ARN/*"],
        "Condition": {
            "StringEquals" : { "s3:DataAccessPointAccount" : "Access point owner's
 account ID" }
        }
    }]
}
```

## 监控和记录通用存储桶的接入点

Amazon S3 记录通过通用存储桶的接入点发出的请求，以及对管理接入点的 API 操作（如 CreateAccessPoint 和 GetAccessPointPolicy）发出的请求。如需监控和管理使用模式，您还可以为接入点配置 Amazon CloudWatch Logs 请求指标。

主题

- CloudWatch 请求指标
- 请求日志

## CloudWatch 请求指标

如需了解和提高使用接入点的应用程序的性能，您可以使用 Amazon S3 的 CloudWatch 请求指标。请求指标帮助您监控 Amazon S3 请求，以快速识别运行问题，并对问题采取措施。

默认情况下，请求指标在存储桶级别可用。但是，您可以使用共享前缀、对象标签或接入点为请求指标定义筛选器。当您创建接入点筛选器时，请求指标配置包括了对指定接入点的请求。您可以接收指标、设置警报和访问控制面板，以查看通过此接入点执行的实时操作。

您必须通过在控制台中配置请求指标或使用 Amazon S3 API 来选择使用请求指标。请求指标在一定的处理延迟之后每隔一分钟提供一次。请求指标的费率与CloudWatch 自定义指标的费率相同。有关更多信息，请参阅 Amazon CloudWatch 定价。

如需创建按接入点筛选的请求指标配置，请参阅 创建按前缀，对象标签或接入点筛选的指标配置。

## 请求日志

您可以通过使用服务器访问日志和 Amazon CloudTrail，记录通过接入点发出的请求和对管理接入点（如 `CreateAccessPoint` 和 `GetAccessPointPolicy`,）的 API 发出的请求。

通过接入点发出的请求 CloudTrail 日志条目将在日志的 `resources` 部分包含接入点 ARN。

例如，假设您有以下配置：

- 区域 *us-west-2* 中名为 *amzn-s3-demo-bucket1* 的存储桶包含名为 *my-image.jpg* 的对象。
- 与 *amzn-s3-demo-bucket1* 关联且名为 *my-bucket-ap* 的接入点
- *123456789012* 的 Amazon Web Services 账户 ID

以下示例显示了上述配置的CloudTrail 日志条目的 `resources` 部分：

```
"resources": [
        {"type": "AWS::S3::Object",
            "ARN": "arn:aws:s3:::amzn-s3-demo-bucket1/my-image.jpg"
        },
        {"accountId": "123456789012",
            "type": "AWS::S3::Bucket",
            "ARN": "arn:aws:s3:::amzn-s3-demo-bucket1"
        },
        {"accountId": "123456789012",
            "type": "AWS::S3::AccessPoint",
```

```
            "ARN": "arn:aws:s3:us-west-2:123456789012:accesspoint/my-bucket-ap"
        }
    ]
```

有关 S3 服务器访问日志的更多信息，请参阅使用服务器访问日志记录来记录请求。有关 Amazon CloudTrail 的更多信息，请参阅《Amazon CloudTrail 用户指南》中的什么是 Amazon CloudTrail？。

# 创建通用存储桶的接入点

您可以使用 Amazon Web Services Management Console、Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 Amazon S3 REST API 创建通用存储桶的 S3 接入点。

默认情况下，您可为每个 Amazon Web Services 账户在每个区域创建最多 10000 个通用存储桶的接入点。如果您需要在单个区域为一个账户使用超过 10000 个接入点，则可以请求增加服务限额。有关服务限额和请求增加限额的更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon 服务限额。

主题


- 创建通用存储桶的接入点
- 创建限制到虚拟私有云的通用存储桶的接入点
- 管理对通用存储桶的接入点的公共访问权限


## 创建通用存储桶的接入点

一个接入点仅仅与一个 Amazon S3 通用存储桶相关联。如果您想使用您的 Amazon Web Services 账户中的存储桶，则必须首先创建存储桶。有关创建存储桶的更多信息，请参阅创建、配置和使用 Amazon S3 通用存储桶。

您也可以创建与另一个 Amazon Web Services 账户中的存储桶关联的跨账户接入点，只要您知道存储桶名称和存储桶拥有者的账户 ID。但是，在获得存储桶拥有者授予的权限之前，创建跨账户接入点不会授予您访问存储桶中数据的权限。存储桶拥有者必须通过存储桶策略向接入点拥有者的账户（您的账户）授予对存储桶的访问权限。有关更多信息，请参阅 授予跨账户接入点的权限。

使用 S3 控制台

创建接入点

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。

2. 在页面顶部的导航栏中，选择当前所显示 Amazon Web Services 区域的名称。接下来，选择要在其中创建接入点的区域。接入点和关联存储桶必须位于同一区域中。
3. 在左侧导航窗格中，选择接入点。
4. 在接入点页面上，选择创建接入点。
5. 在接入点名称字段中，输入接入点的名称。有关命名接入点的更多信息，请参阅通用存储桶的 Amazon S3 接入点的命名规则。
6. 对于存储桶名称，指定要与接入点结合使用的 S3 存储桶。

   要使用您账户中的存储桶，请选择选择此账户中的存储桶，然后输入或浏览目标存储桶。

   要使用其他 Amazon Web Services 账户中的存储桶，请选择指定另一个账户中的存储桶，然后输入该存储桶的 Amazon Web Services 账户 ID 和名称。

   > **Note**
   >
   > 如果您使用其他 Amazon Web Services 账户中的存储桶，存储桶拥有者必须更新存储桶策略才能授权来自接入点的请求。有关存储桶策略示例，请参阅 授予跨账户接入点的权限。

7. 选择网络来源，即互联网或虚拟私有云（VPC）。如果您选择虚拟私有云（VPC），请输入要与接入点一起使用的 VPC ID。

   有关接入点的网络源的更多信息，请参阅创建限制到虚拟私有云的通用存储桶的接入点。
8. 在 Block Public Access settings for this Access Point（阻止此接入点的公有访问设置）下，选择要应用于接入点的屏蔽公共访问权限设置。默认情况下，为新的接入点启用所有屏蔽公共访问权限设置。除非您有特定的需求要禁用任何一个设置，建议您将所有设置保持为启用状态。

   > **Note**
   >
   > 创建接入点后，无法更改其屏蔽公共访问权限设置。

   有关将 Amazon S3 屏蔽公共访问权限与接入点结合使用的更多信息，请参阅管理对通用存储桶的接入点的公共访问权限。
9. （可选）在 Access point policy（接入点策略）- optional（可选）下，指定接入点策略。在保存策略之前，确保解决任何安全警告、错误、一般警告和建议。有关指定接入点策略的更多信息，请参阅通用存储桶的接入点的策略示例。

10. 选择 Create access point（创建接入点）。

使用 Amazon CLI

以下示例命令为账户 *111122223333* 中的存储桶 *amzn-s3-demo-bucket* 创建了一个名为 *example-ap* 的接入点。要创建接入点，您需要向 Amazon S3 发送一个指定以下内容的请求：

- 接入点名称。有关命名规则的信息，请参阅 the section called “通用存储桶的 Amazon S3 接入点的命名规则”。
- 要与接入点关联的存储桶的名称。
- 拥有接入点的 Amazon Web Services 账户的账户 ID。

```
aws s3control create-access-point --name example-ap --account-id 111122223333 --
bucket amzn-s3-demo-bucket
```

当您使用其他 Amazon Web Services 账户中的存储桶创建接入点时，请包括 `--bucket-account-id` 参数。以下示例命令使用位于 Amazon Web Services 账户 *444455556666* 中的存储桶 *amzn-s3-demo-bucket2* 在 Amazon Web Services 账户 *111122223333* 中创建接入点。

```
aws s3control create-access-point --name example-ap --account-id 111122223333 --
bucket amzn-s3-demo-bucket --bucket-account-id 444455556666
```

使用 REST API

可以使用 REST API 创建接入点。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 CreateAccessPoint。

## 创建限制到虚拟私有云的通用存储桶的接入点

创建通用存储桶的接入点时，您可以选择让接入点可通过互联网访问，也可以指定通过该接入点发出的所有请求都必须来自特定虚拟私有云（VPC）。可从 Internet 访问的接入点被认为是具有 `Internet` 网络起源。它可以在 Internet 上的任何位置使用，但受到接入点、底层存储桶和相关资源（如请求的对象）的任何其他访问限制的约束。只能从指定 VPC 访问的接入点的网络起源为 `VPC`，并且 Amazon S3 会拒绝从该 VPC 之外的来源向接入点发出的任何请求。

> **Important**
>
> 您只能在创建接入点时指定接入点的网络起源。创建接入点后，无法更改其网络起源。

要将接入点限制为仅限于 VPC 访问，请在创建接入点的请求中包括 `VpcConfiguration` 参数。在 `VpcConfiguration` 参数中，您指定希望能够使用接入点的 VPC ID。如果请求是通过接入点发出的，则该请求必须源自 VPC，否则 Amazon S3 将拒绝该请求。

您可以使用 Amazon CLI、Amazon SDK 或 REST API 检索接入点的网络起源。如果接入点指定了 VPC 配置，则其网络起源为 `VPC`。否则，接入点的网络起源为 `Internet`。

Example

示例：创建仅限 VPC 访问的接入点

以下示例为账户 `123456789012` 中的存储桶 *`amzn-s3-demo-bucket`* 创建一个名为 `example-vpc-ap` 的接入点，该接入点仅允许从 VPC `vpc-1a2b3c` 访问。然后，该示例验证新接入点是否具有 VPC 网络起源。

Amazon CLI

```
aws s3control create-access-point --name example-vpc-ap --account-id 123456789012 --
bucket amzn-s3-demo-bucket --vpc-configuration VpcId=vpc-1a2b3c
```

```
aws s3control get-access-point --name example-vpc-ap --account-id 123456789012

{
    "Name": "example-vpc-ap",
    "Bucket": "amzn-s3-demo-bucket",
    "NetworkOrigin": "VPC",
    "VpcConfiguration": {
        "VpcId": "vpc-1a2b3c"
    },
    "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": true,
        "IgnorePublicAcls": true,
        "BlockPublicPolicy": true,
        "RestrictPublicBuckets": true
    },
    "CreationDate": "2019-11-27T00:00:00Z"
```

```
}
```

要将接入点与 VPC 搭配使用，您必须修改 VPC 端点的访问策略。VPC 端点允许流量从您的 VPC 流向 Amazon S3。它们具有访问控制策略，用于控制如何允许 VPC 内的资源与 Amazon S3 交互。仅当 VPC 端点策略同时授予对接入点和底层存储桶的访问权限时，从 VPC 通过接入点到 S3 的请求才会成功。

> **Note**
>
> 要使资源只能在 VPC 中访问，请确保为 VPC 端点创建私有托管区域。要使用私有托管区域，请修改您的 VPC 设置，以便 VPC 网络属性 `enableDnsHostnames` 和 `enableDnsSupport` 设置为 `true`。

以下示例策略语句配置 VPC 端点，以允许对名为 `awsexamplebucket1` 的存储桶和名为 `example-vpc-ap` 的接入点执行 `GetObject` 调用。

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Principal": "*",
        "Action": [
            "s3:GetObject"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::awsexamplebucket1/*",
            "arn:aws:s3:us-west-2:123456789012:accesspoint/example-vpc-ap/object/*"
        ]
    }]
}
```

> **Note**
>
> 此示例中的 "Resource" 声明使用 Amazon 资源名称（ARN）指定接入点。有关接入点 ARN 的更多信息，请参阅 使用通用存储桶的 Amazon S3 接入点。

有关 VPC 端点策略的更多信息，请参阅《VPC 用户指南》中的使用 Amazon S3 的端点策略。

有关使用 VPC 端点创建接入点的教程，请参阅 Managing Amazon S3 access with VPC endpoints and access points。

## 管理对通用存储桶的接入点的公共访问权限

通用存储桶的 Amazon S3 接入点对于每个接入点支持独立的屏蔽公共访问权限设置。创建接入点时，可以指定应用于该接入点的屏蔽公共访问权限设置。对于通过接入点发出的任何请求，Amazon S3 会评估该接入点、底层存储桶和存储桶拥有者账户的屏蔽公共访问权限设置。如果这些设置中的任何一个指示应阻止请求，则 Amazon S3 会拒绝请求。

有关 S3 屏蔽公共访问权限特征的更多信息，请参阅阻止对您的 Amazon S3 存储的公有访问。

**Important**

- 默认情况下为接入点启用所有屏蔽公共访问权限设置。您必须明确禁用不希望应用于接入点的任何设置。
- Amazon S3 当前不支持在创建接入点之后更改接入点的屏蔽公共访问权限设置。

### Example

示例：创建具有自定义屏蔽公共访问权限设置的接入点

此示例为账户 123456789012 中的存储桶 *amzn-s3-demo-bucket* 创建名为 example-ap 且具有非默认屏蔽公共访问权限设置的接入点。然后，该示例检索新接入点的配置，以验证其“屏蔽公共访问权限”设置。

Amazon CLI

```
aws s3control create-access-point --name example-ap --account-id
 123456789012 --bucket amzn-s3-demo-bucket--public-access-block-configuration
 BlockPublicAcls=false,IgnorePublicAcls=false,BlockPublicPolicy=true,RestrictPublicBuckets=t
```

```
aws s3control get-access-point --name example-ap --account-id 123456789012

{
    "Name": "example-ap",
```

```
    "Bucket": "amzn-s3-demo-bucket",
    "NetworkOrigin": "Internet",
    "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": false,
        "IgnorePublicAcls": false,
        "BlockPublicPolicy": true,
        "RestrictPublicBuckets": true
    },
    "CreationDate": "2019-11-27T00:00:00Z"
}
```

# 管理通用存储桶的 Amazon S3 接入点

本节介绍如何通过 Amazon Web Services Management Console、Amazon Command Line Interface 或 REST API 来管理通用存储桶的 Amazon S3 接入点。

> **Note**
>
> - 您只能使用通用存储桶的接入点来对对象执行操作。您不能使用接入点执行其他 Amazon S3 操作，例如修改或删除存储桶。有关支持接入点的 S3 操作的完整列表，请参阅通用存储桶的接入点兼容性。
> - 通用存储桶的接入点适用于部分 Amazon 服务和功能，但并不适用于所有此类服务和功能。例如，您不能将跨区域复制配置为通过接入点进行操作。有关与 S3 接入点兼容的 Amazon 服务的完整列表，请参阅通用存储桶的接入点兼容性。

主题


- 列出通用存储桶的接入点
- 查看通用存储桶的接入点的详细信息
- 删除通用存储桶的接入点


## 列出通用存储桶的接入点

本节介绍如何通过 Amazon Web Services Management Console、Amazon Command Line Interface 或 REST API 来列出通用存储桶的接入点。

使用 S3 控制台

列出 Amazon Web Services 账户中的接入点

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在页面顶部的导航栏中，选择当前所显示 Amazon Web Services 区域的名称。接下来，选择要列出其接入点的区域。
3. 在控制台左侧的导航窗格中，选择接入点。
4. （可选）按名称搜索接入点。只有您选择的 Amazon Web Services 区域中的接入点才会出现在此处。
5. 选择要管理或使用的接入点的名称。

使用 Amazon CLI

以下 `list-access-points` 示例命令显示了如何使用 Amazon CLI 列出您的接入点。

以下命令列出了 Amazon Web Services 账户 *111122223333* 的接入点。

```
aws s3control list-access-points --account-id 111122223333
```

以下命令列出了 Amazon Web Services 账户 *111122223333* 的附加到存储桶 *amzn-s3-demo-bucket* 的接入点。

```
aws s3control list-access-points --account-id 111122223333 --bucket amzn-s3-demo-bucket
```

有关更多信息和示例，请参阅《Amazon CLI 命令参考》中的 list-access-points。

使用 REST API

可以使用 REST API 列出接入点。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 ListAccessPoints。

## 查看通用存储桶的接入点的详细信息

本节介绍如何使用 Amazon Web Services Management Console、Amazon Command Line Interface 或 REST API 来查看通用存储桶的接入点的详细信息。

使用 S3 控制台

查看 Amazon Web Services 账户中接入点的详细信息

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在页面顶部的导航栏中，选择当前所显示 Amazon Web Services 区域的名称。接下来，选择要列出其接入点的区域。
3. 在控制台左侧的导航窗格中，选择接入点。
4. （可选）按名称搜索接入点。只有您选择的 Amazon Web Services 区域中的接入点才会出现在此处。
5. 选择要管理或使用的接入点的名称。
6. 选择属性选项卡以查看所选接入点的接入点存储桶、账户 ID、Amazon Web Services 区域、创建日期、网络来源、S3 URI、ARN 和接入点别名。
7. 选择权限选项卡，以查看所选接入点的屏蔽公共访问权限设置和接入点策略。

> **Note**
>
> 创建接入点后，您无法更改接入点的屏蔽公共访问权限设置。

使用 Amazon CLI

以下 `get-access-point` 示例命令显示了如何使用 Amazon CLI 来查看接入点的详细信息。

以下命令列出了 Amazon Web Services 账户 *111122223333* 的接入点 *my-access-point* 的详细信息。

```
aws s3control get-access-point --name my-access-point --account-id 111122223333
```

输出示例：

```
{
    "Name": "my-access-point",
    "Bucket": "amzn-s3-demo-bucket",
    "NetworkOrigin": "Internet",
    "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": true,
```

```
        "IgnorePublicAcls": true,
        "BlockPublicPolicy": true,
        "RestrictPublicBuckets": true
    },
    "CreationDate": "2016-08-29T22:57:52Z",
    "Alias": "my-access-point-u1ny6bhm7moymqx8cuon8o1g4mwikuse2a-s3alias",
    "AccessPointArn": "arn:aws:s3:Amazon Web Services ##:111122223333:accesspoint/my-
access-point",
    "Endpoints": {
        "ipv4": "s3-accesspoint.Amazon Web Services ##.amazonaws.com",
        "fips": "s3-accesspoint-fips.Amazon Web Services ##.amazonaws.com",
        "fips_dualstack": "s3-accesspoint-fips.dualstack.Amazon Web Services #
#.amazonaws.com",
        "dualstack": "s3-accesspoint.dualstack.Amazon Web Services ##.amazonaws.com"
    },
    "BucketAccountId": "111122223333"
}
```

有关更多信息和示例，请参阅《Amazon CLI 命令参考》中的 get-access-point。

使用 REST API

可以使用 REST API 查看接入点的详细信息。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 GetAccessPoint。

## 删除通用存储桶的接入点

本节介绍如何使用 Amazon Web Services Management Console、Amazon Command Line Interface 或 REST API 来删除通用存储桶的接入点。

使用 S3 控制台

删除 Amazon Web Services 账户中的接入点

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在页面顶部的导航栏中，选择当前所显示 Amazon Web Services 区域的名称。接下来，选择要列出其接入点的区域。
3. 在控制台左侧的导航窗格中，选择接入点。
4. （可选）按名称搜索接入点。只有您选择的 Amazon Web Services 区域中的接入点才会出现在此处。

5. 选择要管理或使用的接入点的名称。
6. 在接入点页面中，选择删除以删除您选择的接入点。
7. 要确认删除，请键入接入点的名称，然后选择删除。

使用 Amazon CLI

以下 `delete-access-point` 示例命令显示了如何使用 Amazon CLI 删除接入点。

以下命令删除 Amazon Web Services 账户 *111122223333* 的接入点 *my-access-point*。

```
aws s3control delete-access-point --name my-access-point --account-id 111122223333
```

有关更多信息和示例，请参阅《Amazon CLI 命令参考》中的 delete-access-point。

使用 REST API

可以使用 REST API 查看接入点的详细信息。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 DeleteAccessPoint。

## 使用通用存储桶的 Amazon S3 接入点

以下示例演示如何在 Amazon S3 中将通用存储桶的接入点与兼容的操作结合使用。

> **Note**
>
> S3 会自动为所有接入点生成接入点别名，这些别名可以在任何使用存储桶名称来执行对象级操作的地方使用。有关更多信息，请参阅 通用存储桶的接入点别名。

您只能使用通用存储桶的接入点来对对象执行操作。您不能使用接入点执行其他 Amazon S3 操作，例如修改或删除存储桶。有关支持接入点的 S3 操作的完整列表，请参阅通用存储桶的接入点兼容性。

主题

- 通过通用存储桶的接入点列出对象
- 通过通用存储桶的接入点下载对象
- 通过通用存储桶的接入点配置访问控制列表（ACL）

- 通过通用存储桶的接入点上传对象
- 通过通用存储桶的接入点添加标签集
- 通过通用存储桶的接入点删除对象

## 通过通用存储桶的接入点列出对象

本节介绍如何使用 Amazon Web Services Management Console、Amazon Command Line Interface 或 REST API 通过通用存储桶的接入点列出您的对象。

使用 S3 控制台

在 Amazon Web Services 账户中通过接入点列出对象

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在页面顶部的导航栏中，选择当前所显示 Amazon Web Services 区域的名称。接下来，选择要列出其接入点的区域。
3. 在控制台左侧的导航窗格中，选择接入点。
4. （可选）按名称搜索接入点。只有您选择的 Amazon Web Services 区域中的接入点才会出现在此处。
5. 选择要管理或使用的接入点的名称。
6. 在对象选项卡下，可以查看要通过接入点访问的对象的名称。在使用接入点时，您只能执行接入点权限允许的对象操作。

> **Note**
>
> - 控制台视图始终显示存储桶中的所有对象。如本过程中所述使用接入点会限制您可以对这些对象执行的操作，但不会限制您是否能够看到这些对象存在于存储桶中。
> - Amazon Web Services Management Console不支持使用虚拟私有云（VPC）接入点访问存储桶资源。要从 VPC 接入点访问存储桶资源，请使用 Amazon CLI、Amazon SDK 或 Amazon S3 REST API。

使用 Amazon CLI

以下 `list-objects-v2` 示例命令显示了如何使用 Amazon CLI 通过接入点列出您的对象。

以下命令使用接入点 *my-access-point* 列出 Amazon Web Services 账户 *111122223333* 的对象。

```
aws s3api list-objects-v2 --bucket arn:aws:s3:Amazon Web Services #
#:111122223333:accesspoint/my-access-point
```

> **Note**
>
> S3 会自动为所有接入点生成接入点别名，这些别名可以在任何使用存储桶名称来执行对象级操作的地方使用。有关更多信息，请参阅 通用存储桶的接入点别名。

有关更多信息和示例，请参阅《Amazon CLI 命令参考》中的 list-access-points。

使用 REST API

可以使用 REST API 列出接入点。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 ListObjectsV2。

## 通过通用存储桶的接入点下载对象

本节介绍如何使用 Amazon Web Services Management Console、Amazon Command Line Interface 或 REST API 通过通用存储桶的接入点下载对象。

使用 S3 控制台

在 Amazon Web Services 账户中通过接入点下载对象。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在页面顶部的导航栏中，选择当前所显示 Amazon Web Services 区域的名称。接下来，选择要列出其接入点的区域。
3. 在控制台左侧的导航窗格中，选择接入点。
4. （可选）按名称搜索接入点。只有您选择的 Amazon Web Services 区域中的接入点才会出现在此处。
5. 选择要管理或使用的接入点的名称。
6. 在对象选项卡下，选择要下载的对象的名称。
7. 选择下载。

使用 Amazon CLI

以下 `get-object` 示例命令显示了如何使用 Amazon CLI 通过接入点下载对象。

以下命令使用接入点 *my-access-point* 下载 Amazon Web Services 账户 *111122223333* 的对象 `puppy.jpg`。您必须包含 `outfile`，这是已下载对象的文件名，例如 *my_downloaded_image.jpg*。

```
aws s3api get-object --bucket arn:aws:s3:Amazon Web Services #
#:111122223333:accesspoint/my-access-point --key puppy.jpg my_downloaded_image.jpg
```

> **Note**
>
> S3 会自动为所有接入点生成接入点别名，这些别名可以在任何使用存储桶名称来执行对象级操作的地方使用。有关更多信息，请参阅 通用存储桶的接入点别名。

有关更多信息和示例，请参阅《Amazon CLI 命令参考》中的 get-object。

使用 REST API

您可以使用 REST API 通过接入点下载对象。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 GetObject。

使用 Amazon SDK

可以使用适用于 Python 的 Amazon SDK 通过接入点下载对象。

Python

在以下示例中，使用名为 *my-access-point* 的接入点为 Amazon 账户 *111122223333* 下载名为 *hello.txt* 的文件。

```
import boto3
s3 = boto3.client('s3')
s3.download_file('arn:aws:s3:us-east-1:111122223333:accesspoint/my-access-point',
 'hello.txt', '/tmp/hello.txt')
```

## 通过通用存储桶的接入点配置访问控制列表（ACL）

本节介绍如何使用 Amazon Web Services Management Console、Amazon Command Line Interface 或 REST API 通过通用存储桶的接入点配置 ACL。有关 ACL 的更多信息，请参阅 访问控制列表 (ACL) 概述。

使用 S3 控制台

在 Amazon Web Services 账户中通过接入点配置 ACL

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在页面顶部的导航栏中，选择当前所显示 Amazon Web Services 区域的名称。接下来，选择要列出其接入点的区域。
3. 在控制台左侧的导航窗格中，选择接入点。
4. （可选）按名称搜索接入点。只有您选择的 Amazon Web Services 区域中的接入点才会出现在此处。
5. 选择要管理或使用的接入点的名称。
6. 在对象选项卡下，选择要为其配置 ACL 的对象的名称。
7. 在权限选项卡下，选择编辑以配置对象 ACL。

> **Note**
>
> Amazon S3 当前不支持在创建接入点之后更改接入点的屏蔽公共访问权限设置。

使用 Amazon CLI

以下 `put-object-acl` 示例命令显示如何使用 Amazon CLI，借助 ACL 通过接入点配置访问权限。

以下命令通过 Amazon Web Services 账户 *111122223333* 拥有的接入点将 ACL 应用于现有对象 `puppy.jpg`。

```
aws s3api put-object-acl --bucket arn:aws:s3:Amazon Web Services #
#:111122223333:accesspoint/my-access-point --key puppy.jpg --acl private
```

> **Note**
>
> S3 会自动为所有接入点生成接入点别名，这些别名可以在任何使用存储桶名称来执行对象级操作的地方使用。有关更多信息，请参阅 通用存储桶的接入点别名。

有关更多信息和示例，请参阅《Amazon CLI 命令参考》中的 put-object-acl。

使用 REST API

您可以使用 REST API，借助 ACL 通过接入点配置访问权限。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 PutObjectAcl。

## 通过通用存储桶的接入点上传对象

本节介绍如何使用 Amazon Web Services Management Console、Amazon Command Line Interface 或 REST API 通过通用存储桶的接入点上传对象。

使用 S3 控制台

在 Amazon Web Services 账户中通过接入点上传对象。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在页面顶部的导航栏中，选择当前所显示 Amazon Web Services 区域的名称。接下来，选择要列出其接入点的区域。
3. 在控制台左侧的导航窗格中，选择接入点。
4. （可选）按名称搜索接入点。只有您选择的 Amazon Web Services 区域中的接入点才会出现在此处。
5. 选择要管理或使用的接入点的名称。
6. 在对象选项卡下，选择上传。
7. 将要上传的文件和文件夹拖放到此处，或者选择添加文件或添加文件夹。

> **Note**
>
> 可使用 Amazon S3 控制台上传的文件的最大大小为 160 GB。要上传大于 160GB 的文件，请使用 Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 Amazon S3 REST API。

8. 要更改访问控制列表权限，请选择 Permissions（权限）。
9. 在 Access control list (ACL) [访问控制列表 (ACL)]下，编辑权限。

   有关对象访问权限的信息，请参阅 使用 S3 控制台为对象设置 ACL 权限。您可以向公众（世界上的每一个人）授予对您的对象的读取访问权限，使其能够获取您正在上传的所有文件。但是，我们建议您不要更改公共读取访问的默认设置。授予公有读取访问权限适用于一小部分的使用案例（如存储桶用于网站时）。您始终可以在上传对象后更改对象权限。
10. 要配置其他附加属性，请选择 Properties（属性）。
11. 在存储类下，为正在上传的文件选择存储类。

    有关存储类的更多信息，请参阅 了解和管理 Amazon S3 存储类。
12. 要更新对象的加密设置，请在服务器端加密设置下执行以下操作：

    a. 选择 Specify an encryption key（指定加密密钥）。

    b. 在加密设置下，选择使用默认加密的存储桶设置或覆盖默认加密的存储桶设置。

    c. 如果您选择覆盖默认加密的存储桶设置，则必须配置以下加密设置。

    - 要使用由 Amazon S3 托管的密钥加密上传的文件，请选择 Amazon S3 托管式密钥（SSE-S3）。

      有关更多信息，请参阅 使用具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）。
    - 要使用存储在 Amazon Key Management Service（Amazon KMS）中的密钥加密上传的文件，请选择 Amazon Key Management Service 密钥（SSE-KMS）。然后，为 Amazon KMS 密钥选择以下选项之一：
      - 要从可用的 KMS 密钥列表中进行选择，请选择从您的 Amazon KMS keys 中进行选择，然后从可用密钥的列表中选择您的 KMS 密钥。

        Amazon 托管式密钥（aws/s3）和您的客户自主管理型密钥都显示在此列表中。有关客户自主管理型密钥的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的客户密钥和 Amazon 密钥。
      - 要输入 KMS 密钥 ARN，请选择输入 Amazon KMS key ARN，然后在显示的字段中输入您的 KMS 密钥 ARN。
      - 要在 Amazon KMS 控制台中创建新的客户自主管理型密钥，请选择创建 KMS 密钥。

        有关创建 Amazon KMS key 的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的创建密钥。

> **Important**
>
> 您只能使用与存储桶所在相同的 Amazon Web Services 区域中可用的 KMS 密钥。Amazon S3 控制台仅列出与存储桶位于同一区域中的前 100 个 KMS 密钥。要使用未列出的 KMS 密钥，您必须输入 KMS 密钥 ARN。如果您希望使用其他账户拥有的 KMS 密钥，则必须首先有权使用该密钥，然后必须输入相应的 KMS 密钥 ARN。
>
> Amazon S3 仅支持对称加密 KMS 密钥，不支持非对称 KMS 密钥。有关更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的确定对称和非对称 KMS 密钥。

13. 要使用其他校验和，请选择 On（打开）。然后对于 Checksum function（校验和函数），选择要使用的函数。Amazon S3 在收到整个对象后计算并存储校验和值。您可以使用 Precalculated value（预计算值）框来提供预先计算的值。这样，Amazon S3 会将您提供的值与其计算的值进行比较。如果两个值不匹配，Amazon S3 将生成错误。

    其他校验和使您能够指定要用于验证数据的校验和算法。有关其他校验和的更多信息，请参阅在 Amazon S3 中检查对象完整性。

14. 要向上传的所有对象添加标签，请选择 Add tag (添加标签)。在键字段中输入标签名称。输入标签的值。

    对象标签为您提供了对存储进行分类的方法。每个标签都是一个键-值对。键和标签值区分大小写。对于每个对象，您最多可以有 10 个标签。标签键的长度最大可以为 128 个 Unicode 字符，标签值的长度最大可以为 255 个 Unicode 字符。有关对象标签的更多信息，请参阅 使用标签对存储进行分类。

15. 要添加元数据，请选择添加元数据。

    a. 在类型下，请选择系统定义或用户定义。

       对于系统定义元数据，您可以选择通用的 HTTP 标头，如 Content-Type 和 Content-Disposition。有关系统定义元数据的列表以及您能否添加值的信息，请参阅系统定义的对象元数据。以前缀 `x-amz-meta-` 开头的任何元数据都被视为用户定义的元数据。用户定义元数据会与对象存储在一起，并会在您下载该对象时返回。密钥及其值均必须符合 US-ASCII 标准。用户定义元数据最大可为 2 KB。如需详细了解系统定义和用户定义的元数据，请参阅使用对象元数据。

    b. 对于键，请选择一个键。

c. 键入该键的值。

16. 要上传对象，请选择上传。

Amazon S3 将上传您的对象。上传完成后，您可以在上传：状态页面上看到成功消息。

使用 Amazon CLI

以下 `put-object` 示例命令显示了如何使用 Amazon CLI 通过接入点上传您的对象。

以下命令使用接入点 *my-access-point* 上传 Amazon Web Services 账户 *111122223333* 的对象 `puppy.jpg`。

```
aws s3api put-object --bucket arn:aws:s3:Amazon Web Services #
#:111122223333:accesspoint/my-access-point --key puppy.jpg --body puppy.jpg
```

> **Note**
>
> S3 会自动为所有接入点生成接入点别名，这些接入点别名可以在任何使用存储桶名称来执行对象级操作的地方使用。有关更多信息，请参阅 通用存储桶的接入点别名。

有关更多信息和示例，请参阅《Amazon CLI 命令参考》中的 put-object。

使用 REST API

您可以使用 REST API 通过接入点上传对象。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 PutObject。

使用 Amazon SDK

可以使用适用于 Python 的 Amazon SDK 通过接入点上传对象。

Python

在以下示例中，使用名为 *my-access-point* 的接入点为 Amazon 账户 *111122223333* 上传名为 *hello.txt* 的文件。

```
import boto3
s3 = boto3.client('s3')
s3.upload_file('/tmp/hello.txt', 'arn:aws:s3:us-east-1:111122223333:accesspoint/my-
access-point', 'hello.txt')
```

## 通过通用存储桶的接入点添加标签集

本节介绍如何使用 Amazon Web Services Management Console、Amazon Command Line Interface 或 REST API 通过通用存储桶的接入点添加标签集。有关更多信息，请参阅 使用标签对存储进行分类。

使用 S3 控制台

在 Amazon Web Services 账户中通过接入点添加标签集

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在页面顶部的导航栏中，选择当前所显示 Amazon Web Services 区域的名称。接下来，选择要列出其接入点的区域。
3. 在控制台左侧的导航窗格中，选择接入点。
4. （可选）按名称搜索接入点。只有您选择的 Amazon Web Services 区域中的接入点才会出现在此处。
5. 选择要管理或使用的接入点的名称。
6. 在对象选项卡下，选择要向其添加标签集的对象的名称。
7. 在属性选项卡下，找到标签子标题并选择编辑。
8. 查看列出的对象，然后选择添加标签。
9. 每个对象标签都是一个键值对。输入 Key (键) 和 Value (值)。要添加另一个标签，请选择 Add Tag (添加标签)。

   您最多可以为一个对象输入 10 个标签。
10. 选择保存更改。

使用 Amazon CLI

以下 `put-object-tagging` 示例命令显示了如何使用 Amazon CLI 通过接入点添加标签集。

以下命令使用接入点 *`my-access-point`* 为现有对象 `puppy.jpg` 添加标签集。

```
aws s3api put-object-tagging --bucket arn:aws:s3:Amazon Web Services
 ##:111122223333:accesspoint/my-access-point --key puppy.jpg --tagging
 TagSet=[{Key="animal",Value="true"}]
```

> **Note**
>
> S3 会自动为所有接入点生成接入点别名，这些接入点别名可以在任何使用存储桶名称来执行对象级操作的地方使用。有关更多信息，请参阅 通用存储桶的接入点别名。

有关更多信息和示例，请参阅《Amazon CLI 命令参考》中的 put-object-tagging。

使用 REST API

您可以使用 REST API 通过接入点向对象添加标签集。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 PutObjectTagging。

## 通过通用存储桶的接入点删除对象

本节介绍如何使用 Amazon Web Services Management Console、Amazon Command Line Interface 或 REST API 通过通用存储桶的接入点删除对象。

使用 S3 控制台

在 Amazon Web Services 账户中通过接入点删除一个或多个对象

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在页面顶部的导航栏中，选择当前所显示 Amazon Web Services 区域的名称。接下来，选择要列出其接入点的区域。
3. 在控制台左侧的导航窗格中，选择接入点。
4. （可选）按名称搜索接入点。只有您选择的 Amazon Web Services 区域中的接入点才会出现在此处。
5. 选择要管理或使用的接入点的名称。
6. 在对象选项卡下，选择要删除的一个或多个对象的名称。
7. 查看列出的供删除的对象，然后在确认框中键入 delete。
8. 选择删除对象。

使用 Amazon CLI

以下 `delete-object` 示例命令显示了如何使用 Amazon CLI 通过接入点删除对象。

以下命令使用接入点 *my-access-point* 删除现有对象 puppy.jpg。

```
aws s3api delete-object --bucket arn:aws:s3:Amazon Web Services #
#:111122223333:accesspoint/my-access-point --key puppy.jpg
```

> **Note**
>
> S3 会自动为所有接入点生成接入点别名，这些接入点别名可以在任何使用存储桶名称来执行对象级操作的地方使用。有关更多信息，请参阅 通用存储桶的接入点别名。

有关更多信息和示例，请参阅《Amazon CLI 命令参考》中的 delete-object。

使用 REST API

您可以使用 REST API 通过接入点删除对象。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 DeleteObject。

# 使用 S3 Access Grants 管理访问权限

要遵守最低权限原则，您可以根据应用程序、角色、组或组织单位来定义对 Amazon S3 数据的精细访问权限。根据访问模式的规模和复杂性，可以使用各种方法实现对 Amazon S3 中的数据的精细访问。

对于 Amazon Identity and Access Management（IAM）主体来说，通过定义 IAM 权限策略和 S3 存储桶策略，可以最轻松地管理对 Amazon S3 中的少量和中等数量数据集的访问。只要必要的策略符合 S3 存储桶策略的策略大小限制（20 KB）和 IAM 策略的策略大小限制（5 KB），并且在每个账户允许的 IAM 主体数量内，此策略就将适用。

随着数据集和使用场景不断增多，您可能需要更多的策略空间。为策略语句提供更多空间的一种方法是，使用 S3 接入点作为 S3 存储桶的附加端点，因为每个接入点均可拥有自己的策略。您可以定义非常精细的访问控制模式，因为每个账户在每个 Amazon Web Services 区域内可以拥有数千个接入点，每个接入点的策略大小最多 20 KB。尽管 S3 接入点增加了可用的策略空间，但它需要通过一种机制让客户端发现正确数据集的正确接入点。

第三种方法是实施 IAM 会话代理模式，在该模式中，您可以实施访问决策逻辑并为每个访问会话动态生成短期 IAM 会话凭证。虽然 IAM 会话代理方法支持任意动态权限模式并能有效扩展，但您必须构建访问模式逻辑。

您可以使用 S3 Access Grants 来管理对 Amazon S3 数据的访问权限，而不是使用上述方法。S3 Access Grants 提供了一个简化模型，用于按前缀、存储桶或对象定义对 Amazon S3 中数据的访问权

限。此外，可以使用 S3 Access Grants 向 IAM 主体授予访问权限，并直接向公司目录中的用户或组授予访问权限。

通常，可以通过将用户和组映射到数据集来定义对 Amazon S3 中数据的权限。可以使用 S3 Access Grants 定义 S3 前缀与 Amazon S3 存储桶和对象中的用户与角色的直接访问映射。借助 S3 Access Grants 中的简化访问方案，可以按 S3 前缀向 IAM 主体授予只读、只写或读写访问权限，并直接向公司目录中的用户或组授予只读、只写或读写访问权限。借助这些 S3 Access Grants 功能，应用程序可以代表其当前经过身份验证的用户向 Amazon S3 请求数据。

将 S3 Access Grants 与 Amazon IAM Identity Center 的可信身份传播功能集成后，应用程序可以直接代表经过身份验证的公司目录用户向 Amazon Web Services 服务（包括 S3 Access Grants）发出请求。应用程序不再需要先将用户映射到 IAM 主体。此外，由于最终用户身份将一直传播到 Amazon S3，因此简化了审核哪个用户访问了哪个 S3 对象的过程。您不再需要重构不同的用户和 IAM 会话之间的关系。在将 S3 Access Grants 与 IAM Identity Center 可信身份传播结合使用时，Amazon S3 的每个 Amazon CloudTrail 数据事件均包含对代表其访问数据的最终用户的直接引用。

有关 S3 Access Grants 的更多信息，请参阅以下主题。

主题


- S3 Access Grants 的概念
- S3 Access Grants 和公司目录身份
- 开始使用 S3 Access Grants
- 使用 S3 访问权限管控实例
- 使用 S3 访问权限管控位置
- 在 S3 访问权限管控中处理授权
- 使用访问授权获取 S3 数据
- S3 Access Grants 跨账户访问
- 将 Amazon 标签与 S3 Access Grants 配合使用
- S3 Access Grants 限制
- S3 Access Grants 集成


## S3 Access Grants 的概念

S3 访问权限管控工作流程

S3 访问权限管控工作流程为：

1. 创建 S3 访问权限管控实例。请参阅使用 S3 访问权限管控实例。
2. 在 S3 访问权限管控实例中，在 Amazon S3 数据中注册位置，并将这些位置映射到 Amazon Identity and Access Management（IAM）角色。请参阅注册位置。
3. 为被授权者创建授权，这会向被授权者授予访问 S3 资源的权限。请参阅在 S3 访问权限管控中处理授权。
4. 被授权者从 S3 访问权限管控请求临时凭证。请参阅通过 S3 Access Grants 请求访问 Amazon S3 数据。
5. 被授权者使用这些临时凭证来访问 S3 数据。请参阅使用 S3 访问权限管控提供的凭证访问 S3 数据。

有关更多信息，请参阅 开始使用 S3 Access Grants。

S3 Access Grants 实例

S3 访问权限管控实例 是各个授权 的逻辑容器。创建 S3 访问权限管控实例时，您必须指定 Amazon Web Services 区域。您 Amazon Web Services 账户中的每个 Amazon Web Services 区域都可具有一个 S3 访问权限管控实例。有关更多信息，请参阅 使用 S3 访问权限管控实例。

如果您想使用 S3 访问权限管控向公司目录中的用户和组身份授予访问权限，还必须将 S3 访问权限管控实例与 Amazon IAM Identity Center 实例关联。有关更多信息，请参阅 S3 Access Grants 和公司目录身份。

新创建的 S3 访问权限管控实例为空。您必须在实例中注册一个位置，该位置可以是 S3 默认路径 (`s3://`)、存储桶或存储桶内的前缀。在您注册至少一个位置后，您可以创建访问权限管控，来授予访问该已注册位置中的数据的权限。

位置

S3 访问权限管控位置 将存储桶或前缀映射到 Amazon Identity and Access Management（IAM）角色。S3 访问权限管控代入此 IAM 角色，来向访问该特定位置的被授权者提供临时凭证。您必须先在 S3 访问权限管控实例中注册至少一个位置，然后才能创建访问权限管控。

我们建议您注册默认位置 (`s3://`) 并将其映射到 IAM 角色。默认 S3 路径 (`s3://`) 处的位置涵盖了对您账户的 Amazon Web Services 区域中所有 S3 存储桶的访问权限。创建访问权限管控时，您可以将授予范围缩小到默认位置内的存储桶、前缀或对象。

更复杂的访问管理用例可能要求您注册比默认位置更多的位置。此类用例的一些示例为：

- 假设 *amzn-s3-demo-bucket* 是 S3 访问权限管控实例中的一个注册位置，并且有一个 IAM 角色映射到该位置，但拒绝该 IAM 角色访问存储桶中的特定前缀。在这种情况下，您可以将 IAM 角色无权访问的前缀注册为单独的位置，并将该位置映射到具有必要访问权限的其它 IAM 角色。
- 假设您要创建的授权将访问权限仅限制为虚拟私有云（VPC）端点中的用户。在这种情况下，您可以为存储桶注册一个位置，IAM 角色在该位置限制对 VPC 端点的访问。稍后，当被授权者向 S3 访问权限管控索取凭证时，S3 访问权限管控将代入该位置的 IAM 角色来提供临时凭证。除非调用方位于 VPC 端点内，否则此凭证将拒绝访问特定存储桶。除在授权中指定的常规 READ、WRITE 或 READWRITE 权限外，还会应用此拒绝权限。

如果您的用例要求您在 S3 访问权限管控实例中注册多个位置，则可以注册以下任意位置：

- 默认 S3 位置 (`s3://`)
- 一个存储桶（例如 *amzn-s3-demo-bucket*）或多个存储桶
- 一个存储桶和一个前缀（例如 *amzn-s3-demo-bucket*`/prefix*`）或多个前缀

有关您可以在 S3 访问权限管控实例中注册的最大位置数，请参阅 S3 Access Grants 限制。有关注册 S3 访问权限管控位置的更多信息，请参阅注册位置。

在 S3 访问权限管控实例中注册第一个位置后，您的实例中仍没有任何单个访问权限管控。因此，尚未授予对任何 S3 数据的访问权限。现在，您可以创建访问权限管控来授予访问权限。有关创建授权的更多信息，请参阅在 S3 访问权限管控中处理授权。

授权

S3 访问权限管控实例中的单个授权 可让特定身份（IAM 主体或公司目录中的用户或组）在 S3 访问权限管控实例中注册的位置内获得访问权限。

创建授权时，您不必授予对整个已注册位置的访问权限。您可以缩小某个位置内授权的访问权限范围。如果注册位置是默认 S3 路径 (`s3://`)，则需要将授权的范围缩小到存储桶、存储桶内的前缀或特定对象。如果授权的注册位置是存储桶或前缀，则可以授予对整个存储桶或前缀的访问权限，也可以选择将授权范围缩小到前缀、子前缀或对象。

在授权中，还将授权的访问权限级别设置为 READ、WRITE 或 READWRITE。假设您拥有授权，用于向公司目录组 `01234567-89ab-cdef-0123-456789abcdef` 授予对存储桶 `s3://`*amzn-s3-demo-bucket*`/projects/items/*` 的 READ 访问权限。对于名为 *amzn-s3-demo-bucket* 的存储桶中对象键名称以前缀 `projects/items/` 开头的每个对象，该组中的用户都可以具有 READ 访问权限。

有关您可以在 S3 访问权限管控实例中创建的最大授权数量，请参阅 S3 Access Grants 限制。有关创建授权的更多信息，请参阅创建授权。

S3 Access Grants 临时凭证

创建授权后，利用在授权中指定的身份的获授权应用程序可以请求即时访问凭证。为此，应用程序调用 GetDataAccess S3 API 操作。被授权者可以使用此 API 操作来请求访问您与他们共享的 S3 数据。

S3 Access Grants 实例根据其拥有的授权来评估 GetDataAccess 请求。如果对于请求者存在匹配的授权，则 S3 访问权限管控将代入与匹配授权的已注册位置关联的 IAM 角色。S3 访问权限管控将临时凭证的权限范围限定为仅访问由授权的范围指定的 S3 存储桶、前缀或对象。

虽然临时访问凭证的到期时间默认为 1 小时，但可以将到期时间设置为介于 15 分钟和 12 小时之间的任意值。请参阅 AssumeRole API 参考中的最长持续时间会话。

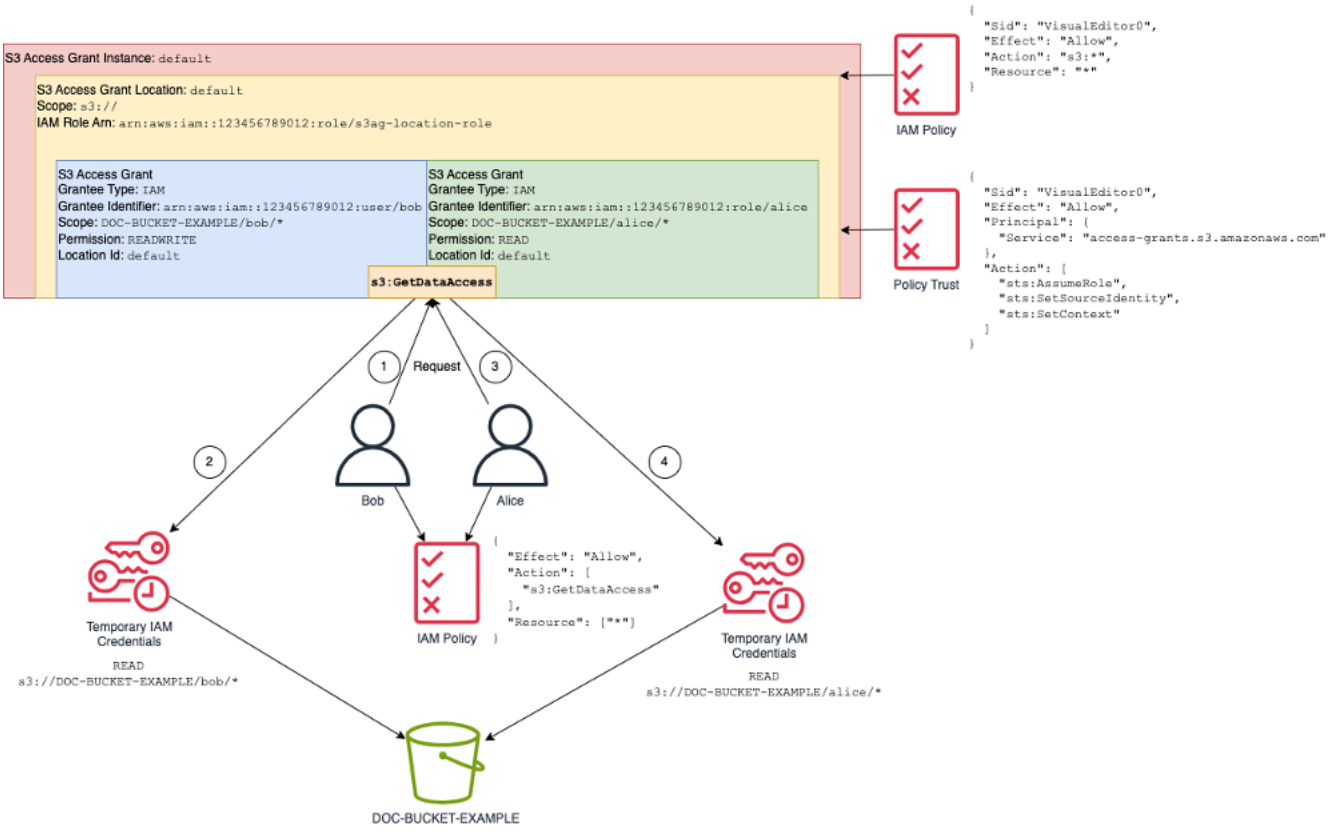
## 工作方式

在下图中，范围为 s3:// 的默认 Amazon S3 位置已注册到 IAM 角色 s3ag-location-role。当通过 S3 Access Grants 获取凭证时，此 IAM 角色有权在账户内执行 Amazon S3 操作。

在此位置，为两个 IAM 用户创建两个单独的访问授权。向 IAM 用户 Bob 授予对 DOC-BUCKET-EXAMPLE 存储桶中的 bob/ 前缀的 READ 和 WRITE 访问权限。仅向另一个 IAM 角色 Alice 授予对 DOC-BUCKET-EXAMPLE 桶中 alice/ 前缀的 READ 访问权限。为 Bob 定义了用于访问 DOC-BUCKET-EXAMPLE 存储桶中的前缀 bob/ 的授权（蓝色）。为 Alice 定义了用于访问 DOC-BUCKET-EXAMPLE 存储桶中的前缀 alice/ 的授权（绿色）。

当 Bob 需要对数据进行 READ 访问时，与其授权所在位置关联的 IAM 角色会调用 S3 Access Grants GetDataAccess API 操作。如果 Bob 尝试对任何以 s3://DOC-BUCKET-EXAMPLE/bob/* 开头的 S3 前缀或对象进行 READ 访问，则 GetDataAccess 请求将返回一组具有对 s3://DOC-BUCKET-EXAMPLE/bob/* 的访问权限的临时 IAM 会话凭证。同样，Bob 可以对任何以 s3://DOC-BUCKET-EXAMPLE/bob/* 开头的 S3 前缀或对象进行 WRITE 访问，因为该授权也允许这样做。

同样，Alice 可以对任何以 s3://DOC-BUCKET-EXAMPLE/alice/ 开头的项进行 READ 访问。但是，如果她尝试对 s3:// 中的任何存储桶、前缀或对象进行任何 WRITE 访问，她将收到“拒绝访问（403 禁止）”错误，因为没有允许她对任何数据进行 WRITE 访问的授权。此外，如果 Alice 请求对 s3://DOC-BUCKET-EXAMPLE/alice/ 外部的数据进行任何级别的访问（READ 或 WRITE），她将再次收到“拒绝访问”错误。




此模式可以扩展到大量的用户和存储桶，并简化对这些权限的管理。您可以添加和删除单个离散授权，而不是在每次需要添加或删除单个用户前缀访问关系时编辑可能很大的 S3 存储桶策略。

## S3 Access Grants 和公司目录身份

您可以使用 Amazon S3 Access Grants 向 Amazon Identity and Access Management（IAM）主体（用户或角色）授予访问权限，无论是在同一个还是其他 Amazon Web Services 账户中。但在许多情况下，访问数据的实体是公司目录中的最终用户。可以使用 S3 Access Grants 直接向公司用户和组授予访问权限，而不是向 IAM 主体授予访问权限。借助 S3 Access Grants，您不再需要将公司身份映射到中间 IAM 主体，即可通过公司应用程序访问您的 S3 数据。

这项新功能（支持使用最终用户身份访问数据）是通过将 S3 Access Grants 实例与 Amazon IAM Identity Center 实例关联来提供的。IAM Identity Center 支持基于标准的身份提供商，并且是 Amazon 中支持最终用户身份的任何服务或功能（包括 S3 Access Grants）的中心。IAM Identity Center 通过其可信身份传播功能来支持验证公司身份。有关更多信息，请参阅跨应用程序的可信身份传播。

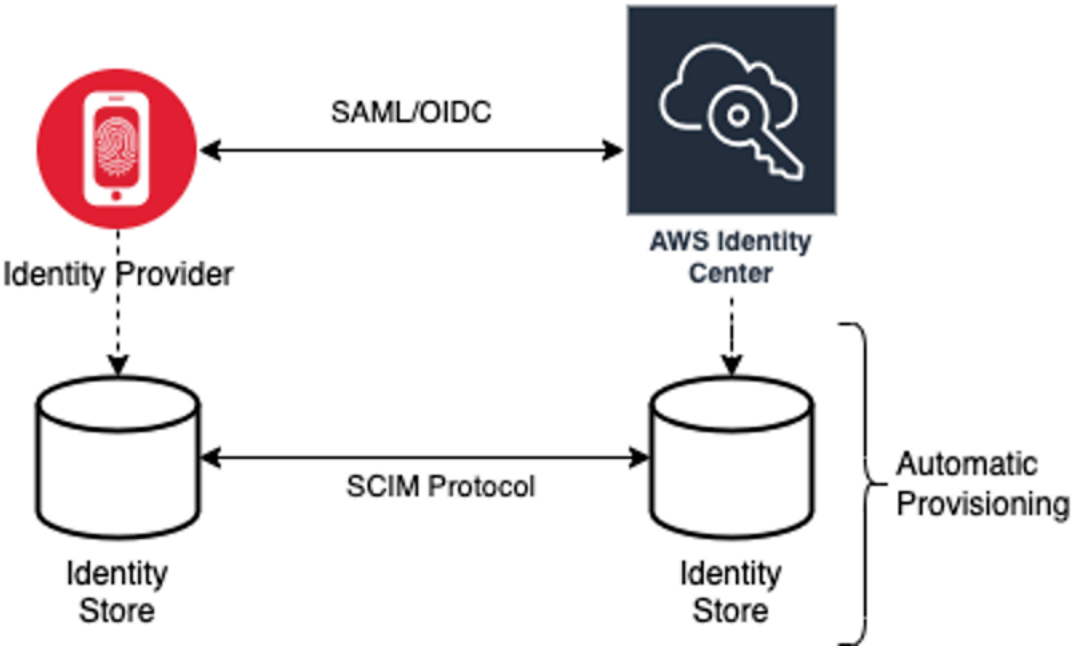
要开始使用 S3 Access Grants 中的人力身份支持，您首先必须从 IAM Identity Center 开始，在公司身份提供商和 IAM Identity Center 之间配置身份预置。IAM Identity Center 支持公司身份提供商，例如 Okta、Microsoft Entra ID（以前称为 Azure Active Directory），或任何其他支持跨域身份管理系统（SCIM）协议的外部身份提供商（IdP）。在将 IAM Identity Center 连接到 IdP 并启用自动预

置时，IdP 中的用户和组将同步到 IAM Identity Center 中的身份存储。此步骤完成后，IAM Identity Center 将拥有自己的用户和组视图，这样您便能使用其他 Amazon Web Services 服务 和功能（例如 S3 Access Grants）来引用它们。有关配置 IAM Identity Center 自动预置的更多信息，请参阅《Amazon IAM Identity Center 用户指南》中的自动预置。

IAM Identity Center 与 Amazon Organizations 集成，这使您能够集中管理多个 Amazon Web Services 账户的权限，而无需手动配置每个账户。在典型企业中，您的身份管理员会为整个企业配置一个 IAM Identity Center 实例，以作为单个身份同步点。此 IAM Identity Center 实例通常在企业的专用 Amazon Web Services 账户中运行。在此通用配置中，您可以从企业内的任何 Amazon Web Services 账户中引用 S3 Access Grants 中的用户和组身份。

但是，如果 Amazon Organizations 管理员尚未配置中央 IAM Identity Center 实例，您可以在与 S3 Access Grants 实例相同的账户中创建一个本地实例。此类配置在概念验证或本地开发使用场景中更常见。在所有情况下，IAM Identity Center 实例都必须在与其关联到的 S3 Access Grants 实例相同的 Amazon Web Services 区域内。

在下面的 IAM Identity Center 配置与外部 IdP 图中，已使用 SCIM 配置 IdP，以将身份存储从 IdP 同步到 IAM Identity Center 中的身份存储。




要将您的公司目录身份与 S3 Access Grants 结合使用，请执行以下操作：

- 在 IAM Identity Center 中设置自动预置，将来自 IdP 的用户和组信息同步到 IAM Identity Center。
- 将您在 IAM Identity Center 中的外部身份源配置为可信令牌颁发机构。有关更多信息，请参阅《Amazon IAM Identity Center 用户指南》中的跨应用程序的可信身份传播。

- 将 S3 Access Grants 实例与 IAM Identity Center 实例关联。您可以在创建 S3 Access Grants 实例时执行此操作。如果您已创建 S3 Access Grants 实例，请参阅 关联或取消关联 IAM Identity Center 实例。

## 目录身份访问 S3 数据的方式

假设您的公司目录用户需要通过公司应用程序（例如文档查看器应用程序）访问您的 S3 数据，该应用程序与您的外部 IdP（例如 Okta）集成以对用户进行身份验证。这些应用程序中的用户身份验证通常将通过用户 Web 浏览器中的重定向来完成。由于目录中的用户不是 IAM 主体，因此您的应用程序需要 IAM 凭证，该凭证可用于代表用户调用 S3 Access Grants `GetDataAccess` API 操作来获取 S3 数据的访问凭证。与自行获得凭证的 IAM 用户和角色不同，您的应用程序需要通过某种方式来表示未映射到 IAM 角色的目录用户，以便该用户能够通过 S3 Access Grants 获得数据访问权限。

从经过身份验证的目录用户到能够代表目录用户向 S3 Access Grants 发出请求的 IAM 调用方是一个过渡，它由应用程序通过 IAM Identity Center 的可信令牌颁发机构功能完成。在对目录用户进行身份验证后，应用程序将获得来自 IdP（例如 Okta）的身份令牌，该令牌代表目录用户，具体取决于 Okta。IAM Identity Center 中的可信令牌颁发机构配置使应用程序能够用此 Okta 令牌（Okta 租户配置为“可信颁发机构”）交换来自 IAM Identity Center 的其他身份令牌，从而安全地表示 Amazon Web Services 服务中的目录用户。之后，数据应用程序将代入一个 IAM 角色，提供来自 IAM Identity Center 的目录用户令牌作为附加上下文。应用程序可使用生成的 IAM 会话来调用 S3 Access Grants。令牌既表示应用程序的身份（IAM 主体本身），也表示目录用户的身份。

此过渡的主要步骤是令牌交换。应用程序通过在 IAM Identity Center 中调用 `CreateTokenWithIAM` API 操作来执行此令牌交换。当然，这也是 Amazon API 调用，需要一个 IAM 主体进行签名。发出此请求的 IAM 主体通常是与应用程序关联的 IAM 角色。例如，如果应用程序在 Amazon EC2 上运行，则 `CreateTokenWithIAM` 请求通常由与运行该应用程序的 EC2 实例关联的 IAM 角色执行。成功调用 `CreateTokenWithIAM` 会生成一个新的身份令牌，该令牌将在 Amazon Web Services 服务中被识别。

在应用程序可以代表目录用户调用 `GetDataAccess` 之前，下一步是让应用程序获取包含目录用户身份的 IAM 会话。应用程序通过 Amazon Security Token Service（Amazon STS）`AssumeRole` 请求执行此操作，该请求还包括目录用户的 IAM Identity Center 令牌作为附加身份上下文。此附加上下文可让 IAM Identity Center 将目录用户的身份传播到下一步。应用程序代入的 IAM 角色需要 IAM 权限才能调用 `GetDataAccess` 操作。

在代入身份持有者 IAM 角色并将目录用户的 IAM Identity Center 令牌作为附加上下文后，应用程序现在便能代表经过身份验证的目录用户向 `GetDataAccess` 发出签名请求。

令牌传播基于以下步骤：

创建 IAM Identity Center 应用程序

首先，在 IAM Identity Center 中创建一个新应用程序。此应用程序将使用一个模板，以便 IAM Identity Center 能够识别您可使用的应用程序设置类型。用于创建应用程序的命令要求您提供 IAM Identity Center 实例 Amazon 资源名称（ARN）、应用程序名称和应用程序提供商 ARN。应用程序提供商是应用程序将用于调用 IAM Identity Center 的 SAML 或 OAuth 应用程序提供商。

要使用以下示例命令，请将 *user input placeholders* 替换为您自己的信息：

```
aws sso-admin create-application \
 --instance-arn "arn:aws:sso:::instance/ssoins-ssoins-1234567890abcdef" \
 --application-provider-arn "arn:aws:sso::aws:applicationProvider/custom" \
 --name MyDataApplication
```

响应：

```
{
   "ApplicationArn": "arn:aws:sso::123456789012:application/ssoins-
ssoins-1234567890abcdef/apl-abcd1234a1b2c3d"
}
```

创建可信令牌颁发机构

现在，您已拥有 IAM Identity Center 应用程序，下一步是配置一个可信令牌颁发机构，它用于将您的 IdP 中的 `IdToken` 值与 IAM Identity Center 令牌交换。在此步骤中，您需要提供以下各项：

- 身份提供商颁发机构 URL
- 可信令牌颁发机构名称
- 声明属性路径
- 身份存储属性路径
- JSON Web 密钥集（JWKS）检索选项

声明属性路径是将用于映射到身份存储属性的身份提供商属性。通常，虽然声明属性路径是用户的电子邮件地址，但您可以使用其他属性来执行映射。

创建一个名为 `oidc-configuration.json` 的文件，其中包含以下信息。要使用此文件，请将 *user input placeholders* 替换为您自己的信息。

```
{
```

```
  "OidcJwtConfiguration":
     {
      "IssuerUrl": "https://login.microsoftonline.com/a1b2c3d4-abcd-1234-b7d5-
b154440ac123/v2.0",
      "ClaimAttributePath": "preferred_username",
      "IdentityStoreAttributePath": "userName",
      "JwksRetrievalOption": "OPEN_ID_DISCOVERY"
     }
}
```

要创建可信的令牌颁发机构，请运行以下命令。要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws sso-admin create-trusted-token-issuer \
  --instance-arn "arn:aws:sso:::instance/ssoins-1234567890abcdef" \
  --name MyEntraIDTrustedIssuer \
  --trusted-token-issuer-type OIDC_JWT \
  --trusted-token-issuer-configuration file://./oidc-configuration.json
```

响应

```
{
  "TrustedTokenIssuerArn": "arn:aws:sso::123456789012:trustedTokenIssuer/
ssoins-1234567890abcdef/tti-43b4a822-1234-1234-1234-a1b2c3d41234"
}
```

将 IAM Identity Center 应用程序与可信令牌颁发机构连接

可信令牌颁发机构需要更多的配置设置才能工作。设置可信令牌颁发机构将信任的受众。受众是由密钥标识的 IdToken 内部的值，可以在身份提供商设置中找到它。例如：

```
1234973b-abcd-1234-abcd-345c5a9c1234
```

创建一个名为 grant.json 的文件，其中包含以下内容。要使用此文件，请更改受众以匹配您的身份提供商设置，并提供上一条命令返回的可信令牌颁发机构 ARN。

```
{
   "JwtBearer":
     {
       "AuthorizedTokenIssuers":
```

```
        [
          {
            "TrustedTokenIssuerArn": "arn:aws:sso::123456789012:trustedTokenIssuer/
ssoins-1234567890abcdef/tti-43b4a822-1234-1234-1234-a1b2c3d41234",
              "AuthorizedAudiences":
                [
                  "1234973b-abcd-1234-abcd-345c5a9c1234"
                ]
           }
        ]
    }
 }
```

运行以下示例命令。要使用此命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws sso-admin put-application-grant \
  --application-arn "arn:aws:sso::123456789012:application/ssoins-
ssoins-1234567890abcdef/apl-abcd1234a1b2c3d" \
  --grant-type "urn:ietf:params:oauth:grant-type:jwt-bearer" \
  --grant file://./grant.json \
```

此命令使用配置设置来设定可信令牌颁发机构以信任 `grant.json` 文件中的受众，并将该受众与第一步中创建的应用程序关联起来以便交换类型 `jwt-bearer` 的令牌。字符串 `urn:ietf:params:oauth:grant-type:jwt-bearer` 不是任意字符串。它是 OAuth JSON Web 令牌（JWT）断言配置文件中的注册命名空间。您可以在 RFC 7523 中找到有关此命名空间的更多信息。

接下来，使用以下命令来设置可信令牌颁发机构在交换身份提供商提供的 `IdToken` 值时将包含的范围。对于 S3 Access Grants，`--scope` 参数的值为 `s3:access_grants:read_write`。

```
aws sso-admin put-application-access-scope \
  --application-arn "arn:aws:sso::111122223333:application/ssoins-
ssoins-111122223333abcdef/apl-abcd1234a1b2c3d" \
  --scope "s3:access_grants:read_write"
```

最后一步是将资源策略附加到 IAM Identity Center 应用程序。此策略将允许您的应用程序 IAM 角色向 API 操作 `sso-oauth:CreateTokenWithIAM` 发出请求，并接受来自 IAM Identity Center 的 `IdToken` 值。

创建一个名为 `authentication-method.json` 的文件，其中包含以下内容。请将 *123456789012* 替换为您的账户 ID。

```
{
   "Iam":
       {
         "ActorPolicy":
             {
                "Version": "2012-10-17",
                    "Statement":
                    [
                        {
                           "Effect": "Allow",
                            "Principal":
                            {
                              "Amazon": "arn:aws:iam::123456789012:role/webapp"
                            },
                           "Action": "sso-oauth:CreateTokenWithIAM",
                            "Resource": "*"
                        }
                    ]
                }
            }
        }
```

要将策略附加到 IAM Identity Center 应用程序，请运行以下命令：

```
aws sso-admin put-application-authentication-method \
   --application-arn "arn:aws:sso::123456789012:application/ssoins-
ssoins-1234567890abcdef/apl-abcd1234a1b2c3d" \
   --authentication-method-type IAM \
   --authentication-method file://./authentication-method.json
```

这将完成通过 Web 应用程序对目录用户使用 S3 Access Grants 的配置设置。您可以直接在应用程序中测试此设置，也可以使用以下命令从 IAM Identity Center 应用程序策略中允许的 IAM 角色调用 `CreateTokenWithIAM` API 操作：

```
aws sso-oidc create-token-with-iam \
   --client-id "arn:aws:sso::123456789012:application/ssoins-ssoins-1234567890abcdef/
apl-abcd1234a1b2c3d"  \
   --grant-type urn:ietf:params:oauth:grant-type:jwt-bearer \
   --assertion IdToken
```

响应将与以下内容类似：

```
{
    "accessToken": "<suppressed long string to reduce space>",
    "tokenType": "Bearer",
    "expiresIn": 3600,
    "refreshToken": "<suppressed long string to reduce space>",
    "idToken": "<suppressed long string to reduce space>",
    "issuedTokenType": "urn:ietf:params:oauth:token-type:refresh_token",
    "scope": [
      "sts:identity_context",
      "s3:access_grants:read_write",
      "openid",
      "aws"
    ]
}
```

如果您对使用 base64 编码的 IdToken 值进行解码，则会看到采用 JSON 格式的键值对。密钥 sts:identity_context 包含应用程序需要在 sts:AssumeRole 请求中发送的值，以包含目录用户的身份信息。以下是解码的 IdToken 的示例：

```
{
    "aws:identity_store_id": "d-996773e796",
    "sts:identity_context": "AQoJb3JpZ2luX2VjEOTtl;<SUPRESSED>",
    "sub": "83d43802-00b1-7054-db02-f1d683aacba5",
    "aws:instance_account": "123456789012",
    "iss": "https://identitycenter.amazonaws.com/ssoins-1234567890abcdef",
    "sts:audit_context": "AQoJb3JpZ2luX2VjEOT<SUPRESSED>==",
    "aws:identity_store_arn": "arn:aws:identitystore::232642235904:identitystore/
d-996773e796",
    "aud": "abcd12344U0gi7n4Yyp0-WV1LWNlbnRyYWwtMQ",
    "aws:instance_arn": "arn:aws:sso:::instance/ssoins-6987d7fb04cf7a51",
    "aws:credential_id": "EXAMPLEHI5glPh40y9TpApJn8...",
    "act": {
       "sub": "arn:aws:sso::232642235904:trustedTokenIssuer/
ssoins-6987d7fb04cf7a51/43b4a822-1020-7053-3631-cb2d3e28d10e"
    },
    "auth_time": "2023-11-01T20:24:28Z",
    "exp": 1698873868,
    "iat": 1698870268
}
```

您可以从 sts:identity_context 中获取值并在 sts:AssumeRole 调用中传递该信息。以下是语法的 CLI 示例。要代入的角色是有权调用 s3:GetDataAccess 的临时角色。

```
aws sts assume-role \
   --role-arn "arn:aws:iam::123456789012:role/temp-role" \
   --role-session-name "TempDirectoryUserRole" \
   --provided-contexts ProviderArn="arn:aws:iam::aws:contextProvider/
IdentityCenter",ContextAssertion="value from sts:identity_context"
```

现在，您可以使用从该调用中接收的凭证来调用 `s3:GetDataAccess` API 操作，并接收可用于访问您的 S3 资源的最终凭证。

## 开始使用 S3 Access Grants

Amazon S3 Access Grants 是 Amazon S3 的一项功能，为 S3 数据提供了可扩展的访问控制解决方案。S3 Access Grants 是 S3 凭证供应商，这意味着您将向 S3 Access Grants 注册您的授权列表和级别。此后，当用户或客户端需要访问您的 S3 数据时，他们首先需向 S3 Access Grants 索要凭证。如果有相应的授权来授予访问权限，则 S3 Access Grants 会分发最低权限的临时访问凭证。之后，用户或客户端可以使用 S3 Access Grants 分发的凭证来访问 S3 数据。考虑到这一点，如果您的 S3 数据要求指示进行复杂或大规模的权限配置，则可以使用 S3 Access Grants 来扩展用户、组、角色和应用程序的 S3 数据权限。

对于大多数使用场景，您可以通过使用带存储桶策略的 Amazon Identity and Access Management（IAM）或基于 IAM 身份的策略来管理 S3 数据的访问控制。

不过，如果您有复杂的 S3 访问控制要求（例如以下要求），则可通过使用 S3 Access Grants 获得大量好处：

- 您达到了存储桶策略大小限制 20 KB。
- 您可以向人类身份（例如 Microsoft Entra ID（以前称作 Azure Active Directory）、Okta 或 Ping 用户和组）授予对 S3 数据的访问权限以进行分析和大数据处理。
- 您必须提供跨账户访问，而不是频繁更新 IAM 策略。
- 您的数据是非结构化的对象级数据，而不是采用行和列格式的结构化数据。

S3 Access Grants 工作流如下所示：

| 步骤 | 描述 |
| --- | --- |
| 1 | 创建 S3 访问权限管控实例 |

| 步骤 | 描述 |
| --- | --- |
| | 要开始使用，请启动一个 S3 Access Grants 实例，其中包含您的个人访问授权。 |
| 2 | 注册位置<br><br>紧接着，注册一个 S3 数据位置（例如默认位置 `s3://`），然后指定 S3 Access Grants 在提供对 S3 数据位置的访问权限时所代入的默认 IAM 角色。您还可以将自定义位置添加到特定的存储桶或前缀，并将其映射到自定义 IAM 角色。 |
| 3 | 创建授权<br><br>创建单个权限授权。在这些权限授权中指定注册的 S3 位置、该位置内的数据访问范围、被授权者的身份及其访问级别（`READ`、`WRITE` 或 `READWRITE` ）。 |
| 4 | 请求对 S3 数据的访问权限<br><br>当用户、应用程序和 Amazon Web Services 服务 需要访问 S3 数据时，他们首先会发出访问请求。S3 Access Grants 决定是否应授权请求。如果有相应的授权来授予访问权限，则 S3 Access Grants 会使用与该授权关联的注册位置的 IAM 角色，以再次将临时凭证分发给请求者。 |
| 5 | 访问 S3 数据<br><br>应用程序使用 S3 Access Grants 分发的临时凭证来访问 S3 数据。 |

## 使用 S3 访问权限管控实例

要开始使用 Amazon S3 Access Grants，您需要先创建一个 S3 Access Grants 实例。您的每个账户在每个 Amazon Web Services 区域 中只能创建一个 S3 Access Grants 实例。S3 Access Grants 实例充当您的 S3 Access Grants 资源的容器，其中包括注册的位置和授权。

利用 S3 Access Grants，您可以为 Amazon Identity and Access Management（IAM）用户和角色创建对 S3 数据的权限授权。如果您已向 Amazon IAM Identity Center 添加公司身份目录，则可以将公司

目录的此 IAM Identity Center 实例与您的 S3 Access Grants 实例相关联。完成此操作后，您可以为公司用户和组创建访问授权。如果您尚未将公司目录添加到 IAM Identity Center，则可以稍后将您的 S3 Access Grants 实例与 IAM Identity Center 实例相关联。

主题


- 创建 S3 访问权限管控实例
- 获取 S3 访问权限管控实例的详细信息
- 列出 S3 访问权限管控实例
- 关联或取消关联 IAM Identity Center 实例
- 删除 S3 Access Grants 实例


## 创建 S3 访问权限管控实例

要开始使用 Amazon S3 Access Grants，您需要先创建一个 S3 Access Grants 实例。您的每个账户在每个 Amazon Web Services 区域 中只能创建一个 S3 Access Grants 实例。S3 Access Grants 实例充当您的 S3 Access Grants 资源的容器，其中包括注册的位置和授权。

利用 S3 Access Grants，您可以为 Amazon Identity and Access Management（IAM）用户和角色创建对 S3 数据的权限授权。如果您已向 Amazon IAM Identity Center 添加公司身份目录，则可以将公司目录的此 IAM Identity Center 实例与您的 S3 Access Grants 实例相关联。完成此操作后，您可以为公司用户和组创建访问授权。如果您尚未将公司目录添加到 IAM Identity Center，则可以稍后将您的 S3 Access Grants 实例与 IAM Identity Center 实例相关联。

您可以使用 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）、Amazon S3 REST API 和 Amazon SDK 创建 S3 Access Grants 实例。

使用 S3 控制台

在使用 S3 Access Grants 授予对 S3 数据的访问权限之前，必须先在 S3 数据所在的同一 Amazon Web Services 区域中创建 S3 Access Grants 实例。

先决条件

如果您想使用公司目录中的身份授予对 S3 数据的访问权限，请向 Amazon IAM Identity Center 添加公司身份目录。如果您尚未准备好执行此操作，可以稍后将您的 S3 Access Grants 实例与 IAM Identity Center 实例关联。

创建 S3 访问权限管控实例

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在导航栏中，选择当前所显示 Amazon Web Services 区域的名称。接下来，选择要切换到的区域。
3. 在左侧导航窗格中，选择 Access Grants。
4. 在 S3 Access Grants 页面上，选择创建 S3 Access Grants 实例。

   a. 在设置 Access Grants 实例向导的步骤 1 中，确认您要在当前的 Amazon Web Services 区域中创建实例。确保这是您的 S3 数据所在的 Amazon Web Services 区域。您的每个账户在每个 Amazon Web Services 区域 中可创建一个 S3 Access Grants 实例。

   b. （可选）如果您已向 Amazon IAM Identity Center 添加公司身份目录，则可以将公司目录的此 IAM Identity Center 实例与您的 S3 Access Grants 实例相关联。

      为此，请选择在**##**中添加 IAM Identity Center 实例。然后输入 IAM Identity Center 实例 Amazon 资源名称（ARN）。

      如果您尚未将公司目录添加到 IAM Identity Center，则可以稍后将您的 S3 Access Grants 实例与 IAM Identity Center 实例相关联。

   c. 要创建 S3 Access Grants 实例，请选择下一步。要注册位置，请参阅步骤 2 – 注册位置。
5. 如果已禁用下一步或创建 S3 Access Grants 实例，则：

   无法创建实例

   - 您可能已在同一个 Amazon Web Services 区域中拥有一个 S3 Access Grants 实例。在左侧导航窗格中，选择 Access Grants。在 S3 Access Grants 页面上，向下滚动到您的账户中的 S3 Access Grants 实例以确定是否已存在实例。
   - 您可能没有创建 S3 Access Grants 实例所需的 `s3:CreateAccessGrantsInstance` 权限。请联系您的账户管理员。有关将 IAM Identity Center 实例与 S3 Access Grants 实例关联时所需的其他权限，请参阅 CreateAccessGrantsInstance。

使用 Amazon CLI

要安装 Amazon CLI，请参阅 Amazon Command Line Interface 用户指南中的安装 Amazon CLI。

要使用以下示例命令，请将 *`user input placeholders`* 替换为您自己的信息。

Example 创建 S3 访问权限管控实例

```
aws s3control create-access-grants-instance \
--account-id 111122223333 \
--region us-east-2
```

响应：

```
{
    "CreatedAt": "2023-05-31T17:54:07.893000+00:00",
    "AccessGrantsInstanceId": "default",
    "AccessGrantsInstanceArn": "arn:aws:s3:us-east-2:111122223333:access-grants/
default"
}
```

使用 REST API

您可以使用 Amazon S3 REST API 创建 S3 Access Grants 实例。有关用于管理 S3 Access Grants 实例的 REST API 支持的信息，请参阅《Amazon Simple Storage Service API 参考》中的以下部分：

- AssociateAccessGrantsIdentityCenter
- CreateAccessGrantsInstance
- DeleteAccessGrantsInstance
- DissociateAccessGrantsIdentityCenter
- GetAccessGrantsInstance
- GetAccessGrantsInstanceForPrefix
- GetAccessGrantsInstanceResourcePolicy
- ListAccessGrantsInstances
- PutAccessGrantsInstanceResourcePolicy

使用 Amazon SDK

此部分中的示例说明了如何使用 Amazon SDK 创建 S3 Access Grants 实例。

Java

此示例创建的 S3 Access Grants 实例可用作您的个人访问授权的容器。您的每个账户在每个 Amazon Web Services 区域 中可具有一个 S3 Access Grants 实例。响应包括实例 ID `default` 和为您的 S3 Access Grants 实例生成的 Amazon 资源名称（ARN）。

Example 创建 S3 Access Grants 实例请求

```
public void createAccessGrantsInstance() {
CreateAccessGrantsInstanceRequest createRequest =
 CreateAccessGrantsInstanceRequest.builder().accountId("111122223333").build();
CreateAccessGrantsInstanceResponse createResponse =
 s3Control.createAccessGrantsInstance(createRequest);LOGGER.info("CreateAccessGrantsInstance
 " + createResponse);
}
```

响应：

```
CreateAccessGrantsInstanceResponse(
CreatedAt=2023-06-07T01:46:20.507Z,
AccessGrantsInstanceId=default,
AccessGrantsInstanceArn=arn:aws:s3:us-east-2:111122223333:access-grants/default)
```

## 获取 S3 访问权限管控实例的详细信息

您可以获取特定 Amazon Web Services 区域中的 Amazon S3 访问权限管控实例的详细信息。可以使用 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）、Amazon S3 REST API 和 Amazon SDK 获取 S3 访问权限管控实例的详细信息。

使用 S3 控制台

获取 S3 访问权限管控实例的详细信息

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Access Grants。
3. 在 S3 Access Grants 页面上，选择包含要使用的 S3 Access Grants 实例的区域。
4. S3 Access Grants 页面列出了您的 S3 Access Grants 实例以及已与您的账户共享的所有跨账户实例。要查看实例的详细信息，请选择查看详细信息。

使用 Amazon CLI

要安装 Amazon CLI，请参阅 Amazon Command Line Interface 用户指南中的安装 Amazon CLI。

要使用以下示例命令，请将 *user input placeholders* 替换为您自己的信息。

Example – 获取 S3 访问权限管控实例的详细信息

```
aws s3control get-access-grants-instance \
 --account-id 111122223333 \
 --region us-east-2
```

响应：

```
{
    "AccessGrantsInstanceArn": "arn:aws:s3:us-east-2: 111122223333:access-grants/
default",
    "AccessGrantsInstanceId": "default",
    "CreatedAt": "2023-05-31T17:54:07.893000+00:00"
}
```

使用 REST API

有关用于管理 S3 Access Grants 实例的 Amazon S3 REST API 支持的信息，请参阅《Amazon Simple Storage Service API 参考》中的以下部分：

- GetAccessGrantsInstance
- GetAccessGrantsInstanceForPrefix

使用 Amazon SDK

此部分中的示例说明了如何使用 Amazon SDK 获取 S3 Access Grants 实例的详细信息。

要使用以下示例，请将 *user input placeholders* 替换为您自己的信息。

Java

Example – 获取 S3 Access Grants 实例

```
public void getAccessGrantsInstance() {
```

```
GetAccessGrantsInstanceRequest getRequest = GetAccessGrantsInstanceRequest.builder()
.accountId("111122223333")
.build();
GetAccessGrantsInstanceResponse getResponse =
 s3Control.getAccessGrantsInstance(getRequest);
LOGGER.info("GetAccessGrantsInstanceResponse: " + getResponse);
}
```

响应：

```
GetAccessGrantsInstanceResponse(
AccessGrantsInstanceArn=arn:aws:s3:us-east-2: 111122223333:access-grants/default,
CreatedAt=2023-06-07T01:46:20.507Z)
```

## 列出 S3 访问权限管控实例

还可以列出 S3 访问权限管控实例，包括已通过 Amazon Resource Access Manager（Amazon RAM）与您共享的实例。

可以使用 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）、Amazon S3 REST API 和 Amazon SDK 列出 S3 访问权限管控实例。

使用 S3 控制台

列出 S3 访问权限管控实例

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Access Grants。
3. 在 S3 Access Grants 页面上，选择包含要使用的 S3 Access Grants 实例的区域。
4. S3 Access Grants 页面列出了您的 S3 Access Grants 实例以及已与您的账户共享的所有跨账户实例。要查看实例的详细信息，请选择查看详细信息。

使用 Amazon CLI

要安装 Amazon CLI，请参阅 Amazon Command Line Interface 用户指南中的安装 Amazon CLI。

要使用以下示例命令，请将 *user input placeholders* 替换为您自己的信息。

Example – 列出账户的所有 S3 Access Grants 实例

此操作将列出账户的 S3 Access Grants 实例。您在每个 Amazon Web Services 区域中只能具有一个 S3 Access Grants 实例。此操作还会列出您的账户有权访问的其他跨账户 S3 Access Grants 实例。

```
aws s3control list-access-grants-instances \
 --account-id 111122223333 \
 --region us-east-2
```

响应：

```
{
    "AccessGrantsInstanceArn": "arn:aws:s3:us-east-2: 111122223333:access-grants/
default",
    "AccessGrantsInstanceId": "default",
    "CreatedAt": "2023-05-31T17:54:07.893000+00:00"
}
```

使用 REST API

有关用于管理 S3 Access Grants 实例的 Amazon S3 REST API 支持的信息，请参阅《Amazon Simple Storage Service API 参考》中的以下部分：

- ListAccessGrantsInstances

使用 Amazon SDK

此部分中的示例说明了如何使用 Amazon SDK 获取 S3 Access Grants 实例的详细信息。

要使用以下示例，请将 *user input placeholders* 替换为您自己的信息。

Java

Example – 列出账户的所有 S3 Access Grants 实例

此操作将列出账户的 S3 Access Grants 实例。您在每个区域只能有一个 S3 Access Grants 实例。此操作还列出了您的账户有权访问的其他跨账户 S3 Access Grants 实例。

```
public void listAccessGrantsInstances() {
ListAccessGrantsInstancesRequest listRequest =
 ListAccessGrantsInstancesRequest.builder()
```

```
.accountId("111122223333")
.build();
ListAccessGrantsInstancesResponse listResponse =
 s3Control.listAccessGrantsInstances(listRequest);
LOGGER.info("ListAccessGrantsInstancesResponse: " + listResponse);
}
```

响应：

```
ListAccessGrantsInstancesResponse(
AccessGrantsInstancesList=[
ListAccessGrantsInstanceEntry(
AccessGrantsInstanceId=default,
AccessGrantsInstanceArn=arn:aws:s3:us-east-2:111122223333:access-grants/default,
CreatedAt=2023-06-07T04:28:11.728Z
)
]
)
```

## 关联或取消关联 IAM Identity Center 实例

在 Amazon S3 Access Grants 中，您可以将公司身份目录的 Amazon IAM Identity Center 实例与 S3 Access Grants 实例相关联。完成此操作后，除了 Amazon Identity and Access Management（IAM）用户和角色之外，您还可以为公司目录用户和组创建访问授权。

如果您不再想为公司目录用户和组创建访问授权，则可以取消您的 IAM Identity Center 实例与 S3 Access Grants 实例的关联。

您可以使用 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）、Amazon S3 REST API 和 Amazon SDK 来关联或取消关联 IAM Identity Center 实例。

使用 S3 控制台

在将 IAM Identity Center 实例与 S3 Access Grants 实例关联之前，您必须将公司身份目录添加到 IAM Identity Center。有关更多信息，请参阅 the section called “S3 Access Grants 和公司目录身份”。

将 IAM Identity Center 实例与 S3 Access Grants 实例关联

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。

2. 在左侧导航窗格中，选择 Access Grants。
3. 在 S3 Access Grants 页面上，选择包含要使用的 S3 Access Grants 实例的区域。
4. 对于实例，选择查看详细信息。
5. 在详细信息页面上的 IAM Identity Center 部分中，选择添加 IAM Identity Center 实例或取消注册已关联的 IAM Identity Center 实例。

使用 Amazon CLI

要安装 Amazon CLI，请参阅 Amazon Command Line Interface 用户指南中的安装 Amazon CLI。

要使用以下示例命令，请将 *user input placeholders* 替换为您自己的信息。

Example – 将 IAM Identity Center 实例与 S3 Access Grants 实例关联

```
aws s3control associate-access-grants-identity-center \
 --account-id 111122223333 \
 --identity-center-arn arn:aws:sso:::instance/ssoins-1234a567bb89012c \
 --profile access-grants-profile \
 --region eu-central-1

// No response body
```

Example – 取消 IAM Identity Center 实例与 S3 Access Grants 实例的关联

```
aws s3control dissociate-access-grants-identity-center \
 --account-id 111122223333 \
 --profile access-grants-profile \
 --region eu-central-1

// No response body
```

使用 REST API

有关用于管理 IAM Identity Center 实例与 S3 Access Grants 实例之间的关联的 Amazon S3 REST API 支持的信息，请参阅《Amazon Simple Storage Service API 参考》中的以下部分：

- AssociateAccessGrantsIdentityCenter
- DissociateAccessGrantsIdentityCenter

# 删除 S3 Access Grants 实例

您可以从账户中的 Amazon Web Services 区域中删除 Amazon S3 Access Grants 实例。但是，您必须先执行以下操作，之后才能删除 S3 Access Grants 实例：

- 删除 S3 Access Grants 实例中的所有资源，包括所有授权和位置。有关更多信息，请参阅删除授权和删除位置。
- 如果您已将 Amazon IAM Identity Center 实例与 S3 Access Grants 实例关联，则必须取消关联 IAM Identity Center 实例。有关更多信息，请参阅关联或取消关联 IAM Identity Center 实例。

> **Important**
>
> 如果您删除 S3 Access Grants 实例，则删除是永久性的，无法撤消。通过此 S3 Access Grants 实例中的授权获得访问权限的所有被授权者都将失去对您的 S3 数据的访问权限。

您可以使用 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）、Amazon S3 REST API 和 Amazon SDK 删除 S3 Access Grants 实例。

使用 S3 控制台

删除 S3 Access Grants 实例

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Access Grants。
3. 在 S3 Access Grants 页面上，选择包含要使用的 S3 Access Grants 实例的区域。
4. 对于实例，选择查看详细信息。
5. 在实例详细信息页面上，选择右上角的删除实例。
6. 在出现的对话框中，选择删除。此操作无法撤消。

使用 Amazon CLI

要安装 Amazon CLI，请参阅 Amazon Command Line Interface 用户指南中的安装 Amazon CLI。

要使用以下示例命令，请将 *user input placeholders* 替换为您自己的信息。

> **Note**
>
> 您必须先删除在 S3 Access Grants 实例中创建的所有授权和位置，之后才能删除 S3 Access Grants 实例。如果您已将 IAM Identity Center 实例与 S3 Access Grants 实例关联，则必须先取消此关联。

Example – 删除 S3 Access Grants 实例

```
aws s3control delete-access-grants-instance \
--account-id 111122223333 \
--profile access-grants-profile \
--region us-east-2 \
--endpoint-url https://s3-control.us-east-2.amazonaws.com \

 // No response body
```

使用 REST API

有关用于删除 S3 Access Grants 实例的 Amazon S3 REST API 支持的信息，请参阅《Amazon Simple Storage Service API 参考》中的 DeleteAccessGrantsInstance。

使用 Amazon SDK

此部分中的示例说明了如何使用 Amazon SDK 删除 S3 Access Grants 实例。

要使用以下示例，请将 *user input placeholders* 替换为您自己的信息。

Java

> **Note**
>
> 您必须先删除在 S3 Access Grants 实例中创建的所有授权和位置，之后才能删除 S3 Access Grants 实例。如果您已将 IAM Identity Center 实例与 S3 Access Grants 实例关联，则必须先取消此关联。

Example – 删除 S3 Access Grants 实例

```
public void deleteAccessGrantsInstance() {
```

```
DeleteAccessGrantsInstanceRequest deleteRequest =
 DeleteAccessGrantsInstanceRequest.builder()
.accountId("111122223333")
.build();
DeleteAccessGrantsInstanceResponse deleteResponse =
 s3Control.deleteAccessGrantsInstance(deleteRequest);
LOGGER.info("DeleteAccessGrantsInstanceResponse: " + deleteResponse);
}
```

# 使用 S3 访问权限管控位置

在您账户的 Amazon Web Services 区域中创建 Amazon S3 访问权限管控实例后，在该实例中注册 S3 位置。S3 访问权限管控位置将默认 S3 位置 (s3://)、存储桶或前缀映射到 Amazon Identity and Access Management（IAM）角色。S3 访问权限管控代入此 IAM 角色，来向正在访问该特定位置的被授权者提供临时凭证。您必须先在 S3 访问权限管控实例中注册至少一个位置，然后才能创建访问权限管控。

您可以注册位置、查看位置的详细信息、编辑位置和删除位置。

> **Note**
>
> 在 S3 访问权限管控实例中注册第一个位置后，您的实例中仍没有任何单个访问权限管控。要创建访问权限管控，请参阅创建授权。

主题

- 注册位置
- 查看已注册位置的详细信息
- 更新已注册位置
- 删除已注册位置

## 注册位置

在您账户的 Amazon Web Services 区域中创建 Amazon S3 访问权限管控实例后，在该实例中注册 S3 位置。S3 访问权限管控位置将默认 S3 位置 (s3://)、存储桶或前缀映射到 Amazon Identity and Access Management（IAM）角色。S3 访问权限管控代入此 IAM 角色，来向正在访问该特定位置的被

授权者提供临时凭证。您必须先在 S3 访问权限管控实例中注册至少一个位置，然后才能创建访问权限管控。

建议的用例

我们建议您注册默认位置 (s3://) 并将其映射到 IAM 角色。默认 S3 路径 (s3://) 中的位置涵盖了对您账户的该 Amazon Web Services 区域中所有 S3 存储桶的访问权限。创建访问权限管控时，您可以将授予范围缩小到默认位置内的存储桶、前缀或对象。

复杂的访问管理用例

更复杂的访问管理用例可能要求您注册比默认位置更多的位置。此类用例的一些示例为：

- 假设 *amzn-s3-demo-bucket* 是 S3 访问权限管控实例中的一个注册位置，并且有一个 IAM 角色映射到该位置，但拒绝该 IAM 角色访问存储桶中的特定前缀。在这种情况下，您可以将 IAM 角色无权访问的前缀注册为单独的位置，并将该位置映射到具有必要访问权限的其它 IAM 角色。
- 假设您要创建的授权将访问权限仅限制为虚拟私有云（VPC）端点中的用户。在这种情况下，您可以为存储桶注册一个位置，IAM 角色在该位置限制对 VPC 端点的访问。稍后，当被授权者向 S3 访问权限管控索取凭证时，S3 访问权限管控将代入该位置的 IAM 角色来提供临时凭证。除非调用方位于 VPC 端点内，否则此凭证将拒绝访问特定存储桶。除在授权中指定的常规 READ、WRITE 或 READWRITE 权限外，还会应用此拒绝权限。

在注册位置时，还必须指定 S3 访问权限管控代入的 IAM 角色，来提供临时凭证和确定特定授权的权限范围。

如果您的用例要求您在 S3 访问权限管控实例中注册多个位置，则可以注册以下任意位置：

| S3 URI | IAM 角色 | 描述 |
| --- | --- | --- |
| s3:// | *Default-IAM-role* | 默认位置 s3:// 包括 Amazon Web Services 区域中的所有存储桶。 |
| s3://*amzn-s3-demo-bucket1* / | *IAM-role-For-bucket* | 此位置包括指定存储桶中的所有对象。 |
| s3://*amzn-s3-demo-bucket1* /*prefix-name* | *IAM-role-For-prefix* | 此位置包括存储桶中对象键名称以此前缀开头的所有对象。 |

在注册特定存储桶或前缀之前，请确保执行以下操作：

- 创建一个或多个存储桶，其中包含要授予其访问权限的数据。这些存储桶必须位于您的 S3 Access Grants 实例所在的 Amazon Web Services 区域中。有关更多信息，请参阅创建存储桶。

  添加前缀是一个可选步骤。前缀是位于对象键名称开头的字符串。可以使用它们来组织存储桶中的对象以及进行访问管理。要向存储桶添加前缀，请参阅创建对象密钥名称。
- 创建一个 IAM 角色，该角色有权访问 Amazon Web Services 区域中的 S3 数据。有关更多信息，请参阅《Amazon IAM Identity Center 用户指南》中的创建 IAM 角色。
- 在 IAM 角色信任策略中，向 S3 访问权限管控服务 (access-grants.s3.amazonaws.com)主体授予对您创建的 IAM 角色的访问权限。为此，您可以创建一个包含以下语句的 JSON 文件。要将信任策略添加到您的账户，请参阅使用自定义信任策略创建角色。

  TestRolePolicy.json

```
{
  "Version": "2012-10-17",
    "Statement": [
    {
      "Sid": "Stmt1234567891011",
      "Effect": "Allow",
      "Principal": {
        "Service":"access-grants.s3.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetSourceIdentity"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount":"accountId",
          "aws:SourceArn":"arn:aws:s3:region:accountId:access-grants/default"
        }
      }
    },
    //Optionally, for an IAM Identity Center use case, add:
    {
      "Sid": "Stmt1234567891012",
        "Effect": "Allow",
        "Principal": {
          "Service": "access-grants.s3.amazonaws.com"
        },
```

```
        "Action": "sts:SetContext",
        "Condition":{
          "StringEquals":{
            "aws:SourceAccount":"accountId",
            "aws:SourceArn":"arn:aws:s3:region:accountId:access-grants/default"
          },
          "ForAllValues:ArnEquals": {
            "sts:RequestContextProviders":"arn:aws:iam::aws:contextProvider/
IdentityCenter"
          }
        }
      }
  ]
}
```

- 创建 IAM 策略来将 Amazon S3 权限附加到您创建的 IAM 角色。请查看以下示例 `iam-policy.json` 文件，并将 *`user input placeholders`* 替换为您自己的信息。

> **Note**
>
> - 如果您使用采用 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密来加密数据，则以下示例将在策略中包含 IAM 角色的必要 Amazon KMS 权限。如果您不使用此功能，则可以从 IAM 策略中删除这些权限。
> - 仅当凭证由 S3 Access Grants 出售时，您才能将 IAM 角色限制为访问 S3 数据。此示例说明如何为特定 S3 Access Grants 实例添加 `Condition` 语句。要使用此 `Condition`，请将 `Condition` 语句中的 S3 访问权限管控实例 ARN 替换为您的 S3 访问权限管控实例 ARN，其格式为：`arn:aws:s3:region:accountId:access-grants/default`

iam-policy.json

```
{
   "Version":"2012-10-17",
   "Statement": [
       {
         "Sid": "ObjectLevelReadPermissions",
         "Effect":"Allow",
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion",
```

```
            "s3:GetObjectAcl",
            "s3:GetObjectVersionAcl",
            "s3:ListMultipartUploadParts"
         ],
         "Resource":[
            "arn:aws:s3:::*"
         ],
         "Condition":{
            "StringEquals": { "aws:ResourceAccount": "accountId" },
            "ArnEquals": {
                "s3:AccessGrantsInstanceArn": ["arn:aws:s3:region:accountId:access-
grants/default"]
            }
        }
      },
      {
         "Sid": "ObjectLevelWritePermissions",
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:PutObjectVersionAcl",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion",
            "s3:AbortMultipartUpload"
         ],
         "Resource":[
            "arn:aws:s3:::*"
         ],
         "Condition":{
            "StringEquals": { "aws:ResourceAccount": "accountId" },
            "ArnEquals": {
                "s3:AccessGrantsInstanceArn": ["arn:aws:s3:Amazon Web Services #
#:accountId:access-grants/default"]
            }
         }
      },
      {
         "Sid": "BucketLevelReadPermissions",
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket"
         ],
         "Resource":[
```

```
            "arn:aws:s3:::*"
         ],
         "Condition":{
            "StringEquals": { "aws:ResourceAccount": "accountId" },
            "ArnEquals": {
                "s3:AccessGrantsInstanceArn": ["arn:aws:s3:Amazon Web Services #
#:accountId:access-grants/default"]
            }
         }
      },
   //Optionally add the following section if you use SSE-KMS encryption
      {
         "Sid": "KMSPermissions",
         "Effect":"Allow",
         "Action":[
            "kms:Decrypt",
            "kms:GenerateDataKey"
         ],
         "Resource":[
            "*"
         ]
      }
   ]
}
```

您可以使用 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）、Amazon S3 REST API 和 Amazon SDK 在 S3 Access Grants 实例中注册位置。

> **Note**
>
> 在 S3 访问权限管控实例中注册第一个位置后，您的实例中仍没有任何单个访问权限管控。要创建访问权限管控，请参阅创建授权。

使用 S3 控制台

您必须先注册至少一个位置，之后才能使用 S3 Access Grants 授予对 S3 数据的访问权限。

在 S3 Access Grants 实例中注册位置

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Access Grants。
3. 在 S3 Access Grants 页面上，选择包含要使用的 S3 Access Grants 实例的区域。

   如果您是首次使用 S3 Access Grants 实例，请确保已完成步骤 1 - 创建 S3 Access Grants 实例，并导航到设置 Access Grants 实例向导的步骤 2。如果您已拥有 S3 Access Grants 实例，请选择查看详细信息，然后从位置选项卡中选择注册位置。

   a. 对于位置范围，请选择浏览 S3 或输入要注册的位置的 S3 URI 路径。有关 S3 URI 格式，请参阅位置格式表。输入 URI 后，您可以选择查看来浏览该位置。
   b. 对于 IAM 角色，请选择下列选项之一：

      - 从现有 IAM 角色中选择

        从下拉列表中选择 IAM 角色。选择一个角色后，选择查看，确保该角色具有管理要注册的位置所需的权限。具体而言，请确保此角色向 S3 Access Grants 授予 `sts:AssumeRole` 和 `sts:SetSourceIdentity` 权限。

      - 输入 IAM 角色 ARN

        导航到 IAM 控制台。复制 IAM 角色的 Amazon 资源名称（ARN），并将它粘贴到此框中。

   c. 要完成此操作，请选择下一步或注册位置。
4. 故障排除：

   无法注册位置

   - 该位置可能已被注册。

     您可能没有 `s3:CreateAccessGrantsLocation` 权限，无法注册位置。请联系您的账户管理员。

使用 Amazon CLI

要安装 Amazon CLI，请参阅 Amazon Command Line Interface 用户指南中的安装 Amazon CLI。

您可以在 S3 Access Grants 实例中注册默认位置 `s3://` 或自定义位置。请确保先创建一个具有该位置的主体访问权限的 IAM 角色，然后确保授予 S3 Access Grants 权限以代入此角色。

要使用以下示例命令，请将 *user input placeholders* 替换为您自己的信息。

Example 创建资源策略

创建允许 S3 Access Grants 代入 IAM 角色的策略。为此，您可以创建一个包含以下语句的 JSON 文件。要将资源策略添加到您的账户，请参阅创建和附加您的第一个客户管理型策略。

TestRolePolicy.json

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1234567891011",
      "Action": ["sts:AssumeRole", "sts:SetSourceIdentity"],
      "Effect": "Allow",
      "Principal": {"Service":"access-grants.s3.amazonaws.com"}
    }
  ]
}
```

Example 创建 角色

运行以下 IAM 命令以创建该角色。

```
aws iam create-role --role-name accessGrantsTestRole \
 --region us-east-2 \
 --assume-role-policy-document file://TestRolePolicy.json
```

运行 `create-role` 命令将返回策略：

```
{
    "Role": {
        "Path": "/",
        "RoleName": "accessGrantsTestRole",
        "RoleId": "AROASRDGX4WM4GH55GIDA",
        "Arn": "arn:aws:iam::111122223333:role/accessGrantsTestRole",
        "CreateDate": "2023-05-31T18:11:06+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
```

```
                    "Sid": "Stmt1685556427189",
                    "Action": [
                        "sts:AssumeRole",
                        "sts:SetSourceIdentity"
                    ],
                    "Effect": "Allow",
                    "Principal": {
                        "Service":"access-grants.s3.amazonaws.com"
                    }
                }
            ]
        }
    }
}
```

Example

创建一个 IAM 策略，将 Amazon S3 权限附加到 IAM 角色。请查看以下示例 `iam-policy.json` 文件，并将 *`user input placeholders`* 替换为您自己的信息。

> **Note**
>
> 如果您使用具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密来加密数据，则以下示例将在策略中添加 IAM 角色的必要 Amazon KMS 权限。如果您不使用此功能，则可以从 IAM 策略中删除这些权限。
> 为了确保在凭证由 S3 Access Grants 分发时，IAM 角色只能用于访问 S3 中的数据，此示例向您说明了如何在 IAM 策略中添加一个指定 S3 Access Grants 实例（`s3:AccessGrantsInstance:` *`InstanceArn`*）的 `Condition` 语句。在使用以下示例策略时，请将 *`user input placeholders`* 替换为您自己的信息。

iam-policy.json

```
{
   "Version":"2012-10-17",
   "Statement": [
       {
         "Sid": "ObjectLevelReadPermissions",
         "Effect":"Allow",
         "Action":[
```

```
            "s3:GetObject",
            "s3:GetObjectVersion",
            "s3:GetObjectAcl",
            "s3:GetObjectVersionAcl",
            "s3:ListMultipartUploadParts"
         ],
         "Resource":[
            "arn:aws:s3:::*"
         ],
         "Condition":{
            "StringEquals": { "aws:ResourceAccount": "accountId" },
            "ArnEquals": {
                "s3:AccessGrantsInstanceArn": ["arn:aws:s3:region:accountId:access-
grants/default"]
            }
        }
      },
      {
         "Sid": "ObjectLevelWritePermissions",
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:PutObjectVersionAcl",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion",
            "s3:AbortMultipartUpload"
         ],
         "Resource":[
            "arn:aws:s3:::*"
         ],
         "Condition":{
            "StringEquals": { "aws:ResourceAccount": "accountId" },
            "ArnEquals": {
                "s3:AccessGrantsInstanceArn": ["arn:aws:s3:Amazon Web Services #
#:accountId:access-grants/default"]
            }
         }
      },
      {
         "Sid": "BucketLevelReadPermissions",
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket"
```

```
         ],
         "Resource":[
            "arn:aws:s3:::*"
         ],
         "Condition":{
            "StringEquals": { "aws:ResourceAccount": "accountId" },
            "ArnEquals": {
                "s3:AccessGrantsInstanceArn": ["arn:aws:s3:Amazon Web Services #
#:accountId:access-grants/default"]
            }
         }
      },
      {
         "Sid": "KMSPermissions",
         "Effect":"Allow",
         "Action":[
            "kms:Decrypt",
            "kms:GenerateDataKey"
         ],
         "Resource":[
            "*"
         ]
      }
   ]
}
```

Example

运行以下命令：

```
aws iam put-role-policy \
--role-name accessGrantsTestRole \
--policy-name accessGrantsTestRole \
--policy-document file://iam-policy.json
```

Example 注册默认位置

```
aws s3control create-access-grants-location \
 --account-id 111122223333 \
 --location-scope s3:// \
 --iam-role-arn arn:aws:iam::111122223333:role/accessGrantsTestRole
```

响应：

```
{"CreatedAt": "2023-05-31T18:23:48.107000+00:00",
    "AccessGrantsLocationId": "default",
    "AccessGrantsLocationArn": "arn:aws:s3:us-east-2:111122223333:access-grants/
default/location/default",
    "LocationScope": "s3://"
    "IAMRoleArn": "arn:aws:iam::111122223333:role/accessGrantsTestRole"
}
```

Example 注册自定义位置

```
aws s3control create-access-grants-location \
 --account-id 111122223333 \
 --location-scope s3://DOC-BUCKET-EXAMPLE/ \
 --iam-role-arn arn:aws:iam::123456789012:role/accessGrantsTestRole
```

响应：

```
{"CreatedAt": "2023-05-31T18:23:48.107000+00:00",
    "AccessGrantsLocationId": "635f1139-1af2-4e43-8131-a4de006eb456",
    "AccessGrantsLocationArn": "arn:aws:s3:us-east-2: 111122223333:access-grants/
default/location/635f1139-1af2-4e43-8131-a4de006eb888",
    "LocationScope": "s3://DOC-BUCKET-EXAMPLE/",
    "IAMRoleArn": "arn:aws:iam::111122223333:role/accessGrantsTestRole"
}
```

使用 REST API

有关用于管理 S3 Access Grants 实例的 Amazon S3 REST API 支持的信息，请参阅《Amazon Simple Storage Service API 参考》中的以下部分：

- CreateAccessGrantsLocation
- DeleteAccessGrantsLocation
- GetAccessGrantsLocation
- ListAccessGrantsLocations
- UpdateAccessGrantsLocation

使用 Amazon SDK

此部分中的示例说明了如何使用 Amazon SDK 注册位置。

要使用以下示例，请将 *user input placeholders* 替换为您自己的信息。

Java

您可以在 S3 Access Grants 实例中注册默认位置 s3:// 或自定义位置。请确保先创建一个具有该位置的主体访问权限的 IAM 角色，然后确保授予 S3 Access Grants 权限以代入此角色。

要使用以下示例命令，请将 *user input placeholders* 替换为您自己的信息。

Example 注册默认位置

请求:

```
public void createAccessGrantsLocation() {
CreateAccessGrantsLocationRequest createRequest =
 CreateAccessGrantsLocationRequest.builder()
.accountId("111122223333")
.locationScope("s3://")
.iamRoleArn("arn:aws:iam::123456789012:role/accessGrantsTestRole")
.build();
CreateAccessGrantsLocationResponse createResponse =
 s3Control.createAccessGrantsLocation(createRequest);
LOGGER.info("CreateAccessGrantsLocationResponse: " + createResponse);
}
```

响应:

```
CreateAccessGrantsLocationResponse(
CreatedAt=2023-06-07T04:35:11.027Z,
AccessGrantsLocationId=default,
AccessGrantsLocationArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
location/default,
LocationScope=s3://,
IAMRoleArn=arn:aws:iam::111122223333:role/accessGrantsTestRole
)
```

Example 注册自定义位置

请求:

```
public void createAccessGrantsLocation() {
```

```
CreateAccessGrantsLocationRequest createRequest =
 CreateAccessGrantsLocationRequest.builder()
.accountId("111122223333")
.locationScope("s3://DOC-BUCKET-EXAMPLE/")
.iamRoleArn("arn:aws:iam::111122223333:role/accessGrantsTestRole")
.build();
CreateAccessGrantsLocationResponse createResponse =
 s3Control.createAccessGrantsLocation(createRequest);
LOGGER.info("CreateAccessGrantsLocationResponse: " + createResponse);
}
```

响应:

```
CreateAccessGrantsLocationResponse(
CreatedAt=2023-06-07T04:35:10.027Z,
AccessGrantsLocationId=18cfe6fb-eb5a-4ac5-aba9-8d79f04c2012,
AccessGrantsLocationArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
location/18cfe6fb-eb5a-4ac5-aba9-8d79f04c2666,
LocationScope= s3://test-bucket-access-grants-user123/,
IAMRoleArn=arn:aws:iam::111122223333:role/accessGrantsTestRole
)
```

## 查看已注册位置的详细信息

您可以获取使用 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）、Amazon S3 REST API 和 Amazon SDK 在 S3 Access Grants 实例中注册的位置的详细信息。

使用 S3 控制台

查看在 S3 Access Grants 实例中注册的位置

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Access Grants。
3. 在 S3 Access Grants 页面上，选择包含要使用的 S3 Access Grants 实例的区域。
4. 对于实例，选择查看详细信息。
5. 在实例的详细信息页面上，选择位置选项卡。
6. 找到要查看的已注册位置。要筛选已注册位置的列表，请使用搜索框。

使用 Amazon CLI

要安装 Amazon CLI，请参阅 Amazon Command Line Interface 用户指南中的安装 Amazon CLI。

要使用以下示例命令，请将 *user input placeholders* 替换为您自己的信息。

Example – 获取已注册位置的详细信息

```
aws s3control get-access-grants-location \
--account-id 111122223333 \
--access-grants-location-id default
```

响应：

```
{
    "CreatedAt": "2023-05-31T18:23:48.107000+00:00",
    "AccessGrantsLocationId": "default",
    "AccessGrantsLocationArn": "arn:aws:s3:us-east-2:111122223333:access-grants/
default/location/default",
    "IAMRoleArn": "arn:aws:iam::111122223333:role/accessGrantsTestRole"
}
```

Example – 列出在 S3 Access Grants 实例中注册的所有位置

要将结果限制为 S3 前缀或存储桶，可以选择使用 `--location-scope s3://bucket-and-or-prefix` 参数。

```
aws s3control list-access-grants-locations \
--account-id 111122223333 \
--region us-east-2
```

响应：

```
{"AccessGrantsLocationsList": [
  {
    "CreatedAt": "2023-05-31T18:23:48.107000+00:00",
    "AccessGrantsLocationId": "default",
    "AccessGrantsLocationArn": "arn:aws:s3:us-east-2:111122223333:access-grants/
default/location/default",
    "LocationScope": "s3://"
```

```
    "IAMRoleArn": "arn:aws:iam::111122223333:role/accessGrantsTestRole"
     },
  {
    "CreatedAt": "2023-05-31T18:23:48.107000+00:00",
    "AccessGrantsLocationId": "635f1139-1af2-4e43-8131-a4de006eb456",
    "AccessGrantsLocationArn": "arn:aws:s3:us-east-2:111122223333:access-grants/
default/location/635f1139-1af2-4e43-8131-a4de006eb888",
    "LocationScope": "s3://amzn-s3-demo-bucket/prefixA*",
    "IAMRoleArn": "arn:aws:iam::111122223333:role/accessGrantsTestRole"
     }
   ]
  }
```

使用 REST API

有关用于获取已注册位置的详细信息或列出在 S3 Access Grants 实例中注册的所有位置的 Amazon S3 REST API 支持的信息，请参阅《Amazon Simple Storage Service API 参考》中的以下部分：

- GetAccessGrantsLocation
- ListAccessGrantsLocations

使用 Amazon SDK

此部分中的示例说明了如何使用 Amazon SDK 获取已注册位置的详细信息，或列出 S3 Access Grants 实例中的所有已注册位置。

要使用以下示例，请将 *user input placeholders* 替换为您自己的信息。

Java

Example – 获取已注册位置的详细信息

```
public void getAccessGrantsLocation() {
GetAccessGrantsLocationRequest getAccessGrantsLocationRequest =
 GetAccessGrantsLocationRequest.builder()
.accountId("111122223333")
.accessGrantsLocationId("default")
.build();
GetAccessGrantsLocationResponse getAccessGrantsLocationResponse =
 s3Control.getAccessGrantsLocation(getAccessGrantsLocationRequest);
LOGGER.info("GetAccessGrantsLocationResponse: " + getAccessGrantsLocationResponse);
```

```
}
```

响应：

```
GetAccessGrantsLocationResponse(
CreatedAt=2023-06-07T04:35:10.027Z,
AccessGrantsLocationId=default,
AccessGrantsLocationArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
location/default,
LocationScope= s3://,
IAMRoleArn=arn:aws:iam::111122223333:role/accessGrantsTestRole
)
```

Example – 列出 S3 Access Grants 实例中的所有已注册位置

要将结果限制为 S3 前缀或存储桶，可以选择在 LocationScope 参数中传递 S3 URI，例如 s3://*bucket-and-or-prefix*。

```
public void listAccessGrantsLocations() {

ListAccessGrantsLocationsRequest listRequest =
 ListAccessGrantsLocationsRequest.builder()
.accountId("111122223333")
.build();

ListAccessGrantsLocationsResponse listResponse =
 s3Control.listAccessGrantsLocations(listRequest);
LOGGER.info("ListAccessGrantsLocationsResponse: " + listResponse);
}
```

响应：

```
ListAccessGrantsLocationsResponse(
AccessGrantsLocationsList=[
ListAccessGrantsLocationsEntry(
CreatedAt=2023-06-07T04:35:11.027Z,
AccessGrantsLocationId=default,
AccessGrantsLocationArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
location/default,
LocationScope=s3://,
IAMRoleArn=arn:aws:iam::111122223333:role/accessGrantsTestRole
),
```

```
ListAccessGrantsLocationsEntry(
CreatedAt=2023-06-07T04:35:10.027Z,
AccessGrantsLocationId=635f1139-1af2-4e43-8131-a4de006eb456,
AccessGrantsLocationArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
location/635f1139-1af2-4e43-8131-a4de006eb888,
LocationScope=s3://amzn-s3-demo-bucket/prefixA*,
IAMRoleArn=arn:aws:iam::111122223333:role/accessGrantsTestRole
)
]
)
```

## 更新已注册位置

您可以更新已在 Amazon S3 Access Grants 实例中注册的位置的 Amazon Identity and Access Management（IAM）角色。对于用于在 S3 Access Grants 中注册位置的每个新的 IAM 角色，请务必向 S3 Access Grants 服务主体（`access-grants.s3.amazonaws.com`）授予该角色的访问权限。为此，请在首次注册位置时使用的同一个信任策略 JSON 文件中为新 IAM 角色添加一个条目。

您可以使用 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）、Amazon S3 REST API 和 Amazon SDK 在 S3 Access Grants 实例中更新位置。

### 使用 S3 控制台

更新在 S3 Access Grants 实例中注册的位置的 IAM 角色

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Access Grants。
3. 在 S3 Access Grants 页面上，选择包含要使用的 S3 Access Grants 实例的区域。
4. 对于实例，选择查看详细信息。
5. 在实例的详细信息页面上，选择位置选项卡。
6. 找到要更新的位置。要筛选位置列表，请使用搜索框。
7. 选择要更新的已注册位置旁边的选项按钮。
8. 更新 IAM 角色，然后选择保存更改。

### 使用 Amazon CLI

要安装 Amazon CLI，请参阅 Amazon Command Line Interface 用户指南中的安装 Amazon CLI。

要使用以下示例命令，请将 *user input placeholders* 替换为您自己的信息。

Example – 更新已注册位置的 IAM 角色

```
aws s3control update-access-grants-location \
--account-id 111122223333 \
--access-grants-location-id 635f1139-1af2-4e43-8131-a4de006eb999 \
--iam-role-arn arn:aws:iam::777788889999:role/accessGrantsTestRole
```

响应：

```
{
    "CreatedAt": "2023-05-31T18:23:48.107000+00:00",
    "AccessGrantsLocationId": "635f1139-1af2-4e43-8131-a4de006eb999",
    "AccessGrantsLocationArn": "arn:aws:s3:us-east-2:777788889999:access-grants/
default/location/635f1139-1af2-4e43-8131-a4de006eb888",
    "LocationScope": "s3://amzn-s3-demo-bucket/prefixB*",
    "IAMRoleArn": "arn:aws:iam::777788889999:role/accessGrantsTestRole"
}
```

使用 REST API

有关用于更新 S3 Access Grants 实例中的位置的 Amazon S3 REST API 支持的信息，请参阅《Amazon Simple Storage Service API 参考》中的 UpdateAccessGrantsLocation。

使用 Amazon SDK

此部分中的示例说明了如何使用 Amazon SDK 更新已注册位置的 IAM 角色。

要使用以下示例，请将 *user input placeholders* 替换为您自己的信息。

Java

Example – 更新已注册位置的 IAM 角色

```
public void updateAccessGrantsLocation() {
UpdateAccessGrantsLocationRequest updateRequest =
 UpdateAccessGrantsLocationRequest.builder()
.accountId("111122223333")
.accessGrantsLocationId("635f1139-1af2-4e43-8131-a4de006eb999")
.iamRoleArn("arn:aws:iam::777788889999:role/accessGrantsTestRole")
.build();
```

```
UpdateAccessGrantsLocationResponse updateResponse =
 s3Control.updateAccessGrantsLocation(updateRequest);
LOGGER.info("UpdateAccessGrantsLocationResponse: " + updateResponse);
}
```

响应：

```
UpdateAccessGrantsLocationResponse(
CreatedAt=2023-06-07T04:35:10.027Z,
AccessGrantsLocationId=635f1139-1af2-4e43-8131-a4de006eb999,
AccessGrantsLocationArn=arn:aws:s3:us-east-2:777788889999:access-grants/default/
location/635f1139-1af2-4e43-8131-a4de006eb888,
LocationScope=s3://amzn-s3-demo-bucket/prefixB*,
IAMRoleArn=arn:aws:iam::777788889999:role/accessGrantsTestRole
)
```

## 删除已注册位置

您可以从 Amazon S3 Access Grants 实例中删除位置注册。删除该位置会将其从 S3 Access Grants 实例取消注册。

您必须先删除与该位置关联的所有授权，之后才能从 S3 Access Grants 实例中删除位置注册。有关如何删除授权的信息，请参阅删除授权。

您可以使用 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）、Amazon S3 REST API 和 Amazon SDK 从 S3 Access Grants 实例中删除位置。

使用 S3 控制台

从 S3 Access Grants 实例中删除位置注册

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Access Grants。
3. 在 S3 Access Grants 页面上，选择包含要使用的 S3 Access Grants 实例的区域。
4. 对于实例，选择查看详细信息。
5. 在实例的详细信息页面上，选择位置选项卡。
6. 找到要更新的位置。要筛选位置列表，请使用搜索框。

7. 选择要删除的已注册位置旁边的选项按钮。
8. 选择注销。
9. 这将出现一个对话框，警告您此操作无法撤消。要删除该位置，请选择取消注册。

使用 Amazon CLI

要安装 Amazon CLI，请参阅 Amazon Command Line Interface 用户指南中的安装 Amazon CLI。

要使用以下示例命令，请将 *user input placeholders* 替换为您自己的信息。

Example – 删除位置注册

```
aws s3control delete-access-grants-location \
--account-id 111122223333 \
--access-grants-location-id  a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
 // No response body
```

使用 REST API

有关用于从 S3 Access Grants 实例中删除位置的 Amazon S3 REST API 支持的信息，请参阅《Amazon Simple Storage Service API 参考》中的 DeleteAccessGrantsLocation。

使用 Amazon SDK

此部分中的示例说明了如何使用 Amazon SDK 删除位置。

要使用以下示例，请将 *user input placeholders* 替换为您自己的信息。

Java

Example – 删除位置注册

```
public void deleteAccessGrantsLocation() {
DeleteAccessGrantsLocationRequest deleteRequest =
 DeleteAccessGrantsLocationRequest.builder()
.accountId("111122223333")
.accessGrantsLocationId("a1b2c3d4-5678-90ab-cdef-EXAMPLE11111")
.build();
DeleteAccessGrantsLocationResponse deleteResponse =
 s3Control.deleteAccessGrantsLocation(deleteRequest);
```

```
LOGGER.info("DeleteAccessGrantsLocationResponse: " + deleteResponse);
}
```

响应：

```
DeleteAccessGrantsLocationResponse()
```

# 在 S3 访问权限管控中处理授权

S3 访问权限管控实例中的单个访问权限管控 可让特定身份 [Amazon Identity and Access Management（IAM）主体或公司目录中的用户或组] 在 S3 访问权限管控实例中注册的位置内获得访问权限。位置将存储桶或前缀映射到 IAM 角色。S3 访问权限管控代入此 IAM 角色，来向被授权者提供临时凭证。

在 S3 访问权限管控实例中注册至少一个位置后，可以创建访问权限管控。

被授权者可以是 IAM 用户或角色，也可以是目录用户或组。目录用户是与 S3 访问权限管控实例关联的公司目录或外部身份源中的用户。有关更多信息，请参阅 S3 Access Grants 和公司目录身份。要从 IAM Identity Center 为特定目录用户或组创建授权，请在 IAM Identity Center 中找到 IAM Identity Center 用来标识该用户的 GUID，例如 `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`。有关如何使用 IAM Identity Center 来查看用户信息的更多信息，请参阅《Amazon IAM Identity Center 用户指南》中的 View user and group assignments。

您可以授予对存储桶、前缀或对象的访问权限。Amazon S3 中的前缀是用于整理存储桶中对象的对象密钥名称开头的字符串。这可以是任何支持的字符串，例如，存储桶中以 `engineering/` 前缀开头的对象键名称。

主题

- 创建授权
- 查看授权
- 删除授权

## 创建授权

S3 访问权限管控实例中的单个访问权限管控 可让特定身份 [Amazon Identity and Access Management（IAM）主体或公司目录中的用户或组] 在 S3 访问权限管控实例中注册的位置内获得访问

权限。位置将存储桶或前缀映射到 IAM 角色。S3 访问权限管控代入此 IAM 角色，来向被授权者提供临时凭证。

在 S3 访问权限管控实例中注册至少一个位置后，可以创建访问权限管控。

被授权者可以是 IAM 用户或角色，也可以是目录用户或组。目录用户是与 S3 访问权限管控实例关联的公司目录或外部身份源中的用户。有关更多信息，请参阅 S3 Access Grants 和公司目录身份。要从 IAM Identity Center 为特定目录用户或组创建授权，请在 IAM Identity Center 中找到 IAM Identity Center 用来标识该用户的 GUID，例如 `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`。有关如何使用 IAM Identity Center 来查看用户信息的更多信息，请参阅《Amazon IAM Identity Center 用户指南》中的 View user and group assignments。

您可以授予对存储桶、前缀或对象的访问权限。Amazon S3 中的前缀是用于整理存储桶中对象的对象密钥名称开头的字符串。这可以是任何支持的字符串，例如，存储桶中以 `engineering/` 前缀开头的对象键名称。

子前缀

在授予对已注册位置的访问权限时，可以使用 `Subprefix` 字段将访问权限范围缩小到位置范围的子集。如果您为授权选择的已注册位置是默认 S3 路径 (`s3://`)，则必须缩小授权范围。无法为默认位置 (`s3://`) 创建访问权限管控，这将向被授权者授予访问 Amazon Web Services 区域中每个存储桶的权限。相反，您必须将授权范围缩小到以下各项之一：

- 存储桶：`s3://`*`bucket`*`/*`
- 存储桶中的前缀：`s3://`*`bucket`*`/`*`prefix`*`*`
- 前缀中的前缀：`s3://`*`bucket`*`/`*`prefixA`*`/`*`prefixB`*`*`
- 对象：`s3://`*`bucket`*`/`*`object-key-name`*

如果您要在已注册位置为存储桶的情况下创建访问权限管控，则可在 `Subprefix` 字段中传递下列项之一来缩小授权范围：

- 存储桶中的前缀：*`prefix`*`*`
- 前缀中的前缀：*`prefixA/prefixB`*`*`
- 对象：*`/object-key-name`*

在创建授权后，Amazon S3 控制台中显示的授权范围或者 API 或 Amazon Command Line Interface（Amazon CLI）响应中返回的 `GrantScope` 是将位置路径与 `Subprefix` 连接后的结果。确保此连接的路径正确映射到要授予其访问权限的 S3 存储桶、前缀或对象。

> **Note**
>
> - 如果要创建的访问权限管控仅授予对一个对象的访问权限，则必须指定授权类型是针对某个对象的。要在 API 调用或 CLI 命令中执行此操作，请传递带有 `Object` 值的 `s3PrefixType` 参数。在 Amazon S3 控制台中，当您创建授权时，在选择位置后，在授权范围下，选中授权范围是一个对象复选框。
> - 如果存储桶尚不存在，则无法创建存储桶的授权。但是，您可以创建对尚不存在的前缀的授权。
> - 有关您可以在 S3 访问权限管控实例中创建的最大授权数量，请参阅 S3 Access Grants 限制。

您可以使用 Amazon S3 控制台、Amazon CLI、Amazon S3 REST API 和 Amazon SDK 创建访问授权。

使用 S3 控制台

创建访问授权

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Access Grants。
3. 在 S3 Access Grants 页面上，选择包含要使用的 S3 Access Grants 实例的区域。

   如果您是首次使用 S3 Access Grants 实例，请确保已完成步骤 2 - 注册位置，并导航到设置 Access Grants 实例向导的步骤 3。如果您已拥有 S3 Access Grants 实例，请选择查看详细信息，然后从授权选项卡中选择创建授权。

   a. 在授权范围部分中，选择或输入已注册位置。

      如果您选择了默认 `s3://` 位置，请使用子前缀框来缩小访问授权的范围。有关更多信息，请参阅子前缀。如果您只授予一个对象的访问权限，请选择授权范围为对象。

   b. 在权限和访问下，选择权限级别，即读取和/或写入。

      然后选择被授权者类型。如果您已将公司目录添加到 IAM Identity Center，并将此 IAM Identity Center 实例与 S3 Access Grants 实例关联，则可以选择 IAM Identity Center 中的目录身份。如果您选择此选项，请从 IAM Identity Center 获取用户或组的 ID，然后在此部分中输入此 ID。

如果被授权者类型是 IAM 用户或角色，请选择 IAM 主体。在 IAM 主体类型下，选择用户或角色。然后，在 IAM 主体用户下，从列表中进行选择或输入身份的 ID。

c. 要创建 S3 Access Grants 授权，请选择下一步或创建授权。

4. 如果已禁用下一步或创建授权，则：

无法创建授权

- 您可能需要先在 S3 Access Grants 实例中注册位置。
- 您可能没有 `s3:CreateAccessGrant` 权限，无法创建访问授权。请联系您的账户管理员。

使用 Amazon CLI

要安装 Amazon CLI，请参阅 Amazon Command Line Interface 用户指南中的安装 Amazon CLI。

以下示例说明如何为 IAM 主体创建访问授权请求以及如何为公司目录用户或组创建访问授权请求。

要使用以下示例命令，请将 *`user input placeholders`* 替换为您自己的信息。

> **Note**
>
> 如果要创建的访问授权仅授予对一个对象的访问权限，请包括必需参数 `--s3-prefix-type Object`。

Example 为 IAM 主体创建访问授权请求

```
aws s3control create-access-grant \
--account-id 111122223333 \
--access-grants-location-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222 \
--access-grants-location-configuration S3SubPrefix=prefixB* \
--permission READ \
--grantee GranteeType=IAM,GranteeIdentifier=arn:aws:iam::123456789012:user/data-consumer-3
```

Example 创建访问授权响应

```
{"CreatedAt": "2023-05-31T18:41:34.663000+00:00",
    "AccessGrantId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
```

```
    "AccessGrantArn": "arn:aws:s3:us-east-2:111122223333:access-grants/default/
grant/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Grantee": {
        "GranteeType": "IAM",
        "GranteeIdentifier": "arn:aws:iam::111122223333:user/data-consumer-3"
    },
    "AccessGrantsLocationId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "AccessGrantsLocationConfiguration": {
        "S3SubPrefix": "prefixB*"
    },
    "GrantScope": "s3://DOC-BUCKET-EXAMPLE/prefix*",
    "Permission": "READ"
}
```

为目录用户或组创建访问授权请求

要为目录用户或组创建访问授权请求，您必须先运行下列命令之一来获取目录用户或组的 GUID。

Example 获取目录用户或组的 GUID

您可以通过 IAM Identity Center 控制台或使用 Amazon CLI 或 Amazon SDK 来查找 IAM Identity Center 用户的 GUID。以下命令列出指定的 IAM Identity Center 实例中的用户及其名称和标识符。

```
aws identitystore list-users --identity-store-id d-1a2b3c4d1234
```

此命令列出指定的 IAM Identity Center 实例中的组。

```
aws identitystore list-groups --identity-store-id d-1a2b3c4d1234
```

Example 为目录用户或组创建访问授权

此命令类似于用来为 IAM 用户或角色创建授权的命令，只是被授权者类型为 DIRECTORY_USER 或 DIRECTORY_GROUP，并且被授权者标识符为目录用户或组的 GUID。

```
aws s3control create-access-grant \
--account-id 123456789012 \
--access-grants-location-id default \
--access-grants-location-configuration S3SubPrefix="amzn-s3-demo-bucket/rafael/*" \
--permission READWRITE \
--grantee GranteeType=DIRECTORY_USER,GranteeIdentifier=83d43802-00b1-7054-db02-
f1d683aacba5 \
```

### 使用 REST API

有关用于管理访问授权的 Amazon S3 REST API 支持的信息，请参阅《Amazon Simple Storage Service API 参考》中的以下部分：

- CreateAccessGrant
- DeleteAccessGrant
- GetAccessGrant
- ListAccessGrants

### 使用 Amazon SDK

此部分中的示例说明了如何使用 Amazon SDK 创建访问授权。

#### Java

要使用以下示例，请将 *user input placeholders* 替换为您自己的信息：

> **Note**
>
> 如果要创建的访问授权仅授予对一个对象的访问权限，请包括必需参数 `.s3PrefixType(S3PrefixType.Object)`。

Example 创建访问授权请求

```
public void createAccessGrant() {
CreateAccessGrantRequest createRequest = CreateAccessGrantRequest.builder()
.accountId("111122223333")
.accessGrantsLocationId("a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa")
.permission("READ")
.accessGrantsLocationConfiguration(AccessGrantsLocationConfiguration.builder().s3SubPrefix("
.grantee(Grantee.builder().granteeType("IAM").granteeIdentifier("arn:aws:iam::111122223333:u
data-consumer-3").build())
.build();
CreateAccessGrantResponse createResponse =
 s3Control.createAccessGrant(createRequest);
LOGGER.info("CreateAccessGrantResponse: " + createResponse);
}
```

Example 创建访问授权响应

```
CreateAccessGrantResponse(
CreatedAt=2023-06-07T05:20:26.330Z,
AccessGrantId=a1b2c3d4-5678-90ab-cdef-EXAMPLE33333,
AccessGrantArn=arn:aws:s3:us-east-2:444455556666:access-grants/default/grant/
a1b2c3d4-5678-90ab-cdef-EXAMPLE33333,
Grantee=Grantee(
GranteeType=IAM,
GranteeIdentifier=arn:aws:iam::111122223333:user/data-consumer-3
),
AccessGrantsLocationId=a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa,
AccessGrantsLocationConfiguration=AccessGrantsLocationConfiguration(
S3SubPrefix=prefixB*
),
GrantScope=s3://DOC-BUCKET-EXAMPLE/prefixB,
Permission=READ
)
```

## 查看授权

您可以使用 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）、Amazon S3 REST API 和 Amazon SDK 来查看 Amazon S3 Access Grants 实例中的访问授权的详细信息。

使用 S3 控制台

查看访问授权的详细信息

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Access Grants。
3. 在 S3 Access Grants 页面上，选择包含要使用的 S3 Access Grants 实例的区域。
4. 对于实例，选择查看详细信息。
5. 在详细信息页面上，选择授权选项卡。
6. 在授权部分中，找到要查看的访问授权。要筛选授权列表，请使用搜索框。

使用 Amazon CLI

要安装 Amazon CLI，请参阅 Amazon Command Line Interface 用户指南中的安装 Amazon CLI。

要使用以下示例命令，请将 *user input placeholders* 替换为您自己的信息。

Example – 获取访问授权的详细信息

```
aws s3control get-access-grant \
--account-id 111122223333 \
--access-grant-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222
```

响应：

```
{
    "CreatedAt": "2023-05-31T18:41:34.663000+00:00",
    "AccessGrantId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "AccessGrantArn": "arn:aws:s3:us-east-2:111122223333:access-grants/default/
grant-a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "Grantee": {
        "GranteeType": "IAM",
        "GranteeIdentifier": "arn:aws:iam::111122223333:user/data-consumer-3"
    },
    "Permission": "READ",
    "AccessGrantsLocationId": "12a6710f-5af8-41f5-b035-0bc795bf1a2b",
    "AccessGrantsLocationConfiguration": {
        "S3SubPrefix": "prefixB*"
    },
    "GrantScope": "s3://amzn-s3-demo-bucket/"
}
```

Example – 列出 S3 Access Grants 实例中的所有访问授权

您可以选择使用以下参数将结果限制为 S3 前缀或 Amazon Identity and Access Management（IAM）身份：

- 子前缀 – `--grant-scope s3://bucket-name/prefix*`
- IAM 身份 – `--grantee-type IAM` 和 `--grantee-identifier arn:aws:iam::123456789000:role/accessGrantsConsumerRole`

```
aws s3control list-access-grants \
--account-id 111122223333
```

响应：

```
{
    "AccessGrantsList": [{"CreatedAt": "2023-06-14T17:54:46.542000+00:00",
            "AccessGrantId": "dd8dd089-b224-4d82-95f6-975b4185bbaa",
            "AccessGrantArn": "arn:aws:s3:us-east-2:111122223333:access-grants/default/
grant/dd8dd089-b224-4d82-95f6-975b4185bbaa",
            "Grantee": {
                "GranteeType": "IAM",
                "GranteeIdentifier": "arn:aws:iam::111122223333:user/data-consumer-3"
            },
            "Permission": "READ",
            "AccessGrantsLocationId": "23514a34-ea2e-4ddf-b425-d0d4bfcarda1",
            "GrantScope": "s3://amzn-s3-demo-bucket/prefixA*"
        },
        {"CreatedAt": "2023-06-24T17:54:46.542000+00:00",
            "AccessGrantId": "ee8ee089-b224-4d72-85f6-975b4185a1b2",
            "AccessGrantArn": "arn:aws:s3:us-east-2:111122223333:access-grants/default/
grant/ee8ee089-b224-4d72-85f6-975b4185a1b2",
            "Grantee": {
                "GranteeType": "IAM",
                "GranteeIdentifier": "arn:aws:iam::111122223333:user/data-consumer-9"
            },
            "Permission": "READ",
            "AccessGrantsLocationId": "12414a34-ea2e-4ddf-b425-d0d4bfcacao0",
            "GrantScope": "s3://amzn-s3-demo-bucket/prefixB*"
        },

    ]
}
```

使用 REST API

您可以使用 Amazon S3 API 操作来查看访问授权的详细信息，并列出 S3 Access Grants 实例中的所有访问授权。有关用于管理访问授权的 REST API 支持的信息，请参阅《Amazon Simple Storage Service API 参考》中的以下部分：

- GetAccessGrant
- ListAccessGrants

使用 Amazon SDK

此部分中的示例说明了如何使用 Amazon SDK 获取访问授权的详细信息。

要使用以下示例，请将 *user input placeholders* 替换为您自己的信息。

Java

Example – 获取访问授权的详细信息

```
public void getAccessGrant() {
GetAccessGrantRequest getRequest = GetAccessGrantRequest.builder()
.accountId("111122223333")
.accessGrantId("a1b2c3d4-5678-90ab-cdef-EXAMPLE22222")
.build();
GetAccessGrantResponse getResponse = s3Control.getAccessGrant(getRequest);
LOGGER.info("GetAccessGrantResponse: " + getResponse);
}
```

响应：

```
GetAccessGrantResponse(
CreatedAt=2023-06-07T05:20:26.330Z,
AccessGrantId=a1b2c3d4-5678-90ab-cdef-EXAMPLE22222,
AccessGrantArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
grant-fd3a5086-42f7-4b34-9fad-472e2942c70e,
Grantee=Grantee(
GranteeType=IAM,
GranteeIdentifier=arn:aws:iam::111122223333:user/data-consumer-3
),
Permission=READ,
AccessGrantsLocationId=12a6710f-5af8-41f5-b035-0bc795bf1a2b,
AccessGrantsLocationConfiguration=AccessGrantsLocationConfiguration(
S3SubPrefix=prefixB*
),
GrantScope=s3://amzn-s3-demo-bucket/
)
```

Example – 列出 S3 Access Grants 实例中的所有访问授权

您可以选择使用以下参数将结果限制为 S3 前缀或（IAM）身份：

- 范围 – `GrantScope=s3://bucket-name/prefix*`
- 被授权者 – `GranteeType=IAM` 和 `GranteeIdentifier=arn:aws:iam::111122223333:role/accessGrantsConsumerRole`

```
public void listAccessGrants() {
ListAccessGrantsRequest listRequest = ListAccessGrantsRequest.builder()
.accountId("111122223333")
.build();
ListAccessGrantsResponse listResponse = s3Control.listAccessGrants(listRequest);
LOGGER.info("ListAccessGrantsResponse: " + listResponse);
}
```

响应：

```
ListAccessGrantsResponse(
AccessGrantsList=[
ListAccessGrantEntry(
CreatedAt=2023-06-14T17:54:46.540z,
AccessGrantId=dd8dd089-b224-4d82-95f6-975b4185bbaa,
AccessGrantArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
grant/dd8dd089-b224-4d82-95f6-975b4185bbaa,
Grantee=Grantee(
GranteeType=IAM, GranteeIdentifier= arn:aws:iam::111122223333:user/data-consumer-3
),
Permission=READ,
AccessGrantsLocationId=23514a34-ea2e-4ddf-b425-d0d4bfcarda1,
GrantScope=s3://amzn-s3-demo-bucket/prefixA
),
ListAccessGrantEntry(
CreatedAt=2023-06-24T17:54:46.540Z,
AccessGrantId=ee8ee089-b224-4d72-85f6-975b4185a1b2,
AccessGrantArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
grant/ee8ee089-b224-4d72-85f6-975b4185a1b2,
Grantee=Grantee(
GranteeType=IAM, GranteeIdentifier= arn:aws:iam::111122223333:user/data-consumer-9
),
Permission=READ,
AccessGrantsLocationId=12414a34-ea2e-4ddf-b425-d0d4bfcacao0,
GrantScope=s3://amzn-s3-demo-bucket/prefixB*
)
]
)
```

## 删除授权

您可以从 Amazon S3 Access Grants 实例中删除访问授权。您无法撤消访问授权删除操作。删除访问授权后，被授权者将再也无法访问您的 Amazon S3 数据。

您可以使用 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）、Amazon S3 REST API 和 Amazon SDK 删除访问授权。

使用 S3 控制台

删除访问授权

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Access Grants。
3. 在 S3 Access Grants 页面上，选择包含要使用的 S3 Access Grants 实例的区域。
4. 对于实例，选择查看详细信息。
5. 在详细信息页面上，选择授权选项卡。
6. 搜索要删除的授权。找到授权后，选择它旁边的单选按钮。
7. 选择删除。这将出现一个对话框，警告您操作无法撤消。再次选择删除以删除授权。

使用 Amazon CLI

要安装 Amazon CLI，请参阅 Amazon Command Line Interface 用户指南中的安装 Amazon CLI。

要使用以下示例命令，请将 *user input placeholders* 替换为您自己的信息。

Example – 删除访问授权

```
aws s3control delete-access-grant \
--account-id 111122223333 \
--access-grant-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111

// No response body
```

使用 REST API

有关用于管理访问授权的 Amazon S3 REST API 支持的信息，请参阅《Amazon Simple Storage Service API 参考》中的 DeleteAccessGrant。

使用 Amazon SDK

此部分中的示例说明了如何使用 Amazon SDK 删除访问授权。要使用以下示例，请将 *user input placeholders* 替换为您自己的信息。

Java

Example – 删除访问授权

```
public void deleteAccessGrant() {
DeleteAccessGrantRequest deleteRequest = DeleteAccessGrantRequest.builder()
.accountId("111122223333")
.accessGrantId("a1b2c3d4-5678-90ab-cdef-EXAMPLE11111")
.build();
DeleteAccessGrantResponse deleteResponse =
 s3Control.deleteAccessGrant(deleteRequest);
LOGGER.info("DeleteAccessGrantResponse: " + deleteResponse);
}
```

响应：

```
DeleteAccessGrantResponse()
```

## 使用访问授权获取 S3 数据

已通过 S3 访问权限管控获得 S3 数据访问权限的被授权者必须从 S3 访问权限管控中请求临时凭证，被授权者使用这些凭证来访问 S3 数据。有关更多信息，请参阅 通过 S3 Access Grants 请求访问 Amazon S3 数据。然后，被授权者使用临时凭证对 S3 数据执行支持的 S3 操作。有关更多信息，请参阅 使用 S3 访问权限管控提供的凭证访问 S3 数据。在请求这些凭证之前，被授权者可以选择请求对 Amazon Web Services 账户的访问授权列表。有关更多信息，请参阅 列出调用方的访问授权。

主题

- 通过 S3 Access Grants 请求访问 Amazon S3 数据
- 使用 S3 访问权限管控提供的凭证访问 S3 数据
- 列出调用方的访问授权

## 通过 S3 Access Grants 请求访问 Amazon S3 数据

使用 S3 访问权限管控创建访问权限管控后，被授权者可以申请凭证，以访问他们已获得访问权限的 S3 数据。被授权者可以是 Amazon Identity and Access Management（IAM）主体、您的公司目录身份或获得授权的应用程序。

应用程序或 Amazon Web Services 服务可以使用 S3 访问权限管控 `GetDataAccess` API 操作来代表被授权者向 S3 访问权限管控请求对 S3 数据的访问权限。`GetDataAccess` 首先验证您是否已向该身份授予对此数据的访问权限。然后，S3 Access Grants 使用 AssumeRole API 操作来获取临时凭证令牌并将其出售给请求方。此临时凭证令牌是 Amazon Security Token Service（Amazon STS）令牌。

`GetDataAccess` 请求必须包含 `target` 参数，该参数指定临时凭证适用于的 S3 数据的范围。此 `target` 范围可以与授权的范围相同，也可以是该范围的子集，但 `target` 范围必须在已向被授权者提供的授权范围内。请求还必须指定 `permission` 参数以指示临时凭证的权限级别，即 `READ`、`WRITE` 或 `READWRITE`。

特权

请求者可以在其凭证请求中指定临时令牌的权限级别。通过使用 `privilege` 参数，请求者可以在授权范围边界内缩小或增大临时凭证的访问范围。`privilege` 参数的默认值为 `Default`，这意味着返回的凭证的目标范围是原始授权范围。`privilege` 的另一个可能值是 `Minimal`。如果 `target` 范围从最初的授权范围缩小，则只要 `target` 范围在授权范围内，就会解除临时凭证的范围以匹配 `target` 范围。

下表详细说明了 `privilege` 参数对两个授权的影响。一个授权具有范围 `S3://amzn-s3-demo-bucket1/bob/*`，其中包括 *amzn-s3-demo-bucket1* 存储桶中的整个 `bob/` 前缀。另一个授权具有范围 `S3://amzn-s3-demo-bucket1/bob/reports/*`，其中仅包括 *amzn-s3-demo-bucket1* 存储桶中的 `bob/reports/` 前缀。

| 授权范围 | 请求的范围 | 特权 | 返回的范围 | 效果 |
| --- | --- | --- | --- | --- |
| S3://*amzn-s3-demo-bucket1* /bob/* | *amzn-s3-demo-bucket1* /bob/* | Default | *amzn-s3-demo-bucket1* /bob/* | 请求者有权访问 *amzn-s3-demo-bucket1* 存储桶中所有带以前缀 *bob/* 开始的密钥名称的对象。 |

| 授权范围 | 请求的范围 | 特权 | 返回的范围 | 效果 |
| --- | --- | --- | --- | --- |
| S3://*amzn-s3-demo-bucket1* /bob/* | *amzn-s3-demo-bucket1* /bob/ | Minimal | *amzn-s3-demo-bucket1* /bob/ | 如果前缀名称 bob/ 后面没有通配符 *，则请求者只能访问 *amzn-s3-demo-bucket1* 存储桶中名为 bob/ 的对象。此类对象并不常见。请求者无权访问任何其他对象，包括那些带以 bob/ 前缀开头的密钥名称的对象。 |
| S3://*amzn-s3-demo-bucket1* /bob/* | *amzn-s3-demo-bucket1* /bob/images/* | Minimal | *amzn-s3-demo-bucket1* /bob/images/* | 请求者有权访问 *amzn-s3-demo-bucket1* 存储桶中所有带以前缀 *bob/images/** 开始的密钥名称的对象。 |
| S3://*amzn-s3-demo-bucket1* /bob/reports/* | *amzn-s3-demo-bucket1* /bob/reports/file.txt | Default | *amzn-s3-demo-bucket1* /bob/reports/* | 请求者有权访问 *amzn-s3-demo-bucket1* 存储桶中所有带以前缀 bob/reports 开始的密钥名称的对象，它是匹配授权的范围。 |
| S3://*amzn-s3-demo-bucket1* /bob/reports/* | *amzn-s3-demo-bucket1* /bob/reports/file.txt | Minimal | *amzn-s3-demo-bucket1* /bob/reports/file.txt | 请求者只能访问 *amzn-s3-demo-bucket1* 存储桶中具有密钥名称 bob/reports/file.txt 的对象。请求者无权访问任何其他对象。 |

目录身份

GetDataAccess 在匹配合适的授权时会考虑请求中涉及的所有身份。对于公司目录身份，GetDataAccess 还会返回用于身份感知会话的 IAM 身份的授权。有关身份感知会话的更多信息，请参阅《Amazon Identity and Access Management 用户指南》中的授予使用身份感知控制台会话的权限。GetDataAccess 生成凭证来将范围限制为受限最严的授权，如下表所示：

| IAM 身份的授权范围 | 目录身份的授权范围 | 请求的范围 | 返回的范围 | 特权 | 效果 |
|---|---|---|---|---|---|
| S3://*amzn-s3-demo-bucket1* / bob/* | *amzn-s3-demo-bucket1* / bob/images/* | S3://*amzn-s3-demo-bucket1* / bob/images/image1.jpeg | S3://*amzn-s3-demo-bucket1* / bob/images/* | Default | 作为 IAM 角色授权的一部分，请求者可以访问键名称以前缀 bob/ 开头的所有对象，但作为目录身份授权的一部分，则仅限于前缀 bob/images/。IAM 角色和目录身份都提供对所请求范围（也即 bob/images/image1.jpeg ）的访问权限，但目录身份的授权限制性更强。因此，返回的范围限于对目录身份的限制性更强的授权。 |
| S3://*amzn-s3-demo-bucket1* / bob/* | *amzn-s3-demo-bucket1* / bob/images/* | S3://*amzn-s3-demo-bucket1* / bob/images/image1.jpeg | S3://*amzn-s3-demo-bucket1* / bob/images/image1.jpeg | Minimal | 由于权限设置为 Minimal，因此，即使身份可以访问更大的范围，也只返回所请求的范围 bob/images/image1.jpeg 。 |

| IAM 身份的授权范围 | 目录身份的授权范围 | 请求的范围 | 返回的范围 | 特权 | 效果 |
| --- | --- | --- | --- | --- | --- |
| | | image1.jpeg | | | |
| S3://*amzn-s3-demo-bucket1* / bob/images/* | *amzn-s3-demo-bucket1* / bob/* | S3://*amzn-s3-demo-bucket1* / bob/images/image1.jpeg | S3://*amzn-s3-demo-bucket1* / bob/images/* | Default | 作为目录身份授权的一部分，请求者可以访问键名称以前缀 bob/ 开头的所有对象，但作为 IAM 角色授权的一部分，则仅限于前缀 bob/images/。IAM 角色和目录身份都提供对所请求范围（也即 bob/images/image1.jpeg ）的访问权限，但 IAM 角色的授权限制性更强。因此，返回的范围限于对 IAM 角色的限制性更强的授权。 |
| S3://*amzn-s3-demo-bucket1* / bob/images/* | *amzn-s3-demo-bucket1* / bob/* | S3://*amzn-s3-demo-bucket1* / bob/images/image1.jpeg | S3://*amzn-s3-demo-bucket1* / bob/images/image1.jpeg | Minimal | 由于权限设置为 Minimal，因此，即使身份可以访问更大的范围，也只返回所请求的范围 bob/images/image1.jpeg 。 |

## 持续时间

durationSeconds 参数设置临时凭证的持续时间（以秒为单位）。默认值为 3600 秒（1 小时），但请求者（被授权者）可以指定介于 900 秒（15 分钟）和 43200 秒（12 小时）之间的范围。如果被授权者请求的值高于此最大值，请求将失败。

> **Note**
>
> 在对临时令牌的请求中，如果位置是对象，请将请求中的 targetType 参数值设置为 Object。仅当位置为对象且权限级别为 Minimal 时需要此参数。如果位置是存储桶或前缀，则无需指定此参数。

示例

可以使用 Amazon Command Line Interface（Amazon CLI）、Amazon S3 REST API 和 Amazon SDK 请求临时凭证。请参阅这些示例。

有关其它信息，请参阅《Amazon Simple Storage Service API Reference》中的 GetDataAccess。

使用 Amazon CLI

要安装 Amazon CLI，请参阅 Amazon Command Line Interface 用户指南中的安装 Amazon CLI。

要使用以下示例命令，请将 *user input placeholders* 替换为您自己的信息。

Example 请求临时凭证

请求:

```
aws s3control get-data-access \
--account-id 111122223333 \
--target s3://amzn-s3-demo-bucket/prefixA* \
--permission READ \
--privilege Default \
--region us-east-2
```

响应:

```
{
"Credentials": {
"AccessKeyId": "Example-key-id",
"SecretAccessKey": "Example-access-key",
"SessionToken": "Example-session-token",
```

```
"Expiration": "2023-06-14T18:56:45+00:00"},
"MatchedGrantTarget": "s3://amzn-s3-demo-bucket/prefixA**",
"Grantee": {
    "GranteeType": "IAM",
    "GranteeIdentifier": "arn:aws:iam::111122223333:role/role-name"
 }
}
```

使用 REST API

有关用于请求 S3 Access Grants 中的临时凭证的 Amazon S3 REST API 支持的信息，请参阅《Amazon Simple Storage Service API 参考》中的 GetDataAccess。

使用 Amazon SDK

此部分中的示例说明被授权者如何使用 Amazon SDK 从 S3 Access Grants 请求临时凭证。

Java

以下代码示例返回被授权者用于访问您的 S3 数据的临时凭证。要使用此代码示例，请将 *user input placeholders* 替换为您自己的信息。

Example 获取临时凭证

请求:

```
public void getDataAccess() {
GetDataAccessRequest getDataAccessRequest = GetDataAccessRequest.builder()
.accountId("111122223333")
.permission(Permission.READ)
.privilege(Privilege.MINIMAL)
.target("s3://amzn-s3-demo-bucket/prefixA*")
.build();
GetDataAccessResponse getDataAccessResponse =
 s3Control.getDataAccess(getDataAccessRequest);
LOGGER.info("GetDataAccessResponse: " + getDataAccessResponse);
}
```

响应:

```
GetDataAccessResponse(
Credentials=Credentials(
AccessKeyId="Example-access-key-id",
```

```
SecretAccessKey="Example-secret-access-key",
SessionToken="Example-session-token",
Expiration=2023-06-07T06:55:24Z
))
```

## 使用 S3 访问权限管控提供的凭证访问 S3 数据

在被授权者通过其访问授权获得临时凭证后，他们可以使用这些临时凭证来调用 Amazon S3 API 操作以访问您的数据。

被授权者可以使用 Amazon Command Line Interface（Amazon CLI）、Amazon SDK 和 Amazon S3 REST API 来访问 S3 数据。此外，可以使用 Amazon Python 和 Java 插件来调用 S3 访问权限管控

使用 Amazon CLI

在被授权者从 S3 Access Grants 获得临时凭证后，他们可以使用这些凭证设置配置文件来检索数据。

要安装 Amazon CLI，请参阅 Amazon Command Line Interface 用户指南中的安装 Amazon CLI。

要使用以下示例命令，请将 *user input placeholders* 替换为您自己的信息。

Example – 设置配置文件

```
aws configure set aws_access_key_id "$accessKey" --profile access-grants-consumer-access-profile
aws configure set aws_secret_access_key "$secretKey" --profile access-grants-consumer-access-profile
aws configure set aws_session_token "$sessionToken" --profile access-grants-consumer-access-profile
```

要使用以下示例命令，请将 *user input placeholders* 替换为您自己的信息。

Example – 获取 S3 数据

被授权者可以使用 get-object Amazon CLI 命令来访问数据。被授权者还可以使用 put-object、ls 和其他 S3 Amazon CLI 命令。

```
aws s3api get-object \
--bucket amzn-s3-demo-bucket1 \
--key myprefix \
--region us-east-2 \
--profile access-grants-consumer-access-profile
```

使用 Amazon SDK

此部分中的示例说明被授权者如何使用 Amazon SDK 访问 S3 数据。

Java

有关如何使用临时凭证获取 S3 数据的示例，请参阅如何使用 Amazon SDK 获取对象和 Amazon SDK for Java 2.x 的 Amazon S3 代码示例。

S3 访问权限管控中支持的 S3 操作

被授权者可以使用 S3 访问权限管控提供的临时凭证，对他们有权访问的 S3 数据执行 S3 操作。以下是被授权者可以执行的受支持 S3 操作的列表。支持哪些操作取决于在访问授权中授予的权限级别，即 `READ`、`WRITE` 或 `READWRITE`。

> **Note**
>
> 除了下面列出的 Amazon S3 权限外，Amazon S3 还可以调用 Amazon Key Management Service（Amazon KMS）Decrypt (`kms:decrypt`) `READ` 权限或 Amazon KMS GenerateDataKey (`kms:generateDataKey`) `WRITE` 权限。这些权限不支持直接访问 Amazon KMS 密钥。

| S3 IAM 操作 | API 操作和文档 | S3 访问权限管控权限 | S3 资源 | | | |
|---|---|---|---|---|---|---|
| `s3:GetObject` | GetObject | `READ` | 对象 | | | |
| `s3:GetObjectVersion` | GetObject | `READ` | 对象 | | | |
| `s3:GetObjectAcl` | GetObjectAcl | `READ` | 对象 | | | |
| `s3:GetObjectVersionAcl` | GetObjectAcl | `READ` | 对象 | | | |

| S3 IAM 操作 | API 操作和文档 | S3 访问权限管控权限 | S3 资源 | | | |
|---|---|---|---|---|---|---|
| s3:ListMultipartUploads | ListParts | READ | 对象 | | | |
| s3:PutObject | PutObject、CreateMultipartUpload、UploadPart、UploadPartCopy、CompleteMultipartUpload | WRITE | 对象 | | | |
| s3:PutObjectAcl | PutObjectAcl | WRITE | 对象 | | | |
| s3:PutObjectVersionAcl | PutObjectAcl | WRITE | 对象 | | | |
| s3:DeleteObject | DeleteObject | WRITE | 对象 | | | |
| s3:DeleteObjectVersion | DeleteObject | WRITE | 对象 | | | |
| s3:AbortMultipartUpload | AbortMultipartUpload | WRITE | 对象 | | | |
| s3:ListBucket | HeadBucket、ListObjectsV2、ListObjects | READ | 存储桶 | | | |

| S3 IAM 操作 | API 操作和文档 | S3 访问权限管控权限 | S3 资源 | | | |
|---|---|---|---|---|---|---|
| s3:ListBucketVersions | ListObjectVersions | READ | 存储桶 | | | |
| s3:ListBucketMultipartUploads | ListMultipartUploads | READ | 存储桶 | | | |

## 列出调用方的访问授权

S3 数据拥有者可以使用 S3 访问权限管控为 Amazon Identity and Access Management（IAM）身份或 Amazon IAM Identity Center 公司目录身份创建访问授权。IAM 身份和 IAM Identity Center 目录身份反过来可以使用 `ListCallerAccessGrants` API 列出这些身份可以访问的所有 Amazon S3 存储桶、前缀和对象，如其 S3 访问权限管控所定义的那样。使用此 API 可以发现 IAM 身份或目录身份可以通过 S3 访问权限管控来访问的所有 S3 数据。

可以使用此功能来构建应用程序，以显示特定最终用户可以访问的数据。例如，适用于 S3 的 Amazon Storage Browser（客户用来访问 S3 存储桶的开源 UI 组件）使用此功能根据最终用户的 S3 访问权限管控，向最终用户提供他们有权在 Amazon S3 中访问的数据。另一个示例是，当构建用于在 Amazon S3 中浏览、上传或下载数据的应用程序时，可以使用此功能在应用程序中构建最终用户可以浏览的树结构。

> **Note**
>
> 对于公司目录身份，在列出调用方的访问权限管控时，S3 访问权限管控将返回用于身份感知会话的 IAM 身份的授权。有关身份感知会话的更多信息，请参阅《Amazon Identity and Access Management 用户指南》中的授予使用身份感知控制台会话的权限。

无论是 IAM 身份还是公司目录身份，被授权者都可以使用 Amazon Command Line Interface（Amazon CLI）、Amazon S3 REST API 和 Amazon SDK 获取其访问授权的列表。

使用 Amazon CLI

要安装 Amazon CLI，请参阅 Amazon Command Line Interface 用户指南中的安装 Amazon CLI。

要使用以下示例命令，请将 *user input placeholders* 替换为您自己的信息。

Example 列出调用方的访问授权

请求:

```
aws s3control list-caller-access-grants \
--account-id 111122223333 \
--region us-east-2
--max-results 5
```

响应:

```
{
 "NextToken": "6J9S...",
 "CallerAccessGrantsList": [
  {
   "Permission": "READWRITE",
   "GrantScope": "s3://amzn-s3-demo-bucket/prefix1/sub-prefix1/*",
   "ApplicationArn": "NA"
  },
  {
   "Permission": "READWRITE",
   "GrantScope": "s3://amzn-s3-demo-bucket/prefix1/sub-prefix2/*",
   "ApplicationArn": "ALL"
  },
  {
   "Permission": "READWRITE",
   "GrantScope": "s3://amzn-s3-demo-bucket/prefix1/sub-prefix3/*",
   "ApplicationArn": "arn:aws:sso::111122223333:application/ssoins-
ssoins-1234567890abcdef/apl-abcd1234a1b2c3d"
  }
 ]
}
```

Example 列出调用方对存储桶的访问授权

可以使用 `grantscope` 参数缩小结果的范围。

请求:

```
aws s3control list-caller-access-grants \
--account-id 111122223333 \
--region us-east-2
--grant-scope "s3://amzn-s3-demo-bucket""
--max-results 1000
```

响应:

```
{
 "NextToken": "6J9S...",
 "CallerAccessGrantsList": [
  {
   "Permission": "READ",
   "GrantScope": "s3://amzn-s3-demo-bucket*",
   "ApplicationArn": "ALL"
  },
  {
   "Permission": "READ",
   "GrantScope": "s3://amzn-s3-demo-bucket/prefix1/*",
   "ApplicationArn": "arn:aws:sso::111122223333:application/ssoins-
ssoins-1234567890abcdef/apl-abcd1234a1b2c3d"
  }
 ]
}
```

使用 REST API

有关 Amazon S3 REST API 支持获取 API 调用方的访问授权列表的信息，请参阅《Amazon Simple Storage Service API 参考》中的 ListCallerAccessGrants。

使用 Amazon SDK

此部分中的示例说明被授权者如何使用 Amazon SDK 从 S3 Access Grants 请求临时凭证。

Java

以下代码示例返回 API 调用方对特定 Amazon Web Services 账户的 S3 数据的访问授权。要使用此代码示例，请将 *user input placeholders* 替换为您自己的信息。

Example 列出调用方的访问授权

请求:

```
Public void ListCallerAccessGrants() {
 ListCallerAccessGrantsRequest listRequest = ListCallerAccessGrantsRequest.builder()
    .withMaxResults(1000)
    .withGrantScope("s3://")
    .accountId("111122223333");
 ListCallerAccessGrantsResponse listResponse =
 s3control.listCallerAccessGrants(listRequest);
 LOGGER.info("ListCallerAccessGrantsResponse: " + listResponse);
 }
```

响应:

```
ListCallerAccessGrantsResponse(
CallerAccessGrantsList=[
 ListCallerAccessGrantsEntry(
  S3Prefix=s3://amzn-s3-demo-bucket/prefix1/,
  Permission=READ,
  ApplicationArn=ALL
 )
])
```

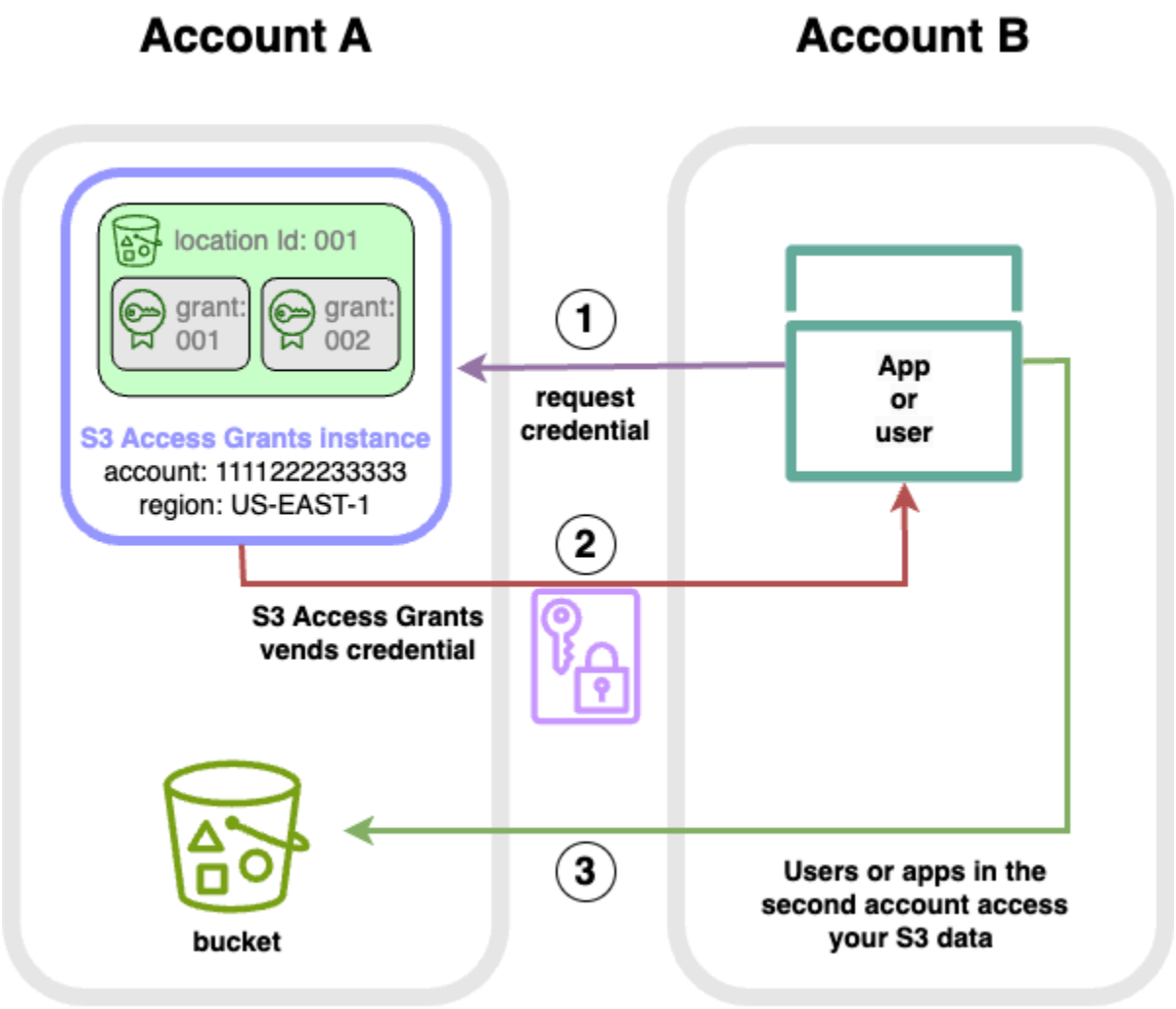
## S3 Access Grants 跨账户访问

利用 S3 Access Grants，您可以授予 Amazon S3 对以下内容的数据访问权限：

- 您账户中的 Amazon Identity and Access Management（IAM）身份
- 其它 Amazon 账户中的 IAM 身份
- 您的 Amazon IAM Identity Center 实例中的目录用户或组

首先，为另一个账户配置跨账户访问。这包括使用资源策略授予对 S3 Access Grants 实例的访问权限。然后，使用授权来授予对您的 S3 数据（存储桶、前缀或对象）的访问权限。

配置跨账户访问后，另一个账户可以从 S3 Access Grants 中请求对您的 Amazon S3 数据的临时访问凭证。下图显示了通过 S3 Access Grants 进行跨账户 S3 访问的用户流程：




1. 第二个账户（B）中的用户或应用程序向账户（A）中存储 Amazon S3 数据的 S3 Access Grants 实例请求凭证。有关更多信息，请参阅 通过 S3 Access Grants 请求访问 Amazon S3 数据。
2. 如果某个授权向第二个账户授予访问您的 Amazon S3 数据的权限，则您的账户（A）中的 S3 Access Grants 实例会返回临时凭证。有关访问授权的更多信息，请参阅在 S3 访问权限管控中处理授权。
3. 第二个账户（B）中的用户或应用程序使用 S3 Access Grants 出售的凭证访问您的账户（A）中的 S3 数据。

## 配置 S3 Access Grants 跨账户访问

要通过 S3 Access Grants 授予跨账户 S3 访问权限，请执行以下步骤：

- 步骤 1：在您的账户（例如，账户 ID 111122223333）中配置在其中存储 S3 数据的 S3 Access Grants 实例。

- 步骤 2：为您的账户 111122223333 中的 S3 Access Grants 实例配置资源策略，来向第二个账户（例如，账户 ID 444455556666）授予访问权限。
- 步骤 3：为第二个账户 444455556666 中的 IAM 主体配置 IAM 权限，以便从您的账户 111122223333 中的 S3 Access Grants 实例请求凭证。
- 步骤 4：在您的账户 111122223333 中创建授权，来向第二个账户 444455556666 中的 IAM 主体授予访问您账户 111122223333 中某些 S3 数据的权限。

### 步骤 1：在您的账户中配置 S3 Access Grants 实例

首先，您的账户 111122223333 中必须有 S3 Access Grants 实例，才能管理对 Amazon S3 数据的访问权限。您必须在存储您要共享的 S3 数据的每个 Amazon Web Services 区域中创建一个 S3 Access Grants 实例。如果您要在多个 Amazon Web Services 区域中共享数据，请为每个 Amazon Web Services 区域重复每个配置步骤。如果您在存储 S3 数据的 Amazon Web Services 区域中已经有一个 S3 Access Grants 实例，请继续下一步。如果您尚未配置 S3 Access Grants 实例，请参阅使用 S3 访问权限管控实例来完成此步骤。

### 步骤 2：配置 S3 Access Grants 实例的资源策略来授予跨账户访问权限

在您的账户 111122223333 中创建 S3 Access Grants 实例来进行跨账户访问后，请为您的账户 111122223333 中的 S3 Access Grants 实例配置基于资源的策略，来授予跨账户访问权限。S3 Access Grants 实例本身支持基于资源的策略。有了正确的基于资源的策略，您就可以向其它 Amazon Web Services 账户中的 Amazon Identity and Access Management（IAM）用户或角色授予对 S3 Access Grants 实例的访问权限。跨账户访问仅授予以下权限（操作）：

- `s3:GetAccessGrantsInstanceForPrefix` – 用户、角色或应用程序可以检索包含特定前缀的 S3 Access Grants 实例。
- `s3:ListAccessGrants`
- `s3:ListAccessLocations`
- `s3:ListCallerAccessGrants`
- `s3:GetDataAccess` – 用户、角色或应用程序可以根据通过 S3 Access Grants 向您授予的访问权限请求临时凭证。使用这些凭证可访问您已获得访问权限的 S3 数据。

您可以选择将其中哪些权限包含在资源策略中。S3 Access Grants 实例上的此资源策略是基于资源的普通策略，支持 IAM 策略语言支持的所有内容。在同一个策略中，例如，您可以使用 `aws:PrincipalArn` 条件向您的账户 111122223333 中的特定 IAM 身份授予访问权限，而不必使用

S3 Access Grants 执行此操作。相反，在您的 S3 Access Grants 实例中，您可以为您账户中的单个 IAM 身份以及其它账户创建授权。通过使用 S3 Access Grants 管理每个访问授权，您可以扩展权限。

如果您已经使用 Amazon Resource Access Manager（Amazon RAM），您可以使用它与其它账户或在您的组织内共享您的 `s3:AccessGrants` 资源。有关更多信息，请参阅使用共享的 Amazon 资源。如果您不使用 Amazon RAM，也可以使用 S3 Access Grants API 操作或 Amazon Command Line Interface（Amazon CLI）来添加资源策略。

使用 S3 控制台

我们建议您使用 Amazon Resource Access Manager（Amazon RAM）控制台与其它账户或在您的组织内共享您的 `s3:AccessGrants` 资源。要跨账户共享 S3 Access Grants，请执行以下操作：

要配置 S3 Access Grants 实例资源策略，请执行以下操作：

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 从 Amazon Web Services 区域选择器中选择 Amazon Web Services 区域。
3. 从左侧导航窗格中，选择 Access Grants。
4. 在 Access Grants 实例页面的此账户中的实例部分，选择共享实例。这会将您重定向至 Amazon RAM 控制台。
5. 选择创建资源共享。
6. 按照 Amazon RAM 步骤创建资源共享。有关更多信息，请参阅 Creating a resource share in Amazon RAM。

使用 Amazon CLI

要安装 Amazon CLI，请参阅 Amazon Command Line Interface 用户指南中的安装 Amazon CLI。

您可以使用 `put-access-grants-instance-resource-policy` CLI 命令添加资源策略。

如果您想将您的账户 `111122223333` 中对于 S3 Access Grants 的跨账户访问权限授予第二个账户 `444455556666`，则您的账户 `111122223333` 中 S3 Access Grants 实例的资源策略应向第二个账户 `444455556666` 授予执行以下操作的权限：

- `s3:ListAccessGrants`
- `s3:ListAccessGrantsLocations`
- `s3:GetDataAccess`

- s3:GetAccessGrantsInstanceForPrefix

在 S3 Access Grants 实例资源策略中，将 S3 Access Grants 实例的 ARN 指定为 Resource，而将第二个账户 444455556666 指定为 Principal。要使用以下示例，请将####### 替换为您自己的信息。

```
{
"Version": "2012-10-17",
"Statement": [
{
 "Effect": "Allow",
 "Principal": {
 "AWS": "444455556666"
},
 "Action": [
  "s3:ListAccessGrants",
  "s3:ListAccessGrantsLocations",
  "s3:GetDataAccess",
  "s3:GetAccessGrantsInstanceForPrefix"
 ],
 "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
} ]
}
```

要添加或更新 S3 Access Grants 实例资源策略，可以使用以下命令。当您使用以下示例命令时，请将 *user input placeholders* 替换为您自己的信息。

Example 添加或更新 S3 Access Grants 实例资源策略

```
aws s3control put-access-grants-instance-resource-policy \
--account-id 111122223333 \
--policy file://resourcePolicy.json \
--region us-east-2
{
 "Policy": "{\n
   \"Version\": \"2012-10-17\",\n
   \"Statement\": [{\n
  \"Effect\": \"Allow\",\n
  \"Principal\": {\n
    \"AWS\": \"444455556666\"\n
  },\n
```

```
   \"Action\": [\n
     \"s3:ListAccessGrants\",\n
     \"s3:ListAccessGrantsLocations\",\n
     \"s3:GetDataAccess\",\n
     \"s3:GetAccessGrantsInstanceForPrefix\",\n
     \"s3:ListCallerAccessGrants"\n
   ],\n
   \"Resource\": \"arn:aws:s3:us-east-2:111122223333:access-grants/default\"\n
     }\n
    ]\n
    }\n",
  "CreatedAt": "2023-06-16T00:07:47.473000+00:00"
 }
```

Example 获取 S3 Access Grants 资源策略

您也可以使用 CLI 来获取或删除 S3 Access Grants 实例的资源策略。

要获取 S3 Access Grants 资源策略，请使用以下示例命令。要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control get-access-grants-instance-resource-policy \
--account-id 111122223333 \
--region us-east-2

{
"Policy": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"Amazon\":\"arn:aws:iam::111122223333:root\"},\"Action\":
[\"s3:ListAccessGrants\",\"s3:ListAccessGrantsLocations\",\"s3:GetDataAccess\",
\"s3:GetAccessGrantsInstanceForPrefix\",\"s3:ListCallerAccessGrants\"],\"Resource\":
\"arn:aws:
s3:us-east-2:111122223333:access-grants/default\"}]}",
"CreatedAt": "2023-06-16T00:07:47.473000+00:00"
}
```

Example 删除 S3 Access Grants 资源策略

要删除 S3 Access Grants 资源策略，请使用以下示例命令。要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control delete-access-grants-instance-resource-policy \
--account-id 111122223333 \
```

```
--region us-east-2

// No response body
```

使用 REST API

您可以使用 PutAccessGrantsInstanceResourcePolicy API 添加资源策略。

如果您想将您的账户 111122223333 中对于 S3 Access Grants 的跨账户访问权限授予第二个账户 444455556666，则您的账户 111122223333 中 S3 Access Grants 实例的资源策略应向第二个账户 444455556666 授予执行以下操作的权限：

- s3:ListAccessGrants
- s3:ListAccessGrantsLocations
- s3:GetDataAccess
- s3:GetAccessGrantsInstanceForPrefix

在 S3 Access Grants 实例资源策略中，将 S3 Access Grants 实例的 ARN 指定为 Resource，而将第二个账户 444455556666 指定为 Principal。要使用以下示例，请将####### 替换为您自己的信息。

```
{
"Version": "2012-10-17",
"Statement": [
{
 "Effect": "Allow",
 "Principal": {
 "AWS": "444455556666"
},
 "Action": [
  "s3:ListAccessGrants",
  "s3:ListAccessGrantsLocations",
  "s3:GetDataAccess",
  "s3:GetAccessGrantsInstanceForPrefix"
 ],
 "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
} ]
}
```

然后，您可以使用 PutAccessGrantsInstanceResourcePolicy API 来配置策略。

有关 REST API 支持更新、获取或删除 S3 Access Grants 实例的资源策略的信息，请参阅《Amazon Simple Storage Service API 参考》中的以下部分：

- PutAccessGrantsInstanceResourcePolicy
- GetAccessGrantsInstanceResourcePolicy
- DeleteAccessGrantsInstanceResourcePolicy

使用 Amazon SDK

本节为您提供 Amazon SDK 示例，说明如何配置 S3 Access Grants 资源策略来向第二个 Amazon 账户授予访问您的某些 S3 数据的权限。

Java

添加、更新、获取或删除资源策略以管理对 S3 Access Grants 实例的跨账户访问。

Example 添加或更新 S3 Access Grants 实例资源策略

如果您想将您的账户 111122223333 中对于 S3 Access Grants 的跨账户访问权限授予第二个账户 444455556666，则您的账户 111122223333 中 S3 Access Grants 实例的资源策略应向第二个账户 444455556666 授予执行以下操作的权限：

- `s3:ListAccessGrants`
- `s3:ListAccessGrantsLocations`
- `s3:GetDataAccess`
- `s3:GetAccessGrantsInstanceForPrefix`

在 S3 Access Grants 实例资源策略中，将 S3 Access Grants 实例的 ARN 指定为 `Resource`，而将第二个账户 444455556666 指定为 `Principal`。要使用以下示例，请将*#######* 替换为您自己的信息。

```
{
"Version": "2012-10-17",
"Statement": [
{
 "Effect": "Allow",
 "Principal": {
 "AWS": "444455556666"
```

```
},
 "Action": [
  "s3:ListAccessGrants",
  "s3:ListAccessGrantsLocations",
  "s3:GetDataAccess",
  "s3:GetAccessGrantsInstanceForPrefix"
 ],
 "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
} ]
}
```

要添加或更新 S3 Access Grants 实例资源策略，请使用以下代码示例：

```
public void putAccessGrantsInstanceResourcePolicy() {
 PutAccessGrantsInstanceResourcePolicyRequest putRequest =
 PutAccessGrantsInstanceResourcePolicyRequest.builder()
 .accountId(111122223333)
 .policy(RESOURCE_POLICY)
 .build();
 PutAccessGrantsInstanceResourcePolicyResponse putResponse =
 s3Control.putAccessGrantsInstanceResourcePolicy(putRequest);
 LOGGER.info("PutAccessGrantsInstanceResourcePolicyResponse: " + putResponse);
 }
```

响应：

```
PutAccessGrantsInstanceResourcePolicyResponse(
 Policy={
 "Version": "2012-10-17",
 "Statement": [{
 "Effect": "Allow",
 "Principal": {
 "Amazon": "444455556666"
 },
 "Action": [
 "s3:ListAccessGrants",
 "s3:ListAccessGrantsLocations",
 "s3:GetDataAccess",
 "s3:GetAccessGrantsInstanceForPrefix",
 "s3:ListCallerAccessGrants"
 ],
 "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
 }]
```

```
 }
 )
```

Example 获取 S3 Access Grants 资源策略

要获取 S3 Access Grants 资源策略，请使用以下代码示例。要使用以下示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
public void getAccessGrantsInstanceResourcePolicy() {
 GetAccessGrantsInstanceResourcePolicyRequest getRequest =
 GetAccessGrantsInstanceResourcePolicyRequest.builder()
 .accountId(111122223333)
 .build();
 GetAccessGrantsInstanceResourcePolicyResponse getResponse =
 s3Control.getAccessGrantsInstanceResourcePolicy(getRequest);
 LOGGER.info("GetAccessGrantsInstanceResourcePolicyResponse: " + getResponse);
 }
```

响应：

```
GetAccessGrantsInstanceResourcePolicyResponse(
 Policy={"Version":"2012-10-17","Statement":[{"Effect":"Allow","Principal":
{"Amazon":"arn:aws:iam::444455556666:root"},"Action":
["s3:ListAccessGrants","s3:ListAccessGrantsLocations","s3:GetDataAccess","s3:GetAccessGrants
east-2:111122223333:access-grants/default"}]},
 CreatedAt=2023-06-15T22:54:44.319Z
 )
```

Example 删除 S3 Access Grants 资源策略

要删除 S3 Access Grants 资源策略，请使用以下代码示例。要使用以下示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
public void deleteAccessGrantsInstanceResourcePolicy() {
 DeleteAccessGrantsInstanceResourcePolicyRequest deleteRequest =
 DeleteAccessGrantsInstanceResourcePolicyRequest.builder()
 .accountId(111122223333)
 .build();
 DeleteAccessGrantsInstanceResourcePolicyResponse deleteResponse =
 s3Control.putAccessGrantsInstanceResourcePolicy(deleteRequest);
 LOGGER.info("DeleteAccessGrantsInstanceResourcePolicyResponse: " + deleteResponse);
```

```
 }
```

响应：

```
DeleteAccessGrantsInstanceResourcePolicyResponse()
```

## 步骤 3：向第二个账户中的 IAM 身份授予在您的账户中调用 S3 Access Grants 实例的权限

在 Amazon S3 数据的拥有者为账户 111122223333 中的 S3 Access Grants 实例配置跨账户策略后，第二个账户 444455556666 的拥有者必须为其 IAM 用户或角色创建基于身份的策略，并且拥有者必须向他们授予访问 S3 Access Grants 实例的权限。在基于身份的策略中，包括以下一项或多项操作，具体取决于在 S3 Access Grants 实例资源策略中授予的权限以及您要授予的权限：

- `s3:ListAccessGrants`
- `s3:ListAccessGrantsLocations`
- `s3:GetDataAccess`
- `s3:GetAccessGrantsInstanceForPrefix`
- `s3:ListCallerAccessGrants`

按照 Amazon 跨账户访问模式，第二个账户 444455556666 中的 IAM 用户或角色必须显式拥有此类权限中的一个或多个。例如，授予 `s3:GetDataAccess` 权限，以便 IAM 用户或角色可以在账户 111122223333 中调用 S3 Access Grants 实例来请求凭证。

要使用此示例命令，请将 *`user input placeholders`* 替换为您自己的信息。

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
  "Effect": "Allow",
  "Action": [
   "s3:GetDataAccess",
  ],
   "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
 }
]
```

```
}
```

有关编辑基于 IAM 身份的策略的信息，请参阅《Amazon Identity and Access Management 指南》中的 Editing IAM policies。

### 步骤 4：在您的账户的 S3 Access Grants 实例中创建授权，来向第二个账户中的 IAM 身份授予访问您的某些 S3 数据的权限

对于最后的配置步骤，您可以在您账户 111122223333 中的 S3 Access Grants 实例中创建一个授权，来向第二个账户 444455556666 中的 IAM 身份授予访问您的账户中某些 S3 数据的权限。您可以使用 Amazon S3 控制台、CLI、API 和 SDK 实现此目的。有关更多信息，请参阅 创建授权。

在授权中，指定第二个账户中 IAM 身份的 Amazon ARN，并指定 S3 数据中您要授予访问权限的具体位置（存储桶、前缀或对象）。此位置必须已在 S3 Access Grants 实例中注册。有关更多信息，请参阅 注册位置。您可以选择指定子前缀。例如，如果您授予访问权限的位置是存储桶，并且您想进一步限制对该存储桶中特定对象的访问权限，则在 `S3SubPrefix` 字段中传递对象键名称。或者，如果您想使用以特定前缀（例如 `2024-03-research-results/`）开头的键名称来限制对存储桶中对象的访问权限，则传递 `S3SubPrefix=2024-03-research-results/`。

以下是用于为第二个账户中的身份创建访问授权的 CLI 命令示例。请参阅创建授权了解更多信息。要使用此示例命令，请将 *`user input placeholders`* 替换为您自己的信息。

```
aws s3control create-access-grant \
--account-id 111122223333 \
--access-grants-location-id default \
--access-grants-location-configuration S3SubPrefix=prefixA* \
--permission READ \
--grantee GranteeType=IAM,GranteeIdentifier=arn:aws:iam::444455556666:role/data-
consumer-1
```

配置跨账户访问后，第二个账户中的用户或角色可以执行以下操作：

- 通过 Amazon RAM 调用 `ListAccessGrantsInstances` 来列出与其共享的 S3 Access Grants 实例。有关更多信息，请参阅 获取 S3 访问权限管控实例的详细信息。
- 从 S3 Access Grants 请求临时凭证。有关如何发出这些请求的更多信息，请参阅通过 S3 Access Grants 请求访问 Amazon S3 数据。

# 将 Amazon 标签与 S3 Access Grants 配合使用

Amazon S3 Access Grants 中的标签与 Amazon S3 中的对象标签具有相似的特征。每个标签都是一个键-值对。您可以在 S3 Access Grants 中标记的资源是 S3 Access Grants 实例、位置和授权。

> **Note**
>
> S3 Access Grants 中的标记使用与对象标记不同的 API 操作。S3 Access Grants 使用 TagResource、UntagResource 和 ListTagsForResource API 操作，其中资源可以是 S3 Access Grants 实例、已注册位置或访问授权。

与对象标签类似，以下限制将适用：

- 可以在创建新的 S3 Access Grants 资源时向其添加标签，也可以向现有资源添加标签。
- 您最多可以将 10 个标签与一个资源关联。如果多个标签与同一资源关联，则它们必须具有唯一的标签键。
- 标签键的长度最大可以为 128 个 Unicode 字符，标签值的长度最大可以为 256 个 Unicode 字符。标签在内部以 UTF-16 表示。采用 UTF-16 时，字符占用 1 或 2 个字符位置。
- 键和值区分大小写。

有关标签限制的更多信息，请参阅《Amazon Billing 用户指南》中的用户定义的标签限制。

您可以使用 Amazon Command Line Interface（Amazon CLI）、Amazon S3 REST API 或 Amazon SDK 在 S3 Access Grants 中标记资源。

使用 Amazon CLI

要安装 Amazon CLI，请参阅 Amazon Command Line Interface 用户指南中的安装 Amazon CLI。

可以在创建 S3 Access Grants 资源时或之后为其添加标签。以下示例说明如何标记或取消标记 S3 Access Grants 实例。可以为已注册位置和访问授权执行类似的操作。

要使用以下示例命令，请将 *user input placeholders* 替换为您自己的信息。

Example – 创建带标签的 S3 Access Grants 实例

```
aws s3control create-access-grants-instance \
 --account-id 111122223333 \
```

```
 --profile access-grants-profile \
 --region us-east-2 \
 --tags Key=tagKey1,Value=tagValue1
```

响应：

```
 {
    "CreatedAt": "2023-10-25T01:09:46.719000+00:00",
    "AccessGrantsInstanceId": "default",
    "AccessGrantsInstanceArn": "arn:aws:s3:us-east-2:111122223333:access-grants/
default"
}
```

Example – 标记已创建的 S3 Access Grants 实例

```
aws s3control tag-resource \
--account-id 111122223333 \
--resource-arn "arn:aws:s3:us-east-2:111122223333:access-grants/default" \
--profile access-grants-profile \
--region us-east-2 \
--tags Key=tagKey2,Value=tagValue2
```

Example – 列出 S3 Access Grants 实例的标签

```
aws s3control list-tags-for-resource \
--account-id 111122223333 \
--resource-arn "arn:aws:s3:us-east-2:111122223333:access-grants/default" \
--profile access-grants-profile \
--region us-east-2
```

响应：

```
{
    "Tags": [
        {
            "Key": "tagKey1",
            "Value": "tagValue1"
        },
        {
            "Key": "tagKey2",
            "Value": "tagValue2"
        }
```

```
    ]
}
```

Example – 取消标记 S3 Access Grants 实例

```
aws s3control untag-resource \
 --account-id 111122223333 \
 --resource-arn "arn:aws:s3:us-east-2:111122223333:access-grants/default" \
 --profile access-grants-profile \
 --region us-east-2 \
 --tag-keys "tagKey2"
```

使用 REST API

可以使用 Amazon S3 API 来标记、取消标记 S3 Access Grants 实例、已注册位置或访问授权，或列出这些项的标签。有关用于管理 S3 Access Grants 标签的 REST API 支持的信息，请参阅《Amazon Simple Storage Service API 参考》中的以下部分：

- TagResource
- UntagResource
- ListTagsForResource

## S3 Access Grants 限制

S3 Access Grants 具有以下限制：

> **Note**
>
> 如果您的使用场景超出了这些限制，请联系 Amazon 支持以请求提高限制。

S3 Access Grants 实例

您的每个账户在每个 Amazon Web Services 区域中可创建 1 个 S3 Access Grants 实例。请参阅创建 S3 Access Grants 实例。

S3 Access Grants 位置

您可以为每个 S3 Access Grants 实例注册 1000 个 S3 Access Grants 位置。请参阅注册 S3 Access Grants 位置。

授权

可以为每个 S3 Access Grants 实例创建 10 万个授权。请参阅创建授权。

## S3 访问权限管控 Amazon Web Services 区域

S3 访问权限管控目前在以下 Amazon Web Services 区域中可用：

| Amazon Web Services 区域 代码 | Amazon Web Services 区域 名称 |
|---|---|
| us-east-1 | 美国东部（弗吉尼亚州北部） |
| us-east-2 | 美国东部（俄亥俄州） |
| us-west-1 | 美国西部（加利福尼亚北部） |
| us-west-2 | 美国西部（俄勒冈州） |
| af-south-1 | 非洲（开普敦） |
| ap-east-1 | 亚太地区（香港） |
| ap-northeast-1 | 亚太地区（东京） |
| ap-northeast-2 | 亚太地区 (首尔) |
| ap-northeast-3 | 亚太地区（大阪） |
| ap-south-1 | 亚太地区（孟买） |
| ap-south-2 | 亚太地区（海得拉巴） |
| ap-southeast-1 | 亚太地区（新加坡） |
| ap-southeast-2 | 亚太地区（悉尼） |
| ap-southeast-3 | 亚太地区（雅加达） |
| ap-southeast-4 | 亚太地区（墨尔本） |

| Amazon Web Services 区域 代码 | Amazon Web Services 区域 名称 |
| --- | --- |
| ca-central-1 | 加拿大（中部） |
| ca-west-1 | 加拿大西部（卡尔加里） |
| eu-central-1 | 欧洲地区（法兰克福） |
| eu-central-2 | 欧洲（苏黎世） |
| eu-north-1 | 欧洲地区（斯德哥尔摩） |
| eu-south-1 | 欧洲地区（米兰） |
| eu-south-2 | 欧洲（西班牙） |
| eu-west-1 | 欧洲地区（爱尔兰） |
| eu-west-2 | 欧洲地区（伦敦） |
| eu-west-3 | 欧洲地区（巴黎） |
| il-central-1 | 以色列（特拉维夫） |
| me-central-1 | 中东（阿联酋） |
| me-south-1 | 中东（巴林） |
| sa-east-1 | 南美洲（圣保罗） |
| us-gov-east-1 | Amazon GovCloud（美国东部） |
| us-gov-west-1 | Amazon GovCloud（美国西部） |

## S3 Access Grants 集成

S3 Access Grants 可与以下 Amazon 服务和功能结合使用。在提供了新的集成时，此页面将更新。

Amazon Athena

使用已启用 IAM Identity Center 的 Athena 工作组

Amazon EMR

使用 S3 Access Grants 启动 Amazon EMR 集群

Amazon EMR on EKS

使用 S3 Access Grants 启动 Amazon EMR on EKS 集群

Amazon EMR Serverless 应用程序

使用 S3 Access Grants 启动 Amazon EMR Serverless 应用程序

Amazon Redshift

Amazon Redshift integration with Amazon S3 Access Grants

Amazon SageMaker AI Studio

将 Amazon S3 访问权限管控与 Amazon SageMaker AI Studio 和适用于 Python 的 SDK（Boto3）插件结合使用

使用适用于 Python 的 SDK（Boto3）插件时，在 Amazon SageMaker AI Studio 笔记本中使用 S3 访问权限管控现在变得更容易了。事先为 IAM 主体和 Amazon IAM Identity Center 目录用户设置访问授权。尽管 Amazon SageMaker AI Studio 并不原生支持身份提供者目录用户，但您可以使用支持这些身份通过 S3 访问权限管控访问 S3 数据的插件，来编写自定义 Python 代码。数据访问是在该插件的协助下进行的，而不是通过 Amazon SageMaker AI 进行的。

Amazon Glue

将 Amazon S3 访问权限管控与 Amazon Glue 结合使用

Amazon IAM Identity Center

跨应用程序的可信身份传播

Amazon Transfer Family

为 Amazon Transfer Family Configure Amazon S3 Access Grants

适用于 S3 的存储浏览器

使用适用于 S3 的存储浏览器大规模管理数据访问权限

开源 Python 框架

Amazon S3 访问权限管控现已与开源 Python 框架集成

# 使用 ACL 管理访问

访问控制列表（ACL）是基于资源的选项之一，可用于管理对存储桶和对象的访问。您可以使用 ACL 向其他 Amazon Web Services 账户授予基本的读/写权限。使用 ACL 管理权限有一些限制。

例如，您可以仅向其他 Amazon Web Services 账户授予权限；您无法向您账户中的用户授予权限。无法授予条件性权限，也无法显式拒绝权限。ACL 适用于特定情景。例如，如果存储桶拥有者允许其他 Amazon Web Services 账户上传对象，则对这些对象的权限只能由拥有此对象的 Amazon Web Services 账户使用对象 ACL 加以管理。

S3 对象所有权是 Amazon S3 存储桶级别的设置，您可以使用该设置来控制上传到存储桶的对象的所有权和禁用或启用 ACL。默认情况下，对象所有权设为强制存储桶拥有者设置，并且所有 ACL 均处于禁用状态。禁用 ACL 后，存储桶拥有者拥有存储桶中的所有对象，并使用访问管理策略来专门管理对这些对象的访问权限。

Amazon S3 中的大多数现代使用案例不再需要使用 ACL。我们建议您将 ACL 保持为禁用状态，除非有需要单独控制每个对象的访问权限的特殊情况。禁用 ACL 后，您可以使用策略来控制对存储桶中所有对象的访问权限，无论是谁将对象上传到您的存储桶。有关更多信息，请参阅 为您的存储桶控制对象所有权和禁用 ACL。。

> **Important**
>
> 如果通用存储桶针对 S3 对象所有权使用强制存储桶拥有者设置，则必须使用策略来授予对通用存储桶及其中对象的访问权限。启用强制存储桶拥有者设置后，设置访问控制列表（ACL）或更新 ACL 的请求将失败并返回 `AccessControlListNotSupported` 错误代码。仍然支持读取 ACL 的请求。

有关 ACL 的更多信息，请参阅以下主题：

主题

- 访问控制列表 (ACL) 概述
- 配置 ACL
- 适用于 ACL 的策略示例

# 访问控制列表 (ACL) 概述

Amazon S3 访问控制列表（ACL）使您可以管理存储桶和对象的访问权限。每个存储桶和对象都有一个作为子资源而附加的 ACL。它定义了哪些 Amazon Web Services 账户或组将被授予访问权限以及访问的类型。收到针对某个资源的请求后，Amazon S3 将检查相应的 ACL 以验证请求者是否拥有所需的访问权限。

S3 对象所有权是 Amazon S3 存储桶级别的设置，您可以使用该设置来控制上传到存储桶的对象的所有权和禁用或启用 ACL。默认情况下，对象所有权设为强制存储桶拥有者设置，并且所有 ACL 均处于禁用状态。禁用 ACL 后，存储桶拥有者拥有存储桶中的所有对象，并使用访问管理策略来专门管理对这些对象的访问权限。

Amazon S3 中的大多数现代使用案例不再需要使用 ACL。我们建议您将 ACL 保持为禁用状态，除非有需要单独控制每个对象的访问权限的特殊情况。禁用 ACL 后，您可以使用策略来控制对存储桶中所有对象的访问权限，无论是谁将对象上传到您的存储桶。有关更多信息，请参阅 为您的存储桶控制对象所有权和禁用 ACL。。

> **Important**
>
> 如果通用存储桶针对 S3 对象所有权使用强制存储桶拥有者设置，则必须使用策略来授予对通用存储桶及其中对象的访问权限。启用强制存储桶拥有者设置后，设置访问控制列表（ACL）或更新 ACL 的请求将失败并返回 `AccessControlListNotSupported` 错误代码。仍然支持读取 ACL 的请求。

创建存储桶或对象时，Amazon S3 将创建一个默认 ACL 以授予资源拥有者对资源的完全控制权限。这显示在下面的示例存储桶 ACL 中（默认对象 ACL 具有相同的结构）：

Example

```
<?xml version="1.0" encoding="UTF-8"?>
<AccessControlPolicy xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Owner>
    <ID>*** Owner-Canonical-User-ID ***</ID>
    <DisplayName>owner-display-name</DisplayName>
  </Owner>
  <AccessControlList>
    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
                xsi:type="Canonical User">
        <ID>*** Owner-Canonical-User-ID ***</ID>
        <DisplayName>display-name</DisplayName>
      </Grantee>
      <Permission>FULL_CONTROL</Permission>
    </Grant>
  </AccessControlList>
</AccessControlPolicy>
```

示例 ACL 包含一个可通过 Amazon Web Services 账户的规范用户 ID 识别拥有者的 `Owner` 元素。有关查找规范用户 ID 的说明，请参阅查找 Amazon Web Services 账户规范用户 ID。`Grant` 元素将识别被授权者（Amazon Web Services 账户或预定义的组）和所授予的权限。此默认的 ACL 拥有一个适用于所有者的 `Grant` 元素。您可以通过添加 `Grant` 元素授予权限，每个授权都将识别被授权者和权限。

> **Note**
>
> ACL 可以拥有最多 100 个授权。

主题


- 谁是被授权者？
- 我能授予哪些许可？
- 常见 Amazon S3 请求的 aclRequired 值
- 示例 ACL
- 标准 ACL


## 谁是被授权者？

> **Important**
>
> 终止支持通知：从 2025 年 10 月 1 日起，Amazon S3 将停止支持创建新的电子邮件受让者访问控制列表（ACL）。在此日期之前创建的电子邮件受让者 ACL 将继续有效，并且仍可通过 Amazon 管理控制台、命令行界面（CLI）、SDK 和 REST API 进行访问。但是，届时您将无法再创建新的电子邮件受让者 ACL。
>
> 在 2025 年 7 月 1 日至 2025 年 10 月 1 日之间，当您尝试创建新的电子邮件受让者 ACL 时，您将开始看到向 Amazon S3 发出的请求的 `HTTP 405` 错误率上升。

此更改影响以下 Amazon Web Services 区域：美国东部（弗吉尼亚州北部）、美国西部（北加利福尼亚）、美国西部（俄勒冈州）、亚太地区（新加坡）、亚太地区（悉尼）、亚太地区（东京)、欧洲地区（爱尔兰）和南美洲（圣保罗）。

被授权者可以是 Amazon Web Services 账户或某个预定义的 Amazon S3 组。您可以使用电子邮件地址或规范用户 ID 向 Amazon Web Services 账户授予权限。但是，如果您在授权请求中提供电子邮件地址，Amazon S3 将为该账户查找规范用户 ID 并将它添加到 ACL。生成的 ACL 始终包含 Amazon Web Services 账户的规范用户 ID，而不是 Amazon Web Services 账户的电子邮件地址。

授予访问权限时，可以将每个被授权者指定为一个 *type*="*value*" 对，其中 *type* 为以下值之一：

- `id` – 如果指定的值是 Amazon Web Services 账户的规范用户 ID
- `uri` – 如果您正在向预定义组授予权限
- `emailAddress` – 如果指定的值是 Amazon Web Services 账户的电子邮件地址

**Important**

仅以下 Amazon 区域中支持使用电子邮件地址指定被授权者：

- 美国东部（弗吉尼亚北部）
- 美国西部（加利福尼亚北部）
- 美国西部（俄勒冈）
- 亚太地区（新加坡）
- 亚太地区（悉尼）
- 亚太地区（东京）
- 欧洲（爱尔兰）
- 南美洲（圣保罗）

有关 Amazon S3 支持的所有区域和端点的列表，请参阅《Amazon Web Services 一般参考》中的区域和端点。

Example 示例：电子邮件地址

例如，以下 `x-amz-grant-read` 标头向由电子邮件地址标识的 Amazon Web Services 账户授予读取对象数据及其元数据的权限：

```
x-amz-grant-read: emailAddress="xyz@example.com", emailAddress="abc@example.com"
```

> **Warning**
>
> 当您需要向其他 Amazon Web Services 账户授权访问您的资源时，注意 Amazon Web Services 账户可以向其账户下的用户授予权限。这称为跨账户访问。有关使用跨账户访问的信息，请参阅 IAM 用户指南中的创建角色以向 IAM 用户委派权限。

查找 Amazon Web Services 账户规范用户 ID

规范用户 ID 与您的 Amazon Web Services 账户关联。此 ID 是一个长串字符，例如：

`79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be`

有关如何查找您账户的规范用户 ID 的信息，请参阅《Amazon 账户管理参考指南》中的 Find the canonical user ID for your Amazon Web Services 账户。

您也可以通过读取 Amazon Web Services 账户 有权访问的存储桶或对象的 ACL，查找 Amazon Web Services 账户 的规范用户 ID。如果某个 Amazon Web Services 账户通过授权请求被授予了许可，ACL 中将新增一个授权条目和账户的规范用户 ID。

> **Note**
>
> 如果您公开存储桶（不建议），则任何未经身份验证的用户都可以将对象上传到该存储桶。这些匿名用户没有 Amazon Web Services 账户。当匿名用户将对象上传到您的存储桶时，Amazon S3 会在 ACL 中添加特殊的规范用户 ID（`65a011a29cdf8ec533ec3d1ccaae921c`）作为对象拥有者。有关更多信息，请参阅 Amazon S3 存储桶和对象所有权。

Amazon S3 预定义的组

Amazon S3 拥有一系列预定义的组。将账户访问权限授予某个组时，您可以指定我们的一个 Amazon S3 URI，而不是规范用户 ID。Amazon S3 提供以下预定义组：

- “经身份验证的用户”组 – 由 `http://acs.amazonaws.com/groups/global/AuthenticatedUsers` 表示。

  该组代表了所有 Amazon Web Services 账户。该组的访问权限允许任何 Amazon Web Services 账户 访问资源。但是，所有的请求必须是已签名的 (经身份验证)。

  > **Warning**
  >
  > 在您向经身份验证的用户组授予访问权限后，世界上任何经身份验证的 Amazon 用户都可以访问您的资源。

- “所有用户”组 – 由 `http://acs.amazonaws.com/groups/global/AllUsers` 表示。

  授予此组的访问权限将允许世界上的任何人访问资源。请求可以是已签名的 (经身份验证)，也可以是未签名的 (匿名)。未签名的请求将省略请求中的 Authentication 标头。

  > **Warning**
  >
  > 强烈建议您绝不要向 All Users 组授予 `WRITE`、`WRITE_ACP` 或 `FULL_CONTROL` 权限。例如，尽管 `WRITE` 权限拒绝非拥有者覆盖或删除现有对象的功能，但 `WRITE` 权限仍支持任何人在您的存储桶中存储对象，而您需要为此付费。有关这些权限的详细信息，请参阅下一节 我能授予哪些许可？。

- “日志传输”组 – 由 `http://acs.amazonaws.com/groups/s3/LogDelivery` 表示。

  对于存储桶的 `WRITE` 权限使该组可以将服务器访问日志（请参阅使用服务器访问日志记录来记录请求）写入存储桶。

> **Note**
>
> 使用 ACL 时，被授权者可以是 Amazon Web Services 账户或者某个预定义的 Amazon S3 组。但是，被授权者不能是 IAM 用户。有关 IAM 中 Amazon 用户和权限的更多信息，请参阅使用 Amazon Identity and Access Management。

## 我能授予哪些许可？

下表列出了 Amazon S3 在 ACL 中支持的权限集。对于对象 ACL 和存储桶 ACL，ACL 权限集相同。但是，根据上下文（存储桶 ACL 或对象 ACL），这些 ACL 权限将授予针对特定存储桶或对象操作的权限。下表列出了权限并描述这些权限在对象和存储桶上下文中的意义。

有关使用 Amazon S3 控制台 ACL 权限的更多信息，请参阅 配置 ACL。

| 许可 | 在存储桶上授权的时间 | 在对象上授权的时间 |
| --- | --- | --- |
| READ | 允许被授权者列出存储桶中的对象 | 允许被授权者读取对象数据及其元数据 |
| WRITE | 允许被授权者在存储桶中创建新对象。对于现有对象的存储桶和对象拥有者，还允许删除和覆写这些对象 | 不适用 |
| READ_ACP | 允许被授权者读取存储桶 ACL | 允许被授权者读取对象 ACL |
| WRITE_ACP | 允许被授权者为适用的存储桶编写 ACL | 允许被授权者为适用的对象编写 ACL |
| FULL_CONTROL | 允许被授予者对存储桶拥有 READ、WRITE、READ_ACP 和 WRITE_ACP 权限 | 允许被授予者对于对象拥有 READ、READ_ACP 和 WRITE_ACP 权限 |

> **Warning**
>
> 在授予对您的 S3 存储桶和对象的访问权限时应谨慎使用。例如，授予对存储桶的 WRITE 权限将允许被授权者创建存储桶中的任何对象。我们强烈建议您在授予权限之前通读整个访问控制列表 (ACL) 概述部分。

### ACL 权限和访问策略权限的映射

如先前表中所示，相比于在访问策略中可设置的权限数目（请参阅Amazon S3 的策略操作），ACL 仅允许授予有限数量的权限。其中的每个权限允许一个或多个 Amazon S3 操作。

下表显示每个 ACL 权限如何映射到相应的访问策略权限。正如您所见，与 ACL 相比，访问策略允许的权限更多。您可以将 ACL 主要用于授予基本的读/写权限（类似于文件系统权限）。有关何时使用 ACL 的更多信息，请参阅 Amazon S3 的身份和访问管理。

有关使用 Amazon S3 控制台 ACL 权限的更多信息，请参阅 配置 ACL。

| ACL 权限 | 当在存储桶上授予 ACL 权限时的相应访问策略 | 当在对象上授予 ACL 权限时的相应访问策略 |
| --- | --- | --- |
| READ | s3:ListBucket 、s3:ListBucketVersions 和 s3:ListBucketMultipartUploads | s3:GetObject 和 s3:GetObjectVersion |
| WRITE | s3:PutObject<br><br>存储桶拥有者可以创建、覆写和删除存储桶中的任何对象，而对象拥有者对其对象拥有 FULL_CONTROL 。<br><br>此外，如果被授权者是存储桶拥有者，使用存储桶 ACL 来授予 WRITE 许可将允许对该存储桶中的任意版本执行 s3:DeleteObjectVersion 操作。 | 不适用 |
| READ_ACP | s3:GetBucketAcl | s3:GetObjectAcl 和 s3:GetObjectVersionAcl |
| WRITE_ACP | s3:PutBucketAcl | s3:PutObjectAcl 和 s3:PutObjectVersionAcl |
| FULL_CONTROL | 等同于授予 READ、WRITE、READ_ACP 和 WRITE_ACP ACL 权限。因此，此 ACL 权限将映射到相应访问策略权限的组合。 | 等同于授予 READ、READ_ACP 和 WRITE_ACP ACL 权限。因此，此 ACL 权限将映射到相应访问策略权限的组合。 |

条件键

授予访问策略权限时，您可以使用条件键通过存储桶策略对某个对象限制 ACL 的值。以下上下文键对应于 ACL。您可以使用这些上下文键强制在请求中使用特定 ACL：

- `s3:x-amz-grant-read` - 需要读取访问权限。
- `s3:x-amz-grant-write` - 需要写入访问权限。
- `s3:x-amz-grant-read-acp` - 需要对存储桶 ACL 的读取访问权限。
- `s3:x-amz-grant-write-acp` - 需要对存储桶 ACL 的写入访问权限。
- `s3:x-amz-grant-full-control` - 需要完全控制权限。
- `s3:x-amz-acl` - 需要一个 标准 ACL。

有关涉及 ACL 特定标头的策略示例，请参阅授予 s3:PutObject 权限，指定了要求存储桶拥有者获得完全控制的条件。有关 Amazon S3 特定条件键的完整列表，请参阅《Service Authorization Reference》中的 Actions, resources, and condition keys for Amazon S3。

有关按 S3 资源类型对 S3 API 操作的权限的更多信息，请参阅 Amazon S3 API 操作所需的权限。

## 常见 Amazon S3 请求的 **`aclRequired`** 值

要识别需要 ACL 进行授权的 Amazon S3 请求，您可以使用 Amazon S3 服务器访问日志或 Amazon CloudTrail 中的 `aclRequired` 值。CloudTrail 或 Amazon S3 服务器访问日志中显示的 `aclRequired` 值取决于调用了哪些操作以及有关请求者、对象拥有者和存储桶拥有者的某些信息。如果不需要 ACL，或者您正在设置 `bucket-owner-full-control` 标准 ACL，或者如果您的存储桶策略允许请求，则 Amazon S3 服务器访问日志中的 `aclRequired` 值字符串为“-”，但 CloudTrail 中不存在该值字符串。

下表列出了 CloudTrail 或 Amazon S3 服务器访问日志中各种 Amazon S3 API 操作的预期 `aclRequired` 值。您可以使用此信息来了解哪些 Amazon S3 操作依赖于 ACL 进行授权。在下表中，A、B 和 C 代表与请求者、对象拥有者和存储桶拥有者关联的不同账户。带有星号（*）的条目表示账户 A、B 或 C 中的任意一个。

> **Note**
>
> 除非另有说明，否则下表中的 `PutObject` 操作表示未设置 ACL 的请求，除非该 ACL 是 `bucket-owner-full-control` ACL。`aclRequired` 为 null 值表示 Amazon CloudTrail 日志中不存在 `aclRequired`。

下表显示 CloudTrail 的 `aclRequired` 值。

| 操作名称 | 请求者 | 对象拥有者 | 存储桶拥有者 | 存储桶策略授予访问权限 | **aclRequired 值** | Reason |
|---|---|---|---|---|---|---|
| GetObject | A | A | A | 是或否 | null | 同一账户的访问 |
| GetObject | A | B | A | 是或否 | null | 强制存储桶拥有者的同账户访问 |
| GetObject | A | A | B | 是 | null | 存储桶策略授予的跨账户访问 |
| GetObject | A | A | B | 否 | 是 | 跨账户访问依赖于 ACL |
| GetObject | A | A | B | 是 | null | 存储桶策略授予的跨账户访问 |
| GetObject | A | B | B | 否 | 是 | 跨账户访问依赖于 ACL |
| GetObject | A | B | C | 是 | null | 存储桶策略授予的跨账户访问 |
| GetObject | A | B | C | 否 | 是 | 跨账户访问依赖于 ACL |
| PutObject | A | 不适用 | A | 是或否 | null | 同一账户的访问 |

| 操作名称 | 请求者 | 对象拥有者 | 存储桶拥有者 | 存储桶策略授予访问权限 | **aclRequired** 值 | Reason |
|---|---|---|---|---|---|---|
| PutObject | A | 不适用 | B | 是 | null | 存储桶策略授予的跨账户访问 |
| PutObject | A | 不适用 | B | 否 | 是 | 跨账户访问依赖于 ACL |
| 使用 ACL 的 PutObject（bucket-owner-full-control 除外） | * | 不适用 | * | 是或否 | 是 | 请求授予 ACL |
| ListObjects | A | 不适用 | A | 是或否 | null | 同一账户的访问 |
| ListObjects | A | 不适用 | B | 是 | null | 存储桶策略授予的跨账户访问 |
| ListObjects | A | 不适用 | B | 否 | 是 | 跨账户访问依赖于 ACL |
| DeleteObject | A | 不适用 | A | 是或否 | null | 同一账户的访问 |
| DeleteObject | A | 不适用 | B | 是 | null | 存储桶策略授予的跨账户访问 |

| 操作名称 | 请求者 | 对象拥有者 | 存储桶拥有者 | 存储桶策略授予访问权限 | **aclRequired 值** | Reason |
|---|---|---|---|---|---|---|
| DeleteObject | A | 不适用 | B | 否 | 是 | 跨账户访问依赖于 ACL |
| PutObjectAcl | * | * | * | 是或否 | 是 | 请求授予 ACL |
| PutBucketAcl | * | 不适用 | * | 是或否 | 是 | 请求授予 ACL |

> **Note**
>
> 除非另有说明，否则下表中的 REST.PUT.OBJECT 操作表示未设置 ACL 的请求，除非该 ACL 是 bucket-owner-full-control ACL。aclRequired 值字符串为“-”表示 Amazon S3 服务器访问日志中的 null 值。

下表显示 Amazon S3 服务器访问日志的 aclRequired 值。

| 操作名称 | 请求者 | 对象拥有者 | 存储桶拥有者 | 存储桶策略授予访问权限 | **aclRequired 值** | Reason |
|---|---|---|---|---|---|---|
| REST.GET.OBJECT | A | A | A | 是或否 | - | 同一账户的访问 |
| REST.GET.OBJECT | A | B | A | 是或否 | - | 强制存储桶拥有者的同账户访问 |

| 操作名称 | 请求者 | 对象拥有者 | 存储桶拥有者 | 存储桶策略授予访问权限 | **aclRequired** 值 | Reason |
|---|---|---|---|---|---|---|
| REST.GET.OBJECT | A | A | B | 是 | - | 存储桶策略授予的跨账户访问 |
| REST.GET.OBJECT | A | A | B | 否 | 是 | 跨账户访问依赖于 ACL |
| REST.GET.OBJECT | A | B | B | 是 | - | 存储桶策略授予的跨账户访问 |
| REST.GET.OBJECT | A | B | B | 否 | 是 | 跨账户访问依赖于 ACL |
| REST.GET.OBJECT | A | B | C | 是 | - | 存储桶策略授予的跨账户访问 |
| REST.GET.OBJECT | A | B | C | 否 | 是 | 跨账户访问依赖于 ACL |
| REST.PUT.OBJECT | A | 不适用 | A | 是或否 | - | 同一账户的访问 |
| REST.PUT.OBJECT | A | 不适用 | B | 是 | - | 存储桶策略授予的跨账户访问 |
| REST.PUT.OBJECT | A | 不适用 | B | 否 | 是 | 跨账户访问依赖于 ACL |

| 操作名称 | 请求者 | 对象拥有者 | 存储桶拥有者 | 存储桶策略授予访问权限 | **aclRequired** 值 | Reason |
|---|---|---|---|---|---|---|
| 使用 ACL 的 REST.PUT.OBJECT （bowner-full-control 除外） | * | 不适用 | * | 是或否 | 是 | 请求授予 ACL |
| REST.GET.BUCKET | A | 不适用 | A | 是或否 | - | 同一账户的访问 |
| REST.GET.BUCKET | A | 不适用 | B | 是 | - | 存储桶策略授予的跨账户访问 |
| REST.GET.BUCKET | A | 不适用 | B | 否 | 是 | 跨账户访问依赖于 ACL |
| REST.DELETE.OBJECT | A | 不适用 | A | 是或否 | - | 同一账户的访问 |
| REST.DELETE.OBJECT | A | 不适用 | B | 是 | - | 存储桶策略授予的跨账户访问 |
| REST.DELETE.OBJECT | A | 不适用 | B | 否 | 是 | 跨账户访问依赖于 ACL |
| REST.PUT.ACL | * | * | * | 是或否 | 是 | 请求授予 ACL |

## 示例 ACL

下面的存储桶上的示例 ACL 可识别资源所有者和一系列的授权。格式是指 Amazon S3 REST API 中的 ACL 的 XML 表示形式。存储桶拥有者拥有资源的 FULL_CONTROL。此外，ACL 还演示了如何将对于某个资源的权限授予两个 Amazon Web Services 账户（由规范用户 ID 标识）以及上一节讨论的两个预定义 Amazon S3 组。

Example

```
<?xml version="1.0" encoding="UTF-8"?>
<AccessControlPolicy xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Owner>
    <ID>Owner-canonical-user-ID</ID>
    <DisplayName>display-name</DisplayName>
  </Owner>
  <AccessControlList>
    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:type="CanonicalUser">
        <ID>Owner-canonical-user-ID</ID>
        <DisplayName>display-name</DisplayName>
      </Grantee>
      <Permission>FULL_CONTROL</Permission>
    </Grant>

    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:type="CanonicalUser">
        <ID>user1-canonical-user-ID</ID>
        <DisplayName>display-name</DisplayName>
      </Grantee>
      <Permission>WRITE</Permission>
    </Grant>

    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:type="CanonicalUser">
        <ID>user2-canonical-user-ID</ID>
        <DisplayName>display-name</DisplayName>
      </Grantee>
      <Permission>READ</Permission>
    </Grant>
```

```
    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="Group">
        <URI>http://acs.amazonaws.com/groups/global/AllUsers</URI>
      </Grantee>
      <Permission>READ</Permission>
    </Grant>
    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="Group">
        <URI>http://acs.amazonaws.com/groups/s3/LogDelivery</URI>
      </Grantee>
      <Permission>WRITE</Permission>
    </Grant>

  </AccessControlList>
</AccessControlPolicy>
```

## 标准 ACL

Amazon S3 支持一系列预定义的授权，称为标准 ACL。每个标准 ACL 都有一组预定义的被授权者和许可。下表列出了一系列标准 ACL 和相关联的预定义授权。

| 标准 ACL | 适用于 | 添加到 ACL 的权限 |
| --- | --- | --- |
| `private` | 存储桶和对象 | 所有者将获得 `FULL_CONTROL` 。其他人没有访问权限 (默认)。 |
| `public-read` | 存储桶和对象 | 所有者将获得 `FULL_CONTROL` 。`AllUsers` 组 (参阅 谁是被授权者？) 将获得 `READ` 访问权限。 |
| `public-read-write` | 存储桶和对象 | 所有者将获得 `FULL_CONTROL` 。`AllUsers` 组将获得 `READ` 和 `WRITE` 访问权限。通常不建议在存储桶上授予该权限。 |
| `aws-exec-read` | 存储桶和对象 | 所有者将获得 `FULL_CONTROL` 。Amazon EC2 从 Amazon S3 获取对 `READ` Amazon Machine Image (AMI) 服务包的 `GET` 访问权限。 |
| `authenticated-read` | 存储桶和对象 | 所有者将获得 `FULL_CONTROL` 。`AuthenticatedUsers` 组将获得 `READ` 访问权限。 |

| 标准 ACL | 适用于 | 添加到 ACL 的权限 |
| --- | --- | --- |
| `bucket-owner-read` | 对象 | 对象所有者将获得 `FULL_CONTROL` 。存储桶拥有者将获得 `READ` 访问权限。如果您在创建存储段时指定此标准的 ACL，Amazon S3 将忽略它。 |
| `bucket-owner-full-control` | 对象 | 对象所有者和存储桶拥有者均可获得对对象的 `FULL_CONTROL` 。如果您在创建存储段时指定此标准的 ACL，Amazon S3 将忽略它。 |
| `log-delivery-write` | 存储桶 | `LogDelivery` 组将获得针对存储桶的 `WRITE` 和 `READ_ACP` 许可。有关日志的更多信息，请参阅（使用服务器访问日志记录来记录请求）。 |

> **Note**
>
> 您可以在请求中仅指定这些标准 ACL 中的一个。

您可以使用 `x-amz-acl` 请求标头在请求中指定标准 ACL。当 Amazon S3 收到包含标准 ACL 的请求时，它会向资源的 ACL 添加预定义的授权。

## 配置 ACL

本节介绍如何使用访问控制列表（ACL）管理 S3 存储桶和对象的访问权限。您可以使用 Amazon Web Services Management Console、Amazon Command Line Interface（CLI）、REST API 或 Amazon SDK 向资源 ACL 添加授权。

存储桶和对象的权限是相互独立的。对象不继承其存储桶的权限。例如，如果您创建了一个存储桶并授予一个用户写入权限，则将无法访问此用户的对象，除非此用户显式授予您访问权限。

您可以向其他 Amazon Web Services 账户用户或预定义的组授予权限。您将向其授予权限的用户或组称作被授权者。默认情况下，拥有者（即创建存储桶的 Amazon Web Services 账户）具有完全权限。

您为用户或组授予的每项权限都会在 ACL 中添加一个与该存储桶关联的条目。ACL 列出了授权，这些授权确定了被授权者和授予的权限。

S3 对象所有权是 Amazon S3 存储桶级别的设置，您可以使用该设置来控制上传到存储桶的对象的所有权和禁用或启用 ACL。默认情况下，对象所有权设为强制存储桶拥有者设置，并且所有 ACL 均处于

禁用状态。禁用 ACL 后，存储桶拥有者拥有存储桶中的所有对象，并使用访问管理策略来专门管理对这些对象的访问权限。

Amazon S3 中的大多数现代使用案例不再需要使用 ACL。我们建议您将 ACL 保持为禁用状态，除非有需要单独控制每个对象的访问权限的特殊情况。禁用 ACL 后，您可以使用策略来控制对存储桶中所有对象的访问权限，无论是谁将对象上传到您的存储桶。有关更多信息，请参阅 为您的存储桶控制对象所有权和禁用 ACL。。

> **Important**
>
> 如果通用存储桶针对 S3 对象所有权使用强制存储桶拥有者设置，则必须使用策略来授予对通用存储桶及其中对象的访问权限。启用强制存储桶拥有者设置后，设置访问控制列表（ACL）或更新 ACL 的请求将失败并返回 `AccessControlListNotSupported` 错误代码。仍然支持读取 ACL 的请求。

> **Warning**
>
> 我们强烈建议您避免向所有人（公有访问）或经过身份验证的用户组（所有经 Amazon 身份验证的用户）群组授予写入访问权限。有关向这些组授予写访问权限的效果的更多信息，请参阅 Amazon S3 预定义的组。

使用 S3 控制台为存储桶设置 ACL 权限

控制台显示重复被授权者的组合访问授权。要查看 ACL 的完整列表，请使用 Amazon S3 REST API、Amazon CLI 或 Amazon SDK。

下表显示了您可以在 Amazon S3 控制台中为存储桶配置的 ACL 权限。

存储桶的 Amazon S3 控制台 ACL 权限

| 控制台权限 | ACL 权限 | 访问 |
| --- | --- | --- |
| Objects（对象）– List（列表） | `READ` | 允许被授权者列出存储桶中的对象 |

| 控制台权限 | ACL 权限 | 访问 |
| --- | --- | --- |
| Objects（对象）— Write（写） | WRITE | 允许被授权者在存储桶中创建新对象。对于现有对象的存储桶和对象所有者，还允许删除和覆写这些对象。 |
| Bucket ACL（存储桶 ACL）– Read（读取） | READ_ACP | 允许被授权者读取存储桶 ACL |
| BucketACL（存储桶 ACL）— Write（写入） | WRITE_ACP | 允许被授权者为适用的存储桶编写 ACL |
| 所有人（公共访问）：Objects（对象）— List（列表） | READ | 授予存储桶中对象的公共读取访问权限。当您向所有人授予列表访问权限（公共读取权限）时，则任何人都可以访问存储桶中的对象。 |
| 所有人（公共访问）：Bucket ACL（存储桶 ACL）— Read（读取） | READ_ACP | 授予存储桶 ACL 公共读取访问权限。当您向所有人授予读取访问权限（公共访问权限）时，则任何人都可以访问存储桶 ACL。 |

有关 ACL 权限的更多信息，请参阅 访问控制列表 (ACL) 概述。

> **Important**
>
> 如果通用存储桶针对 S3 对象所有权使用强制存储桶拥有者设置，则必须使用策略来授予对通用存储桶及其中对象的访问权限。启用强制存储桶拥有者设置后，设置访问控制列表（ACL）或更新 ACL 的请求将失败并返回 `AccessControlListNotSupported` 错误代码。仍然支持读取 ACL 的请求。

为存储桶设置 ACL 权限

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在 Buckets（存储桶）列表中，请选择要为其配置权限的存储桶的名称。
4. 选择 Permissions (权限)。
5. 在 Access control list (访问控制列表) 下，请选择 Edit (编辑)。

   您可以编辑存储桶的以下 ACL 权限：

   对象

   - 列出 – 允许被授权者列出存储桶中的对象。
   - 写入 – 允许被授权者在存储桶中创建新对象。对于现有对象的存储桶和对象所有者，还允许删除和覆写这些对象。

     在 S3 控制台中，您只能向 S3 日志传输组和存储桶拥有者（您的 Amazon Web Services 账户）授予写入访问权限。我们强烈建议您不要向其他被授权者授予写入访问权限。但是，如果您需要授予写入访问权限，可以使用 Amazon CLI、Amazon SDK 或 REST API。

   Bucket ACL

   - 读取 – 允许被授权者读取存储桶 ACL。
   - 写入 – 允许被授权者为适用的存储桶编写 ACL
6. 要更改存储桶拥有者的权限，请在 Bucket owner（your Amazon Web Services 账户）（存储桶拥有者 [您的 Amazon 账户]）旁清除或从以下 ACL 权限中选择：

   - Objects（对象）– List（列出）或 Write（写入）

- Bucket ACL（存储桶 ACL）– Read（读取）或 Write（写入）

拥有者是指 Amazon Web Services 账户根用户，而不是 Amazon Identity and Access Management IAM 用户。有关根用户的更多信息，请参阅《IAM 用户指南》中的 Amazon Web Services 账户根用户。

7. 要向公众（互联网上的所有人）授予或撤消权限，请在 每个人（公共访问）旁清除或从以下 ACL 权限中选择：

   - Objects（对象）– List（列表）
   - Bucket ACL（存储桶 ACL）– Read（读取）

   > **Warning**
   >
   > 在授予 Everyone 组对您的 S3 存储桶的公有访问权限时应谨慎使用。如果您向此组授予访问权限，那么世界上的任何人都可以访问您的存储桶。我们强烈建议您绝对不要授予对 S3 存储桶的任何类型的公有写入权限。

8. 要向拥有 Amazon Web Services 账户的任何人授予或撤消权限，请在 Authenticated Users group (anyone with an Amazon Web Services 账户) (已经过身份验证的用户组 [拥有 Amazon 账户的任何人]) 旁清除或从以下 ACL 权限中进行选择：

   - Objects（对象）– List（列表）
   - Bucket ACL（存储桶 ACL）– Read（读取）

9. 要授予或撤消 Amazon S3 将服务器访问日志写入存储桶的权限，请在 S3 log delivery group（S3 日志传输组）下清除或从以下 ACL 权限中进行选择：

   - Objects（对象）– List（列出）或 Write（写入）
   - Bucket ACL（存储桶 ACL）– Read（读取）或 Write（写入）

   如果存储桶设置为目标存储桶以接收访问日志，则存储桶权限必须允许日志传输组对存储桶有写入权限。当您在存储桶上启用服务器访问日志记录时，Amazon S3 控制台会向 Log Delivery（日志传输）组授予对您选择用来接收日志的目标存储桶的写入权限。有关服务器访问日志记录的更多信息，请参阅 启用 Amazon S3 服务器访问日志记录。

10. 要授予对其他 Amazon Web Services 账户 的访问权限，请执行以下操作：

    a. 请选择 Add grantee（添加被授权者）。

b. 在 Grantee (被授权者) 框中，输入其他 Amazon Web Services 账户的规范 ID。

c. 从以下 ACL 权限中进行选择：

- Objects（对象）– List（列出）或 Write（写入）
- Bucket ACL（存储桶 ACL）– Read（读取）或 Write（写入）

> **Warning**
>
> 当您需要向其他 Amazon Web Services 账户授权访问您的资源时，注意 Amazon Web Services 账户可以向其账户下的用户授予权限。这称为跨账户访问。有关使用跨账户访问的信息，请参阅 IAM 用户指南中的创建角色以向 IAM 用户委派权限。

11. 要删除对其他 Amazon Web Services 账户的访问权限，请在 Access for other Amazon Web Services 账户 (其他 Amazon 账户的访问权限) 下，请选择 Remove (删除)。
12. 要保存您的更改，请选择 Save Changes (保存更改)。

使用 S3 控制台为对象设置 ACL 权限

控制台显示重复被授权者的组合访问授权。要查看 ACL 的完整列表，请使用 Amazon S3 REST API、Amazon CLI 或 Amazon SDK。下表显示了您可以在 Amazon S3 控制台中为对象配置的 ACL 权限。

对象的 Amazon S3 控制台 ACL 权限

| 控制台权限 | ACL 权限 | 访问 |
| --- | --- | --- |
| Object（对象）— Read（读取） | `READ` | 允许被授权者读取对象数据及其元数据 |
| Object ACL（对象 ACL）— Read（读取） | `READ_ACP` | 允许被授权者读取对象 ACL |

| 控制台权限 | ACL 权限 | 访问 |
| --- | --- | --- |
| Object ACL（对象 ACL）— Write（写入） | `WRITE_ACP` | 允许被授权者为适用的对象编写 ACL |

有关 ACL 权限的更多信息，请参阅 访问控制列表 (ACL) 概述。

> **Important**
>
> 如果通用存储桶针对 S3 对象所有权使用强制存储桶拥有者设置，则必须使用策略来授予对通用存储桶及其中对象的访问权限。启用强制存储桶拥有者设置后，设置访问控制列表（ACL）或更新 ACL 的请求将失败并返回 `AccessControlListNotSupported` 错误代码。仍然支持读取 ACL 的请求。

为对象设置 ACL 权限

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Bucket（存储桶）列表中，请选择包含对象的存储桶的名称。
3. 在 objects（对象）列表中，请选择要为其设置权限的对象的名称。
4. 请选择 Permissions。
5. 在访问控制列表 (ACL) 下，请选择 Edit (编辑)。

   您可以编辑对象的以下 ACL 权限：

   对象

   - 读取 – 允许被授权者读取对象数据及其元数据。

   对象 ACL

   - 读取 – 允许被授权者读取对象 ACL。

- 写入 – 允许被授权者为适用的对象编写 ACL。在 S3 控制台中，您只能向存储桶拥有者（您的 Amazon Web Services 账户）授予写入访问权限。我们强烈建议您不要向其他被授权者授予写入访问权限。但是，如果您需要授予写入访问权限，可以使用 Amazon CLI、Amazon SDK 或 REST API。

6. 您可以管理对象的以下访问权限：

   a. 对象所有者的访问权限

      拥有者是指 Amazon Web Services 账户根用户，而不是 Amazon Identity and Access Management IAM 用户。有关根用户的更多信息，请参阅《IAM 用户指南》中的 Amazon Web Services 账户根用户。

      要更改拥有者的对象访问权限，请在 Access for object owner (对象所有者的访问权限) 下，请选择 Your Amazon Account (owner) (您的 Amazon 账户 [所有者])。

      选中要更改的权限所对应的复选框，然后选择 Save (保存)。

   b. 其他 Amazon Web Services 账户的访问权限

      要向其他 Amazon Web Services 账户 的 Amazon 用户授予权限，请在 Access for other Amazon Web Services 账户 (其他 Amazon 账户的访问权限) 下面，请选择 Add account (添加账户)。在 Enter an ID (输入 ID) 字段中，输入要向其授予对象权限的 Amazon 用户的规范 ID。有关查找规范 ID 的信息，请参阅《Amazon Web Services 一般参考》中的您的 Amazon Web Services 账户标识符。您可以添加多达 99 个用户。

      选中要向用户授予的权限所对应的复选框，然后选择 Save (保存)。要显示有关权限的信息，请选择帮助图标。

   c. 公有访问权限

      要向一般公众 (世界上的每个人) 授予对您的对象的访问权限，请在 Public access (公开访问) 下面选择 Everyone (所有人)。授予公有访问权限意味着世界上的任何人都可以访问该对象。

      选中要授予的权限所对应的复选框，然后选择 Save (保存)。

      > ⚠ Warning
      >
      > - 在授予 Everyone (所有人) 组对您的 Amazon S3 对象的匿名访问权限时应谨慎使用。如果您向此组授予访问权限，那么世界上的任何人都可以访问您的对象。如果您需要为所有人授予访问权限，我们强烈建议您仅授予读取对象的权限。

- 我们强烈建议您不要为 Everyone (所有人) 组授予写入对象权限。这样做将允许任何人覆盖对象的 ACL 权限。

### 使用 Amazon SDK

本节提供了有关如何在存储桶和对象上配置访问控制列表 (ACL) 授予的示例。

> **Important**
>
> 如果通用存储桶针对 S3 对象所有权使用强制存储桶拥有者设置，则必须使用策略来授予对通用存储桶及其中对象的访问权限。启用强制存储桶拥有者设置后，设置访问控制列表（ACL）或更新 ACL 的请求将失败并返回 `AccessControlListNotSupported` 错误代码。仍然支持读取 ACL 的请求。

#### Java

本节提供了有关如何在存储桶和对象上配置访问控制列表（ACL）授予的示例。第一个示例将创建具有标准 ACL（请参阅标准 ACL）的存储桶，创建自定义权限授予列表，然后将标准 ACL 替换为包含自定义授予的 ACL。第二个示例演示如何使用 `AccessControlList.grantPermission()` 方法修改 ACL。

Example 创建存储桶并指定用于向 S3 日志传输组授予权限的标准 ACL

此示例将创建一个存储桶。在请求中，此示例指定了一个标准 ACL，该 ACL 向日志传输组授予将日志写入到存储桶的权限。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.io.IOException;
import java.util.ArrayList;

public class CreateBucketWithACL {
```

```
   public static void main(String[] args) throws IOException {
       Regions clientRegion = Regions.DEFAULT_REGION;
       String bucketName = "*** Bucket name ***";
       String userEmailForReadPermission = "*** user@example.com ***";

       try {
           AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                   .withRegion(clientRegion)
                   .build();

           // Create a bucket with a canned ACL. This ACL will be replaced by the
           // setBucketAcl()
           // calls below. It is included here for demonstration purposes.
           CreateBucketRequest createBucketRequest = new
CreateBucketRequest(bucketName, clientRegion.getName())
                   .withCannedAcl(CannedAccessControlList.LogDeliveryWrite);
           s3Client.createBucket(createBucketRequest);

           // Create a collection of grants to add to the bucket.
           ArrayList<Grant> grantCollection = new ArrayList<Grant>();

           // Grant the account owner full control.
           Grant grant1 = new Grant(new
CanonicalGrantee(s3Client.getS3AccountOwner().getId()),
                   Permission.FullControl);
           grantCollection.add(grant1);

           // Grant the LogDelivery group permission to write to the bucket.
           Grant grant2 = new Grant(GroupGrantee.LogDelivery, Permission.Write);
           grantCollection.add(grant2);

           // Save grants by replacing all current ACL grants with the two we just
created.
           AccessControlList bucketAcl = new AccessControlList();
           bucketAcl.grantAllPermissions(grantCollection.toArray(new Grant[0]));
           s3Client.setBucketAcl(bucketName, bucketAcl);

           // Retrieve the bucket's ACL, add another grant, and then save the new
ACL.
           AccessControlList newBucketAcl = s3Client.getBucketAcl(bucketName);
           Grant grant3 = new Grant(new
EmailAddressGrantee(userEmailForReadPermission), Permission.Read);
           newBucketAcl.grantAllPermissions(grant3);
           s3Client.setBucketAcl(bucketName, newBucketAcl);
```

```
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Example 更新现有对象的 ACL

此示例将更新对象上的 ACL。该示例执行以下任务：

- 检索对象的 ACL
- 通过删除所有现有权限来清除该 ACL
- 添加两个权限：对所有者的完全访问权限以及对通过电子邮件地址标识的用户的 WRITE_ACP 权限 (请参阅 我能授予哪些许可？)。
- 将 ACL 保存到对象

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.AccessControlList;
import com.amazonaws.services.s3.model.CanonicalGrantee;
import com.amazonaws.services.s3.model.EmailAddressGrantee;
import com.amazonaws.services.s3.model.Permission;

import java.io.IOException;

public class ModifyACLExistingObject {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
```

```
        String bucketName = "*** Bucket name ***";
        String keyName = "*** Key name ***";
        String emailGrantee = "*** user@example.com ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Get the existing object ACL that we want to modify.
            AccessControlList acl = s3Client.getObjectAcl(bucketName, keyName);

            // Clear the existing list of grants.
            acl.getGrantsAsList().clear();

            // Grant a sample set of permissions, using the existing ACL owner for
 Full
            // Control permissions.
            acl.grantPermission(new CanonicalGrantee(acl.getOwner().getId()),
 Permission.FullControl);
            acl.grantPermission(new EmailAddressGrantee(emailGrantee),
 Permission.WriteAcp);

            // Save the modified ACL back to the object.
            s3Client.setObjectAcl(bucketName, keyName, acl);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

Example 创建存储桶并指定用于向 S3 日志传输组授予权限的标准 ACL

此 C# 示例将创建一个存储桶。在请求中，代码还将指定一个标准 ACL，该 ACL 向日志传输组授予将日志写入到存储桶的权限。

有关设置和运行代码示例的信息，请参阅《适用于 .NET 的 Amazon SDK 开发人员指南》中的适用于 .NET 的 Amazon SDK 入门。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class ManagingBucketACLTest
    {
        private const string newBucketName = "*** bucket name ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;

        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            CreateBucketUseCannedACLAsync().Wait();
        }

        private static async Task CreateBucketUseCannedACLAsync()
        {
            try
            {
                // Add bucket (specify canned ACL).
                PutBucketRequest putBucketRequest = new PutBucketRequest()
                {
                    BucketName = newBucketName,
                    BucketRegion = S3Region.EUW1, // S3Region.US,
                                                  // Add canned ACL.
                    CannedACL = S3CannedACL.LogDeliveryWrite
                };
```

```
                PutBucketResponse putBucketResponse = await
 client.PutBucketAsync(putBucketRequest);

                // Retrieve bucket ACL.
                GetACLResponse getACLResponse = await client.GetACLAsync(new
 GetACLRequest
                {
                    BucketName = newBucketName
                });
            }
            catch (AmazonS3Exception amazonS3Exception)
            {
                Console.WriteLine("S3 error occurred. Exception: " +
 amazonS3Exception.ToString());
            }
            catch (Exception e)
            {
                Console.WriteLine("Exception: " + e.ToString());
            }
        }
    }
}
```

Example 更新现有对象的 ACL

此 C# 示例将更新现有对象上的 ACL。该示例执行以下任务：

- 检索对象的 ACL。
- 通过删除所有现有权限来清除该 ACL。
- 添加两个权限：对所有者的完全访问权限以及对通过电子邮件地址标识的用户的 WRITE_ACP 权限。
- 通过发送 `PutAcl` 请求来保存该 ACL。

有关设置和运行代码示例的信息，请参阅《适用于 .NET 的 Amazon SDK 开发人员指南》中的适用于 .NET 的 Amazon SDK 入门。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
```

```
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class ManagingObjectACLTest
    {
        private const string bucketName = "*** bucket name ***";
        private const string keyName = "*** object key name ***";
        private const string emailAddress = "*** email address ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;
        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            TestObjectACLTestAsync().Wait();
        }
        private static async Task TestObjectACLTestAsync()
        {
            try
            {
                    // Retrieve the ACL for the object.
                    GetACLResponse aclResponse = await client.GetACLAsync(new
 GetACLRequest
                    {
                        BucketName = bucketName,
                        Key = keyName
                    });

                    S3AccessControlList acl = aclResponse.AccessControlList;

                    // Retrieve the owner (we use this to re-add permissions after
 we clear the ACL).
                    Owner owner = acl.Owner;

                    // Clear existing grants.
                    acl.Grants.Clear();

                    // Add a grant to reset the owner's full permission (the
 previous clear statement removed all permissions).
                    S3Grant fullControlGrant = new S3Grant
                    {
                        Grantee = new S3Grantee { CanonicalUser = owner.Id },
```

```
                        Permission = S3Permission.FULL_CONTROL

                    };

                    // Describe the grant for the permission using an email address.
                    S3Grant grantUsingEmail = new S3Grant
                    {
                        Grantee = new S3Grantee { EmailAddress = emailAddress },
                        Permission = S3Permission.WRITE_ACP
                    };
                    acl.Grants.AddRange(new List<S3Grant> { fullControlGrant,
grantUsingEmail });

                    // Set a new ACL.
                    PutACLResponse response = await client.PutACLAsync(new
PutACLRequest
                    {
                        BucketName = bucketName,
                        Key = keyName,
                        AccessControlList = acl
                    });
            }
            catch (AmazonS3Exception amazonS3Exception)
            {
                Console.WriteLine("An AmazonS3Exception was thrown. Exception: " +
amazonS3Exception.ToString());
            }
            catch (Exception e)
            {
                Console.WriteLine("Exception: " + e.ToString());
            }
        }
    }
}
```

使用 REST API

Amazon S3 API 使您可以在创建存储段或对象时设置 ACL。Amazon S3 还提供 API 以在现有存储段或对象上设置 ACL。这些 API 提供了以下方法来设置 ACL：

- 使用请求标头设置 ACL — 发送创建资源（存储桶或对象）的请求时，您可以使用请求标头设置 ACL。使用这些标头时，您可以指定一个标准 ACL 或者显式指定授权 (显式识别被授权者和许可)。

- 使用请求正文设置 ACL — 当您发送在现有资源上设置 ACL 的请求时，您可以在请求标头或正文中设置 ACL。

有关管理 ACL 的 REST API 支持的信息，请参阅 Amazon Simple Storage Service API 参考中的以下部分：

- GetBucketAcl
- PutBucketAcl
- GetObjecAcl
- PutObjectAcl
- PutObject
- CreateBucket
- CopyObject
- CreateMultipartUpload

> **Important**
>
> 如果通用存储桶针对 S3 对象所有权使用强制存储桶拥有者设置，则必须使用策略来授予对通用存储桶及其中对象的访问权限。启用强制存储桶拥有者设置后，设置访问控制列表（ACL）或更新 ACL 的请求将失败并返回 `AccessControlListNotSupported` 错误代码。仍然支持读取 ACL 的请求。

访问控制列表 (ACL) 特定的请求标头

您可以使用标头授予基于访问控制列表 (ACL) 的权限。默认情况下，所有的对象都是私有的。只有所有者具有完全访问权限控制。添加新的对象时，您可以向单个 Amazon Web Services 账户或 Amazon S3 定义的预定义组授予权限。然后，这些权限将添加到对象上的访问控制列表 (ACL)。有关更多信息，请参阅 访问控制列表 (ACL) 概述。

通过此操作，您可以使用以下两种方法之一授予访问权限：

- 标准 ACL (**`x-amz-acl`**) — Amazon S3 支持一系列预定义的 ACL，称为标准 ACL。每个标准 ACL 都有一组预定义的被授权者和许可。有关更多信息，请参阅 标准 ACL。

- 访问权限 – 要向特定 Amazon Web Services 账户 或组显式授予访问权限，请使用以下标头。每个标头映射到 Amazon S3 在 ACL 中支持的特定权限。有关更多信息，请参阅 访问控制列表 (ACL) 概述。在标头中，您可以指定获得特定权限的被授权者的列表。
  - x-amz-grant-read
  - x-amz-grant-write
  - x-amz-grant-read-acp
  - x-amz-grant-write-acp
  - x-amz-grant-full-control

使用 Amazon CLI

有关使用 Amazon CLI 管理 ACL 的更多信息，请参阅 Amazon CLI 命令参考中的 put-bucket-acl。

> **Important**
>
> 如果通用存储桶针对 S3 对象所有权使用强制存储桶拥有者设置，则必须使用策略来授予对通用存储桶及其中对象的访问权限。启用强制存储桶拥有者设置后，设置访问控制列表（ACL）或更新 ACL 的请求将失败并返回 `AccessControlListNotSupported` 错误代码。仍然支持读取 ACL 的请求。

## 适用于 ACL 的策略示例

您可在存储桶策略中使用条件键来控制针对 Amazon S3 的访问权限。

主题

- 授予 s3:PutObject 权限，指定了要求存储桶拥有者获得完全控制的条件
- 授予 s3:PutObject 权限，指定了关于 x-amz-acl 标头的条件

### 授予 s3:PutObject 权限，指定了要求存储桶拥有者获得完全控制的条件

PUT Object 操作允许特定于访问控制列表 (ACL) 的标头，可用于授予基于 ACL 的权限。通过使用这些键，存储桶拥有者可设置条件，要求用户上传对象时需具有特定访问权限。

假设账户 A 拥有一个存储桶，而账户管理员想要授予账户 B 中的用户 Dave 上传对象的权限。默认情况下，Dave 上传的对象由账户 B 拥有，而账户 A 对这些对象没有权限。由于存储桶拥有者要支

付账单，需要对 Dave 上传的对象具有全部权限。要实现这一目的，账户 A 管理员可向 Dave 授予 `s3:PutObject` 权限，指定的条件要求请求包含 ACL 特定标头（用于显式授予全部权限）或使用标准 ACL。有关更多信息，请参阅 PUT Object。

需要 x-amz-full-control 标头

您可以要求在请求中具有 `x-amz-full-control` 标头，授予存储桶拥有者完全控制权限。以下存储桶策略向用户 Dave 授予 `s3:PutObject` 权限，使用 `s3:x-amz-grant-full-control` 条件键指定了条件，要求此请求包含 `x-amz-full-control` 标头。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "statement1",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::AccountB-ID:user/Dave"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::awsexamplebucket1/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-grant-full-control": "id=AccountA-CanonicalUserID"
        }
      }
    }
  ]
}
```

> **Note**
>
> 此示例是关于跨账户权限的。不过，如果 Dave（正在获得权限）属于拥有存储桶的 Amazon Web Services 账户，则该条件权限不是必需的。这是因为，Dave 所属的父账户拥有用户上传的对象。

添加显式拒绝

上述存储桶策略向账户 B 中的用户 Dave 授予条件权限。当该策略生效时，Dave 可通过其他某个策略获得没有任何条件的相同权限。例如，Dave 可能属于一个组，并且您为该组授予 `s3:PutObject` 权

限而没有指定任何条件。为避免这些权限漏洞，可通过添加显式拒绝编写更严格的访问策略。在该示例中，如果用户 Dave 的请求没有包含必要标头向存储桶拥有者授予全部权限，则您显式拒绝他的上传权限。显式拒绝始终取代授予的其他任何权限。以下是添加了显式拒绝的经修订的访问策略示例。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "statement1",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::AccountB-ID:user/AccountBadmin"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::awsexamplebucket1/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-grant-full-control": "id=AccountA-CanonicalUserID"
                }
            }
        },
        {
            "Sid": "statement2",
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::AccountB-ID:user/AccountBadmin"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::awsexamplebucket1/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-grant-full-control": "id=AccountA-CanonicalUserID"
                }
            }
        }
    ]
}
```

使用 Amazon CLI 测试策略

如果您有两个 Amazon Web Services 账户，则可使用 Amazon Command Line Interface (Amazon CLI) 测试此策略。您可以附加此策略，并使用 Dave 的凭证通过以下 Amazon CLI `put-object` 命令测试权限。通过添加 `--profile`参数提供 Dave 的凭证。通过添加 `--grant-full-control` 参数

可向存储桶拥有者授予完全控制权限。有关设置和使用 Amazon CLI 的更多信息，请参阅《Amazon S3 API 参考》中的 Developing with Amazon S3 using the Amazon CLI。

```
aws s3api put-object --bucket examplebucket --key HappyFace.jpg --body c:\HappyFace.jpg
 --grant-full-control id="AccountA-CanonicalUserID" --profile AccountBUserProfile
```

需要 x-amz-acl 标头

您可以要求 x-amz-acl 标头，带有向存储桶拥有者授予完全控制权限的标准 ACL。如果要求在请求中使用 x-amz-acl 标头，您可以替换 Condition 块中的键值对并指定 s3:x-amz-acl 条件键，如以下示例中所示。

```
"Condition": {
    "StringEquals": {
        "s3:x-amz-acl": "bucket-owner-full-control"
    }
}
```

要使用 Amazon CLI 测试权限，则指定 --acl 参数。然后 Amazon CLI 在其发送此请求时添加 x-amz-acl 标头。

```
aws s3api put-object --bucket examplebucket --key HappyFace.jpg --body c:\HappyFace.jpg
 --acl "bucket-owner-full-control" --profile AccountBadmin
```

## 授予 s3:PutObject 权限，指定了关于 x-amz-acl 标头的条件

如果请求包含可使对象公开可读的 x-amz-acl 标头，则以下存储桶策略向两个 Amazon Web Services 账户授予 s3:PutObject 权限。Condition 块使用 StringEquals 条件，并且提供键值对 "s3:x-amz-acl":["public-read"]，以进行评估。在该键值对中，s3:x-amz-acl 是特定于 Amazon S3 的键，如前缀 s3: 所示。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
         "Sid":"AddCannedAcl",
            "Effect":"Allow",
         "Principal": {
                "AWS": [
```

```
                "arn:aws:iam::Account1-ID:root",
    "arn:aws:iam::Account2-ID:root"
    ]
            },
         "Action":"s3:PutObject",
            "Resource": ["arn:aws:s3:::awsexamplebucket1/*"],
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl":["public-read"]
                }
            }
        }
    ]
}
```

> **Important**
>
> 并非所有条件对所有操作都有意义。例如，在授予 `s3:CreateBucket` Amazon S3 权限的策略上包含 `s3:LocationConstraint` 条件是有意义的。但是，在授予 `s3:GetObject` 权限的策略中包含此条件没有意义。Amazon S3 可测试是否存在此类涉及 Amazon S3 特定条件的语义错误。但如果要创建针对 IAM 用户或角色的策略，并且包含了语义上无效的 Amazon S3 条件，则不报告错误，因为 IAM 无法验证 Amazon S3 条件。

# 阻止对您的 Amazon S3 存储的公有访问

Amazon S3 屏蔽公共访问权限特征提供接入点、存储桶和账户设置，帮助您管理对 Amazon S3 资源的公有访问。默认情况下，新存储桶、接入点和对象不允许公有访问。但是，用户可以修改存储桶策略、接入点策略或对象权限以允许公有访问。S3 屏蔽公共访问权限设置会覆盖这些策略和权限，以便于您可以限制这些资源的公有访问。

借助 S3 屏蔽公共访问权限，账户管理员和存储桶拥有者可以轻松设置集中控制，以控制对已实施的 Amazon S3 资源的公有访问（与资源的创建方式无关）。

有关配置公有块访问的说明，请参阅配置屏蔽公共访问权限。

当 Amazon S3 收到访问存储桶或对象的请求时，它将确定该存储桶或存储桶拥有者的账户是否应用了屏蔽公共访问权限设置。如果请求是通过接入点发出，则 Amazon S3 还会检查接入点的屏蔽公共访问权限设置。如果现有的屏蔽公共访问权限设置禁止请求的访问，则 Amazon S3 将拒绝该请求。

Amazon S3 屏蔽公共访问权限提供四种设置。这些设置彼此独立，可任意组合使用。每个设置都可以应用于接入点、存储桶或整个 Amazon Web Services 账户。如果接入点、存储桶或账户的屏蔽公共访问权限设置不同，则 Amazon S3 应用接入点、存储桶和账户设置的最严格组合。

当 Amazon S3 评估屏蔽公共访问权限设置是否禁止某一操作时，它将拒绝违反接入点、存储桶或账户设置的任何请求。

**Important**

通过访问控制列表（ACL）、接入点策略或存储桶策略，或者同时通过这几项向存储桶和对象授予公有访问权限。为了帮助确保您的所有 Amazon S3 接入点、存储桶和对象阻止了公有访问，我们建议为您的账户启用屏蔽公共访问权限的所有四个设置。这些设置阻止所有当前和将来的存储桶和接入点的公有访问。

在应用这些设置之前，请确认您的应用程序在没有公有访问的情况下能够正常工作。如果您需要对存储桶或对象进行某种级别的公有访问，例如，按照 使用 Amazon S3 托管静态网站 中所述托管静态网站，则可以自定义各个设置以符合您的存储使用案例要求。

启用“屏蔽公共访问权限”可防止通过直接附加到 S3 资源的资源策略或访问控制列表（ACL）来授予公共访问权限，有助于保护您的资源。除了启用“屏蔽公共访问权限”之外，还要仔细检查以下策略，来确认它们不会授予公共访问权限：

- 附加到关联 Amazon 主体（例如 IAM 角色）的基于身份的策略
- 附加到关联 Amazon 资源 [例如 Amazon Key Management Service（KMS）密钥] 的基于资源的策略

**Note**

- 您只能为接入点、存储桶和 Amazon Web Services 账户启用屏蔽公共访问权限设置。Amazon S3 不支持基于每个对象的屏蔽公共访问权限设置。
- 在将屏蔽公共访问权限设置应用于某一账户时，这些设置将应用于全球所有 Amazon Web Services 区域。这些设置可能不会立即或同时在所有区域生效，但最终会传播到所有区域。

主题

- 屏蔽公共访问权限设置
- 在接入点上执行屏蔽公共访问权限操作
- “公有”的含义

- 使用适用于 S3 的 IAM Access Analyzer 查看公有存储桶
- 权限
- 配置屏蔽公共访问权限
- 为您的账户配置屏蔽公共访问权限设置
- 为 S3 存储桶配置屏蔽公共访问权限设置

## 屏蔽公共访问权限设置

S3 屏蔽公共访问权限提供四种设置。您可以任意组合将这些设置应用于单个接入点、存储桶或整个 Amazon Web Services 账户。如果您将某一设置应用于某个账户，则该设置将应用于该账户拥有的所有存储桶和接入点。同样，如果您将设置应用于某个存储桶，则该设置将应用于与该存储桶关联的所有接入点。

下表包含可用设置。

| 名称 | 描述 |
| --- | --- |
| `BlockPublicAcls` | 将此选项设置为 `TRUE` 会引发以下行为：<br>• 如果指定的访问控制列表（ACL）为公有，`PutBucketAcl` 和 `PutObjectAcl` 调用将失败。<br>• 如果请求包含公有 ACL，则 `PutObject` 调用失败。<br>• 如果将此设置应用于某个账户，则当请求包含公有 ACL 时，`PUT Bucket` 调用将失败。<br><br>将此设置设为 `TRUE` 时，指定操作将失败（通过 REST API、Amazon CLI 或 Amazon SDK 请求的操作）。但是，不会修改用于存储桶和对象的现有策略和 ACL。此设置不仅允许您针对公有访问提供保护，还允许您审核、优化或更改存储桶或对象的现有策略和 ACL。<br><br>**Note**<br>接入点没有与其关联的 ACL。如果您将此设置应用于接入点，则该设置将充当到底层存储桶的传递途径。如果某个接入点启用了此设置， |

| 名称 | 描述 |
| --- | --- |
| | 则无论存储桶实际上是否启用了此设置，通过该接入点发出的请求表现为就像底层存储桶启用了此设置。 |
| IgnorePublicAcls | 将此选项设置为 TRUE 会使 Amazon S3 忽略存储桶及其包含的任何对象上的所有公有 ACL。通过此设置，您可以安全地屏蔽由 ACL 授予的公共访问权限，同时仍支持包含公有 ACL 的 PutObject 调用（与 BlockPublicAcls 相反，后者拒绝包含公有 ACL 的 PutObject 调用）。启用此设置不影响任何现有 ACL 的持久性，也不会阻止设置新的公有 ACL。<br><br>**Note**<br>接入点没有与其关联的 ACL。如果您将此设置应用于接入点，则该设置将充当到底层存储桶的传递途径。如果某个接入点启用了此设置，则无论存储桶实际上是否启用了此设置，通过该接入点发出的请求表现为就像底层存储桶启用了此设置。 |

| 名称 | 描述 |
| --- | --- |
| BlockPublicPolicy | 针对存储桶将此选项设置为 TRUE，将导致 Amazon S3 在指定的存储桶策略支持公共访问权限时拒绝对 PutBucketPolicy 的调用。如果指定的策略支持公共访问权限，则对于存储桶将此选项设置为 TRUE，也会导致 Amazon S3 拒绝对存储桶的所有相同账户接入点的 PutAccessPointPolicy 调用。<br><br>如果（为接入点或基础存储桶）指定的策略支持公共访问权限，则对于接入点将此选项设置 TRUE，将导致 Amazon S3 拒绝通过该接入点对 PutAccessPointPolicy 和 PutBucketPolicy 进行的调用。<br><br>您可以使用此设置以允许用户管理接入点和存储桶策略，而不允许其公开共享存储桶或其包含的对象。启用此设置不会影响现有接入点或存储桶策略。<br><br>**Important**<br>要有效地使用此设置，我们建议您在账户级别应用此设置。存储桶策略可能允许用户更改存储桶的屏蔽公共访问权限设置。因此，有权更改存储桶策略的用户可以插入允许其为存储桶禁用屏蔽公共访问权限设置的策略。如果为整个账户而非特定存储桶启用此设置，即使用户更改存储桶策略以禁用此设置，Amazon S3 仍会阻止公有策略。 |
| RestrictPublicBuckets | 将此选项设置为 TRUE 会将对具有公有策略的接入点或存储桶的访问限制为该存储桶拥有者账户和接入点拥有者账户中的 Amazon 服务主体和授权用户。此设置会阻止对接入点或存储桶的所有跨账户访问（Amazon 服务主体的访问除外），但仍允许该账户内的用户管理接入点或存储桶。<br><br>启用此设置不影响现有的接入点或存储桶策略，但 Amazon S3 会阻止派生自任何公有接入点或存储桶策略的公有和跨账户访问，包括到特定账户的非公有委派。 |

**Important**

- 调用 GetBucketAcl 和 GetObjectAcl 始终返回指定存储桶或对象的已就位的有效权限。例如，假设存储桶有一个 ACL 用于授予公有访问权限，但该存储桶还启用了

IgnorePublicAcls 设置。在此情况下，GetBucketAcl 将返回可反映 Amazon S3 正在实施的访问权限的 ACL，而不是与存储桶关联的实际 ACL。

- 屏蔽公共访问权限设置不更改现有的策略或 ACL。因此，删除屏蔽公共访问权限设置会使具有公有策略或 ACL 的存储桶或对象再次变为可公开访问。

## 在接入点上执行屏蔽公共访问权限操作

为了对接入点执行屏蔽公共访问权限操作，请使用 Amazon CLI 服务 s3control。

> **Important**
>
> 创建接入点后，无法更改接入点的屏蔽公共访问权限设置。只有在创建接入点时，才能为接入点指定屏蔽公共访问权限设置。

## “公有”的含义

### ACL

如果存储桶或对象 ACL 可向预定义的 AllUsers 或 AuthenticatedUsers 组的成员授予任何权限，则 Amazon S3 将其视为公有。有关预定义组的更多信息，请参阅 Amazon S3 预定义的组。

### 存储桶策略

在评估存储桶策略时，Amazon S3 先假定该策略是公有的。然后对策略进行评估，以确定它是否符合非公有条件。当存储桶策略必须仅授予针对以下一个或多个项目的固定值（不包含通配符或 Amazon Identity and Access Management 策略变量的值）的访问权限时，才会将该策略视为非公有：

- Amazon 主体、用户、角色或服务主体（例如 aws:PrincipalOrgID）
- 一组无类别域间路由（CIDR）块，使用 aws:SourceIp。有关 CIDR 的更多信息，请参阅 RFC 编辑器网站上的 RFC 4632。

> **Note**
>
> 根据 aws:SourceIp 条件键授予访问权限且 IP 范围非常宽泛（例如 0.0.0.0/1）的存储桶策略将评估为“公有”。这包括大于 /8（对于 IPv4）和 /32（对于 IPv6，不包括 RFC1918

私有范围）的值。屏蔽公共访问权限将拒绝这些“公有”策略，并阻止跨账户访问已在使用这些“公有”策略的存储桶。

- aws:SourceArn
- aws:SourceVpc
- aws:SourceVpce
- aws:SourceOwner
- aws:SourceAccount
- aws:userid，在模式“AROLEID:*”之外
- s3:DataAccessPointArn

> **Note**
>
> 在存储桶策略中使用时，只要账户 ID 已固定，此值就可以包含接入点名称的通配符，而无需将策略呈现为公有。例如，允许访问 arn:aws:s3:us-west-2:123456789012:accesspoint/* 也会允许访问与区域 123456789012 中的账户 us-west-2 关联的任何接入点，而无需将存储桶策略呈现为公有。此行为对于接入点策略有所不同。有关更多信息，请参阅 接入点。

- s3:DataAccessPointAccount

有关存储桶策略的更多信息，请参阅 Amazon S3 的存储桶策略。

> **Note**
>
> 使用多值上下文键时，必须使用 ForAllValues 或 ForAnyValue 集合运算符。

Example ：公有存储桶策略

根据这些规则，以下示例策略被视为公有。

```
{
  "Principal": "*",
  "Resource": "*",
  "Action": "s3:PutObject",
  "Effect": "Allow"
```

```
 }
```

```
{
  "Principal": "*",
  "Resource": "*",
  "Action": "s3:PutObject",
  "Effect": "Allow",
  "Condition": { "StringLike": {"aws:SourceVpc": "vpc-*"}}
 }
```

您可以通过使用固定值来包含上面所列的任何条件键将这些策略变为非公有。例如，可以通过将 aws:SourceVpc 设置为固定值，将上面的最后一个策略变为非公有，类似于以下内容：

```
{
  "Principal": "*",
  "Resource": "*",
  "Action": "s3:PutObject",
  "Effect": "Allow",
  "Condition": {"StringEquals": {"aws:SourceVpc": "vpc-91237329"}}
 }
```

## Amazon S3 如何评估同时包含公有和非公有访问授权的存储桶策略

此示例演示 Amazon S3 如何评估同时包含公有和非公有访问授权的存储桶策略。

假设存储桶有一个策略可向一组固定主体授予访问权限。根据前面描述的规则，此策略不是公有策略。因此，如果您启用 RestrictPublicBuckets 设置，该策略将按编写内容保持有效，因为 RestrictPublicBuckets 只应用于具有公有策略的存储桶。但是，如果您向该策略中添加公有语句，则 RestrictPublicBuckets 将对该存储桶生效。它仅允许存储桶拥有者账户的 Amazon 服务主体和授权用户访问该存储桶。

例如，假定“Account-1”拥有的一个存储桶包含以下内容：

1. 向 Amazon CloudTrail（它是 Amazon 服务主体）授予访问权限的语句。
2. 向账户“Account-2”授予访问权限的语句
3. 向公众授予访问权限的语句，例如通过指定 "Principal": "*" 且没有限制性的 Condition

由于第三条语句，此策略符合公有策略的条件。实施此策略并启用 RestrictPublicBuckets 后，Amazon S3 将仅允许 CloudTrail 进行访问。请注意，尽管语句 2 不是公有，但

Amazon S3 仍禁用“Account-2”的访问。这是因为，语句 3 将整个策略都渲染为公有，因此 `RestrictPublicBuckets` 适用。因此，即使策略向特定账户“Account-2”委派访问权限，Amazon S3 仍禁用跨账户访问。但如果您从该策略中删除语句 3，则该策略不符合公有条件，并且 `RestrictPublicBuckets` 不再适用。因此，即使将 `RestrictPublicBuckets` 保持启用状态，“Account-2”也会重获存储桶的访问权限。

### 接入点

与存储桶相比，Amazon S3 评估接入点的屏蔽公共访问权限设置略有不同。Amazon S3 用于确定接入点策略何时为公用的规则对接入点和存储桶来说通常是相同的，但以下情况除外：

- 具有 VPC 网络起源的接入点始终被视为非公有，而无论其接入点策略的内容如何。
- 使用 `s3:DataAccessPointArn` 向一组接入点授予访问权限的接入点策略被视为公有。请注意，此行为与存储桶策略不同。例如，对于与 `s3:DataAccessPointArn` 匹配的 `arn:aws:s3:us-west-2:123456789012:accesspoint/*` 值授予访问权限的存储桶策略不会被视为公有。但是，在接入点策略中使用相同的语句会使接入点变为公有。

## 使用适用于 S3 的 IAM Access Analyzer 查看公有存储桶

您可以使用适用于 S3 的 IAM Access Analyzer 来查看具有存储桶 ACL、存储桶策略或授予公共访问权限的接入点策略的存储桶。如果存在已配置为允许互联网上的任何人或其他 Amazon Web Services 账户（包括组织外部的 Amazon Web Services 账户）访问的存储桶，适用于 S3 的 IAM Access Analyzer 会向您发出提醒。您会收到每个公共存储桶或共享存储桶的结果，其中报告了公共或共享访问的来源和级别。

在适用于 S3 的 IAM Access Analyzer 中，只需单击一下即可屏蔽对存储桶的所有公共访问权限。您还可以向下钻取到存储桶级别权限设置，以配置精细访问。对于需要公共或共享访问的特定和经验证的使用案例，您可以通过对存储桶的结果进行归档来确认和记录存储桶保持公开或共享的意图。

在极少数情况下，适用于 S3 的 IAM 访问权限分析器和 Amazon S3 屏蔽公共访问权限评估可能会因存储桶是否为公有而有所不同。之所以出现这种情况，是因为 Amazon S3 屏蔽公共访问权限除了评估公有访问权限外，还会对操作是否存在进行验证。假设存储桶策略包含一条 `Action` 语句，它支持公众访问 Amazon S3 不支持的操作（例如 `s3:NotASupportedAction`）。在这种情况下，Amazon S3 屏蔽公共访问权限会将存储桶评估为公有，因为如果稍后该操作变成受支持的，则这样的语句可能会使存储桶变为公有的。如果 Amazon S3 屏蔽公共访问权限和适用于 S3 的 IAM 访问权限分析器的评估存在差异，我们建议您查看存储桶策略并移除任何不受支持的操作。

有关适用于 S3 的 IAM Access Analyzer 的更多信息，请参阅[使用适用于 S3 的 IAM Access Analyzer 查看存储桶访问权限]。

## 权限

要使用 Amazon S3 屏蔽公共访问权限特征，您必须拥有以下权限。

| 操作 | 所需权限 |
| --- | --- |
| GET 存储桶策略状态 | s3:GetBucketPolicyStatus |
| GET 存储桶屏蔽公共访问权限设置 | s3:GetBucketPublicAccessBlock |
| PUT 存储桶屏蔽公共访问权限设置 | s3:PutBucketPublicAccessBlock |
| DELETE 存储桶屏蔽公共访问权限设置 | s3:PutBucketPublicAccessBlock |
| GET 账户屏蔽公共访问权限设置 | s3:GetAccountPublicAccessBlock |
| PUT 账户屏蔽公共访问权限设置 | s3:PutAccountPublicAccessBlock |
| DELETE 账户屏蔽公共访问权限设置 | s3:PutAccountPublicAccessBlock |
| PUT 接入点屏蔽公共访问权限设置 | s3:CreateAccessPoint |

> **Note**
>
> DELETE 操作所需权限与 PUT 操作相同。没有单独用于 DELETE 操作的权限。

## 配置屏蔽公共访问权限

有关为 Amazon Web Services 账户、Amazon S3 存储桶和接入点配置屏蔽公共访问权限的更多信息，请参阅以下主题：

- 为您的账户配置屏蔽公共访问权限设置
- 为 S3 存储桶配置屏蔽公共访问权限设置
- 在接入点上执行屏蔽公共访问权限操作

# 为您的账户配置屏蔽公共访问权限设置

Amazon S3 屏蔽公共访问权限提供接入点、存储桶和账户的设置，帮助您管理对 Amazon S3 资源的公有访问。默认情况下，新存储桶、接入点和对象不允许公有访问。

有关更多信息，请参阅 阻止对您的 Amazon S3 存储的公有访问。

> **Note**
>
> 账户级别设置会覆盖各个对象的设置。将您的账户配置为屏蔽公共访问权限后，将覆盖对账户内单个对象所设定的任何公共访问权限设置。

您可以使用 S3 控制台、Amazon CLI、Amazon SDK 和 REST API 为账户中的所有存储桶配置屏蔽公共访问权限设置。有关更多信息，请参阅以下部分。

要为存储桶配置屏蔽公共访问权限设置，请参阅 为 S3 存储桶配置屏蔽公共访问权限设置。有关接入点的信息，请参阅 在接入点上执行屏蔽公共访问权限操作。

使用 S3 控制台

Amazon S3 屏蔽公共访问权限将阻止所有在设置中允许对 S3 存储桶中的数据进行公有访问的应用程序。本部分介绍如何为 Amazon Web Services 账户 中的所有 S3 存储桶编辑屏蔽公共访问权限设置。有关屏蔽公共访问权限的更多信息，请参阅阻止对您的 Amazon S3 存储的公有访问。

为 Amazon Web Services 账户 中的所有 S3 存储桶编辑屏蔽公共访问权限设置

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 请选择 Block Public Access settings for this account (阻止此账户的公有访问设置)。
3. 请选择 Edit（编辑）以便为 Amazon Web Services 账户 中的所有存储桶更改屏蔽公共访问权限设置。
4. 请选择要更改的设置，然后选择 Save changes (保存更改)。
5. 当系统要求确认时，请输入 **`confirm`**。然后选择 Confirm (确认) 以保存更改。

使用 Amazon CLI

您可以通过 Amazon CLI 使用 Amazon S3 屏蔽公共访问权限。有关设置和使用 Amazon CLI 的更多信息，请参阅什么是 Amazon Command Line Interface？

Account

为了对账户执行屏蔽公共访问权限操作，请使用 Amazon CLI 服务 `s3control`。使用此服务的账户级别的操作如下所示：

- `PutPublicAccessBlock`（对于账户）
- `GetPublicAccessBlock`（对于账户）
- `DeletePublicAccessBlock`（对于账户）

有关更多信息和示例，请参阅《Amazon CLI Reference》中的 put-public-access-block。

使用 Amazon SDK

Java

以下示例展示了如何将 Amazon S3 屏蔽公共访问权限与 适用于 Java 的 Amazon SDK 结合使用，以在 Amazon S3 账户中放置公有访问阻止配置。

```
AWSS3ControlClientBuilder controlClientBuilder =
 AWSS3ControlClientBuilder.standard();
controlClientBuilder.setRegion(<region>);
controlClientBuilder.setCredentials(<credentials>);

AWSS3Control client = controlClientBuilder.build();
client.putPublicAccessBlock(new PutPublicAccessBlockRequest()
  .withAccountId(<account-id>)
  .withPublicAccessBlockConfiguration(new PublicAccessBlockConfiguration()
    .withIgnorePublicAcls(<value>)
    .withBlockPublicAcls(<value>)
    .withBlockPublicPolicy(<value>)
    .withRestrictPublicBuckets(<value>)));
```

**Important**

此示例仅适用于使用 `AWSS3Control` 客户端类的账户级别操作。对于存储桶级别的操作，请参阅前面的示例。

Other SDKs

有关使用其它 Amazon SDK 的信息，请参阅《Amazon S3 API 参考》中的 Developing with Amazon S3 using the Amazon SDKs。

使用 REST API

有关通过 REST API 使用 Amazon S3 屏蔽公共访问权限的信息，请参阅 Amazon Simple Storage Service API 参考中的以下主题。

- 账户级别操作
  - PutPublicAccessBlock
  - GetPublicAccessBlock
  - DeletePublicAccessBlock

## 为 S3 存储桶配置屏蔽公共访问权限设置

Amazon S3 屏蔽公共访问权限提供接入点、存储桶和账户的设置，帮助您管理对 Amazon S3 资源的公有访问。默认情况下，新存储桶、接入点和对象不允许公有访问。

有关更多信息，请参阅 阻止对您的 Amazon S3 存储的公有访问。

您可以使用 S3 控制台、Amazon CLI、Amazon SDK 和 REST API 授予对一个或多个存储桶的公共访问权限。您还可以对已经设为公共的存储桶屏蔽公共访问权限。有关更多信息，请参阅以下部分。

要为账户中的每个存储桶配置“屏蔽公共访问权限”设置，请参阅为您的账户配置屏蔽公共访问权限设置。有关为接入点配置屏蔽公共访问权限的信息，请参阅 在接入点上执行屏蔽公共访问权限操作。

使用 S3 控制台

Amazon S3 屏蔽公共访问权限将阻止使用允许对 S3 存储桶中的数据进行公有访问的任何设置的应用程序。本部分介绍如何为一个或多个 S3 存储桶编辑屏蔽公共访问权限设置。有关使用 Amazon CLI、Amazon SDK 和 Amazon S3 REST API 阻止公有访问的信息，请参阅阻止对您的 Amazon S3 存储的公有访问。

您可以从 IAM Access Analyzer 列的存储桶列表中查看您的存储桶是否可以公开访问。有关更多信息，请参阅 使用适用于 S3 的 IAM Access Analyzer 查看存储桶访问权限。

如果您在列出桶及其公有访问设置时看到 `Error`，则您可能不具备所需的权限。检查以确保您已将以下权限添加到您的用户或角色策略：

```
s3:GetAccountPublicAccessBlock
s3:GetBucketPublicAccessBlock
s3:GetBucketPolicyStatus
s3:GetBucketLocation
s3:GetBucketAcl
s3:ListAccessPoints
s3:ListAllMyBuckets
```

在极少数情况下，请求也可能因 Amazon Web Services 区域中断而失败。

为单个 S3 存储桶编辑 Amazon S3 屏蔽公共访问权限设置

如何您需要为单个 S3 存储桶更改公有访问设置，请执行以下步骤。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Bucket name（存储桶名称）列表中，请选择所需的存储桶的名称。
3. 选择 Permissions (权限)。
4. 选择屏蔽公共访问权限（存储桶设置）旁边的编辑，以更改存储桶的公共访问权限设置。有关四个 Amazon S3 屏蔽公共访问权限设置的更多信息，请参阅 屏蔽公共访问权限设置。
5. 选择其中一个设置，然后选择保存更改。
6. 当系统要求确认时，请输入 **`confirm`**。然后选择 Confirm (确认) 以保存更改。

还可以在创建存储桶时更改 Amazon S3 屏蔽公共访问权限设置。有关更多信息，请参阅 创建通用存储桶。

使用 Amazon CLI

要对存储桶屏蔽公共访问权限或删除公共访问权限屏蔽，请使用 Amazon CLI 服务 `s3api`。使用此服务的存储桶级别的操作如下所示：

- `PutPublicAccessBlock`（对于存储桶）
- `GetPublicAccessBlock`（对于存储桶）
- `DeletePublicAccessBlock`（对于存储桶）
- `GetBucketPolicyStatus`

有关更多信息和示例，请参阅《Amazon CLI 参考》中的 put-public-access-block。

使用 Amazon SDK

Java

```
AmazonS3 client = AmazonS3ClientBuilder.standard()
   .withCredentials(<credentials>)
   .build();

client.setPublicAccessBlock(new SetPublicAccessBlockRequest()
  .withBucketName(<bucket-name>)
  .withPublicAccessBlockConfiguration(new PublicAccessBlockConfiguration()
    .withBlockPublicAcls(<value>)
    .withIgnorePublicAcls(<value>)
    .withBlockPublicPolicy(<value>)
    .withRestrictPublicBuckets(<value>)));
```

**Important**

此示例仅适用于使用 AmazonS3 客户端类的存储桶级别操作。对于账户级别的操作，请参阅以下示例。

Other SDKs

有关使用其它 Amazon SDK 的信息，请参阅《Amazon S3 API 参考》中的 Developing with Amazon S3 using the Amazon SDKs。

使用 REST API

有关通过 REST API 使用 Amazon S3 屏蔽公共访问权限的信息，请参阅 Amazon Simple Storage Service API 参考中的以下主题。

- 存储桶级别操作
  - PutPublicAccessBlock
  - GetPublicAccessBlock
  - DeletePublicAccessBlock
  - GetBucketPolicyStatus

# 使用适用于 S3 的 IAM Access Analyzer 查看存储桶访问权限

如果存在已配置为允许互联网上的任何人或其他 Amazon Web Services 账户（包括组织外部的 Amazon Web Services 账户）访问的 S3 存储桶，适用于 S3 的 IAM Access Analyzer 会向您发出提醒。对于每个公共存储桶或共享存储桶，您会收到有关公共或共享访问的来源和级别的信息。例如，适用于 S3 的 IAM Access Analyzer 可能会显示存储桶具有通过存储桶访问控制列表（ACL）、存储桶策略，多区域接入点策略或接入点策略提供的读取或写入访问权限。有了这些调查结果，您就可以立即采取精确的纠正措施，将存储桶访问权限恢复为您期望的设置。

在适用于 S3 的 IAM Access Analyzer 中查看存在风险的存储桶时，只需单击一下即可对存储桶屏蔽所有公共访问权限。我们建议您阻止所有对存储桶的访问，除非您需要公有访问才能支持特定使用案例。在阻止所有公有访问之前，请确保您的应用程序在没有公有访问权限的情况下可以继续正常工作。有关更多信息，请参阅 阻止对您的 Amazon S3 存储的公有访问。

您还可以向下钻取到存储桶级别权限设置，以配置精细访问。对于需要公有访问的特定和经验证的使用案例（例如静态网站托管、公共下载或跨账户共享），您可以通过对存储桶的结果进行归档来确认和记录存储桶保持公开或共享的意图。您可以随时重新访问和修改这些存储桶配置。您还可以将结果下载为 CSV 格式的报告以供审计使用。

Amazon S3 控制台上提供适用于 S3 的 IAM Access Analyzer，无需额外费用。适用于 S3 的 IAM Access Analyzer 由 Amazon Identity and Access Management（IAM）IAM Access Analyzer 提供支持。要在 Amazon S3 控制台中使用适用于 S3 的 IAM Access Analyzer，您必须访问 IAM 控制台，然后按区域启用 IAM Access Analyzer。

有关 IAM Access Analyzer 的更多信息，请参阅《IAM 用户指南》中的什么是 IAM Access Analyzer？有关适用于 S3 的 IAM Access Analyzer 的更多信息，请查看以下部分。

**Important**

- 适用于 S3 的 IAM Access Analyzer 需要账户级分析器。要使用适用于 S3 的 IAM Access Analyzer，您必须访问 IAM Access Analyzer 并创建具有一个账户作为信任区域的分析器。有关更多信息，请参阅《IAM 用户指南》中的启用 IAM Access Analyzer。
- 适用于 S3 的 IAM Access Analyzer 不分析附加到跨账户接入点的接入点策略。之所以出现这种行为，是因为接入点及其策略位于信任区域（即账户）之外。如果您尚未将 `RestrictPublicBuckets` 屏蔽公共访问权限设置应用于存储桶或账户，则在 Buckets with public access（具有公有访问的存储桶）下列出了委托访问跨账户接入点的存储桶。当您应用 `RestrictPublicBuckets` 屏蔽公共访问权限设置时，该存储桶将在可从其他

Amazon Web Services 账户（包括第三方 Amazon Web Services 账户）访问的存储桶下报告。

- 添加或修改存储桶策略或存储桶 ACL 后，IAM Access Analyzer 会在 30 分钟内根据更改生成和更新调查发现。与账户级屏蔽公共访问权限设置相关的调查结果可能在您更改设置后长达 6 小时无法生成或更新。创建、删除多区域接入点或更改其策略后，最多可能会在 6 小时内生成或更新与多区域接入点相关的调查结果。

主题


- 适用于 S3 的 IAM Access Analyzer 提供哪些信息？
- 启用适用于 S3 的 IAM Access Analyzer
- 阻止所有公有访问
- 查看和更改桶访问权限
- 对存储桶结果进行归档
- 激活已归档的存储桶结果
- 查看结果详细信息
- 下载适用于 S3 的 IAM Access Analyzer 报告


## 适用于 S3 的 IAM Access Analyzer 提供哪些信息？

适用于 S3 的 IAM Access Analyzer 提供可在 Amazon Web Services 账户之外访问的存储桶的调查发现。Internet 上的任何人均可访问在 Buckets with public access（具有公有访问权限的存储桶）下面列出的存储桶。如果适用于 S3 的 IAM Access Analyzer 识别出公有存储桶，您还会在页面顶部看到一条警告，其中显示您的区域中公有存储桶的数量。可从其他 Amazon Web Services 账户（包括第三方 Amazon Web Services 账户）访问的存储桶下面列出的存储桶将与其他 Amazon Web Services 账户（包括组织外部的账户）有条件地共享。

对于每个存储桶，适用于 S3 的 IAM Access Analyzer 提供以下信息：

- Bucket name（存储桶名称）
- 被 Access Analyzer 发现 - 当适用于 S3 的 IAM Access Analyzer 发现了公有存储桶或共享存储桶访问时。
- 共享方式 - 如何通过存储桶策略、存储桶 ACL 或多区域接入点策略或接入点策略共享存储桶。多区域接入点和跨账户接入点反映在接入点下。可以通过策略和 ACL 来共享存储桶。如果您想要找到并查看存储桶访问的来源，您可以使用此列中的信息作为起点，立即采取精确的纠正措施。

- Status（状态）- 存储桶结果的状态。适用于 S3 的 IAM Access Analyzer 显示所有公有存储桶和共享存储桶的调查发现。
  - Active (活动) - 结果尚未审核。
  - Archived (已归档) - 结果已按预期审核和确认。
  - All（全部）– 公共存储桶或与其他 Amazon Web Services 账户（包括组织外部的 Amazon Web Services 账户）共享的存储桶的所有结果。
- Access level（访问级别）- 为存储桶授予的访问权限：
  - List (列出) - 列出资源。
  - Read (读取) - 读取但不编辑资源内容和属性。
  - Write (写入) - 创建、删除或修改资源。
  - Permissions (权限) - 授予或修改资源权限。
  - Tagging (标记) - 更新与资源关联的标记。

## 启用适用于 S3 的 IAM Access Analyzer

要使用适用于 S3 的 IAM Access Analyzer，您必须完成以下先决条件步骤。

1. 授予所需的权限。

   有关更多信息，请参阅《IAM 用户指南》中的使用 IAM Access Analyzer 所需的权限。
2. 请访问 IAM 以便为要使用 IAM Access Analyzer 的每个区域创建账户级分析器。

   适用于 S3 的 IAM Access Analyzer 需要账户级分析器。要使用适用于 S3 的 IAM Access Analyzer，您必须创建具有一个账户作为信任区域的分析器。有关更多信息，请参阅《IAM 用户指南》中的启用 IAM Access Analyzer。

## 阻止所有公有访问

如果您想要通过单击一次对存储桶屏蔽所有访问权限，则可以使用适用于 S3 的 IAM Access Analyzer 中的屏蔽所有公共访问权限按钮。当您阻止对存储桶的所有公有访问时，系统不会授予公有访问权限。我们建议您阻止所有对存储桶的公有访问，除非您需要公有访问才能支持特定和经验证的使用案例。在阻止所有公有访问之前，请确保您的应用程序在没有公有访问权限的情况下可以继续正常工作。

如果您不想阻止对存储桶的所有公有访问，则可以在 Amazon S3 控制台上编辑屏蔽公共访问权限设置，以配置存储桶的精细访问级别。有关更多信息，请参阅 阻止对您的 Amazon S3 存储的公有访问。

在极少数情况下，适用于 S3 的 IAM 访问权限分析器和 Amazon S3 屏蔽公共访问权限评估可能会因存储桶是否为公有而有所不同。之所以出现这种情况，是因为 Amazon S3 屏蔽公共访问权限除了评估公有访问权限外，还会对操作是否存在进行验证。假设存储桶策略包含一条 `Action` 语句，它支持公众访问 Amazon S3 不支持的操作（例如 `s3:NotASupportedAction`）。在这种情况下，Amazon S3 屏蔽公共访问权限会将存储桶评估为公有，因为如果稍后该操作变成受支持的，则这样的语句可能会使存储桶变为公有的。如果 Amazon S3 屏蔽公共访问权限和适用于 S3 的 IAM 访问权限分析器的评估存在差异，我们建议您查看存储桶策略并移除任何不受支持的操作。

使用适用于 S3 的 IAM Access Analyzer 对存储桶屏蔽所有公共访问权限

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中的 Dashboards（控制面板）下，请选择 Access analyzer for S3（S3 的访问分析器）。
3. 在适用于 S3 的 IAM Access Analyzer 中，选择一个存储桶。
4. 请选择 Block all public access (阻止所有公有访问)。
5. 要确认您阻止对存储桶的所有公有访问的意图，请在 Block all public access（bucket settings）[阻止所有公有访问（存储桶设置）] 中输入 **`confirm`**。

   Amazon S3 会阻止对存储桶的所有公有访问。存储桶调查发现的状态更新为已解决，并且存储桶从适用于 S3 的 IAM Access Analyzer 列表中消失。如果要查看已解决的桶，请在 IAM 控制台上打开 IAM Access Analyzer。

## 查看和更改桶访问权限

如果不打算对公有账户或其他 Amazon Web Services 账户 （包括组织外部的账户）授予访问权限，可以修改存储桶 ACL、存储桶策略，多区域接入点策略或接入点策略来删除对存储桶的访问权限。Shared through（共享方式）列显示存储桶访问权限的所有来源：存储桶策略、存储桶 ACL 和/或接入点策略。多区域接入点和跨账户接入点反映在接入点下。

查看和更改存储桶策略、存储桶 ACL，多区域接入点策略或接入点策略

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在导航窗格中，请选择 Access analyzer for S3 (S3 访问分析器)。
3. 要查看是否已通过存储桶策略、存储桶 ACL 多区域接入点策略或接入点策略授予公有访问权限或共享访问权限，请查看共享方式列。

4. 在存储桶下，请选择您想要更改或查看其存储桶策略、存储桶 ACL 多区域接入点策略或接入点策略的存储桶的名称。
5. 如果要更改或查看存储桶 ACL：
   a. 选择权限。
   b. 请选择访问控制列表。
   c. 查看您的存储桶 ACL，并根据需要进行更改。

   有关更多信息，请参阅 配置 ACL。
6. 如果要更改或查看存储桶策略：
   a. 选择权限。
   b. 请选择存储桶策略。
   c. 根据需要查看或更改存储桶策略。

   有关更多信息，请参阅 使用 Amazon S3 控制台添加存储桶策略。
7. 如果要更改或查看多区域接入点策略：
   a. 请选择多区域接入点。
   b. 请选择多区域接入点名称。
   c. 根据需要查看或更改多区域接入点策略。

   有关更多信息，请参阅 权限。
8. 如果要查看或更改接入点策略：
   a. 请选择接入点。
   b. 请选择接入点名称。
   c. 根据需要查看或更改访问权限。

   有关更多信息，请参阅 管理通用存储桶的 Amazon S3 接入点。

如果您编辑或删除存储桶 ACL、存储桶策略或接入点策略以删除公有访问或共享访问权限，则存储桶结果的状态会更新为已解决。已解决的桶调查发现从适用于 S3 的 IAM Access Analyzer 列表中消失，但您可以在 IAM Access Analyzer 中查看它们。

## 对存储桶结果进行归档

如果存储桶对公共账户或其他 Amazon Web Services 账户（包括组织外部的账户）授予访问权限，以便支持特定使用案例（例如，静态网站、公共下载或跨账户共享），则可以归档该存储桶的结果。当您对存储桶结果进行归档时，即表示您确认并记录存储桶保持公开或共享的意图。已归档的存储桶调查发现将保留在适用于 S3 的 IAM Access Analyzer 列表中，以便您始终知道哪些存储桶是公有存储桶或共享存储桶。

在适用于 S3 的 IAM Access Analyzer 中归档存储桶调查发现

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在导航窗格中，请选择 Access analyzer for S3（S3 访问分析器）。
3. 在适用于 S3 的 IAM Access Analyzer 中，选择一个活动的存储桶。
4. 要确认您想让公共账户或其他 Amazon Web Services 账户（包括组织外部的账户）访问此存储桶的意图，请选择 Archive（归档）。
5. 输入 **`confirm`**，然后选择 Archive (归档)。

## 激活已归档的存储桶结果

对结果进行归档后，您可以随时重新访问这些结果并将其状态更改回活动状态，这表明存储桶需要另一次审核。

在适用于 S3 的 IAM Access Analyzer 中激活归档的存储桶调查发现

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在导航窗格中，请选择 Access analyzer for S3（S3 访问分析器）。
3. 请选择已归档的存储桶结果。
4. 请选择 Mark as active (标记为活动)。

## 查看结果详细信息

如果您需要查看有关桶的更多信息，可以在 IAM 控制台上的 IAM Access Analyzer 中打开桶调查发现详细信息。

在适用于 S3 的 IAM Access Analyzer 中查看调查发现详细信息

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。

2. 在导航窗格中，请选择 Access analyzer for S3（S3 访问分析器）。
3. 在适用于 S3 的 IAM Access Analyzer 中，选择一个存储桶。
4. 请选择 View details (查看详细信息)。

   调查发现详细信息将在 IAM 控制台上的 IAM Access Analyzer 中打开。

## 下载适用于 S3 的 IAM Access Analyzer 报告

您可以将存储桶结果下载为 CSV 格式的报告，供审计使用。该报告包含的信息与您在 Amazon S3 控制台的适用于 S3 的 IAM Access Analyzer 中看到的信息相同。

下载报告

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，请选择 Access analyzer for S3（S3 的访问分析器）。
3. 在“Region (区域)”筛选器中，请选择相应的区域。

   适用于 S3 的 IAM Access Analyzer 会更新以显示所选区域的存储桶。
4. 请选择 Download report (下载报告)。

   系统会生成 CSV 报告并保存到您的计算机中。

# 使用存储桶拥有者条件验证存储桶所有权

Amazon S3 存储桶拥有者条件可确保您在 S3 操作中使用的存储桶属于您期望的 Amazon Web Services 账户。

大多数 S3 操作从特定 S3 存储桶读取或写入特定 S3 存储桶。这些操作包括上传、复制和下载对象、检索或修改存储桶配置以及检索或修改对象配置。执行这些操作时，您可以通过在请求中包含存储桶名称来指定要使用的存储桶。例如，要从 S3 检索对象，您需要发出一个请求，指定存储桶的名称和要从该存储桶中检索的对象键。

由于 Amazon S3 会根据存储桶的名称识别存储桶，因此在请求中使用错误存储桶名称的应用程序可能会无意中对非预期存储桶执行操作。为了帮助避免此类情况下的意外存储桶交互，您可以使用存储桶拥有者条件。存储桶拥有者条件使您能够验证目标存储桶是否由预期 Amazon Web Services 账户拥有，从而为 S3 操作具有预期效果提供了额外保证。

主题

- 何时使用存储桶拥有者条件
- 验证存储桶拥有者
- 示例
- 限制和局限性


## 何时使用存储桶拥有者条件

我们建议您在执行受支持的 S3 操作并知道预期存储桶拥有者的账户 ID 时使用存储桶拥有者条件。存储桶拥有者条件适用于所有 S3 对象操作和大多数 S3 存储桶操作。有关不支持存储桶拥有者条件的 S3 操作的列表，请参阅 限制和局限性。

要了解使用存储桶拥有者条件的好处，请考虑以下涉及 Amazon 客户 Bea 的场景：

1. Bea 开发使用 Amazon S3 的应用程序。在开发过程中，Bea 使用仅限测试的 Amazon Web Services 账户创建名为 `bea-data-test` 的存储桶，并将其应用程序配置为向 `bea-data-test` 发出请求。
2. Bea 部署其应用程序，但忘记将应用程序重新配置为使用其生产 Amazon Web Services 账户中的存储桶。
3. 在生产中，Bea 的应用程序向 `bea-data-test` 发出请求，这成功了。这导致生产数据写入 Bea 测试账户中的存储桶。

Bea 可以通过使用存储桶拥有者条件来帮助防范此类情况。使用存储桶拥有者条件，Bea 可以在其请求中包含预期存储桶拥有者的 Amazon Web Services 账户 ID。然后，Amazon S3 在处理每个请求之前检查存储桶拥有者的账户 ID。如果实际存储桶拥有者与预期存储桶拥有者不匹配，则请求将失败。

如果 Bea 使用存储桶拥有者条件，则之前描述的场景不会导致 Bea 的应用程序无意中写入测试存储桶。她的应用程序在步骤 3 中发出的请求将失败，并显示 `Access Denied` 错误消息。通过使用存储桶拥有者条件，Bea 帮助消除意外与错误 Amazon Web Services 账户 中的存储桶交互的风险。

## 验证存储桶拥有者

要使用存储桶拥有者条件，请在请求中包含一个参数，用于指定预期存储桶拥有者。大多数 S3 操作仅涉及单个存储桶，并且只需此单个参数即可使用存储桶拥有者条件。对于 `CopyObject` 操作，此第一个参数指定目标存储桶的预期拥有者，您包含第二个参数来指定源存储桶的预期拥有者。

当您发出包含存储桶拥有者条件参数的请求时，S3 会在处理该请求之前根据指定参数检查存储桶拥有者的账户 ID。如果参数与存储桶拥有者的账户 ID 匹配，S3 将处理该请求。如果参数与存储桶拥有者的账户 ID 不匹配，则该请求将失败并显示 `Access Denied` 错误消息。

您可以通过 Amazon Command Line Interface（Amazon CLI）、Amazon SDK 和 Amazon S3 REST API 来使用存储桶拥有者条件。通过 Amazon CLI 和 Amazon S3 REST API 使用存储桶拥有者条件时，请使用以下参数名称。

| 访问方法 | 用于非复制操作的参数 | 复制操作源参数 | 复制操作目标参数 |
| --- | --- | --- | --- |
| Amazon CLI | `--expected-bucket-owner` | `--expected-source-bucket-owner` | `--expected-bucket-owner` |
| Amazon S3 REST API | `x-amz-expected-bucket-owner` 标头 | `x-amz-source-expected-bucket-owner` 标头 | `x-amz-expected-bucket-owner` 标头 |

通过 Amazon SDK 使用存储桶拥有者条件所需的参数名称因语言而异。要确定所需的参数，请参阅所需语言的 SDK 文档。您可以在用于在 Amazon 上进行构建的工具中找到 SDK 文档。

## 示例

以下示例演示如何使用 Amazon CLI 或 Amazon SDK for Java 2.x 在 Amazon S3 中实施存储桶拥有者条件。

Example

示例：上传对象

以下示例将对象上传到 S3 存储桶*amzn-s3-demo-bucket1*，使用存储桶拥有者条件来确保 *amzn-s3-demo-bucket1* 由 Amazon Web Services 账户 111122223333 拥有。

Amazon CLI

```
aws s3api put-object \
                --bucket amzn-s3-demo-bucket1 --key exampleobject --
body example_file.txt \
```

```
                --expected-bucket-owner 111122223333
```

Amazon SDK for Java 2.x

```
public void putObjectExample() {
    S3Client s3Client = S3Client.create();;
    PutObjectRequest request = PutObjectRequest.builder()
            .bucket("amzn-s3-demo-bucket1")
            .key("exampleobject")
            .expectedBucketOwner("111122223333")
            .build();
    Path path = Paths.get("example_file.txt");
    s3Client.putObject(request, path);
}
```

Example

示例：复制对象

以下示例将对象 object1 从 S3 存储桶*amzn-s3-demo-bucket1* 复制到 S3 存储桶*amzn-s3-demo-bucket2*。根据下表，它使用存储桶拥有者条件来确保存储桶由预期账户拥有。

| 存储桶 | 预期拥有者 |
| --- | --- |
| *amzn-s3-demo-bucket1* | 111122223333 |
| *amzn-s3-demo-bucket2* | 444455556666 |

Amazon CLI

```
aws s3api copy-object --copy-source amzn-s3-demo-bucket1/object1 \
                          --bucket amzn-s3-demo-bucket2 --key object1copy \
                          --expected-source-bucket-owner 111122223333 --expected-
bucket-owner 444455556666
```

Amazon SDK for Java 2.x

```
public void copyObjectExample() {
```

```
        S3Client s3Client = S3Client.create();
        CopyObjectRequest request = CopyObjectRequest.builder()
                .copySource("amzn-s3-demo-bucket1/object1")
                .destinationBucket("amzn-s3-demo-bucket2")
                .destinationKey("object1copy")
                .expectedSourceBucketOwner("111122223333")
                .expectedBucketOwner("444455556666")
                .build();
        s3Client.copyObject(request);
    }
```

Example

示例：检索存储桶策略

以下示例检索 S3 存储桶*amzn-s3-demo-bucket1* 的访问策略，使用存储桶拥有者条件来确保 *amzn-s3-demo-bucket1* 由 Amazon Web Services 账户 111122223333 拥有。

Amazon CLI

```
aws s3api get-bucket-policy --bucket amzn-s3-demo-bucket1 --expected-bucket-
owner 111122223333
```

Amazon SDK for Java 2.x

```
public void getBucketPolicyExample() {
    S3Client s3Client = S3Client.create();
    GetBucketPolicyRequest request = GetBucketPolicyRequest.builder()
            .bucket("amzn-s3-demo-bucket1")
            .expectedBucketOwner("111122223333")
            .build();
    try {
        GetBucketPolicyResponse response = s3Client.getBucketPolicy(request);
    }
    catch (S3Exception e) {
        // The call was transmitted successfully, but Amazon S3 couldn't process
        // it, so it returned an error response.
        e.printStackTrace();
    }
}
```

## 限制和局限性

Amazon S3 存储桶拥有者条件具有以下限制和局限性：

- 存储桶拥有者条件参数的值必须是 Amazon Web Services 账户 ID（12 位字母数字值）。不支持服务主体。
- 存储桶拥有者条件不适用于 CreateBucket、ListBuckets 或 Amazon S3 控制中包含的任何操作。Amazon S3 将忽略对这些操作的请求中包含的任何存储桶拥有者条件参数。
- 存储桶拥有者条件仅验证在验证参数中指定的账户是否拥有该存储桶。存储桶拥有者条件不检查存储桶的配置。它也不能保证存储桶的配置符合任何特定条件或与任何过去的状态匹配。

# 为您的存储桶控制对象所有权和禁用 ACL。

S3 对象所有权是 Amazon S3 存储桶级别的设置，您可以使用该设置来控制上传到存储桶的对象的所有权并禁用或启用访问控制列表（ACL）。默认情况下，对象所有权设为强制存储桶拥有者设置，并且所有 ACL 均处于禁用状态。禁用 ACL 后，存储桶拥有者拥有存储桶中的所有对象，并使用访问管理策略来专门管理对数据的访问权限。

Amazon S3 中的大多数现代使用案例不再需要使用 ACL，我们建议您将 ACL 保持为禁用状态，除非有必须单独控制每个对象的访问权限的特殊情况。禁用 ACL 后，您可以使用策略来更轻松地控制对存储桶中每个对象的访问权限，无论是谁将对象上传到存储桶。

对象所有权有三个设置，您可以使用它来控制上传到存储桶的对象的所有权，并禁用或启用 ACL：

已禁用 ACL

- 强制存储桶拥有者（默认）– ACL 已禁用，存储桶拥有者自动拥有并完全控制存储桶中的每个对象。ACL 不再影响 S3 存储桶中对数据的权限。存储桶使用策略来定义访问控制。

已启用 ACL

- Bucket owner preferred（首选存储桶拥有者）— 存储桶拥有者拥有并完全控制其他账户使用 `bucket-owner-full-control` 标准 ACL 写入存储桶的新对象。
- 对象编写者— 该 Amazon Web Services 账户上传对象拥有该对象，对其拥有完全控制权，并且可以通过 ACL 授予其他用户访问该对象的权限。

对于 S3 中的大多数现代使用案例，我们建议您通过应用强制存储桶拥有者设置，并根据需要使用存储桶策略与账户外的用户共享数据，来将 ACL 保持为禁用状态。这种方法可简化权限管理。您可以在新创建的存储桶和现有存储桶上禁用 ACL。对于新创建的存储桶，默认情况下 ACL 处于禁用状态。如果现有存储桶中已有对象，在禁用 ACL 后，对象和存储桶 ACL 将不再是访问评估的一部分，并且根据策略授予或拒绝访问权限。对于现有存储桶，您可以在禁用 ACL 后随时重新启用它们，并恢复原先存在的存储桶和对象 ACL。

在禁用 ACL 之前，我们建议您查看存储桶策略，以确保它涵盖了您打算在账户外授予对存储桶访问权限的所有方式。禁用 ACL 后，存储桶仅接受未指定 ACL 的 PUT 请求或具有存储桶拥有者完全控制 ACL 的 PUT 请求，例如 `bucket-owner-full-control` 标准 ACL 或以 XML 表示的此 ACL 的等效形式。支持存储桶拥有者完全控制 ACL 的现有应用程序没有影响。包含其他 ACL 的 PUT 请求（例如，向某些 Amazon Web Services 账户的自定义授权）失败并返回带有错误代码 `AccessControlListNotSupported` 的 `400` 错误。

反之，具有首选存储桶拥有者设置的存储桶将继续接受和遵守存储桶和对象 ACL。有了这个设置，用 `bucket-owner-full-control` 标准的 ACL 编写的新对象将自动归存储桶拥有者而不是对象编写者所有。所有其他 ACL 行为都保持不变。为了要求所有 Amazon S3 PUT 操作都包含 `bucket-owner-full-control` 标准的 ACL，您可以添加一个存储桶策略，该策略只允许使用该 ACL 上传对象。

要查看哪些对象所有权设置应用于您的存储桶，您可以使用 Amazon S3 Storage Lens 存储统计管理工具指标。S3 Storage Lens 存储统计管理工具是一项云存储分析功能，您可以使用它在整个组织范围内了解对象存储的使用情况和活动。有关更多信息，请参阅使用 S3 Storage Lens 存储统计管理工具查找对象所有权设置。

> **Note**
>
> 有关将 Amazon S3 Express One Zone 存储类与目录存储桶配合使用的更多信息，请参阅 S3 Express One Zone 和使用目录存储桶。

## 对象所有权设置

此表显示了每个对象所有权设置对 ACL、对象、Object Ownership 和对象上传的影响。

| 设置 | 适用于 | 对 Object Ownership 的影响 | 对 ACL 的影响 | 已接受上传 |
| --- | --- | --- | --- | --- |
| 强制存储桶拥有者（默认） | 所有新的和现有对象 | 存储桶拥有者拥有每个对象。 | ACL 已禁用，不再影响存储桶的访问权限。设置或更新 ACL 的请求失败。然而，我们仍然支持读取 ACL 的请求。<br><br>存储桶拥有者拥有完全所有权和控制<br><br>对象编写者不再拥有完全的所有权和控制权。 | 使用存储桶拥有者完全控制 ACL 进行上传或未指定 ACL 的上传 |
| 首选存储桶拥有者 | 新对象 | 如果对象上传包含 `bucket-owner-full-control` 标准 ACL，存储桶拥有者拥有该对象。<br><br>使用其他 ACL 上传的对象归写入账户所有。 | ACL 可以更新并可以授予权限。<br><br>如果对象上传包含 `bucket-owner-full-control` 标准 ACL，存储桶拥有者具有完全控制权限，对象编写者不再具有完全控制权限。 | 所有上传项 |
| 对象编写者 | 新对象 | 对象编写者拥有该对象。 | ACL 可以更新并可以授予权限。<br><br>对象编写者具有完全控制权限。 | 所有上传项 |

# 通过禁用 ACL 引起的更改

当应用对象所有权的强制存储桶拥有者设置时，将禁用 ACL，并且您将自动拥有并完全控制存储桶中的每个对象，而无需执行任何其他操作。强制存储桶拥有者是所有新创建的存储桶的默认设置。应用强制存储桶拥有者设置后，您将看到三个变化：

- 所有存储桶 ACL 和对象 ACL 都被禁用，这将为您提供作为存储桶拥有者的完全访问权限。当您对存储桶或对象执行读取 ACL 请求时，您将看到仅向存储桶拥有者授予完全访问权限。
- 作为存储桶拥有者，您自动拥有并完全控制存储桶中的每个对象。
- ACL 不再影响存储桶的访问权限。因此，您数据的访问控制是基于策略执行的，例如 Amazon Identity and Access Management（IAM）基于身份的策略、Amazon S3 存储桶策略、VPC 端点策略以及 Organizations 服务控制策略（SCP）或资源控制策略（RCP）。

如果您使用 S3 版本控制，则存储桶拥有者拥有并完全控制存储桶中的所有对象版本。应用强制存储桶拥有者设置不会添加对象的新版本。

只有在新对象使用存储桶拥有者完全控制 ACL 或未指定 ACL 时，才能将新对象上传到存储桶。如果指定任何其他 ACL，对象上传将失败。有关更多信息，请参阅 故障排除。

因为以下示例中使用 Amazon Command Line Interface（Amazon CLI）的 `PutObject` 操作包含 `bucket-owner-full-control` 固有的 ACL，所以目标可以上传至 ACL 禁用的存储桶中。

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key key-name --body path-to-file --
acl bucket-owner-full-control
```

因为以下 `PutObject` 操作没有指定 ACL，对于禁用 ACL 的存储桶，它也会成功。

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key key-name --body path-to-file
```

> **Note**
>
> 如果其他 Amazon Web Services 账户 在上传后需要对象的访问权限，您必须通过存储桶策略向这些账户授予其他权限。有关更多信息，请参阅 演练：使用策略管理针对 Amazon S3 资源的访问权限。

重新启用 ACL

您可以随时从强制存储桶拥有者设置更改为另一个对象所有权设置来重新启用 ACL。如果在应用强制存储桶拥有者设置之前使用了对象 ACL 进行权限管理，并且您没有将这些对象 ACL 权限迁移到存储桶策略中，则在重新启用 ACL 后，这些权限将恢复。此外，在应用强制存储桶拥有者设置时写入存储桶的对象仍然归存储桶拥有者所有。

例如，如果您从强制存储桶拥有者设置更改回对象编写者设置，则作为存储桶拥有者，您将不再拥有和完全控制以前由其他 Amazon Web Services 账户拥有的对象。反之，上传账户将再次拥有这些对象。其他账户拥有的对象使用 ACL 获取权限，因此您不能使用策略向这些对象授予权限。但是，您作为存储桶拥有者，在应用强制存储桶拥有者设置时，仍然拥有写入存储桶的任何对象。这些对象不归对象编写者所有，即使您重新启用 ACL 也是如此。

有关使用 Amazon Web Services Management Console、Amazon Command Line Interface（CLI）、REST API 或 Amazon SDK 启用和管理 ACL 的说明，请参阅配置 ACL。

## 禁用 ACL 的先决条件

在为现有存储桶禁用 ACL 之前，请先完成以下先决条件。

- 查看存储桶和对象 ACL 并迁移 ACL 权限
- 识别需要 ACL 进行授权的请求
- 查看和更新使用 ACL 相关条件密钥的存储桶策略

## Object Ownership 权限

要应用、更新或删除存储桶的对象所有权设置，您需要 `s3:PutBucketOwnershipControls` 权限。要返回存储桶的对象所有权设置，您需要 `s3:GetBucketOwnershipControls` 权限。有关更多信息，请参阅 在创建存储桶时设置对象所有权 和 查看 S3 存储桶的对象所有权设置。

## 禁用所有新存储桶的 ACL

默认情况下，所有新存储桶都是在应用强制存储桶拥有者设置的情况下创建的，且 ACL 处于禁用状态。我们建议将 ACL 保持为禁用状态。作为一般规则，我们建议您使用基于 S3 资源的策略（存储桶策略和接入点策略）或 IAM 策略进行访问控制，而不是 ACL。策略是一种经过简化，且更灵活的访问控制选项。借助存储桶策略和接入点策略，您可以定义广泛适用于针对 Amazon S3 资源的所有请求的规则。

# 复制和 Object Ownership

当您使用 S3 复制，并且源存储桶和目标存储桶由不同的 Amazon Web Services 账户拥有时，您可以禁用 ACL（对于对象所有权应用强制存储桶拥有者设置），以将副本拥有权更改为拥有目标存储桶的 Amazon Web Services 账户。此设置模拟现有的所有者覆盖行为，而无需 `s3:ObjectOwnerOverrideToBucketOwner` 权限。在采用强制存储桶拥有者设置的情况下复制到目标存储桶的所有对象都归目标存储桶拥有者所有。有关复制配置的所有者覆盖选项的更多信息，请参阅 更改副本拥有者。

## 设置对象所有权

您可以使用 Amazon S3 控制台、Amazon CLI、Amazon SDK、Amazon S3 REST API 或 Amazon CloudFormation 应用对象所有权设置。以下 REST API 和 Amazon CLI 命令支持 Object Ownership：

| REST API | Amazon CLI | 描述 |
| --- | --- | --- |
| PutBucketOwnershipControls | put-bucket-ownership-controls | 为现有 S3 存储桶创建或修改对象所有权设置。 |
| CreateBucket | create-bucket | 使用创建存储桶 `x-amz-object-ownership` 请求标头以指定对象所有权设置。 |
| GetBucketOwnershipControls | get-bucket-ownership-controls | 检索 Amazon S3 存储桶的对象所有权设置。 |
| DeleteBucketOwnershipControls | delete-bucket-ownership-controls | 删除 Amazon S3 存储桶的对象所有权设置。 |

有关应用和使用 Object Ownership 设置的更多信息，请参阅以下主题。

主题

- 禁用 ACL 的先决条件
- 在创建存储桶时设置对象所有权
- 为现有存储桶设置对象所有权
- 查看 S3 存储桶的对象所有权设置
- 禁用所有新存储桶的 ACL 并强制执行 Object Ownership

- 故障排除

# 禁用 ACL 的先决条件

Amazon S3 中的存储桶访问控制列表（ACL）是一种机制，可让您为 S3 存储桶中的单个对象定义精细权限，并指定哪些 Amazon 账户或组可以访问和修改这些对象。Amazon S3 中的大多数现代使用案例不再需要使用 ACL。我们建议您使用 Amazon Identity and Access Management（IAM）和存储桶策略来管理访问权限，并将 ACL 保持为禁用状态，除非有需要单独控制每个对象的访问权限的特殊情况。

如果您在存储桶上启用了 ACL，则在禁用 ACL 之前，请完成以下先决条件：

主题

- 查看存储桶和对象 ACL 并迁移 ACL 权限
- 识别需要 ACL 进行授权的请求
- 查看和更新使用 ACL 相关条件密钥的存储桶策略
- 使用案例示例

## 查看存储桶和对象 ACL 并迁移 ACL 权限

禁用 ACL 时，存储桶和对象 ACL 授予的权限不再影响访问。在禁用 ACL 之前，请查看存储桶和对象 ACL。

您现有的每个存储桶和对象 ACL 在 IAM 策略中都有等效的。下面的存储桶策略示例向您演示存储桶和对象 ACL 的 `READ` 和 `WRITE` 权限如何映射到 IAM 权限。有关如何将每个 ACL 转换为 IAM 权限的更多信息，请参阅 ACL 权限和访问策略权限的映射。

在禁用 ACL 之前：

- 如果存储桶 ACL 授予您 Amazon 账户之外的访问权限，首先必须将存储桶 ACL 权限迁移到存储桶策略中。
- 接下来，将存储桶 ACL 重置为默认的私有 ACL。
- 我们还建议您查看对象级 ACL 权限并将其迁移到存储桶策略中。

如果存储桶 ACL 向账户以外的其他人授予读取或写入权限，在可以禁用 ACL 之前，必须将这些权限迁移到存储桶策略。迁移这些权限后，可以将对象所有权设置为强制存储桶拥有者设置。如果您不迁移在

账户之外授予读取或写入访问权限的存储桶 ACL，则应用强制存储桶拥有者设置的请求将失败，并返回 InvalidBucketAclWithObjectOwnership 错误代码。

如果您的存储桶 ACL 授予 Amazon Web Services 账户 以外的访问权限，在禁用 ACL 之前，您必须将存储桶 ACL 权限迁移到存储桶策略中，然后将存储桶 ACL 重置为默认私有 ACL。如果不迁移和重置，则应用强制存储桶拥有者设置来禁用 ACL 的请求将失败，并返回 InvalidBucketAclWithObjectOwnership 错误代码。我们还建议您查看对象 ACL 权限并将其迁移到存储桶策略中。

要查看 ACL 权限并将其迁移至存储桶策略，请参阅以下主题。

主题

- 存储桶策略示例
- 使用 S3 控制台查看和迁移 ACL 权限
- 使用 Amazon CLI 查看和迁移 ACL 权限

### 存储桶策略示例

这些示例存储桶策略将为您显示如何针对第三方 Amazon Web Services 账户 将 READ 和 WRITE 存储桶和对象 ACL 权限迁移至存储桶策略，对于策略，READ_ACP 和 WRITE_ACP ACL 相关性较小，这是因为其授予 ACL 相关的权限（s3:GetBucketAcl、s3:GetObjectAcl、s3:PutBucketAcl 和s3:PutObjectAcl）。

#### Example – 存储桶的 **READ** ACL

如果您的存储桶具有 READ ACL 来向 Amazon Web Services 账户 *111122223333* 授予列出存储桶内容的权限，则您可以编写授予对存储桶的 s3:ListBucket、s3:ListBucketVersions、s3:ListBucketMultipartUploads 权限的存储桶策略。

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
    "Sid": "Permission to list the objects in a bucket",
    "Effect": "Allow",
    "Principal": {
     "AWS": [
```

```
      "arn:aws:iam::111122223333:root"
     ]
    },
    "Action": [
     "s3:ListBucket",
     "s3:ListBucketVersions",
     "s3:ListBucketMultipartUploads"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
   }
  ]
 }
```

Example – 存储桶中每个对象的 **READ** ACL

如果存储桶中的每个对象都有向 Amazon Web Services 账户 *111122223333* 授予访问权限的 READ ACL，则您可以编写存储桶策略，以便为存储桶中的每个对象授予对此账户的 `s3:GetObject` 和 `s3:GetObjectVersion` 权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
    "Sid": "Read permission for every object in a bucket",
    "Effect": "Allow",
    "Principal": {
     "AWS": [
      "arn:aws:iam::111122223333:root"
     ]
    },
    "Action": [
     "s3:GetObject",
     "s3:GetObjectVersion"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
   }
  ]
 }
```

此示例资源元素授予对特定对象的访问权限。

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket/OBJECT-KEY"
```

Example – 授予将对象写入存储桶的权限的 **WRITE** ACL

如果您的存储桶具有 WRITE ACL 以向 Amazon Web Services 账户 *111122223333* 授予将对象写入存储桶的权限，则您可以编写授予对存储桶的 s3:PutObject 权限的存储桶策略。

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
    "Sid": "Permission to write objects to a bucket",
    "Effect": "Allow",
    "Principal": {
     "AWS": [
      "arn:aws:iam::111122223333:root"
     ]
    },
    "Action": [
     "s3:PutObject"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
   }
  ]
 }
```

使用 S3 控制台查看和迁移 ACL 权限

查看存储桶的 ACL 权限

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets（存储桶）列表中，请选择存储桶名称。
3. 选择 Permissions（权限）选项卡。
4. 在 Access control list（ACL）（访问控制列表）中，查看您的存储桶 ACL 权限。

查看对象的 ACL 权限

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Bucket（存储桶）列表中，选择包含对象的存储桶名称。
3. 在 Objects（对象）列表中，请选择对象名称。

4. 选择 Permissions（权限）选项卡。
5. 在 Access control list (ACL)（访问控制列表）中，查看您的对象 ACL 权限。

要迁移 ACL 权限并更新存储桶 ACL

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets（存储桶）列表中，请选择存储桶名称。
3. 在 Permissions（权限）标签页中，在 Bucket policy（存储桶策略）下，请选择 Edit（编辑）。
4. 在 Policy（策略）框中添加或更新存储桶策略。

   有关示例存储桶策略，请参阅 存储桶策略示例 和 使用案例示例。
5. 选择保存更改。
6. 更新存储桶 ACL以移除授予其他组或 Amazon Web Services 账户 的 ACL。
7. 为对象所有权应用强制存储桶拥有者设置。

使用 Amazon CLI 查看和迁移 ACL 权限

1. 要返回存储桶的存储桶 ACL，请使用 get-bucket-acl Amazon CLI 命令：

```
aws s3api get-bucket-acl --bucket amzn-s3-demo-bucket
```

   例如，此存储桶 ACL 授予 WRITE 和 READ 访问第三方账户。在此 ACL 中，第三方账户由 canonical user ID（规范的用户 ID）识别。要应用强制存储桶拥有者设置并禁用 ACL，您必须将第三方账户的这些权限迁移到存储桶策略。

```
{
  "Owner": {
   "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
   "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID"
  },
  "Grants": [
   {
    "Grantee": {
     "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
     "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID",
     "Type": "CanonicalUser"
```

```
    },
    "Permission": "FULL_CONTROL"
   },
   {
    "Grantee": {
     "DisplayName": "THIRD-PARTY-EXAMPLE-ACCOUNT",
     "ID":
"72806de9d1ae8b171cca9e2494a8d1335dfced4ThirdPartyAccountCanonicalUserID",
     "Type": "CanonicalUser"
    },
    "Permission": "READ"
   },
   {
    "Grantee": {
     "DisplayName": "THIRD-PARTY-EXAMPLE-ACCOUNT",
     "ID":
"72806de9d1ae8b171cca9e2494a8d1335dfced4ThirdPartyAccountCanonicalUserID",
     "Type": "CanonicalUser"
    },
    "Permission": "WRITE"
   }
  ]
}
```

有关其他示例 ACL，请参阅 使用案例示例。

2. 将存储桶 ACL 权限迁移到存储桶策略：

此示例存储桶策略为第三方账户授予 `s3:PutObject` 和 `s3:ListBucket` 权限。在存储桶策略中，第三方账户由 Amazon Web Services 账户 ID（*111122223333*）标识。

```
aws s3api put-bucket-policy --bucket amzn-s3-demo-bucket --policy file://
policy.json

 policy.json:
 {
  "Version": "2012-10-17",
  "Statement": [
   {
    "Sid": "PolicyForCrossAccountAllowUpload",
    "Effect": "Allow",
    "Principal": {
     "AWS": [
```

```
      "arn:aws:iam::111122223333:root"
     ]
    },
    "Action": [
     "s3:PutObject",
     "s3:ListBucket"
    ],
    "Resource": [
     "arn:aws:s3:::amzn-s3-demo-bucket",
     "arn:aws:s3:::amzn-s3-demo-bucket/*"
   }
  ]
}
```

有关更多示例存储桶策略，请参阅 存储桶策略示例 和 使用案例示例。

3. 要返回特定对象的 ACL，请使用 get-object-acl Amazon CLI 命令。

```
aws s3api get-object-acl --bucket amzn-s3-demo-bucket --key EXAMPLE-OBJECT-KEY
```

4. 如果需要，请将对象 ACL 权限迁移到存储桶策略中。

此示例资源元素授予对存储桶策略中特定对象的访问权限。

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket/EXAMPLE-OBJECT-KEY"
```

5. 将存储桶的 ACL 重置为默认的 ACL。

```
aws s3api put-bucket-acl --bucket amzn-s3-demo-bucket --acl private
```

6. 为对象所有权应用强制存储桶拥有者设置。

## 识别需要 ACL 进行授权的请求

要识别需要 ACL 进行授权的 Amazon S3 请求，您可以使用 Amazon S3 服务器访问日志或 Amazon CloudTrail 中的 `aclRequired` 值。如果请求需要 ACL 进行授权，或者如果您具有指定 ACL 的 PUT 请求，则字符串为 `Yes`。如果不需要 ACL，或者您正在设置 `bucket-owner-full-control` 标准 ACL，或者如果您的存储桶策略允许请求，则 Amazon S3 服务器访问日志中的 `aclRequired` 值字符串为“`-`”，但 CloudTrail 中不存在该值字符串。有关预期 `aclRequired` 值的更多信息，请参阅常见 Amazon S3 请求的 `aclRequired` 值。

如果您的 PutBucketAcl 或 PutObjectAcl 请求的标头授予基于 ACL 的权限（bucket-owner-full-control 标准 ACL 除外），则必须先删除这些标头，然后才能禁用 ACL。否则，您的请求将失败。

对于需要 ACL 进行授权的所有其他请求，请将这些 ACL 权限迁移到存储桶策略。然后，在启用强制存储桶拥有者设置之前，删除所有存储桶 ACL。

> **Note**
>
> 请勿删除对象 ACL。否则，依赖于对象 ACL 获取权限的应用程序将失去访问权限。

如果您发现没有请求需要 ACL 进行授权，则可以继续禁用 ACL。有关识别请求的更多信息，请参阅使用 Amazon S3 服务器访问日志来确定请求和使用 CloudTrail 识别 Amazon S3 请求。

## 查看和更新使用 ACL 相关条件密钥的存储桶策略

应用强制存储桶拥有者设置以禁用 ACL 后，只有在请求使用存储桶拥有者完全控制 ACL 或未指定 ACL 的情况下，才能将新对象上传到存储桶。在禁用 ACL 之前，请查看存储桶策略以了解 ACL 相关的条件密钥。

如果您的存储桶策略使用 ACL 相关的条件密钥来要求 bucket-owner-full-control 储存的 ACL（例如，s3:x-amz-acl），您无需更新存储桶策略。以下存储桶策略使用 s3:x-amz-acl 以要求 bucket-owner-full-control 储存的 ACL 用于 S3 PutObject 请求。这项策略仍旧要求对象编写者指定 bucket-owner-full-control 标准的 ACL。但是，禁用 ACL 的存储桶仍然接受此 ACL，因此请求将继续成功，无需客户端更改。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Only allow writes to my bucket with bucket owner full control",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:user/ExampleUser"
                ]
            },
            "Action": [
                "s3:PutObject"
            ],
```

```
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
            }
        }
    ]
}
```

但是，如果您的存储桶策略使用的是要求不同 ACL 的 ACL 相关条件密钥，则必须移除此条件密钥。此示例存储桶策略要求 public-read ACL 用于 S3 PutObject 请求，因此必须在禁用 ACL 之前进行更新。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Only allow writes to my bucket with public read access",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:user/ExampleUser"                ]
            },
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "public-read"
                }
            }
        }
    ]
}
```

## 使用案例示例

以下示例向您演示如何针对特定使用案例将 ACL 权限迁移到存储桶策略。

主题

- 为服务器访问日志记录授予对 S3 日志传输组的访问权限
- 授予存储桶中对象的公共读取访问权限。
- 授予 Amazon ElastiCache（Redis OSS）对 Amazon S3 存储桶的访问权限

为服务器访问日志记录授予对 S3 日志传输组的访问权限

如果要应用强制存储桶拥有者设置以便对服务器访问日志记录目标存储桶（也称作目标存储桶）禁用 ACL，必须将 S3 日志传输组的存储桶 ACL 权限迁移到存储桶策略中的日志记录服务主体（logging.s3.amazonaws.com）。有关日志交付权限的更多信息，请参阅 日志传输的权限。

此存储桶 ACL 授予 WRITE 和 READ_ACP 访问 S3 日志传输组的权限：

```
{
    "Owner": {
        "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
        "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID"
    },
    "Grants": [
        {
            "Grantee": {
                "Type": "CanonicalUser",
                "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
                "ID":
 "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID"
            },
            "Permission": "FULL_CONTROL"
        },
        {
            "Grantee": {
                "Type": "Group",
                "URI": "http://acs.amazonaws.com/groups/s3/LogDelivery"
            },
            "Permission": "WRITE"
        },
        {
            "Grantee": {
                "Type": "Group",
                "URI": "http://acs.amazonaws.com/groups/s3/LogDelivery"
            },
            "Permission": "READ_ACP"
        }
    ]
```

```
}
```

将 S3 日志传输组的存储桶 ACL 权限迁移到存储桶策略中的日志录入服务主体

1. 将以下存储桶策略添加到目标存储桶，并替换示例值。

```
aws s3api put-bucket-policy --bucket amzn-s3-demo-bucket --policy file://
policy.json

policy.json:      {
    {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3ServerAccessLogsPolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "logging.s3.amazonaws.com"
            },
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/EXAMPLE-LOGGING-PREFIX*",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:::SOURCE-BUCKET-NAME"
                },
                "StringEquals": {
                    "aws:SourceAccount": "SOURCE-AWS-ACCOUNT-ID"
                }
            }
        }
    ]
}
```

2. 将目标存储桶的 ACL 重置为默认 ACL。

```
aws s3api put-bucket-acl --bucket amzn-s3-demo-bucket --acl private
```

3. 为目标存储桶的对象所有权应用强制存储桶拥有者设置。

授予存储桶中对象的公共读取访问权限。

如果您的对象 ACL 授予对存储桶中所有对象的公共读取访问权限，则可以将这些 ACL 权限迁移到存储桶策略。

此对象 ACL 授予对存储桶中对象的公共读取访问权限：

```
{
    "Owner": {
        "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
        "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID"
    },
    "Grants": [
        {
            "Grantee": {
                "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
                "ID":
 "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID",
                "Type": "CanonicalUser"
            },
            "Permission": "FULL_CONTROL"
        },
        {
            "Grantee": {
                "Type": "Group",
                "URI": "http://acs.amazonaws.com/groups/global/AllUsers"
            },
            "Permission": "READ"
        }
    ]
}
```

要将公共读取 ACL 权限迁移到存储桶策略

1. 要向存储桶中的所有对象授予公有读取权限，请添加以下存储桶策略，替换示例值。

```
aws s3api put-bucket-policy --bucket amzn-s3-demo-bucket --policy
 file://policy.json

policy.json:
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "PublicReadGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        }
    ]
}
```

要授予对存储桶策略中特定对象的公共访问权限，请使用以下 Resource 元素的格式。

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket/OBJECT-KEY"
```

要使用特定的前缀授予对所有对象的公共访问权，请使用以下 Resource 元素的格式。

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket/PREFIX/*"
```

2. 为对象所有权应用强制存储桶拥有者设置。

授予 Amazon ElastiCache（Redis OSS）对 Amazon S3 存储桶的访问权限

您可以将 ElastiCache（Redis OSS）备份导出到 S3 存储桶中，这样您就可以从 ElastiCache 外部访问备份。要将备份导出到 S3 存储桶，您必须授予 ElastiCache 权限，以便将快照复制到存储桶。如果您已在存储桶 ACL 中授予了对 ElastiCache 的权限，则必须在应用强制存储桶拥有者设置以禁用 ACL 之前将这些权限迁移到存储桶策略。有关更多信息，请参阅 Amazon ElastiCache User Guide（Amazon ElastiCache 用户指南）中的 Grant ElastiCache access to your Amazon S3 存储桶（授予 ElastiCache 访问 Amazon S3 存储桶的权限）。

以下示例显示了向 ElastiCache 授予权限的存储桶 ACL 权限。

```
{
    "Owner": {
        "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
        "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID"
    },
    "Grants": [
```

```
        {
            "Grantee": {
                "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
                "ID":
 "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID",
                "Type": "CanonicalUser"
            },
            "Permission": "FULL_CONTROL"
        },
        {
            "Grantee": {
                "DisplayName": "aws-scs-s3-readonly",
                "ID":
 "540804c33a284a299d2547575ce1010f2312ef3da9b3a053c8bc45bf233e4353",
                "Type": "CanonicalUser"
            },
            "Permission": "READ"
        },
        {
            "Grantee": {
                "DisplayName": "aws-scs-s3-readonly",
                "ID":
 "540804c33a284a299d2547575ce1010f2312ef3da9b3a053c8bc45bf233e4353",
                "Type": "CanonicalUser"
            },
            "Permission": "WRITE"
        },
        {
            "Grantee": {
                "DisplayName": "aws-scs-s3-readonly",
                "ID":
 "540804c33a284a299d2547575ce1010f2312ef3da9b3a053c8bc45bf233e4353",
                "Type": "CanonicalUser"
            },
            "Permission": "READ_ACP"
        }
    ]
}
```

将用于 ElastiCache（Redis OSS）的存储桶 ACL 权限迁移到存储桶策略

1. 将以下存储桶策略添加到存储桶，替换示例值。

```
aws s3api put-bucket-policy --bucket amzn-s3-demo-bucket --policy
 file://policy.json

policy.json:
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt15399483",
            "Effect": "Allow",
            "Principal": {
                "Service": "Region.elasticache-snapshot.amazonaws.com"
            },
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketAcl",
                "s3:ListMultipartUploadParts",
                "s3:ListBucketMultipartUploads"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        }
    ]
}
```

2. 将存储桶的 ACL 重置为默认的 ACL：

```
aws s3api put-bucket-acl --bucket amzn-s3-demo-bucket --acl private
```

3. 为对象所有权应用强制存储桶拥有者设置。

## 在创建存储桶时设置对象所有权

创建存储桶时，您可以配置 S3 对象所有权。要为现有存储桶设置对象所有权，请参阅 为现有存储桶设置对象所有权。

S3 对象所有权是 Amazon S3 存储桶级设置，您可以使用它禁用 access control lists（ACLs）（访问控制列表 ACL），并获取存储桶中每个对象的所有权，从而简化了对存储在 Amazon S3 中的数据的访问管理。默认情况下，S3 对象所有权设为强制存储桶拥有者设置，并且对于新存储桶禁用 ACL。禁用 ACL 后，存储桶拥有者拥有存储桶中的每个对象，并使用访问管理策略来专门管理对数据的访问权限。我们建议您将 ACL 保持为禁用状态，除非有必须单独控制每个对象的访问权限的特殊情况。

对象所有权有三个设置，您可以使用它来控制上传到存储桶的对象的所有权，并禁用或启用 ACL：

已禁用 ACL

- 强制存储桶拥有者（默认）– ACL 已禁用，存储桶拥有者自动拥有并完全控制存储桶中的每个对象。ACL 不再影响 S3 存储桶中对数据的权限。存储桶使用策略来定义访问控制。

已启用 ACL

- Bucket owner preferred（首选存储桶拥有者）— 存储桶拥有者拥有并完全控制其他账户使用 `bucket-owner-full-control` 标准 ACL 写入存储桶的新对象。
- 对象编写者— 该 Amazon Web Services 账户上传对象拥有该对象，对其拥有完全控制权，并且可以通过 ACL 授予其他用户访问该对象的权限。

权限：要应用 Bucket owner enforced（强制存储桶拥有者）设置或 Bucket owner preferred（首选存储桶拥有者）设置，必须有以下权限：`s3:CreateBucket` 和 `s3:PutBucketOwnershipControls`。在应用了 Object writer（对象编写者）设置的情况下创建存储桶时，不需要额外的权限。有关 Amazon S3 权限的更多信息，请参阅《Service Authorization Reference》中的 Actions, resources, and condition keys for Amazon S3。

有关按 S3 资源类型对 S3 API 操作的权限的更多信息，请参阅 Amazon S3 API 操作所需的权限。

> **Important**
>
> Amazon S3 中的大多数现代使用案例不再需要使用 ACL，我们建议您禁用 ACL，除非在需要单独控制每个对象的访问的异常情况下。使用对象所有权，您可以禁用 ACL 并依赖策略进行访问控制。禁用 ACL 时，您可以轻松维护具有通过不同的 Amazon 账户上传的对象的存储桶。作为存储桶拥有者，您拥有存储桶中的所有对象，并可以使用策略管理对它们的访问。

使用 S3 控制台

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在页面顶部的导航栏中，选择当前所显示 Amazon Web Services 区域的名称。接下来，选择要在其中创建存储桶的区域。

   > **Note**
   >
   > - 存储桶创建后，便无法再更改其区域。
   > - 要最大程度地减少延迟和成本以及满足法规要求，请选择一个靠近您的区域。在某一区域存储的对象将一直留在该区域，除非您特意将其转移到其他区域。有关 Amazon S3 Amazon Web Services 区域的列表，请参阅《Amazon Web Services 一般参考》中的 Amazon Web Services 服务 端点。

3. 在左侧导航窗格中，选择通用存储桶。
4. 选择创建存储桶。此时将打开创建存储桶页面。
5. 对于存储桶名称，请输入存储桶的名称。

   存储桶名称必须满足以下要求：

   - 在分区中是唯一的。分区是区域的分组。Amazon 目前有三个分区：aws（商用区域）、aws-cn（中国区域）和 aws-us-gov（Amazon GovCloud (US) Regions）。
   - 长度必须介于 3 到 63 个字符之间。
   - 只能由小写字母、数字、句点 (.) 和连字符 (-) 组成。为了获得最佳兼容性，我们建议您避免在存储桶名称中使用句点 (.)，但仅用于静态网站托管的存储桶除外。
   - 以字母或数字开头和结尾。
   - 有关存储桶命名规则的完整列表，请参阅通用存储桶命名规则。

   > **Important**
   >
   > - 创建存储桶后，便无法更改其名称。
   > - 请勿在存储桶名称中包含敏感信息。存储桶名称会显示在指向存储桶中的对象的 URL 中。

6. （可选）在常规配置下，您可以选择将现有存储桶的设置复制到新存储桶。如果您不想复制现有存储桶的设置，请跳到下一步。

> **Note**
>
> 此选项：
>
> - 在 Amazon CLI 中不可用，仅在 Amazon S3 控制台中可用
> - 不会将存储桶策略从现有存储桶复制到新存储桶

要复制现有存储桶的设置，请在从现有存储桶复制设置下，选择选择存储桶。将打开选择存储桶窗口。找到包含您要复制的设置的存储桶，然后选择选择存储桶。选择存储桶窗口关闭，而创建存储桶窗口重新打开。

在从现有存储桶复制设置下，您现在将看到您选择的存储桶的名称。新存储桶的设置现在与您选择的存储桶的设置相匹配。如果要移除复制的设置，请选择恢复默认设置。在创建存储桶页面上查看其余的存储桶设置。如果您不想进行任何更改，可以跳到最后一步。

7. 在 Object Ownership（对象所有权）下方，要禁用或启用 ACL，并控制上传到存储桶中的对象的所有权，请选择以下设置之一：

已禁用 ACL

- 强制存储桶拥有者（默认）：ACL 已禁用，存储桶拥有者自动拥有并完全控制通用存储桶中的每个对象。ACL 不再影响对 S3 通用存储桶中数据的访问权限。存储桶专门使用策略来定义访问控制。

  默认情况下，ACL 处于禁用状态。Amazon S3 中的大多数现代使用案例不再需要使用 ACL。我们建议您将 ACL 保持为禁用状态，除非有必须单独控制每个对象的访问权限的特殊情况。有关更多信息，请参阅 为您的存储桶控制对象所有权和禁用 ACL。。

已启用 ACL

- Bucket owner preferred（首选存储桶拥有者）— 存储桶拥有者拥有并完全控制其他账户使用 `bucket-owner-full-control` 标准 ACL 写入存储桶的新对象。

  如果应用首选存储桶拥有者设置，以要求所有 Amazon S3 上传都包含 `bucket-owner-full-control` 标准 ACL，则可以添加存储桶策略，该策略只允许使用此 ACL 上传对象。

- 对象编写者— 该 Amazon Web Services 账户上传对象拥有该对象，对其拥有完全控制权，并且可以通过 ACL 授予其他用户访问该对象的权限。

> **Note**
>
> 默认设置为强制存储桶拥有者。要应用默认设置并将 ACL 保持为禁用状态，只需要 `s3:CreateBucket` 权限。要启用 ACL，您必须具有 `s3:PutBucketOwnershipControls` 权限。

8. 在此存储桶的屏蔽公共访问权限设置中，请选择要应用于存储桶的屏蔽公共访问权限设置。

   默认情况下，启用所有四个“屏蔽公共访问权限”设置。我们建议您将所有设置保持为启用状态，除非您知道您需要为您的特定使用案例关闭其中一个或多个设置。有关屏蔽公共访问权限的更多信息，请参阅阻止对您的 Amazon S3 存储的公有访问。

   > **Note**
   >
   > 要启用所有“屏蔽公共访问权限”设置，只需要 `s3:CreateBucket` 权限。要关闭任何“屏蔽公共访问权限”设置，您必须拥有 `s3:PutBucketPublicAccessBlock` 权限。

9. （可选）默认情况下，存储桶版本控制处于禁用状态。版本控制是在相同的存储桶中保留对象的多个变量的方法。对于 存储桶中存储的每个对象，您可以使用版本控制功能来保留、检索和还原它们的各个版本。使用版本控制能够更加轻松地从用户意外操作和应用程序故障中恢复数据。有关版本控制的更多信息，请参阅使用 S3 版本控制保留对象的多个版本。

   要在存储桶上启用版本控制，请选择启用。

10. （可选）在 Tags（标签）下，您可以选择向存储桶添加标签。利用 Amazon 成本分配功能，可以使用存储桶标签来对存储桶的使用计费添加注释。一个标签即为一个键值对，用于表示用户分配给存储桶的标记。有关更多信息，请参阅 the section called “使用成本分配标签”。

    要添加存储桶标签，请输入 Key（键），并（可选）输入 Value（值），然后选择 Add Tag（添加标签）。

11. 要配置默认加密，请在加密类型下，选择以下选项之一：

    - 具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）
    - 具有 Amazon Key Management Service 密钥的服务器端加密（SSE-KMS）

- 具有 Amazon Key Management Service（Amazon KMS）密钥的双层服务器端加密（DSSE-KMS）

> **Important**
>
> 如果您将 SSE-KMS 或 DSSE-KMS 选项用于默认加密配置，则您将受到 Amazon KMS 的每秒请求数（RPS）配额限制。有关 Amazon KMS 限额以及如何请求增加限额的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的限额。

通过将具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）用作基本加密配置级别，对存储桶和新对象进行加密。有关默认加密的更多信息，请参阅为 Amazon S3 存储桶设置默认服务器端加密行为。有关 SSE-S3 的更多信息，请参阅使用具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）。

有关使用服务器端加密对数据进行加密的更多信息，请参阅the section called “数据加密”。

12. 如果您选择具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）或具有 Amazon Key Management Service（Amazon KMS）密钥的双层服务器端加密（DSSE-KMS），请执行以下操作：

    a. 在 Amazon KMS 密钥下，通过以下方式之一指定您的 KMS 密钥：

    - 要从可用的 KMS 密钥列表中进行选择，请选择从您的 Amazon KMS keys 密钥中进行选择，并从可用密钥的列表中选择您的 KMS 密钥。

      Amazon 托管式密钥 (aws/s3) 和您的客户自主管理型密钥都显示在此列表中。有关客户自主管理型密钥的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的客户密钥和 Amazon 密钥。
    - 要输入 KMS 密钥 ARN，请选择输入 Amazon KMS key ARN，然后在显示的字段中输入您的 KMS 密钥 ARN。
    - 要在 Amazon KMS 控制台中创建新的客户自主管理型密钥，请选择创建 KMS 密钥。

      有关创建 Amazon KMS key 的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的创建密钥。

> **Important**
>
> 您只能使用与存储桶所在相同的 Amazon Web Services 区域中可用的 KMS 密钥。Amazon S3 控制台仅列出与存储桶位于同一区域中的前 100 个 KMS 密钥。要使用未列出的 KMS 密钥，您必须输入 KMS 密钥 ARN。如果您希望使用由其它账户拥有的 KMS 密钥，则必须首先有权使用该密钥，然后必须输入相应的 KMS 密钥 ARN。有关 KMS 密钥的跨账户权限的更多信息，请参阅《Amazon Key Management Service Developer Guide》中的 Creating KMS keys that other accounts can use。有关 SSE-KMS 的更多信息，请参阅 使用 Amazon KMS (SSE-KMS) 指定服务器端加密。有关 DSSE-KMS 的更多信息，请参阅the section called “双层服务器端加密（DSSE-KMS）”。
>
> 在 Amazon S3 中使用 Amazon KMS key 进行服务器端加密时，您必须选择对称加密 KMS 密钥。Amazon S3 仅支持对称加密 KMS 密钥，而不支持非对称 KMS 密钥。有关更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的确定对称和非对称 KMS 密钥。

b. 将存储桶配置为使用 SSE-KMS 进行默认加密时，还可以使用 S3 存储桶密钥。S3 存储桶密钥可通过减少从 Amazon S3 到 Amazon KMS 的请求流量，降低加密成本。有关更多信息，请参阅 使用 Amazon S3 存储桶密钥降低 SSE-KMS 的成本。DSSE-KMS 不支持 S3 存储桶密钥。

   默认情况下，S3 存储桶密钥在 Amazon S3 控制台中处于启用状态。我们建议将 S3 存储桶密钥保留为启用状态以降低成本。要为存储桶禁用 S3 存储桶密钥，请在存储桶密钥下选择禁用。

13. （可选）S3 对象锁定有助于保护新对象不被删除或覆盖。有关更多信息，请参阅 使用对象锁定以锁定对象。如果要启用 S3 对象锁定，请执行以下操作：

    a. 选择高级设置。

> **Important**
>
> 启用对象锁定会自动为存储桶启用版本控制。启用并成功创建存储桶后，还必须在存储桶的属性选项卡上配置对象锁定默认保留设置和法定保留设置。

    b. 如果要启用对象锁定，请选择 Enable（启用），阅读出现的警告，并予以确认。

> **Note**
>
> 要创建启用了对象锁定的存储桶，您必须具有以下权限：s3:CreateBucket、s3:PutBucketVersioning 和 s3:PutBucketObjectLockConfiguration。

14. 选择创建存储桶。

使用 Amazon CLI

要在创建新存储桶时设置对象所有权，请使用带有 --object-ownership 参数的 create-bucket Amazon CLI 命令。

下面的例子使用 Amazon CLI 为新存储桶应用了强制存储桶拥有者设置：

```
aws s3api create-bucket --bucket  amzn-s3-demo-bucket --region us-east-1 --object-
ownership BucketOwnerEnforced
```

> **Important**
>
> 如果您在使用 Amazon CLI 创建存储桶时未设置对象所有权，则默认设置将为 ObjectWriter（启用 ACL）。

使用适用于 Java 的 Amazon 软件开发工具包

下面的例子使用 适用于 Java 的 Amazon SDK 为新存储桶设置了强制存储桶拥有者设置：

```
    // Build the ObjectOwnership for CreateBucket
    CreateBucketRequest createBucketRequest = CreateBucketRequest.builder()
            .bucket(bucketName)
            .objectOwnership(ObjectOwnership.BucketOwnerEnforced)
            .build()

     // Send the request to Amazon S3
     s3client.createBucket(createBucketRequest);
```

使用 Amazon CloudFormation

要在创建新存储桶时使用 `AWS::S3::Bucket` Amazon CloudFormation 资源以设置对象所有权，请参阅《Amazon CloudFormation 用户指南》中的 AWS::S3::Bucket 中的 OwnershipControls。

使用 REST API

要为 S3 对象所有权应用强制存储桶拥有者设置，请使用 `x-amz-object-ownership` 请求标头设置为 `BucketOwnerEnforced` 的 `CreateBucket` API 操作。有关信息和示例，请参阅《Amazon Simple Storage Service API 参考》中的 CreateBucket。

后续步骤：在应用对象所有权的强制存储桶拥有者或首选存储桶拥有者设置后，您可以进一步执行以下步骤：

- Bucket owner enforced（强制存储桶拥有者）—通过使用 IAM 或企业策略借助禁用的 ACL 要求创建所有新的存储桶。
- Bucket owner preferred（首选存储桶拥有者）—添加 S3 存储桶策略，要求将所有对象上传到存储桶中都需要 `bucket-owner-full-control` 预定义 ACL。

## 为现有存储桶设置对象所有权

您可以在现有 S3 存储桶上配置 S3 对象所有权。要在创建存储桶时应用对象所有权，请参阅 在创建存储桶时设置对象所有权。

S3 对象所有权是 Amazon S3 存储桶级设置，您可以使用它禁用 access control lists（ACLs）（访问控制列表 ACL），并获取存储桶中每个对象的所有权，从而简化了对存储在 Amazon S3 中的数据的访问管理。默认情况下，S3 对象所有权设为强制存储桶拥有者设置，并且对于新存储桶禁用 ACL。禁用 ACL 后，存储桶拥有者拥有存储桶中的每个对象，并使用访问管理策略来专门管理对数据的访问权限。我们建议您将 ACL 保持为禁用状态，除非有必须单独控制每个对象的访问权限的特殊情况。

对象所有权有三个设置，您可以使用它来控制上传到存储桶的对象的所有权，并禁用或启用 ACL：

已禁用 ACL

- 强制存储桶拥有者（默认）– ACL 已禁用，存储桶拥有者自动拥有并完全控制存储桶中的每个对象。ACL 不再影响 S3 存储桶中对数据的权限。存储桶使用策略来定义访问控制。

已启用 ACL

- Bucket owner preferred（首选存储桶拥有者）— 存储桶拥有者拥有并完全控制其他账户使用 `bucket-owner-full-control` 标准 ACL 写入存储桶的新对象。
- 对象编写者— 该 Amazon Web Services 账户上传对象拥有该对象，对其拥有完全控制权，并且可以通过 ACL 授予其他用户访问该对象的权限。

先决条件：在应用强制存储桶拥有者设置以禁用 ACL 之前，您必须将存储桶 ACL 权限迁移到存储桶策略并将存储桶 ACL 重置为默认私有 ACL。我们还建议您将对象 ACL 权限迁移到存储桶策略，并编辑需要存储桶拥有者完全控制 ACL 以外的 ACL 的存储桶策略。有关更多信息，请参阅 禁用 ACL 的先决条件。

Permissions（权限）：要使用此操作，您必须拥有 `s3:PutBucketOwnershipControls` 权限。有关 Amazon S3 权限的更多信息，请参阅《Service Authorization Reference》中的 Actions, resources, and condition keys for Amazon S3。

有关按 S3 资源类型对 S3 API 操作的权限的更多信息，请参阅 Amazon S3 API 操作所需的权限。

使用 S3 控制台

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets（存储桶）列表中，请选择要将 S3 对象所有权设置应用到的存储桶的名称。
3. 选择 Permissions（权限）选项卡。
4. 在 Object Ownership（对象所有权）下方，请选择 Edit（编辑）。
5. 在 Object Ownership（对象所有权）下方，要禁用或启用 ACL，并控制上传到存储桶中的对象的所有权，请选择以下设置之一：

   已禁用 ACL

   - Bucket owner enforced（强制存储桶拥有者）— ACL 被禁用，存储桶拥有者自动拥有并完全控制存储桶中的每个对象。ACL 不再影响 S3 存储桶中对数据的权限。存储桶使用策略来定义访问控制。

     要通过使用 IAM 或 Amazon Organizations 策略借助禁用的 ACL 要求创建所有新的存储桶，请参阅 禁用所有新存储桶的 ACL（强制存储桶拥有者）。

已启用 ACL

- Bucket owner preferred（首选存储桶拥有者）— 存储桶拥有者拥有并完全控制其他账户使用 `bucket-owner-full-control` 标准 ACL 写入存储桶的新对象。

  如果应用首选存储桶拥有者设置，以要求所有的 Amazon S3 上传都包含 `bucket-owner-full-control` 存储的 ACL，可以 add a bucket policy（添加存储桶策略），该策略只允许对象使用此 ACL 上传。
- 对象编写者— 该 Amazon Web Services 账户上传对象拥有该对象，对其拥有完全控制权，并且可以通过 ACL 授予其他用户访问该对象的权限。

6. 请选择保存。

使用 Amazon CLI

要为现有存储桶应用 Object Ownership 设置，请使用带有 `--ownership-controls` 参数的 `put-bucket-ownership-controls` 命令。所有权的有效值为 `BucketOwnerEnforced`、`BucketOwnerPreferred` 或 `ObjectWriter`。

下面的例子使用 Amazon CLI 为现有的存储桶应用强制存储桶拥有者设置：

```
aws s3api put-bucket-ownership-controls --bucket amzn-s3-demo-bucket --ownership-controls="Rules=[{ObjectOwnership=BucketOwnerEnforced}]"
```

有关 `put-bucket-ownership-controls` 的信息，请参阅《Amazon Command Line Interface 用户指南》中的 put-bucket-ownership-controls。

使用适用于 Java 的 Amazon SDK

此示例使用 适用于 Java 的 Amazon SDK 对现有存储桶应用了存储桶拥有者的 `BucketOwnerEnforced` 设置：

```
        // Build the ObjectOwnership for BucketOwnerEnforced
        OwnershipControlsRule rule = OwnershipControlsRule.builder()
               .objectOwnership(ObjectOwnership.BucketOwnerEnforced)
               .build();

        OwnershipControls ownershipControls = OwnershipControls.builder()
                  .rules(rule)
```

```
                .build()

        // Build the PutBucketOwnershipControlsRequest
        PutBucketOwnershipControlsRequest putBucketOwnershipControlsRequest =
              PutBucketOwnershipControlsRequest.builder()
                      .bucket(BUCKET_NAME)
                      .ownershipControls(ownershipControls)
                      .build();

        // Send the request to Amazon S3
        s3client.putBucketOwnershipControls(putBucketOwnershipControlsRequest);
```

使用 Amazon CloudFormation

要使用 Amazon CloudFormation 以便为现有存储桶应用对象所有权设置，请参阅《Amazon CloudFormation 用户指南》中的 AWS::S3::Bucket OwnershipControls。

使用 REST API

要使用 REST API 将 Object Ownership 设置应用于现有 S3 存储桶，请使用 `PutBucketOwnershipControls`。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 PutBucketOwnershipControls。

后续步骤：在应用对象所有权的强制存储桶拥有者或首选存储桶拥有者设置后，您可以进一步执行以下步骤：

- Bucket owner enforced（强制存储桶拥有者）—通过使用 IAM 或企业策略借助禁用的 ACL 要求创建所有新的存储桶。
- Bucket owner preferred（首选存储桶拥有者）—添加 S3 存储桶策略，要求将所有对象上传到存储桶中都需要 `bucket-owner-full-control` 预定义 ACL。

## 查看 S3 存储桶的对象所有权设置

S3 对象所有权是 Amazon S3 存储桶级设置，您可以使用它禁用 access control lists（ACLs）（访问控制列表 ACL），并获取存储桶中每个对象的所有权，从而简化了对存储在 Amazon S3 中的数据的访问管理。默认情况下，S3 对象所有权设为强制存储桶拥有者设置，并且对于新存储桶禁用 ACL。禁用 ACL 后，存储桶拥有者拥有存储桶中的每个对象，并使用访问管理策略来专门管理对数据的访问权限。我们建议您将 ACL 保持为禁用状态，除非有必须单独控制每个对象的访问权限的特殊情况。

对象所有权有三个设置，您可以使用它来控制上传到存储桶的对象的所有权，并禁用或启用 ACL：

已禁用 ACL

- 强制存储桶拥有者（默认）– ACL 已禁用，存储桶拥有者自动拥有并完全控制存储桶中的每个对象。ACL 不再影响 S3 存储桶中对数据的权限。存储桶使用策略来定义访问控制。

已启用 ACL

- Bucket owner preferred（首选存储桶拥有者）— 存储桶拥有者拥有并完全控制其他账户使用 `bucket-owner-full-control` 标准 ACL 写入存储桶的新对象。
- 对象编写者— 该 Amazon Web Services 账户上传对象拥有该对象，对其拥有完全控制权，并且可以通过 ACL 授予其他用户访问该对象的权限。

查看 Amazon S3 存储桶的对象所有权设置。要为新的存储桶设置对象所有权，请参阅 在创建存储桶时设置对象所有权。要为现有存储桶设置对象所有权，请参阅 为现有存储桶设置对象所有权。

Permissions（权限）：要使用此操作，您必须拥有 `s3:GetBucketOwnershipControls` 权限。有关 Amazon S3 权限的更多信息，请参阅《Service Authorization Reference》中的 Actions, resources, and condition keys for Amazon S3。

有关按 S3 资源类型对 S3 API 操作的权限的更多信息，请参阅 Amazon S3 API 操作所需的权限。

使用 S3 控制台

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets（存储桶）列表中，请选择要将对象所有权设置应用到的存储桶的名称。
3. 选择 Permissions（权限）选项卡。
4. 在 Object Ownership（对象所有权）下方，您可以查看存储桶的对象所有权设置。

使用 Amazon CLI

要检索 S3 存储桶的 S3 对象所有权设置，请使用 get-bucket-ownership-controls Amazon CLI 命令。

```
aws s3api get-bucket-ownership-controls --bucket amzn-s3-demo-bucket
```

使用 REST API

要检索 S3 存储桶的 Object Ownership 设置，请使用 `GetBucketOwnershipControls` API 操作。有关更多信息，请参阅 GetBucketOwnershipControls。

# 禁用所有新存储桶的 ACL 并强制执行 Object Ownership

建议禁用 Amazon S3 存储桶上的 ACL。可以通过为 S3 对象所有权应用强制存储桶拥有者设置来实现这一点。应用此设置时，ACL 将被禁用，并且您自动拥有并完全控制存储桶中的所有对象。若要求在禁用 ACL 的情况下创建所有新存储桶，请使用 Amazon Identity and Access Management（IAM）策略或 Amazon Organizations 服务控制策略（SCP），如下一节所述。

要在不禁用 ACL 的情况下强制对新对象的对象所有权，您可以应用“首选存储桶拥有者”设置。当您应用此设置时，我们强烈建议您更新存储桶策略，以要求对存储桶的所有 PUT 请求使用 `bucket-owner-full-control` 标准 ACL。确保还更新客户端，以将 `bucket-owner-full-control` 标准 ACL 从其他账户发送至存储桶。

主题


- 禁用所有新存储桶的 ACL（强制存储桶拥有者）
- 要求 Amazon S3 PUT 操作使用存储桶拥有者完全控制的标准 ACL（首选存储桶拥有者）


## 禁用所有新存储桶的 ACL（强制存储桶拥有者）

下面的示例 IAM 策略拒绝特定 IAM 用户或角色的 `s3:CreateBucket` 权限，除非为对象所有权应用了强制存储桶拥有者设置。`Condition` 块中的键值对指定 `s3:x-amz-object-ownership` 为其密钥，并将 `BucketOwnerEnforced` 设为其值。换句话说，只有在 IAM 用户为对象所有权设定强制存储桶拥有者设置并禁用 ACL 时，这些用户才能创建存储桶。您还可以将此策略用作 Amazon 企业的边界的 SCP。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RequireBucketOwnerFullControl",
            "Action": "s3:CreateBucket",
            "Effect": "Deny",
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-object-ownership": "BucketOwnerEnforced"
```

```
                }
            }
        }
    ]
}
```

## 要求 Amazon S3 **PUT** 操作使用存储桶拥有者完全控制的标准 ACL（首选存储桶拥有者）

通过为对象所有权使用“首选存储桶拥有者”设置，您作为存储桶拥有者，拥有并完全控制其他账户使用 bucket-owner-full-control 标准 ACL 向存储桶写入的新对象。但是，如果其他账户在没有 bucket-owner-full-control 标准 ACL 的情况下将对象写入存储桶，对象编写者将保持完全控制访问权限。作为存储桶拥有者，只有指定了 bucket-owner-full-control 标准的 ACL，才能实现允许写入的存储桶策略。

> **Note**
>
> 如果在应用强制存储桶拥有者设置的情况下禁用了 ACL，则作为存储桶拥有者，您将自动拥有并完全控制存储桶中的所有对象。您无需使用此部分来更新存储桶策略来强制执行存储桶拥有者的对象所有权。

以下存储桶策略指定只有当对象的 ACL 设置为 111122223333 时，账户 *amzn-s3-demo-bucket* 才能将对象上传到 *bucket-owner-full-control*。请务必将 *111122223333* 替换为您的账户，*amzn-s3-demo-bucket* 替换为存储桶的名称。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Only allow writes to my bucket with bucket owner full control",
         "Effect": "Allow",
         "Principal": {
            "AWS": [
               "arn:aws:iam::111122223333:user/ExampleUser"
            ]
         },
         "Action": [
            "s3:PutObject"
         ],
```

```
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
               "StringEquals": {
                  "s3:x-amz-acl": "bucket-owner-full-control"
               }
            }
         }
      ]
}
```

以下是一个复制操作示例，其中包括使用 Amazon Command Line Interface（Amazon CLI）的 `bucket-owner-full-control` 标准 ACL。

```
aws s3 cp file.txt s3://amzn-s3-demo-bucket --acl bucket-owner-full-control
```

存储桶策略生效之后，如果客户端不包含 `bucket-owner-full-control` 标准 ACL，则操作将失败，上传者将收到以下错误：

调用 PutObject 操作时发生错误 (AccessDenied)：访问被拒绝。

> **Note**
>
> 如果客户端在上传后需要访问对象，则必须向上传账户授予其他权限。有关授予账户对资源的访问权限的信息，请参阅 演练：使用策略管理针对 Amazon S3 资源的访问权限。

## 故障排除

在应用 S3 对象所有权的强制存储桶拥有者设置时，访问控制列表（ACL）将被禁用，作为存储桶拥有者的您将自动拥有存储桶中的所有对象。ACL 不再影响存储桶中对象的权限。您可使用策略授予权限。所有 S3 PUT 请求都必须指定 `bucket-owner-full-control` 标准 ACL 或不指定 ACL，否则这些请求将失败。有关更多信息，请参阅 为您的存储桶控制对象所有权和禁用 ACL。。

如果指定了无效的 ACL 或存储桶 ACL 权限授予 Amazon Web Services 账户 外部的访问权限，您可能会看到以下错误响应。

### AccessControlListNotSupported

为对象所有权应用强制存储桶拥有者设置之后，将禁用 ACL。设置 ACL 或更新 ACL 的请求失败，并显示 `400` 错误，并返回 AccessControlListNotSupported 错误代码。仍然支持读取 ACL 的请求。读取

ACL 的请求始终返回一个响应，显示对存储桶拥有者的完全控制权。在 PUT 操作中，您必须指定存储桶拥有者完全控制 ACL 或不指定 ACL。否则，您的 PUT 操作将失败。

以下示例 `put-object` Amazon CLI 命令包括 `public-read` 标准 ACL。

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key object-key-name --body doc-example-body --acl public-read
```

如果存储桶使用强制存储桶拥有者设置来禁用 ACL，则此操作将失败，上传者会收到以下错误消息：

调用 PutObject 操作时发生错误（AccessControlListNotSupported）：存储桶不允许 ACL

### InvalidBucketAclWithObjectOwnership

如果您想应用强制存储桶拥有者设置来禁用 ACL，则存储桶 ACL 必须仅向存储桶拥有者提供完全控制权。您的存储桶 ACL 无法访问外部 Amazon Web Services 账户 或任何其他团体。例如，如果您的 `CreateBucket` 请求设置强制存储桶拥有者并指定一个存储桶 ACL，用于提供对外部 Amazon Web Services 账户的访问权限，您的请求会失败并显示 `400` 错误，并且返回 InvalidBucketAclWithObjectOwnership 错误代码。同样，如果您的 `PutBucketOwnershipControls` 请求对于具有存储桶 ACL（可向其他人授予权限）的存储桶设置强制存储桶拥有者，请求将失败。

Example ：授予存储桶 ACL 公有读取访问权限。

例如，如果现有存储桶 ACL 授予公共读取访问权限，则在将这些 ACL 权限迁移到存储桶策略并将存储桶 ACL 重置为默认私有 ACL 之前，您无法对于对象所有权应用强制存储桶拥有者设置。有关更多信息，请参阅 禁用 ACL 的先决条件。

此示例存储桶 ACL 授予公共读取访问权限：

```
{
    "Owner": {
        "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID"
    },
    "Grants": [
        {
            "Grantee": {
                "ID":
 "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID",
                "Type": "CanonicalUser"
```

```
            },
            "Permission": "FULL_CONTROL"
        },
        {
            "Grantee": {
                "Type": "Group",
                "URI": "http://acs.amazonaws.com/groups/global/AllUsers"
            },
            "Permission": "READ"
        }
    ]
}
```

以下示例 `put-bucket-ownership-controls` Amazon CLI 命令对于对象所有权应用强制存储桶拥有者设置：

```
aws s3api put-bucket-ownership-controls --bucket amzn-s3-demo-bucket --ownership-
controls Rules=[{ObjectOwnership=BucketOwnerEnforced}]
```

由于存储桶 ACL 授予公共读取访问权限，因此请求失败并返回以下错误代码：

调用 PutBucketOwnershipControls 操作时发生错误（InvalidBucketAclWithObjectOwnership）：存储桶不能含有带有 ObjectOwnership's BucketOwnerEnforced 设置的 ACL

# Amazon S3 中的安全性

Amazon 十分重视云安全性。作为 Amazon 客户，您将从专为满足大多数安全敏感型组织的要求而打造的数据中心和网络架构中受益。

安全性是 Amazon 和您的共同责任。责任共担模式将其描述为云本身的安全性和云中的安全性：

云的安全性

Amazon 负责保护在 Amazon Web Services 云 中运行 Amazon 服务的基础设施。Amazon 还向您提供可安全使用的服务。作为 Amazon 合规性计划的一部分，我们的安全措施的有效性定期由第三方审计员进行测试和验证。要了解适用于 Amazon S3 的合规性计划，请参阅Amazon合规性计划范围内的服务。

云中的安全性

您的责任由您使用的 Amazon 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您组织的要求以及适用的法律法规。对于 Amazon S3，您的责任包括以下各个方面：

- 管理数据，包括对象所有权和加密。
- 对资产进行分类。
- 使用 IAM 角色管理您数据的访问权以及其他服务配置来应用适当的权限。
- 启用侦测性控制，例如适用于 Amazon S3 的 Amazon CloudTrail 或 Amazon GuardDuty。

此文档将帮助您了解如何在使用 Amazon S3 时应用责任共担模式。以下主题说明如何配置 Amazon S3 以实现您的安全性和合规性目标。您还将了解如何使用其他 Amazon 服务来帮助您监控和保护您的 Amazon S3 资源。

> **Note**
>
> 有关将 Amazon S3 Express One Zone 存储类与目录存储桶配合使用的更多信息，请参阅 S3 Express One Zone 和使用目录存储桶。

主题

- Amazon S3 的安全最佳实践
- Amazon S3 中的数据保护

- 利用加密来保护数据
- 互联网络流量隐私
- Amazon S3 的合规性验证
- Amazon S3 中的恢复能力
- Amazon S3 中的基础设施安全性
- Amazon S3 中的配置和漏洞分析
- 访问权限管理

# Amazon S3 的安全最佳实践

Amazon S3 提供了在您开发和实施自己的安全策略时需要考虑的大量安全特征。以下最佳实操是一般准则，并不代表完整的安全解决方案。这些最佳实践可能不适合您的环境或不满足您的环境要求，请将其视为有用的建议而不是惯例。

主题


- Amazon S3 安全最佳实践
- Amazon S3 监控和审计最佳实践
- 使用托管式 Amazon 安全服务监控数据安全


## Amazon S3 安全最佳实践

Amazon S3 的以下最佳实践可以帮助预防安全事故。

禁用访问控制列表（ACL)

S3 对象所有权是 Amazon S3 存储桶级别的设置，您可以使用该设置来控制上传到存储桶的对象的所有权和禁用或启用 ACL。默认情况下，对象所有权设为强制存储桶拥有者设置，并且所有 ACL 均处于禁用状态。禁用 ACL 后，存储桶拥有者拥有存储桶中的所有对象，并使用访问管理策略来专门管理对数据的访问权限。

Amazon S3 中的大多数现代使用案例不再要求使用访问控制列表（ACL）。我们建议您禁用 ACL，除非有必须单独控制每个对象的访问权限的特殊情况。要禁用 ACL 并获得存储桶中每个对象的所有权，请为 S3 对象所有权应用强制存储桶拥有者设置。禁用 ACL 时，您可以轻松通过不同的 Amazon Web Services 账户 上传的对象维护存储桶。

禁用 ACL 时，数据的访问控制基于策略，如下所示：

- Amazon Identity and Access Management（IAM）用户策略
- S3 存储桶策略
- 虚拟私有云（VPC）端点策略
- Amazon Organizations 服务控制策略（SCP）
- Amazon Organizations 资源控制策略（RCP）

禁用 ACL 简化了权限管理和审计。对于新存储桶，默认情况下 ACL 处于禁用状态。您还可以对现有存储桶禁用 ACL。如果现有存储桶中已有对象，在禁用 ACL 后，对象和存储桶 ACL 将不再是访问评估过程的一部分。相反，将根据策略授予或拒绝访问权限。

在禁用 ACL 之前，请确保执行以下操作：

- 查看存储桶策略，以确保此策略涵盖了您打算在账户外授予对存储桶的访问权限的所有方式。
- 将存储桶 ACL 重置为默认（由存储桶拥有者完全控制）。

禁用 ACL 后，会出现以下行为：

- 您的存储桶仅接受未指定 ACL 的 PUT 请求或指定了存储桶拥有者完全控制的 ACL 的 PUT 请求。这些 ACL 包括 `bucket-owner-full-control` 标准 ACL 或以 XML 表示的此 ACL 的等效形式。
- 支持存储桶拥有者完全控制 ACL 的现有应用程序没有影响。
- 包含其他 ACL 的 PUT 请求（例如，向某些 Amazon Web Services 账户 进行自定义授权）将失败并返回 HTTP 状态代码 `400 (Bad Request)`，和错误代码 `AccessControlListNotSupported`。

有关更多信息，请参阅 为您的存储桶控制对象所有权和禁用 ACL。。

确保您的 Amazon S3 存储桶使用正确的策略且不可公有访问

除非您明确要求互联网上的任何人都能读写您的 S3 存储桶，否则请确保 S3 存储桶不是公有的。以下是您可以采取的屏蔽公共访问权限的一些步骤：

- 使用 S3 屏蔽公共访问权限。借助 S3 屏蔽公共访问权限，您可以轻松地设置集中控制，以限制对 Amazon S3 资源的公共访问。无论资源是如何创建的，都会实施这些集中控制。有关更多信息，请参阅 阻止对您的 Amazon S3 存储的公有访问。
- 找出允许使用通配符身份的 Amazon S3 存储桶策略，例如 `"Principal": "*"`（这实际上意味着“任何人”）。还要找出允许通配符操作 `"*"` 的策略（这实际上允许用户在 Amazon S3 存储桶中执行任何操作）。
- 类似地，找出向“任何人”或者“任何经过身份验证的 Amazon 用户”提供读、写或完全访问权限的 Amazon S3 存储桶访问控制列表（ACL）。
- 使用 `ListBuckets` API 操作扫描所有 Amazon S3 存储桶。然后，使用 `GetBucketAcl`、`GetBucketWebsite` 和 `GetBucketPolicy` 确定每个存储桶是否拥有符合要求的访问控制和符合要求的配置。
- 使用 Amazon Trusted Advisor 检查您的 Amazon S3 实现。
- 考虑使用 s3-bucket-public-read-prohibited 和 s3-bucket-public-write-prohibited 托管式 Amazon Config 规则 来实施持续的侦测性控制。

有关更多信息，请参阅 Amazon S3 的身份和访问管理。

### 实施最低权限访问

在授予权限时，您可以决定谁获得哪些 Amazon S3 资源的哪些权限。您可以对这些资源启用希望允许的特定操作。因此，我们建议您仅授予执行任务所需的权限。实施最低权限访问对于减小安全风险以及可能由错误或恶意意图造成的影响至关重要。

为实现最低权限访问，可以使用以下工具：

- Amazon S3 的策略操作 和 IAM 实体的权限边界
- Amazon S3 如何与 IAM 配合使用
- 访问控制列表 (ACL) 概述

有关选择一个或多个前述机制时所要考虑的事项的指南，请参阅 Amazon S3 的身份和访问管理。

### 将 IAM 角色用于需要 Amazon S3 访问权限的应用程序和 Amazon Web Services 服务

为了使在 Amazon EC2 或其他 Amazon Web Services 服务上运行的应用程序能够访问 Amazon S3 资源，应用程序必须在其 Amazon API 请求中包含有效的 Amazon 凭证。我们建议您不要直接在应用程序或 Amazon EC2 实例中存储 Amazon 凭证，这些是不会自动轮换的长期凭证，如果它们受到损害，可能会对业务产生重大影响。

而是使用 IAM 角色来管理需要访问 Amazon S3 的应用程序或服务的临时凭证。在使用角色时，您不需要将长期凭证（如用户名和密码或访问密钥）分配给 Amazon EC2 实例或 Amazon Web Services 服务（例如 Amazon Lambda）。角色可提供临时权限供应用程序在调用其他 Amazon 资源时使用。

有关更多信息，请参阅 IAM 用户指南中的以下主题：

- IAM 角色
- 针对角色的常见情形：用户、应用程序和服务

### 考虑加密静态数据

您可以通过以下选项在 Amazon S3 中保护静态数据：

- 服务器端加密 – 默认情况下，所有 Amazon S3 存储桶都配置了加密，所有上传到 S3 存储桶的新对象都会自动静态加密。具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）是 Amazon S3 中每个存储桶的默认加密配置。要使用其他类型的加密，您可以指定要在 S3 PUT 请求中使用的服务器端加密类型，也可以在目标存储桶中设置默认加密配置。

  Amazon S3 也提供了以下服务器端加密选项：

  - 具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）

- 具有 Amazon Key Management Service（Amazon KMS）密钥的双层服务器端加密（DSSE-KMS）
- 具有客户提供密钥的服务器端加密（SSE-C）

有关更多信息，请参阅 使用服务器端加密保护数据。

- 客户端加密 – 在客户端加密数据并将加密的数据上传到 Amazon S3。在这种情况下，您需要管理加密过程、加密密钥和相关的工具。如服务器端加密一样，客户端加密可以帮助减少面临的风险：通过使用存储在一个不同机制（而不是存储数据本身的机制）中的密钥来加密数据。

Amazon S3 提供多个客户端加密选项。有关更多信息，请参阅 使用客户端加密保护数据。

实施传输中数据加密

您可以使用 HTTPS（TLS）帮助防止潜在攻击者使用中间人攻击或类似攻击来窃听或操纵网络流量。我们建议通过在 Amazon S3 存储桶策略中使用 aws:SecureTransport 条件，以只允许通过 HTTPS（TLS）的加密连接。有关更多信息，请参阅示例 S3 存储桶策略管理基于 HTTP 或 HTTPS 请求的访问权限。除了拒绝 HTTP 请求外，我们还建议您对 `tlsDetails.tlsVersion NOT EXISTS` 设置 Amazon CloudWatch 警报，以便在有人尝试对您的内容进行 HTTP 访问时提醒您。有关如何配置 Amazon CloudWatch 警报的更多信息，请参阅《Amazon CloudTrail User Guide》中的 Creating CloudWatch alarms for CloudTrail events: examples 和 CloudTrail record contents。

> **Important**
>
> 我们建议您的应用程序不要固定 Amazon S3 TLS 证书，因为 Amazon 不支持固定公开信任的证书。S3 会自动续订证书，而续订可能在证书到期之前的任何时候发生。续订证书会生成新的公有-私有密钥对。如果您固定了最近使用新公钥续订的 S3 证书，则在您的应用程序使用新证书之前，您将无法连接到 S3。

也可以考虑使用 s3-bucket-ssl-requests-only 托管式 Amazon Config 规则来实施持续的侦测性控制。

考虑使用 S3 对象锁定

借助 S3 对象锁定，您可以使用“一次写入，多次读取”（WORM）模式存储对象。S3 对象锁定可以帮助阻止意外或不当删除数据。例如，您可以使用 S3 对象锁定来帮助保护您的 Amazon CloudTrail 日志。

有关更多信息，请参阅 使用对象锁定以锁定对象。

### 启用 S3 版本控制

S3 版本控制是在相同的存储桶中保留对象的多个版本的方法。对于 存储桶中存储的每个对象，您可以使用版本控制功能来保留、检索和还原它们的各个版本。使用版本控制能够轻松从用户意外操作和应用程序故障中恢复数据。

也可以考虑使用 s3-bucket-versioning-enabled 托管式 Amazon Config 规则来实施持续的侦测性控制。

有关更多信息，请参阅 使用 S3 版本控制保留对象的多个版本。

### 考虑使用 Amazon S3 跨区域复制

虽然 Amazon S3 在默认情况下跨多个地理位置不同的可用区存储数据，但合规性要求所规定的数据存储距离可能更远。通过 S3 跨区域复制（CRR），可以在远距离 Amazon Web Services 区域之间复制数据以帮助满足这些要求。CRR 允许在不同 Amazon Web Services 区域 中的存储桶之间自动以异步方式复制对象。有关更多信息，请参阅 在区域内和跨区域复制对象。

> **Note**
>
> CRR 要求源和目标 S3 存储桶都已启用版本控制。

也可以考虑使用 s3-bucket-replication-enabled 托管式 Amazon Config 规则来实施持续的侦测性控制。

### 考虑使用 VPC 端点进行 Amazon S3 访问

Amazon S3 的 Virtual Private Cloud（VPC）端点是 VPC 内的逻辑实体，仅允许连接到 Amazon S3。VPC 端点可以帮助防止流量穿越开放的互联网。

Amazon S3 的 VPC 端点提供多种方式来控制对 Amazon S3 数据的访问：

- 通过使用 S3 存储桶策略，您可以控制允许通过特定 VPC 端点进行访问的请求、用户或组。
- 可以使用 S3 存储桶策略控制哪些 VPC 或 VPC 端点有权访问 S3 存储桶。
- 您可以使用没有 Internet 网关的 VPC 来阻止数据泄露。

有关更多信息，请参阅 使用存储桶策略控制从 VPC 端点的访问。

### 使用托管式 Amazon 安全服务监控数据安全

多项托管式 Amazon 安全服务可以帮助您识别、评测和监控 Amazon S3 数据的安全和合规风险。这些服务还可以帮助您保护数据免受这些风险的影响。这些服务包括自动检测、监控和保护功能，

旨在从单个 Amazon Web Services 账户的 Amazon S3 资源扩展到跨数千个账户的多个组织的资源。

有关更多信息，请参阅 使用托管式 Amazon 安全服务监控数据安全。

## Amazon S3 监控和审计最佳实践

Amazon S3 的以下最佳实践可以帮助检测潜在的安全弱点和事故。

识别和审计您的所有 Amazon S3 存储桶

确定您的 IT 资产是监管和安全性的一个至关重要的方面。您需要了解您所有的 Amazon S3 资源，以评估它们的安全态势并对潜在的薄弱领域采取措施。要审计您的资源，我们建议您执行以下操作：

- 使用标签编辑器确定和标记安全敏感性或审计敏感性资源，然后在您需要搜索这些资源时使用这些标签。有关更多信息，请参阅《标记 Amazon 资源用户指南》中的搜索要标记的资源。
- 出于业务、合规性和法规要求，使用 S3 清单来审计和报告对象的复制和加密状态。有关更多信息，请参阅 使用 S3 清单对数据进行编目和分析。
- 为您的 Amazon S3 资源创建资源组。有关更多信息，请参阅《Amazon Resource Groups 用户指南》中的什么是 Resource Groups？。

使用 Amazon 监控工具实施监控

监控是保持 Amazon S3 和您的 Amazon 解决方案的可靠性、安全性、可用性和性能的重要部分。Amazon 提供了一些可用来监控 Amazon S3 和您的其他 Amazon Web Services 服务的工具和服务。例如，您可以监控 Amazon S3 的 Amazon CloudWatch 指标，特别是 `PutRequests`、`GetRequests`、`4xxErrors` 和 `DeleteRequests` 指标。有关更多信息，请参阅使用 Amazon CloudWatch 监控指标和Amazon S3 中的日志记录和监控。

有关另一个示例，请参阅示例：Amazon S3 存储桶活动。此示例介绍如何创建 CloudWatch 警报，当执行 Amazon S3 API 调用以 PUT 或 `DELETE` 存储桶策略、存储桶生命周期、存储桶复制配置时，或者 PUT 存储桶 ACL 时，会触发此警报。

启用 Amazon S3 服务器访问日志记录

服务器访问日志记录详细地记录对存储桶提出的各种请求。服务器访问日志可以在安全和访问审计方面为您提供帮助，帮您了解您的客户群和了解您的 Amazon S3 账单。有关启用服务器访问日志记录的说明，请参阅 使用服务器访问日志记录来记录请求。

也可以考虑使用 s3-bucket-logging-enabled Amazon Config 托管式规则来实施持续的侦测性控制。

使用 Amazon CloudTrail

Amazon CloudTrail 提供用户、角色或 Amazon Web Services 服务在 Amazon S3 中执行的操作的记录。您可以使用 CloudTrail 收集的信息确定以下事项：

- 向 Amazon S3 发出的请求
- 发出请求的 IP 地址
- 谁发出了请求
- 发出请求的时间
- 有关该请求的其他详细信息

例如，您可以确定影响数据访问的 PUT 操作的 CloudTrail 条目，尤其是 `PutBucketAcl`、`PutObjectAcl`、`PutBucketPolicy` 和 `PutBucketWebsite`。

当您设置 Amazon Web Services 账户时，默认情况下 CloudTrail 处于启用状态。您可以在 CloudTrail 控制台中查看最近的事件。要为 Amazon S3 存储桶创建活动和事件的持续记录，您可以在 CloudTrail 控制台中创建跟踪。有关更多信息，请参阅《Amazon CloudTrail 用户指南》中的记录数据事件。

创建跟踪时，可以配置 CloudTrail 以记录数据事件。数据事件是在资源上或在资源内执行的资源操作的记录。在 Amazon S3 中，数据事件记录单个存储桶的对象级 API 活动。CloudTrail 支持 Amazon S3 对象级 API 操作的子集，例如 `GetObject`、`DeleteObject` 和 `PutObject`。有关 CloudTrail 如何与 Amazon S3 配合使用的更多信息，请参阅 使用 Amazon CloudTrail 记录 Amazon S3 API 调用。在 Amazon S3 控制台中，您还可以将 S3 存储桶配置为 为 S3 存储桶和对象启用 CloudTrail 事件日志记录。

Amazon Config 提供了托管规则（`cloudtrail-s3-dataevents-enabled`），您可以使用该规则来确认至少有一个 CloudTrail 跟踪正在记录 S3 存储桶的数据事件。有关更多信息，请参阅 Amazon Config 开发人员指南中的 cloudtrail-s3-dataevents-enabled。

Enable Amazon Config（启用 Gem）

此主题中列出的几个最佳实践建议创建 Amazon Config 规则。Amazon Config 有助于评测、审计和评价您的 Amazon 资源的配置。Amazon Config 监控资源配置，以便您能够针对需要的安全配置评估所记录的配置。利用 Amazon Config，您可以：

- 查看 Amazon 资源之间的配置和关系的更改
- 调查详细的资源配置历史记录

- 根据内部指南中指定的配置确定总体合规性

使用 Amazon Config 可帮助您简化合规性审核、安全性分析、变更管理和操作故障排除。有关更多信息，请参阅 Amazon Config 开发人员指南中的使用控制台设置 Amazon Config。当指定要记录的资源类型时，确保您包括了 Amazon S3 资源。

> **Important**
>
> 在评估 Amazon S3 资源时，Amazon Config 托管式规则仅支持通用存储桶。Amazon Config 不记录目录存储桶的配置更改。有关更多信息，请参阅《Amazon Config 开发人员指南》中的 Amazon Config 托管式规则和 Amazon Config 托管式规则列表。

有关如何使用 Amazon Config 的示例，请参阅《Amazon 安全博客》上的如何使用 Amazon Config 来监控和响应允许公共访问的 Amazon S3 存储桶。

使用 S3 Storage Lens 存储统计管理工具

S3 Storage Lens 存储统计管理工具是一项云存储分析功能，您可以使用它在整个组织范围内了解对象存储的使用情况和活动。S3 Storage Lens 存储统计管理工具还分析指标以提供上下文建议，您可以使用这些建议来优化存储成本并应用最佳实践来保护数据。

通过 S3 Storage Lens 存储统计管理工具，您可以使用指标生成摘要见解，例如，了解整个组织中有多少存储空间，或增长最快的存储桶和前缀是哪些。您还可以使用 S3 Storage Lens 存储统计管理工具指标来识别成本优化机会，实施数据保护和访问管理最佳实践，并提高应用程序工作负载的性能。

例如，您可以识别没有 S3 生命周期规则的存储桶，以中止超过 7 天的未完成分段上传。您还可以识别未遵循数据保护最佳实践（例如使用 S3 复制或 S3 版本控制）的存储桶。有关更多信息，请参阅了解 Amazon S3 Storage Lens。

监控 Amazon 安全公告

我们建议您经常为您的 Amazon Web Services 账户检查在 Trusted Advisor 中发布的安全公告。尤其要关注有关具有“开放访问权限”的 Amazon S3 存储桶的警告。您可以使用 describe-trusted-advisor-checks 通过编程方式来实现这一点。

此外，积极地监控向您的每一个 Amazon Web Services 账户注册的原始电子邮件地址。Amazon 将使用该电子邮件地址就可能影响您的紧急安全事件与您联系。

具有广泛影响的 Amazon 操作性问题将在 Amazon Health Dashboard 服务运行状况上发布。操作性问题也通过 Amazon Health Dashboard 发布到各个账户。有关更多信息，请参阅 Amazon Health 文档。

## 使用托管式 Amazon 安全服务监控数据安全

多项托管式 Amazon 安全服务可以帮助您识别、评测和监控 Amazon S3 数据的安全和合规风险。这些服务还可以帮助您保护数据免受这些风险的影响。这些服务包括自动检测、监控和保护功能，旨在从单个 Amazon Web Services 账户的 Amazon S3 资源扩展到跨数千个 Amazon Web Services 账户的多个组织的资源。

Amazon 检测和响应服务可以帮助您识别潜在的安全配置错误、威胁或意外行为，以便您可以快速响应环境中潜在未经授权或恶意的活动。Amazon 数据保护服务可以帮助您监控和保护您的数据、账户和工作负载，使其免受未经授权的访问。这些服务还有助于您发现 Amazon S3 数据资产中的敏感数据 [如个人身份信息（PII）]。

为帮助您识别和评估数据安全与合规性风险，托管式 Amazon 安全服务会生成调查发现，以告知您与 Amazon S3 数据有关的潜在安全事件或问题。调查发现提供相关详细信息，您可以使用这些信息，根据事件/响应工作流和策略对这些风险进行调查、评测并采取措施。您可以使用每项服务直接访问调查发现数据。还可以将数据发送到其他应用程序、服务和系统，例如安全事故和事件管理系统（SIEM）。

要监控 Amazon S3 数据的安全性，请考虑使用以下这些托管式 Amazon 安全服务。

Amazon GuardDuty

Amazon GuardDuty 是一项威胁检测服务，可持续监控您的 Amazon Web Services 账户和工作负载中是否存在恶意活动，并提供详细的安全调查发现以供查看和补救。

使用 GuardDuty 中的 S3 保护特征，您可以配置 GuardDuty 来分析 Amazon S3 资源的 Amazon CloudTrail 管理和数据事件。然后，GuardDuty 会监控这些事件中是否存在恶意和可疑活动。为了为分析提供信息并识别潜在的安全风险，GuardDuty 使用威胁情报源和机器学习。

GuardDuty 可以监控 Amazon S3 资源的不同类型的活动。例如，Amazon S3 的 CloudTrail 管理事件包括存储桶级别的操作，例如 `ListBuckets`、`DeleteBucket` 和 `PutBucketReplication`。Amazon S3 的 CloudTrail 数据事件包括对象级操作，例如 `GetObject`、`ListObjects` 和 `PutObject`。如果 GuardDuty 检测到异常或潜在恶意的活动，它会生成调查发现来通知您。

有关更多信息，请参阅《Amazon GuardDuty 用户指南》中的 Amazon GuardDuty 中的 Amazon S3 保护。

### Amazon Detective

Amazon Detective 简化了调查流程，并帮助您进行更快、更有效的安全调查。Detective 提供预构建的数据聚合、摘要和上下文，可以帮助您分析和评测可能的安全问题的性质和程度。

Detective 会自动提取基于时间的事件，例如来自 Amazon CloudTrail 的 API 调用和您的 Amazon 资源的 Amazon VPC 流日志。它还采集 Amazon GuardDuty 生成的调查发现。然后，Detective 使用机器学习、统计分析和图形理论生成可视化效果，以帮助您更快地进行有效的安全调查。

这些可视化效果提供了统一的交互式视图，可供您了解资源行为及此类行为随时间推移的相互作用。您可以浏览此行为图以检查潜在的恶意操作，例如登录尝试失败或可疑的 API 调用。您还可以查看这些操作如何影响资源（如 S3 存储桶和对象）。

有关更多信息，请参阅《Amazon Detective 管理指南》。

### IAM Access Analyzer

Amazon Identity and Access Management Access Analyzer（IAM Access Analyzer）可帮助您识别与外部实体共享的资源。还可以使用 IAM Access Analyzer 根据策略语法和最佳实践验证 IAM 策略，并根据 Amazon CloudTrail 日志中的访问活动生成 IAM 策略。

IAM Access Analyzer 使用基于逻辑的推理来分析 Amazon 环境中的资源策略，例如存储桶策略。借助适用于 S3 的 IAM Access Analyzer，当 S3 存储桶配置为允许互联网上的任何人或其他 Amazon Web Services 账户（包括组织外部的账户）访问时，将向您发出提醒。例如，适用于 S3 的 IAM Access Analyzer 可能会报告存储桶具有通过存储桶访问控制列表（ACL）、存储桶策略、多区域接入点策略或接入点策略提供的读取或写入访问权限。您会收到每个公共存储桶或共享存储桶的调查发现，其中指出了公共或共享访问的来源和级别。有了这些调查发现，您就可以立即采取精确的纠正措施，将存储桶访问权限恢复为您期望的设置。

有关更多信息，请参阅 使用适用于 S3 的 IAM Access Analyzer 查看存储桶访问权限。

### Amazon Macie

Amazon Macie 是一项安全服务，旨在使用机器学习和模式匹配来发现敏感数据。Macie 提供对数据安全风险的可见性，并实现针对这些风险的自动防护。借助 Macie，您可以自动发现和报告 Amazon S3 数据资产中的敏感数据，以更好地了解组织在 S3 中存储的数据。

要使用 Macie 检测敏感数据，您可以使用内置标准和技术，这些标准和技术旨在检测许多国家和地区的大量且不断增长的敏感数据类型列表。这些敏感数据类型包括多种类型的个人身份信息

（PII）、财务数据和凭证数据。您还可以使用自己定义的自定义标准：旨在定义要匹配的文本模式的正则表达式，以及（可选）用于优化结果的字符序列和邻近规则。

如果 Macie 在 S3 对象中检测到敏感数据，Macie 会生成安全调查发现来通知您。此调查发现提供有关受影响的对象、Macie 发现的敏感数据的类型和出现次数的信息，以及其他详细信息，以帮助您调查受影响的 S3 存储桶和对象。有关更多信息，请参阅《Amazon Macie 用户指南》。

Amazon Security Hub

Amazon Security Hub 是一项安全态势管理服务，该服务可执行安全最佳实践检查，将来自多个来源的警报和调查发现聚合为单一格式，并支持自动补救。

Security Hub 从集成的 Amazon Partner Network 安全解决方案和 Amazon Web Services 服务（包括 Amazon Detective、Amazon GuardDuty、IAM Access Analyzer 和 Amazon Macie）收集并提供安全调查发现数据。Security Hub 还可以根据 Amazon 最佳实践和支持的行业标准运行持续的自动化安全检查，从而生成自己的调查发现。

然后，Security Hub 关联并整合各提供方的调查发现，以帮助确定调查发现的优先级并处理最重要的调查发现。它还为自定义操作提供支持，您可以使用自定义操作来为特定类别的调查发现调用响应或补救操作。

使用 Security Hub，您可以评测 Amazon S3 资源的安全性和合规性状态，也可以将其作为对组织在单个 Amazon Web Services 区域和跨多个区域的安全状况进行更广泛分析的一部分。这包括分析安全趋势和确定优先级最高的安全问题。您还可以聚合来自多个 Amazon Web Services 区域的调查发现，并监控和处理来自单个区域的聚合调查发现数据。

有关更多信息，请参阅《Amazon Security Hub 用户指南》中的 Amazon Simple Storage Service 控制。

# Amazon S3 中的数据保护

Amazon S3 为任务关键型和主要数据存储提供了高度持久的存储基础设施。S3 Standard、S3 Intelligent-Tiering、S3 Standard-IA、S3 Glacier Instant Retrieval、S3 Glacier Flexible Retrieval、S3 Glacier Deep Archive 在 Amazon Web Services 区域 中至少三个可用区的多个设备上冗余存储对象。可用区是 Amazon Web Services 区域 中一个或多个具有冗余电源、网络和连接的离散数据中心。可用区与任何其他可用区之间有意义的距离（许多公里数）在物理上隔开，尽管所有可用区之间的距离都在 100 公里（60 英里）以内。S3 One Zone-IA 存储类将数据冗余存储在单个可用区中的多个设备上。这些服务旨在通过快速检测和修复任何丢失的冗余来处理并发设备故障，还可以使用校验和定期验证数据的完整性。

Amazon S3 standard 存储提供以下特征：

- 以 Amazon S3 服务等级协议作为后盾
- 设计目的是在指定年度内为对象提供 99.999999999% 的持久性和 99.99% 的可用性
- S3 Standard、S3 Intelligent-Tiering、S3 Standard-IA、S3 Glacier Instant Retrieval、S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 都是为了在整个 Amazon S3 可用区丢失的情况下维持数据。

Amazon S3 使用版本控制功能进一步保护您的数据。对于 Amazon S3 存储桶中存储的每个对象，您可以使用版本控制功能来保存、检索和还原它们的每个版本。使用版本控制能够轻松从用户意外操作和应用程序故障中恢复数据。默认情况下，请求会检索最新写入的版本。您可以通过指定请求中对象的版本，来检索该对象的旧版本。

除了 S3 版本控制之外，您还可以使用 Amazon S3 对象锁定和 S3 复制来保护您的数据。有关更多信息，请参阅教程：使用 S3 版本控制、S3 对象锁定和 S3 复制保护 Amazon S3 上的数据免遭意外删除或应用程序错误。

出于数据保护的目的，我们建议您保护 Amazon Web Services 账户凭证并使用 Amazon Identity and Access Management 设置单个用户账户，以便仅向每个用户提供履行其工作职责所需的权限。

如果在通过命令行界面或 API 访问 Amazon 时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准 (FIPS) 第 140-2 版》。

下面的安全最佳实践也探讨 Amazon S3 中的数据保护：

- Implement server-side encryption
- Enforce encryption of data in transit
- Consider using Macie with Amazon S3
- Identify and audit all your Amazon S3 buckets
- Monitor Amazon Web Services security advisories

# 利用加密来保护数据

> **Important**
>
> Amazon S3 现在将具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）作为 Amazon S3 中每个存储桶的基本加密级别。从 2023 年 1 月 5 日起，上传到 Amazon S3 的所有新对象都

将自动加密，不会产生额外费用，也不会影响性能。S3 存储桶默认加密配置和上传的新对象的自动加密状态可在 Amazon CloudTrail 日志、S3 清单、S3 Storage Lens 存储统计管理工具、Amazon S3 控制台中获得，并可用作 Amazon Command Line Interface 和 Amazon SDK 中的附加 Amazon S3 API 响应标头。有关更多信息，请参阅默认加密常见问题解答。

数据保护指在数据传输（发往和离开 Amazon S3 时）和处于静态（存储在 Amazon S3 数据中心的磁盘上时）期间保护数据。您可以使用安全套接字层/传输层安全性（SSL/TLS）或客户端加密来保护传输中数据。为保护 Amazon S3 中的静态数据，您具有以下选项：

- 服务器端加密 – Amazon S3 在将对象保存到 Amazon 数据中心的磁盘之前对其进行加密，然后在下载对象时对其进行解密。

  默认情况下，所有 Amazon S3 存储桶都配置了加密，所有上传到 S3 存储桶的新对象都会自动静态加密。具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）是 Amazon S3 中每个存储桶的默认加密配置。要使用其他类型的加密，您可以指定要在 S3 PUT 请求中使用的服务器端加密类型，也可以在目标存储桶中设置默认加密配置。

  如果您想在 PUT 请求中指定不同的加密类型，则可以使用具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）、具有 Amazon KMS 密钥的双层服务器端加密（DSSE-KMS）或具有客户提供的密钥的服务器端加密（SSE-C）。如果您想在目标存储桶中设置不同的默认加密配置，则可以使用 SSE-KMS 或 DSSE-KMS。

  有关服务器端加密的每个选项的更多信息，请参阅使用服务器端加密保护数据。

  要配置服务器端加密，请参阅：

  - 指定具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）
  - 使用 Amazon KMS (SSE-KMS) 指定服务器端加密
  - the section called “指定 DSSE-KMS”
  - 指定使用客户提供的密钥的服务器端加密 (SSE-C)。

- 客户端加密 – 您在客户端加密数据并将加密的数据上传到 Amazon S3。在这种情况下，您需要管理加密过程、加密密钥和相关的工具。

  要配置客户端加密，请参阅 使用客户端加密保护数据。

要查看存储字节的加密百分比，您可以使用 Amazon S3 Storage Lens 存储统计管理工具指标。S3 Storage Lens 存储统计管理工具是一项云存储分析功能，您可以使用它在整个组织范围内了解对象存

储的使用情况和活动。有关更多信息，请参阅使用 S3 Storage Lens 存储统计管理工具访问存储活动和使用情况。有关指标的完整列表，请参阅 S3 Storage Lens 存储统计管理工具指标词汇表。

有关服务器端加密和客户端加密的更多信息，请查看下面的主题。

主题


- 使用服务器端加密保护数据
- 使用客户端加密保护数据


## 使用服务器端加密保护数据

> **Important**
>
> Amazon S3 现在将具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）作为 Amazon S3 中每个存储桶的基本加密级别。从 2023 年 1 月 5 日起，上传到 Amazon S3 的所有新对象都将自动加密，不会产生额外费用，也不会影响性能。S3 存储桶默认加密配置和上传的新对象的自动加密状态可在 Amazon CloudTrail 日志、S3 清单、S3 Storage Lens 存储统计管理工具、Amazon S3 控制台中获得，并可用作 Amazon Command Line Interface 和 Amazon SDK 中的附加 Amazon S3 API 响应标头。有关更多信息，请参阅默认加密常见问题解答。

服务器端加密是指由接收数据的应用程序或服务在目标位置对数据进行加密。Amazon S3 在将您的数据写入 Amazon 数据中心内的磁盘时会在对象级别加密这些数据，并在您访问这些数据时解密这些数据。只要您验证了您的请求并且拥有访问权限，您访问加密和未加密对象的方式就没有区别。例如，如果您使用预签名的 URL 来共享您的对象，那么对于加密和解密的对象，该 URL 的工作方式是相同的。此外，在您列出存储桶中的对象时，列表 API 操作会返回所有对象的列表（无论对象是否加密）。

默认情况下，所有 Amazon S3 存储桶都配置了加密，所有上传到 S3 存储桶的新对象都会自动静态加密。具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）是 Amazon S3 中每个存储桶的默认加密配置。要使用其他类型的加密，您可以指定要在 S3 PUT 请求中使用的服务器端加密类型，也可以在目标存储桶中设置默认加密配置。

如果您想在 PUT 请求中指定不同的加密类型，则可以使用具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）、具有 Amazon KMS 密钥的双层服务器端加密（DSSE-KMS）或具有客户提供的密钥的服务器端加密（SSE-C）。如果您想在目标存储桶中设置不同的默认加密配置，则可以使用 SSE-KMS 或 DSSE-KMS。

> **Note**
>
> 您不能对同一个对象应用不同类型的服务器端加密。

如果您需要加密现有对象，请使用 S3 批量操作和 S3 清单。有关更多信息，请参阅使用 Amazon S3 批量操作加密对象和使用批量操作批量执行对象操作。

对于服务器端加密，您有四个互斥的选项，具体取决于您选择如何管理加密密钥和要应用的加密层数。

具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）

默认情况下，所有 Amazon S3 存储桶都配置了加密。服务器端加密的默认选项是使用 Amazon S3 托管式密钥（SSE-S3）。每个对象都使用唯一的密钥来进行加密。作为额外的保护措施，SSE-S3 使用定期轮换的根密钥加密密钥本身。SSE-S3 使用可用的最强数据块密码之一 [即 256 位高级加密标准（AES-256）] 来加密您的数据。有关更多信息，请参阅 使用具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）。

具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）

具有 Amazon KMS keys 的服务器端加密（SSE-KMS）是通过将 Amazon KMS 服务与 Amazon S3 集成来提供的。使用 Amazon KMS，您可以更好地控制您的密钥。例如，您可以查看单独的密钥、编辑控制策略以及遵循 Amazon CloudTrail 中的密钥。此外，您还可以创建和管理客户自主管理型密钥，或者使用对于您、服务和区域为唯一的 Amazon 托管式密钥。有关更多信息，请参阅 使用具有 Amazon KMS 密钥的服务器端加密（SSE-KMS）。

具有 Amazon Key Management Service（Amazon KMS）密钥的双层服务器端加密（DSSE-KMS）

使用 Amazon KMS keys 的双层服务器端加密（DSSE-KMS）与 SSE-KMS 类似，但 DSSE-KMS 应用的是两层单独的对象级加密，而不是一层。由于两层加密都应用于服务器端的对象，因此您可以使用各种 Amazon Web Services 服务和工具来分析 S3 中的数据，同时使用可以满足合规性要求的加密方法。有关更多信息，请参阅 使用具有 Amazon KMS 密钥的双层服务器端加密（DSSE-KMS）。

具有客户提供密钥的服务器端加密（SSE-C）

使用具有客户提供的密钥的服务器端加密（SSE-C）时，您管理加密密钥，而 Amazon S3 管理加密（在它对磁盘进行写入时）和解密（在您访问您的对象时）。有关更多信息，请参阅 使用具有客户提供的密钥的服务器端加密（SSE-C）。

# 为 Amazon S3 存储桶设置默认服务器端加密行为

> **Important**
>
> Amazon S3 现在将具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）作为 Amazon S3 中每个存储桶的基本加密级别。从 2023 年 1 月 5 日起，上传到 Amazon S3 的所有新对象都将自动加密，不会产生额外费用，也不会影响性能。S3 存储桶默认加密配置和上传的新对象的自动加密状态可在 Amazon CloudTrail 日志、S3 清单、S3 Storage Lens 存储统计管理工具、Amazon S3 控制台中获得，并可用作 Amazon Command Line Interface 和 Amazon SDK 中的附加 Amazon S3 API 响应标头。有关更多信息，请参阅默认加密常见问题解答。

默认情况下，所有 Amazon S3 存储桶都配置了加密，并且通过具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）来自动加密对象。此加密设置适用于 Amazon S3 存储桶中的所有对象。

如果您需要对密钥进行更多控制，例如管理密钥轮换和访问策略授予，则可以选择使用具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS），或具有 Amazon KMS 密钥的双层服务器端加密（DSSE-KMS）。有关编辑 KMS 密钥的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的编辑密钥。

> **Note**
>
> 我们已更改存储桶，以自动加密新上传的对象。如果您之前创建的存储桶没有默认加密，则 Amazon S3 在默认情况下将使用 SSE-S3 为存储桶启用加密。对于已配置 SSE-S3 或 SSE-KMS 的现有存储桶的默认加密配置，不会进行任何更改。如果您想使用 SSE-KMS 加密您的对象，则必须在存储桶设置中更改加密类型。有关更多信息，请参阅 使用具有 Amazon KMS 密钥的服务器端加密（SSE-KMS）。

当您将存储桶配置为使用 SSE-KMS 的默认加密时，您还可以启用 S3 存储桶密钥，以减少从 Amazon S3 到 Amazon KMS 的请求流量并降低加密成本。有关更多信息，请参阅 使用 Amazon S3 存储桶密钥降低 SSE-KMS 的成本。

要识别已启用 SSE-KMS 进行默认加密的存储桶，您可以使用 Amazon S3 Storage Lens 存储统计管理工具指标。S3 Storage Lens 存储统计管理工具是一项云存储分析功能，您可以使用它在整个组织范围内了解对象存储的使用情况和活动。有关更多信息，请参阅使用 S3 Storage Lens 存储统计管理工具保护您的数据。

在使用服务器端加密时，Amazon S3 在将对象保存到其磁盘上之前对其进行加密，并在下载对象时对其进行解密。有关使用服务器端加密和加密密钥管理来保护数据的更多信息，请参阅使用服务器端加密保护数据。

有关默认加密所需的权限的更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 PutBucketEncryption。

您可以使用 Amazon S3 控制台、Amazon SDK、Amazon S3 REST API 和 Amazon 命令行界面（Amazon CLI）为 S3 存储桶配置 Amazon S3 默认加密行为。

加密现有对象

要加密现有未加密的 Amazon S3 对象，可以使用 Amazon S3 批量操作。您为 S3 批量操作提供了要操作的对象列表，而批量操作调用相应的 API 来执行指定的操作。您可以使用批量操作复制操作复制现有的未加密对象，并将其作为加密对象写回同一存储桶。单个批量操作作业可对数十亿个对象执行指定操作。有关更多信息，请参阅 使用批量操作批量执行对象操作 和 Amazon 存储博客的博客文章：使用 Amazon S3 批量操作加密对象。

也可以使用 `CopyObject` API 操作或 `copy-object` Amazon CLI 命令加密现有对象。有关更多信息，请参阅 Amazon 存储博客的博客文章：使用 Amazon CLI 加密现有 Amazon S3 对象。

> **Note**
>
> 将默认存储桶加密设置为 SSE-KMS 的 Amazon S3 存储桶不能用作 the section called “记录服务器访问” 的目标存储桶。对于服务器访问日志目标存储桶，仅支持 SSE-S3 默认加密。

使用 SSE-KMS 加密进行跨账户操作

在对跨账户操作使用加密时，请注意以下事项：

- 如果未在请求时提供 Amazon KMS key Amazon 资源名称（ARN）或别名，也未通过存储桶的默认加密配置提供它们时，则使用 Amazon 托管式密钥（`aws/s3`）。
- 如果您使用您的 KMS 密钥所在的相同 Amazon Web Services 账户中的 Amazon Identity and Access Management（IAM）主体上传或访问 S3 对象，则可以使用 Amazon 托管式密钥（`aws/s3`）。
- 如果您希望授予对 S3 对象的跨账户访问权限，请使用客户自主管理型密钥。您可以配置客户托管式密钥的策略，以便允许从其他账户进行访问。

- 如果您指定客户托管式 KMS 密钥，我们建议您使用完全限定的 KMS 密钥 ARN。如果您改为使用 KMS 密钥别名，Amazon KMS 将解析请求者账户中的密钥。这一行为可能导致使用属于请求者而不是存储桶拥有者的 KMS 密钥来加密数据。
- 您必须指定您（请求者）已被授予 `Encrypt` 权限的密钥。有关更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的允许密钥用户使用 KMS 密钥进行加密操作。

有关何时使用客户自主管理型密钥和 Amazon KMS 托管密钥的更多信息，请参阅我是应使用 Amazon 托管式密钥 还是使用客户自主管理型密钥来加密 Amazon S3 中的对象？

将默认加密用于复制

在为复制目标存储桶启用默认加密后，将应用以下加密行为：

- 如果未对源存储桶中的对象进行加密，则将使用目标存储桶的默认加密设置对目标存储桶中的副本对象进行加密。因此，源对象的实体标签（ETag）与副本对象的 ETag 不同。如果您有使用 ETag 的应用程序，则必须更新这些应用程序以弥补这种差异。
- 如果使用具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）、具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）或具有 Amazon KMS 密钥的双层服务器端加密（DSSE-KMS）来加密源存储桶中的对象，则目标存储桶中的副本对象使用与源对象相同类型的加密。不会使用目标存储桶的默认加密设置。

有关使用 SSE-KMS 进行默认加密的更多信息，请参阅复制加密对象。

将 Amazon S3 存储桶密钥用于默认加密

当将存储桶配置为使用 SSE-KMS 作为新对象的默认加密行为时，还可以配置 S3 存储桶密钥。S3 存储桶密钥可减少从 Amazon S3 到 Amazon KMS 的事务数量，从而降低 SSE-KMS 的成本。

当您将存储桶配置为使用 S3 存储桶密钥对新对象进行 SSE-KMS 加密时，Amazon KMS 会生成存储桶级别密钥，该密钥用于为存储桶中的对象创建唯一的数据密钥。此 S3 存储桶密钥在 Amazon S3 内限时使用，从而减少了 Amazon S3 向 Amazon KMS 发出请求，以完成加密操作的需求。

有关使用 S3 存储桶密钥的更多信息，请参阅 使用 Amazon S3 存储桶密钥。

配置默认加密

> **Important**
>
> Amazon S3 现在将具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）作为 Amazon S3 中每个存储桶的基本加密级别。从 2023 年 1 月 5 日起，上传到 Amazon S3 的所有新对象都

将自动加密，不会产生额外费用，也不会影响性能。S3 存储桶默认加密配置和上传的新对象的自动加密状态可在 Amazon CloudTrail 日志、S3 清单、S3 Storage Lens 存储统计管理工具、Amazon S3 控制台中获得，并可用作 Amazon Command Line Interface 和 Amazon SDK 中的附加 Amazon S3 API 响应标头。有关更多信息，请参阅默认加密常见问题解答。

默认设置情况下，Amazon S3 存储桶启用了存储桶加密，并且通过具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）来自动加密新对象。这种加密适用于您的 Amazon S3 存储桶中的所有新对象，并且不收取任何费用。

如果您需要对加密密钥进行更多控制，例如管理密钥轮换和访问策略授予，则可以选择使用具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS），或具有 Amazon KMS 密钥的双层服务器端加密（DSSE-KMS）。有关 SSE-KMS 的更多信息，请参阅 使用 Amazon KMS (SSE-KMS) 指定服务器端加密。有关 DSSE-KMS 的更多信息，请参阅the section called “双层服务器端加密（DSSE-KMS）”。

如果您希望使用其他账户拥有的 KMS 密钥，则您必须有权使用该密钥。有关 KMS 密钥的跨账户权限的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的创建其他账户可以使用的 KMS 密钥。

当您将默认存储桶加密设置为 SSE-KMS 时，还可以配置 S3 存储桶密钥以降低 Amazon KMS 请求成本。有关更多信息，请参阅 使用 Amazon S3 存储桶密钥降低 SSE-KMS 的成本。

> **Note**
>
> 如果使用 PutBucketEncryption 将默认存储桶加密设置为 SSE-KMS，则应验证您的 KMS 密钥 ID 是否正确。Amazon S3 不验证 PutBucketEncryption 请求中提供的 KMS 密钥 ID。

对 S3 存储桶使用默认加密不会产生额外的费用。请求配置默认加密行为会产生标准 Amazon S3 请求费用。有关定价的信息，请参阅 Amazon S3 定价。对于 SSE-KMS 和 DSSE-KMS，将会产生 Amazon KMS 费用，这些费用在 Amazon KMS 定价中列出。

默认加密不支持具有客户提供的密钥的服务器端加密（SSE-C）。

您可以使用 Amazon S3 控制台、Amazon SDK、Amazon S3 REST API 和 Amazon Command Line Interface（Amazon CLI）为 S3 存储桶配置 Amazon S3 默认加密。

启用默认加密之前需要注意的更改

在为存储桶启用默认加密后，将会应用以下加密行为：

- 在启用默认加密之前，存储桶中已存在的对象的加密没有变化。
- 在启用默认加密后上传对象时：
  - 如果您的 PUT 请求标头不包含加密信息，则 Amazon S3 将使用存储桶的默认加密设置来加密对象。
  - 如果您的 PUT 请求标头包含加密信息，则 Amazon S3 将使用 PUT 请求中的加密信息加密对象，然后再将对象存储在 Amazon S3 中。
- 如果您将 SSE-KMS 或 DSSE-KMS 选项用于默认加密配置，则您将受到 Amazon KMS 的每秒请求数（RPS）限额限制。有关 Amazon KMS 限额以及如何请求增加限额的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的限额。

> **Note**
>
> 在启用默认加密之前上传的对象将不会加密。有关加密现有对象的信息，请参阅the section called “设置默认存储桶加密”。

使用 S3 控制台

在 Amazon S3 存储桶上配置默认加密

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 在 Buckets（存储桶）列表中，请选择您想要的存储桶的名称。
4. 选择属性选项卡。
5. 在默认加密下，选择编辑。
6. 要配置加密，请在加密类型下，选择以下选项之一：
   - 具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）
   - 具有 Amazon Key Management Service 密钥的服务器端加密（SSE-KMS）
   - 具有 Amazon Key Management Service 密钥的双层服务器端加密（DSSE-KMS）

> **Important**
>
> 如果您将 SSE-KMS 或 DSSE-KMS 选项用于默认加密配置，则您将受到 Amazon KMS 的每秒请求数（RPS）限额限制。有关 Amazon KMS 限额以及如何请求增加限额的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的限额。

默认情况下，存储桶和新对象使用 SSE-S3 加密，除非您为存储桶指定其他类型的默认加密。有关默认加密的更多信息，请参阅为 Amazon S3 存储桶设置默认服务器端加密行为。

有关使用 Amazon S3 服务器端加密对数据进行加密的更多信息，请参阅使用具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）。

7. 如果您选择具有 Amazon Key Management Service 密钥的服务器端加密（SSE-KMS）或具有 Amazon Key Management Service 密钥的双层服务器端加密（DSSE-KMS），请执行以下操作：

   a. 在 Amazon KMS 密钥下，通过以下方式之一指定您的 KMS 密钥：

   - 要从可用的 KMS 密钥列表中进行选择，请选择从您的 Amazon KMS keys 密钥中进行选择，并从可用密钥的列表中选择您的 KMS 密钥。

     Amazon 托管式密钥 (aws/s3) 和您的客户自主管理型密钥都显示在此列表中。有关客户自主管理型密钥的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的客户密钥和 Amazon 密钥。
   - 要输入 KMS 密钥 ARN，请选择输入 Amazon KMS key ARN，然后在显示的字段中输入您的 KMS 密钥 ARN。
   - 要在 Amazon KMS 控制台中创建新的客户自主管理型密钥，请选择创建 KMS 密钥。

     有关创建 Amazon KMS key 的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的创建密钥。

> **Important**
>
> 您只能使用与存储桶所在相同 Amazon Web Services 区域 中启用的 KMS 密钥。选择从您的 KMS 密钥中选择时，S3 控制台每个区域仅列出 100 个 KMS 密钥。如果在同一区域中有超过 100 个 KMS，您只会在 S3 控制台中看到前 100 个 KMS 密钥。要使用控制台中未列出的 KMS 密钥，请选择输入 Amazon KMS key ARN，然后输入 KMS 密钥 ARN。

在 Amazon S3 中使用 Amazon KMS key 进行服务器端加密时，您必须选择对称加密 KMS 密钥。Amazon S3 仅支持对称加密 KMS 密钥。有关这些密钥的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的对称加密 KMS 密钥。

有关将 SSE-KMS 与 Amazon S3 结合使用的更多信息，请参阅使用具有 Amazon KMS 密钥的服务器端加密（SSE-KMS）。有关使用 DSSE-KMS 的更多信息，请参阅the section called "双层服务器端加密（DSSE-KMS）"。

b. 将存储桶配置为使用 SSE-KMS 进行默认加密时，您还可以启用 S3 存储桶密钥。S3 存储桶密钥可通过减少从 Amazon S3 到 Amazon KMS 的请求流量，降低加密成本。有关更多信息，请参阅 使用 Amazon S3 存储桶密钥降低 SSE-KMS 的成本。

要使用 S3 存储桶密钥，请在 Bucket Key（存储桶密钥）下，选择 Enable（启用）。

> **Note**
>
> DSSE-KMS 不支持 S3 存储桶密钥。

8. 选择保存更改。

使用 Amazon CLI

这些示例说明如何使用 SSE-S3 或将 SSE-KMS 与 S3 存储桶密钥结合使用来配置默认加密。

有关默认加密的更多信息，请参阅为 Amazon S3 存储桶设置默认服务器端加密行为。有关使用 Amazon CLI 配置默认加密的更多信息，请参阅 put-bucket-encryption。

Example – 使用 SSE-S3 进行默认加密

此示例使用 Amazon S3 托管密钥来配置默认存储桶加密。

```
aws s3api put-bucket-encryption --bucket amzn-s3-demo-bucket --server-side-encryption-
configuration '{
    "Rules": [
        {
            "ApplyServerSideEncryptionByDefault": {
                "SSEAlgorithm": "AES256"
            }
        }
    ]
```

```
}'
```

Example – 使用 S3 存储桶密钥通过 SSE-KMS 进行默认加密

此示例使用 S3 存储桶密钥通过 SSE-KMS 配置默认存储桶加密。

```
aws s3api put-bucket-encryption --bucket amzn-s3-demo-bucket --server-side-encryption-
configuration '{
    "Rules": [
            {
                "ApplyServerSideEncryptionByDefault": {
                    "SSEAlgorithm": "aws:kms",
                    "KMSMasterKeyID": "KMS-Key-ARN"
                },
                "BucketKeyEnabled": true
            }
        ]
    }'
```

使用 REST API

使用 REST API `PutBucketEncryption` 操作可启用默认加密，并设置要使用的服务器端加密类型：SSE-S3、SSE-KMS 或 DSSE-KMS。

有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 PutBucketEncryption。

使用 Amazon CloudTrail 和 Amazon EventBridge 监控默认加密

> **Important**
>
> Amazon S3 现在将具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）作为 Amazon S3 中每个存储桶的基本加密级别。从 2023 年 1 月 5 日起，上传到 Amazon S3 的所有新对象都将自动加密，不会产生额外费用，也不会影响性能。S3 存储桶默认加密配置和上传的新对象的自动加密状态可在 Amazon CloudTrail 日志、S3 清单、S3 Storage Lens 存储统计管理工具、Amazon S3 控制台中获得，并可用作 Amazon Command Line Interface 和 Amazon SDK 中的附加 Amazon S3 API 响应标头。有关更多信息，请参阅默认加密常见问题解答。

您可以使用 Amazon CloudTrail 事件跟踪 Amazon S3 存储桶的默认加密配置请求。CloudTrail 日志中使用以下 API 事件名称：

- PutBucketEncryption
- GetBucketEncryption
- DeleteBucketEncryption

您还可以创建 EventBridge 规则，以匹配这些 API 调用的 CloudTrail 事件。有关 CloudTrail 事件的更多信息，请参阅使用控制台为存储桶中的对象启用日志记录功能。有关 EventBridge 事件的更多信息，请参阅 Amazon Web Services 服务中的事件。

您可以使用 CloudTrail 日志执行对象级 Amazon S3 操作，以跟踪向 Amazon S3 发出的 PUT 和 POST 请求。您可以使用这些操作来验证在传入 PUT 请求不包含加密标头时是否使用默认加密来加密对象。

当 Amazon S3 使用默认加密设置来加密对象时，日志将包含以下字段之一作为名称/值对："SSEApplied":"Default_SSE_S3"、"SSEApplied":"Default_SSE_KMS" 或 "SSEApplied":"Default_DSSE_KMS"。

当 Amazon S3 使用 PUT 加密标头来加密对象时，日志将包含以下字段之一作为名称/值对："SSEApplied":"SSE_S3"、"SSEApplied":"SSE_KMS"、"SSEApplied":"DSSE_KMS" 或 "SSEApplied":"SSE_C"。

对于分段上传，该信息包含在 InitiateMultipartUpload API 操作请求中。有关使用 CloudTrail 和 CloudWatch 的更多信息，请参阅Amazon S3 中的日志记录和监控。

默认加密常见问题解答

Amazon S3 现在将具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）作为 Amazon S3 中每个存储桶的基本加密级别。从 2023 年 1 月 5 日起，上传到 Amazon S3 的所有新对象都将自动加密，不会产生额外费用，也不会影响性能。使用 256 位高级加密标准（AES-256）的 SSE-S3 会自动应用于所有新存储桶和任何尚未配置默认加密的现有 S3 存储桶。S3 存储桶默认加密配置和上传的新对象的自动加密状态可在 Amazon CloudTrail 日志、S3 清单、S3 Storage Lens 存储统计管理工具、Amazon S3 控制台中获得，并可用作 Amazon Command Line Interface（Amazon CLI）和 Amazon SDK 中的附加 Amazon S3 API 响应标头。

以下各部分回答了有关此更新的问题。

Amazon S3 会更改已配置了默认加密的现有存储桶的默认加密设置吗？

不会。对于已配置 SSE-S3 或具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）的现有存储桶的默认加密配置，不会发生任何更改。有关如何设置存储桶的默认加密行为的更多信息，请参阅为 Amazon S3 存储桶设置默认服务器端加密行为。有关 SSE-S3 和 SSE-KMS 加密设置的更多信息，请参阅使用服务器端加密保护数据。

是否会在未配置默认加密的现有存储桶上启用默认加密？

是。Amazon S3 现在在所有现有未加密的存储桶上配置默认加密，以应用具有 Amazon S3 托管密钥的服务器端加密（SSE-S3），作为对上传到这些存储桶的新对象的基本加密级别。已在现有未加密存储桶中的对象不会自动加密。

如何查看新对象上传的默认加密状态？

目前，您可以在 Amazon CloudTrail 日志、S3 清单、S3 Storage Lens 存储统计管理工具、Amazon S3 控制台中查看新上传的对象的默认加密状态，并可将其作为 Amazon Command Line Interface（Amazon CLI）和 Amazon SDK 中的附加 Amazon S3 API 响应标头。

- 要查看您的 CloudTrail 事件，请参阅《Amazon CloudTrail 用户指南》中的在 CloudTrail 控制台中查看 CloudTrail 事件。CloudTrail 日志为针对 Amazon S3 的 PUT 和 POST 请求提供 API 跟踪。当使用默认加密来加密存储桶中的对象时，关于 PUT 和 POST API 请求的 CloudTrail 日志将包含以下字段作为名称/值对：`"SSEApplied":"Default_SSE_S3"`。
- 要查看 S3 清单中新对象上传的自动加密状态，请将 S3 清单报告配置为包含 Encryption（加密）元数据字段，然后在报告中查看每个新对象的加密状态。有关更多信息，请参阅设置 Amazon S3 清单。
- 要在 S3 Storage Lens 存储统计管理工具中查看新对象上传的自动加密状态，请配置 S3 Storage Lens 存储统计管理工具控制面板，并在控制面板的 Data protection（数据保护）类别中查看 Encrypted bytes（加密字节数）和 Encrypted object count（加密对象计数）指标。有关更多信息，请参阅使用 S3 控制台和在控制面板上查看 S3 Storage Lens 存储统计管理工具指标。
- 要在 Amazon S3 控制台中查看存储桶级别的自动加密状态，请在 Amazon S3 控制台中查看 Amazon S3 存储桶的默认加密。有关更多信息，请参阅 配置默认加密。
- 要在 Amazon Command Line Interface（Amazon CLI）和 Amazon SDK 中将自动加密状态作为附加 Amazon S3 API 响应标头来查看，请在使用对象操作 API（如 PutObject 和 GetObject）时检查响应标头 `x-amz-server-side-encryption`。

我需要做什么才能利用这一更改？

您无需对现有应用程序进行任何更改。由于针对您的所有存储桶都启用了默认加密，因此上传到 Amazon S3 的所有新对象都会自动加密。

我能否对正写入我的存储桶的新对象禁用加密？

不能。SSE-S3 是新的基本加密级别，适用于上传到您的存储桶的所有新对象。您无法再为新对象上传禁用加密。

我的费用会受到影响吗？

不会。使用 SSE-S3 进行默认加密不会产生额外的成本。像往常一样，将向您收取存储、请求和其他 S3 特征的费用。有关定价信息，请参阅 Amazon S3 定价。

Amazon S3 会加密我现有的未加密对象吗？

不会。从 2023 年 1 月 5 日开始，Amazon S3 仅自动加密新上传的对象。要加密现有对象，您可以使用 S3 批量操作创建对象的加密副本。这些加密副本将保留现有的对象数据和名称，并将使用您指定的加密密钥进行加密。有关更多详细信息，请参阅 Amazon 存储博客中的 Encrypting objects with Amazon S3 Batch Operations（使用 Amazon S3 批量操作加密对象）。

在此版本之前，我没有为我的存储桶启用加密。我需要更改访问对象的方式吗？

不需要。使用 SSE-S3 进行默认加密，在将您的数据写入 Amazon S3 时会自动加密这些数据，并在您访问时解密这些数据。访问自动加密的对象的方式没有变化。

我需要更改访问客户端加密的对象的方式吗？

不需要。所有在上传到 Amazon S3 之前经过加密的客户端加密对象都作为 Amazon S3 中已加密的加密文字对象到达。这些对象现在将具有额外的 SSE-S3 加密层。使用客户端加密对象的工作负载不要求对客户端服务或授权设置进行任何更改。

> **Note**
>
> 未使用 Amazon 提供者的已更新版本的 HashiCorp Terraform 用户在创建没有客户定义的加密配置的新 S3 存储桶后，可能会看到意想不到的偏差。为避免这种偏差，请将您的 Terraform Amazon 提供者版本更新为以下版本之一：任何 4.x 发行版、3.76.1 或 2.70.4。

## 使用具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）

> **Important**
>
> Amazon S3 现在将具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）作为 Amazon S3 中每个存储桶的基本加密级别。从 2023 年 1 月 5 日起，上传到 Amazon S3 的所有新对象都将自动加密，不会产生额外费用，也不会影响性能。S3 存储桶默认加密配置和上传的新对象的自动加密状态可在 Amazon CloudTrail 日志、S3 清单、S3 Storage Lens 存储统计管理工具、Amazon S3 控制台中获得，并可用作 Amazon Command Line Interface 和 Amazon SDK 中的附加 Amazon S3 API 响应标头。有关更多信息，请参阅默认加密常见问题解答。

默认情况下，向 Amazon S3 存储桶上传的所有新对象都使用具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）进行加密。

服务器端加密可保护静态数据。Amazon S3 使用唯一的密钥来加密每个对象。作为额外的保护，它将使用定期轮换的密钥加密密钥本身。Amazon S3 服务器端加密使用 256 位高级加密标准 Galois/Counter 模式（AES-GCM）对所有上传的对象进行加密。

使用具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）不会产生额外费用。然而，请求配置默认加密特征会产生标准 Amazon S3 请求费用。有关定价的信息，请参阅 Amazon S3 定价。

如果您要求仅使用 Amazon S3 托管密钥对上传的数据进行加密，则可以使用以下存储桶策略。例如，以下存储桶策略拒绝上传对象的权限，除非请求包含用于请求服务器端加密的 `x-amz-server-side-encryption` 标头：

```
{
  "Version": "2012-10-17",
  "Id": "PutObjectPolicy",
  "Statement": [
    {
      "Sid": "DenyObjectsThatAreNotSSES3",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition": {
        "StringNotEquals": {
          "s3:x-amz-server-side-encryption": "AES256"
        }
      }
    }
  ]
}
```

> **Note**
>
> 服务器端加密仅加密对象数据而非加密对象元数据。

### 服务器端加密的 API 支持

默认情况下，所有 Amazon S3 存储桶都配置了加密，所有上传到 S3 存储桶的新对象都会自动静态加密。具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）是 Amazon S3 中每个存储桶的默认加密配

置。要使用其他类型的加密，您可以指定要在 S3 PUT 请求中使用的服务器端加密类型，也可以在目标存储桶中设置默认加密配置。

如果您想在 PUT 请求中指定不同的加密类型，则可以使用具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）、具有 Amazon KMS 密钥的双层服务器端加密（DSSE-KMS）或具有客户提供的密钥的服务器端加密（SSE-C）。如果您想在目标存储桶中设置不同的默认加密配置，则可以使用 SSE-KMS 或 DSSE-KMS。

要使用对象创建 REST API 配置服务器端加密，必须提供 `x-amz-server-side-encryption` 请求标头。有关 REST API 的信息，请参阅 使用 REST API。

以下 Amazon S3 API 支持此标头：

- PUT 操作 - 在使用 PUT API 上传数据时指定请求标头。有关更多信息，请参阅 PUT Object。
- 启动分段上传 - 当使用分段上传 API 操作上传大型对象时，在启动请求中指定标头。有关更多信息，请参阅启动分段上传。
- COPY 操作 - 在复制对象时，您同时具有源对象和目标对象。有关更多信息，请参阅 PUT Object - 复制。

> **Note**
>
> 当使用 POST 操作上传对象时，请在表单字段中提供相同的信息，而不是提供请求标头。有关更多信息，请参阅 POST 对象。

Amazon SDK 还提供了一个可用于请求服务器端加密的包装程序 API。您还可以使用 Amazon Web Services Management Console 来上传对象并请求服务器端加密。

有关更多常规信息，请参阅《Amazon Key Management Service 开发人员指南》中的 Amazon KMS 概念。

主题

- 指定具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）

## 指定具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）

默认情况下，所有 Amazon S3 存储桶都配置了加密，所有上传到 S3 存储桶的新对象都会自动静态加密。具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）是 Amazon S3 中每个存储桶的默认加密配

置。要使用其他类型的加密，您可以指定要在 S3 PUT 请求中使用的服务器端加密类型，也可以在目标存储桶中设置默认加密配置。

如果您想在 PUT 请求中指定不同的加密类型，则可以使用具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）、具有 Amazon KMS 密钥的双层服务器端加密（DSSE-KMS）或具有客户提供的密钥的服务器端加密（SSE-C）。如果您想在目标存储桶中设置不同的默认加密配置，则可以使用 SSE-KMS 或 DSSE-KMS。

您可以使用 S3 控制台、REST API、Amazon SDK 和 Amazon Command Line Interface（Amazon CLI）指定 SSE-S3。有关更多信息，请参阅 为 Amazon S3 存储桶设置默认服务器端加密行为。

使用 S3 控制台

本主题介绍如何使用 Amazon Web Services Management Console设置或更改对象的加密类型。使用控制台复制对象时，Amazon S3 将按原样复制对象。这意味着，如果对源对象加密，则也会对目标对象加密。可以使用控制台添加或更改对象的加密。

> **Note**
>
> - 如果对象小于 5 GB，则可以更改对象的加密。如果对象大于 5GB，必须使用 Amazon CLI 或 Amazon SDK 来更改对象的加密。
> - 有关更改对象的加密所需的其它权限的列表，请参阅 the section called “S3 API 操作所需的权限”。有关授予此权限的示例策略，请参阅the section called “基于身份的策略示例”。
> - 如果更改对象的加密，则会创建一个新对象来替换旧对象。如果启用 S3 版本控制，则会创建对象的新版本，而现有对象将变为旧版本。更改属性的角色也会成为新对象（或对象版本）的拥有者。

更改对象的加密

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在导航窗格中，选择存储桶，然后选择通用存储桶选项卡。导航到包含要更改的对象的 Amazon S3 存储桶或文件夹。
3. 选中要更改的对象所对应的复选框。
4. 在操作菜单上，从显示的选项列表中选择编辑服务器端加密。
5. 滚动到服务器端加密部分。

6. 在加密设置下，选择使用默认加密的存储桶设置或覆盖默认加密的存储桶设置。
7. 如果您选择覆盖默认加密的存储桶设置，请配置以下加密设置。
   - 在加密类型下，选择具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）。SSE-S3 使用最强的数据块密码之一 [即 256 位高级加密标准（AES-256）] 来加密每个对象。有关更多信息，请参阅 使用具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）。
8. 在其它复制设置下，选择是要复制源设置、请勿指定设置还是指定设置。复制源设置是默认选项。如果您只想复制不带源设置属性的对象，请选择请勿指定设置。选择指定设置，来指定存储类、ACL、对象标签、元数据、服务器端加密和其它校验和的设置。
9. 选择保存更改。

> **Note**
>
> 此操作将加密应用于所有指定的对象。加密文件夹时，请等待保存操作完成，然后再将新对象添加到文件夹。

使用 REST API

创建对象时（即，上传新对象或复制现有对象时），您可以通过向请求添加 `x-amz-server-side-encryption` 标头来指定您是否希望 Amazon S3 使用 Amazon S3 托管式密钥（SSE-S3）加密您的数据。将标头的值设置为 Amazon S3 支持的加密算法 `AES256`。Amazon S3 通过返回响应标头 `x-amz-server-side-encryption` 来确认已使用 SSE-S3 存储对象。

以下 REST 上传 API 操作接受 `x-amz-server-side-encryption` 请求标头。

- PUT Object
- PUT Object – 复制
- POST 对象
- 开始分段上传

使用分段上传 API 操作上传大型对象时，您可以通过为启动分段上传请求添加 `x-amz-server-side-encryption` 标头来指定服务器端加密。复制现有对象时，不论源对象是否已经加密，都不会加密目标对象，除非您显式请求服务器端加密。

使用 SSE-S3 加密存储对象后，以下 REST API 操作的响应标头将返回 `x-amz-server-side-encryption` 标头。

- PUT Object
- PUT Object – 复制
- POST 对象
- 开始分段上传
- 上传分段
- 上传分段 – 复制
- 完成分段上传
- GET Object
- HEAD Object

> **Note**
>
> 如果您的对象使用 SSE-S3，请不要发送 GET 请求和 HEAD 请求的加密请求标头，否则会收到 HTTP 状态代码 400（错误请求）错误。

使用 Amazon SDK

使用 Amazon SDK 时，您可以请求 Amazon S3 使用具有 Amazon S3 托管式加密密钥的服务器端加密（SSE-S3）。这部分提供了以多种语言使用 Amazon SDK 的示例。有关其他 SDK 的信息，请转到示例代码和库。

Java

当您使用 适用于 Java 的 Amazon SDK 上传对象时，可以使用 SSE-S3 为对象加密。要请求服务器端加密，请使用 `ObjectMetadata` 的 `PutObjectRequest` 属性设置 `x-amz-server-side-encryption` 请求标头。当您调用 `AmazonS3Client` 的 `putObject()` 方法时，Amazon S3 将加密并保存数据。

当使用分段上传 API 操作上传对象时，还可以请求 SSE-S3 加密：

- 使用高级别分段上传 API 操作时，请在上传对象时使用 `TransferManager` 方法将服务器端加密应用于对象。可以使用将 `ObjectMetadata` 视为参数的任一上传方法。有关更多信息，请参阅 使用分段上传操作上传对象。
- 当使用低级别分段上传 API 操作时，应在启动分段上传时指定服务器端加密。您通过调用 `ObjectMetadata` 方法添加

`InitiateMultipartUploadRequest.setObjectMetadata()` 属性。有关更多信息，请参阅 使用 Amazon SDK（低级别 API）。

不能直接更改对象的加密状态 (加密未加密的对象或解密已加密的对象)。要更改对象的加密状态，请为对象创建一个副本，从而为副本指定所需的加密状态，然后删除原始对象。仅当您显式请求服务器端加密时，Amazon S3 才会加密复制的对象。要通过 Java API 请求加密复制的对象，请使用 `ObjectMetadata` 属性在 `CopyObjectRequest` 中指定服务器端加密。

Example 示例

以下示例演示如何使用 适用于 Java 的 Amazon SDK 设置服务器端加密。它展示了如何执行以下任务：

- 使用 SSE-S3 上传新对象。
- 通过为对象创建副本来更改对象的加密状态 (本示例中为加密之前未加密的对象)。
- 检查对象的加密状态。

有关服务器端加密的更多信息，请参阅 使用 REST API。有关创建和测试有效示例的说明，请参阅《适用于 Java 的 Amazon SDK 开发人员指南》中的入门。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.internal.SSEResultBase;
import com.amazonaws.services.s3.model.*;

import java.io.ByteArrayInputStream;

public class SpecifyServerSideEncryption {

    public static void main(String[] args) {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String keyNameToEncrypt = "*** Key name for an object to upload and encrypt
 ***";
```

```
        String keyNameToCopyAndEncrypt = "*** Key name for an unencrypted object to
be encrypted by copying ***";
        String copiedObjectKeyName = "*** Key name for the encrypted copy of the
unencrypted object ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withRegion(clientRegion)
                    .withCredentials(new ProfileCredentialsProvider())
                    .build();

            // Upload an object and encrypt it with SSE.
            uploadObjectWithSSEEncryption(s3Client, bucketName, keyNameToEncrypt);

            // Upload a new unencrypted object, then change its encryption state
            // to encrypted by making a copy.
            changeSSEEncryptionStatusByCopying(s3Client,
                    bucketName,
                    keyNameToCopyAndEncrypt,
                    copiedObjectKeyName);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }

    private static void uploadObjectWithSSEEncryption(AmazonS3 s3Client, String
bucketName, String keyName) {
        String objectContent = "Test object encrypted with SSE";
        byte[] objectBytes = objectContent.getBytes();

        // Specify server-side encryption.
        ObjectMetadata objectMetadata = new ObjectMetadata();
        objectMetadata.setContentLength(objectBytes.length);

objectMetadata.setSSEAlgorithm(ObjectMetadata.AES_256_SERVER_SIDE_ENCRYPTION);
        PutObjectRequest putRequest = new PutObjectRequest(bucketName,
                keyName,
                new ByteArrayInputStream(objectBytes),
```

```
                objectMetadata);

        // Upload the object and check its encryption status.
        PutObjectResult putResult = s3Client.putObject(putRequest);
        System.out.println("Object \"" + keyName + "\" uploaded with SSE.");
        printEncryptionStatus(putResult);
    }

    private static void changeSSEEncryptionStatusByCopying(AmazonS3 s3Client,
            String bucketName,
            String sourceKey,
            String destKey) {
        // Upload a new, unencrypted object.
        PutObjectResult putResult = s3Client.putObject(bucketName, sourceKey,
"Object example to encrypt by copying");
        System.out.println("Unencrypted object \"" + sourceKey + "\" uploaded.");
        printEncryptionStatus(putResult);

        // Make a copy of the object and use server-side encryption when storing the
        // copy.
        CopyObjectRequest request = new CopyObjectRequest(bucketName,
                sourceKey,
                bucketName,
                destKey);
        ObjectMetadata objectMetadata = new ObjectMetadata();

objectMetadata.setSSEAlgorithm(ObjectMetadata.AES_256_SERVER_SIDE_ENCRYPTION);
        request.setNewObjectMetadata(objectMetadata);

        // Perform the copy operation and display the copy's encryption status.
        CopyObjectResult response = s3Client.copyObject(request);
        System.out.println("Object \"" + destKey + "\" uploaded with SSE.");
        printEncryptionStatus(response);

        // Delete the original, unencrypted object, leaving only the encrypted copy
in
        // Amazon S3.
        s3Client.deleteObject(bucketName, sourceKey);
        System.out.println("Unencrypted object \"" + sourceKey + "\" deleted.");
    }

    private static void printEncryptionStatus(SSEResultBase response) {
        String encryptionStatus = response.getSSEAlgorithm();
        if (encryptionStatus == null) {
```

```
            encryptionStatus = "Not encrypted with SSE";
        }
        System.out.println("Object encryption status is: " + encryptionStatus);
    }
}
```

.NET

在上传对象时，可指示 Amazon S3 加密对象。要更改现有对象的加密状态，请复制该对象并删除源对象。默认情况下，仅当您显式请求目标对象的服务器端加密时，复制操作才会加密目标。要在 CopyObjectRequest 中指定 SSE-S3，请添加以下内容：

```
ServerSideEncryptionMethod = ServerSideEncryptionMethod.AES256
```

有关如何复制对象的有效示例，请参阅 使用 Amazon SDK。

以下示例将上传对象。在请求中，该示例指示 Amazon S3 加密对象。该示例随后检索对象元数据并验证使用的加密方法。有关设置和运行代码示例的信息，请参阅《适用于 .NET 的 Amazon SDK 开发人员指南》中的适用于 .NET 的 Amazon SDK 入门。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class SpecifyServerSideEncryptionTest
    {
        private const string bucketName = "*** bucket name ***";
        private const string keyName = "*** key name for object created ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;

        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            WritingAnObjectAsync().Wait();
        }
```

```
        static async Task WritingAnObjectAsync()
        {
            try
            {
                var putRequest = new PutObjectRequest
                {
                    BucketName = bucketName,
                    Key = keyName,
                    ContentBody = "sample text",
                    ServerSideEncryptionMethod = ServerSideEncryptionMethod.AES256
                };

                var putResponse = await client.PutObjectAsync(putRequest);

                // Determine the encryption state of an object.
                GetObjectMetadataRequest metadataRequest = new
 GetObjectMetadataRequest
                {
                    BucketName = bucketName,
                    Key = keyName
                };
                GetObjectMetadataResponse response = await
 client.GetObjectMetadataAsync(metadataRequest);
                ServerSideEncryptionMethod objectEncryption =
 response.ServerSideEncryptionMethod;

                Console.WriteLine("Encryption method used: {0}",
 objectEncryption.ToString());
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered ***. Message:'{0}' when writing
 an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
        }
    }
}
```

PHP

本主题介绍如何使用 适用于 PHP 的 Amazon SDK 版本 3 中的类来将 SSE-S3 添加到您上传到 Amazon S3 的对象。有关适用于 Ruby 的 Amazon 开发工具包 API 的更多信息，请转到适用于 Ruby 的 Amazon 开发工具包 – 版本 2。

要将对象上传到 Amazon S3，请使用 Aws\S3\S3Client::putObject() 方法。要将 x-amz-server-side-encryption 请求标头添加到您的上传请求，请使用值 ServerSideEncryption 指定 AES256 参数，如以下代码示例中所示。有关服务器端加密请求的信息，请参阅 使用 REST API。

```
 require 'vendor/autoload.php';

use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';

// $filepath should be an absolute path to a file on disk.
$filepath = '*** Your File Path ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// Upload a file with server-side encryption.
$result = $s3->putObject([
    'Bucket'               => $bucket,
    'Key'                  => $keyname,
    'SourceFile'           => $filepath,
    'ServerSideEncryption' => 'AES256',
]);
```

作为响应，Amazon S3 会返回 x-amz-server-side-encryption 标头以及已用于加密对象数据的加密算法的值。

在使用分段上传 API 操作上传大型对象时，您可以为正在上传的对象指定 SSE-S3，如下所示：

- 如果您使用低级别分段上传 API 操作，请在调用 Aws\S3\S3Client::createMultipartUpload() 方法时指定服务器端加密。要向请求添加 x-amz-server-side-encryption 请求标头，请使用值

array 指定 ServerSideEncryption 参数的 AES256 密钥。有关低级别分段上传 API 操作的更多信息，请参阅使用 Amazon SDK（低级别 API）。

- 当使用高级别分段上传 API 操作时，请使用 CreateMultipartUpload API 操作的 ServerSideEncryption 参数来指定服务器端加密。有关将 setOption() 方法与高级别分段上传 API 操作结合使用的示例，请参阅使用分段上传操作上传对象。

要确定现有对象的加密状态，请通过调用 Aws\S3\S3Client::headObject() 方法检索对象元数据，如下面的 PHP 代码示例所示。

```
 require 'vendor/autoload.php';

use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// Check which server-side encryption algorithm is used.
$result = $s3->headObject([
    'Bucket' => $bucket,
    'Key'    => $keyname,
]);
echo $result['ServerSideEncryption'];
```

要更改现有对象的加密状态，请使用 Aws\S3\S3Client::copyObject() 方法复制对象并删除源对象。默认情况下，copyObject() 不会加密目标，除非您通过将值 AES256 用于 ServerSideEncryption 参数，显式请求对目标对象进行服务器端加密。以下 PHP 代码示例将复制对象并向复制的对象添加服务器端加密。

```
 require 'vendor/autoload.php';

use Aws\S3\S3Client;

$sourceBucket = '*** Your Source Bucket Name ***';
$sourceKeyname = '*** Your Source Object Key ***';
```

```
$targetBucket = '*** Your Target Bucket Name ***';
$targetKeyname = '*** Your Target Object Key ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// Copy an object and add server-side encryption.
$s3->copyObject([
    'Bucket'               => $targetBucket,
    'Key'                  => $targetKeyname,
    'CopySource'           => "$sourceBucket/$sourceKeyname",
    'ServerSideEncryption' => 'AES256',
]);
```

有关更多信息，请参阅以下主题：

- 面向 Amazon S3 Aws\S3\S3Client 类的 适用于 PHP 的 Amazon SDK
- 适用于 PHP 的 Amazon SDK 文档

Ruby

在使用 适用于 Ruby 的 Amazon SDK 上传对象时，您可以指定使用 SSE-S3 对存储的对象进行静态加密。在您读回对象时，它将自动解密。

下面的 适用于 Ruby 的 Amazon SDK 版本 3 示例演示了如何指定对上传到 Amazon S3 的文件进行静态加密。

```
require 'aws-sdk-s3'

# Wraps Amazon S3 object actions.
class ObjectPutSseWrapper
  attr_reader :object

  # @param object [Aws::S3::Object] An existing Amazon S3 object.
  def initialize(object)
    @object = object
  end
```

```
  def put_object_encrypted(object_content, encryption)
    @object.put(body: object_content, server_side_encryption: encryption)
    true
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't put your content to #{object.key}. Here's why: #{e.message}"
    false
  end
end

# Example usage:
def run_demo
  bucket_name = "amzn-s3-demo-bucket"
  object_key = "my-encrypted-content"
  object_content = "This is my super-secret content."
  encryption = "AES256"

  wrapper = ObjectPutSseWrapper.new(Aws::S3::Object.new(bucket_name,
 object_content))
  return unless wrapper.put_object_encrypted(object_content, encryption)

  puts "Put your content into #{bucket_name}:#{object_key} and encrypted it with
 #{encryption}."
end

run_demo if $PROGRAM_NAME == __FILE__
```

下面的代码示例演示了如何确定现有对象的加密状态。

```
require 'aws-sdk-s3'

# Wraps Amazon S3 object actions.
class ObjectGetEncryptionWrapper
  attr_reader :object

  # @param object [Aws::S3::Object] An existing Amazon S3 object.
  def initialize(object)
    @object = object
  end

  # Gets the object into memory.
  #
  # @return [Aws::S3::Types::GetObjectOutput, nil] The retrieved object data if
 successful; otherwise nil.
```

```
  def object
    @object.get
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't get object #{@object.key}. Here's why: #{e.message}"
  end
end

# Example usage:
def run_demo
  bucket_name = "amzn-s3-demo-bucket"
  object_key = "my-object.txt"

  wrapper = ObjectGetEncryptionWrapper.new(Aws::S3::Object.new(bucket_name,
 object_key))
  obj_data = wrapper.get_object
  return unless obj_data

  encryption = obj_data.server_side_encryption.nil? ? 'no' :
 obj_data.server_side_encryption
  puts "Object #{object_key} uses #{encryption} encryption."
end

run_demo if $PROGRAM_NAME == __FILE__
```

如果存储在 Amazon S3 中的对象没有使用服务器端加密，则该方法将返回 null。

要更改现有对象的加密状态，请复制该对象并删除源对象。默认情况下，复制方法不会加密目标，除非您明确请求服务器端加密。您可以通过在选项的哈希参数中指定 server_side_encryption 值来请求对目标对象进行加密，如下面的 Ruby 代码示例所示。此代码示例演示如何复制对象和使用 SSE-S3 加密副本。

```
require 'aws-sdk-s3'

# Wraps Amazon S3 object actions.
class ObjectCopyEncryptWrapper
  attr_reader :source_object

  # @param source_object [Aws::S3::Object] An existing Amazon S3 object. This is
 used as the source object for
  #                                        copy actions.
  def initialize(source_object)
    @source_object = source_object
  end
```

```
  # Copy the source object to the specified target bucket, rename it with the target
 key, and encrypt it.
  #
  # @param target_bucket [Aws::S3::Bucket] An existing Amazon S3 bucket where the
 object is copied.
  # @param target_object_key [String] The key to give the copy of the object.
  # @return [Aws::S3::Object, nil] The copied object when successful; otherwise,
 nil.
  def copy_object(target_bucket, target_object_key, encryption)
    @source_object.copy_to(bucket: target_bucket.name, key: target_object_key,
 server_side_encryption: encryption)
    target_bucket.object(target_object_key)
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't copy #{@source_object.key} to #{target_object_key}. Here's why:
 #{e.message}"
  end
end

# Example usage:
def run_demo
  source_bucket_name = "amzn-s3-demo-bucket1"
  source_key = "my-source-file.txt"
  target_bucket_name = "amzn-s3-demo-bucket2"
  target_key = "my-target-file.txt"
  target_encryption = "AES256"

  source_bucket = Aws::S3::Bucket.new(source_bucket_name)
  wrapper = ObjectCopyEncryptWrapper.new(source_bucket.object(source_key))
  target_bucket = Aws::S3::Bucket.new(target_bucket_name)
  target_object = wrapper.copy_object(target_bucket, target_key, target_encryption)
  return unless target_object

  puts "Copied #{source_key} from #{source_bucket_name} to
 #{target_object.bucket_name}:#{target_object.key} and "\
       "encrypted the target with #{target_object.server_side_encryption}
 encryption."
end

run_demo if $PROGRAM_NAME == __FILE__
```

使用 Amazon CLI

要在使用 Amazon CLI 上传对象时指定 SSE-S3，请使用以下示例。

```
aws s3api put-object --bucket amzn-s3-demo-bucket1 --key object-key-name --server-side-encryption AES256  --body file path
```

有关更多信息，请参阅 Amazon CLI 参考中的 put-object。要在使用 Amazon CLI 复制对象时指定 SSE-S3，请参阅 copy-object。

使用 Amazon CloudFormation

有关使用 Amazon CloudFormation 设置加密的示例，请参阅《Amazon CloudFormation 用户指南》的 `AWS::S3::Bucket ServerSideEncryptionRule` 主题中的使用默认加密创建存储桶和通过 Amazon KMS 服务器端加密使用 S3 存储桶密钥创建存储桶示例。

## 使用具有 Amazon KMS 密钥的服务器端加密（SSE-KMS）

> **Important**
>
> Amazon S3 现在将具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）作为 Amazon S3 中每个存储桶的基本加密级别。从 2023 年 1 月 5 日起，上传到 Amazon S3 的所有新对象都将自动加密，不会产生额外费用，也不会影响性能。S3 存储桶默认加密配置和上传的新对象的自动加密状态可在 Amazon CloudTrail 日志、S3 清单、S3 Storage Lens 存储统计管理工具、Amazon S3 控制台中获得，并可用作 Amazon Command Line Interface 和 Amazon SDK 中的附加 Amazon S3 API 响应标头。有关更多信息，请参阅默认加密常见问题解答。

服务器端加密是指由接收数据的应用程序或服务在目标位置对数据进行加密。

Amazon S3 对于上传的新对象自动启用具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）。

除非您另行指定，否则默认情况下存储桶使用 SSE-S3 来加密对象。但是，您可以选择将存储桶配置为改为使用具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）。有关更多信息，请参阅 使用 Amazon KMS (SSE-KMS) 指定服务器端加密。

Amazon KMS 是一项服务，可将安全、高度可用的硬件和软件结合起来，以提供可扩展到云的密钥管理系统。Amazon S3 使用具有 Amazon KMS 的服务器端加密（SSE-KMS）来加密您的 S3 对象数据。此外，当为对象请求 SSE-KMS 时，S3 校验和（作为对象元数据的一部分）将以加密形式存储。有关校验和的更多信息，请参阅在 Amazon S3 中检查对象完整性。

如果使用 KMS 密钥，您可以通过 Amazon Web Services Management Console或 Amazon KMS API 使用 Amazon KMS 来执行以下操作：

- 集中创建、查看、编辑、监控、启用或禁用、轮换以及安排删除 KMS 密钥。
- 定义控制如何使用和谁可以使用 KMS 密钥的策略。
- 审计 KMS 密钥的使用情况，以确保正确使用。Amazon KMS API 支持审计，但 Amazon KMSAmazon Web Services Management Console 不支持。

Amazon KMS 中的安全控制可帮助您满足与加密相关的合规性要求。您可以利用这些 KMS 密钥来保护在 Amazon S3 存储桶中的数据。将 SSE-KMS 加密用于 S3 存储桶时，Amazon KMS keys 必须位于该存储桶所在的同一区域中。

使用 Amazon KMS keys 密钥需要支付额外费用。有关更多信息，请参阅 Amazon Key Management Service 开发人员指南中的 Amazon KMS key 概念和 Amazon KMS 定价。

权限

要成功向 Amazon S3 发出 `PutObject` 请求以使用 Amazon KMS 密钥来加密对象，您需要对密钥拥有 `kms:GenerateDataKey` 权限。要下载使用 Amazon KMS key加密的对象，您需要对密钥拥有 `kms:Decrypt` 权限。要执行分段上传以使用 Amazon KMS key来加密对象，您必须对密钥拥有 `kms:GenerateDataKey` 和 `kms:Decrypt` 权限。

> **Important**
>
> 仔细查看在您的 KMS 密钥政策中授予的权限。始终将客户自主管理型 KMS 密钥政策权限仅限制为必须访问相关 Amazon KMS 密钥操作的 IAM 主体和 Amazon 服务。有关更多信息，请参阅Amazon KMS 中的密钥策略。

主题


- Amazon KMS keys
- Amazon S3 存储桶密钥
- 需要服务器端加密
- 加密上下文
- 发送对 Amazon KMS 加密对象的请求
- 使用 Amazon KMS (SSE-KMS) 指定服务器端加密

- 使用 Amazon S3 存储桶密钥降低 SSE-KMS 的成本

### Amazon KMS keys

当您使用具有 Amazon KMS 的服务器端加密（SSE-KMS）时，您可以使用默认的 Amazon 托管式密钥，也可以指定您已创建的客户托管式密钥。Amazon KMS 支持信封加密。S3 将 Amazon KMS 特征用于信封加密来进一步保护您的数据。信封加密是一种加密方法，它使用数据密钥对明文数据进行加密，然后使用 KMS 密钥对该数据密钥进行加密。有关信封加密的更多信息，请参阅 Amazon Key Management Service 开发人员指南中的信封加密。

如果未指定客户托管密钥，首次将使用 SSE-KMS 加密的对象添加到存储桶时，Amazon S3 会自动在 Amazon Web Services 账户 中创建 Amazon 托管式密钥。默认情况下，Amazon S3 将此 KMS 密钥用于 SSE-KMS。

> **Note**
>
> 通过 SSE-KMS（使用 Amazon 托管式密钥）加密的对象不能跨账户共享。如果您需要跨账户共享 SSE-KMS 数据，则必须使用来自 Amazon KMS 的客户自主管理型密钥。

如果要使用客户托管式密钥进行 SSE-KMS 加密，可以在配置 SSE-KMS 之前创建对称加密客户托管式密钥。然后，为存储桶配置 SSE-KMS 时，请指定现有的客户托管密钥。有关对称加密密钥的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的对称加密 KMS 密钥。

创建客户托管密钥可为您提供更大的灵活性和控制力。例如，您可以创建、轮换和禁用客户托管密钥。您还可以定义访问控制和审核用于保护数据的客户托管密钥。有关客户托管式密钥和 Amazon 托管式密钥的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的客户密钥和 Amazon 密钥。

> **Note**
>
> 与标准 KMS 密钥不同，当您将服务器端加密与存储在外部密钥存储中的客户托管式密钥结合使用时，您有责任确保密钥材料的可用性和耐久性。有关外部密钥存储及其如何更改责任共担模式的更多信息，请参阅《Amazon Key Management Service 开发者指南》中的外部密钥存储。

使用 SSE-KMS 加密进行跨账户操作

在对跨账户操作使用加密时，请注意以下事项：

- 如果未在请求时提供 Amazon KMS key Amazon 资源名称（ARN）或别名，也未通过存储桶的默认加密配置提供它们时，则使用 Amazon 托管式密钥（`aws/s3`）。
- 如果您使用您的 KMS 密钥所在的相同 Amazon Web Services 账户中的 Amazon Identity and Access Management（IAM）主体上传或访问 S3 对象，则可以使用 Amazon 托管式密钥（`aws/s3`）。
- 如果您希望授予对 S3 对象的跨账户访问权限，请使用客户自主管理型密钥。您可以配置客户托管式密钥的策略，以便允许从其他账户进行访问。
- 如果您指定客户托管式 KMS 密钥，我们建议您使用完全限定的 KMS 密钥 ARN。如果您改为使用 KMS 密钥别名，Amazon KMS 将解析请求者账户中的密钥。这一行为可能导致使用属于请求者而不是存储桶拥有者的 KMS 密钥来加密数据。
- 您必须指定您（请求者）已被授予 `Encrypt` 权限的密钥。有关更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的允许密钥用户使用 KMS 密钥进行加密操作。

有关何时使用客户自主管理型密钥和 Amazon KMS 托管密钥的更多信息，请参阅我是应使用 Amazon 托管式密钥 还是使用客户自主管理型密钥来加密 Amazon S3 中的对象？

SSE-KMS 加密工作流程

如果您选择使用 Amazon 托管式密钥或客户托管式密钥加密数据，则 Amazon KMS 和 Amazon S3 执行以下信封加密操作：

1. Amazon S3 请求明文数据密钥以及使用指定 KMS 密钥加密的数据密钥的副本。
2. Amazon KMS 生成数据密钥，使用 KMS 密钥为其进行加密，然后将明文数据密钥和加密的数据密钥发送到 Amazon S3。
3. Amazon S3 使用数据密钥加密数据，并在使用后尽快从内存中删除该明文密钥。
4. Amazon S3 将加密的数据密钥作为元数据与加密数据一起存储。

当请求解密数据时，Amazon S3 和 Amazon KMS 将执行以下操作：

1. Amazon S3 在 `Decrypt` 请求中向 Amazon KMS 发送加密的数据密钥。
2. Amazon KMS 使用相同的 KMS 密钥为加密的数据密钥解密，然后将明文数据密钥返回到 Amazon S3。

3. Amazon S3 使用明文数据密钥解密已加密的数据，并尽快从内存中删除该明文数据密钥。

> **Important**
>
> 在 Amazon S3 中使用 Amazon KMS key 进行服务器端加密时，您必须选择对称加密 KMS 密钥。Amazon S3 仅支持对称加密 KMS 密钥。有关这些密钥的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的对称加密 KMS 密钥。

### 审计 SSE-KMS 加密

要识别指定 SSE-KMS 的请求，您可以使用 Amazon S3 Storage Lens 存储统计管理工具指标中的 All SSE-KMS requests（所有 SSE-KMS 请求）和 % all SSE-KMS requests（所有 SSE-KMS 请求的百分比）指标。S3 Storage Lens 存储统计管理工具是一项云存储分析功能，您可以使用它在整个组织范围内了解对象存储的使用情况和活动。还可以使用启用 SSE-KMS 的存储桶计数和启用 SSE-KMS 的存储桶百分比，来了解使用 SSE-KMS 进行默认存储桶加密的存储桶计数。有关更多信息，请参阅使用 S3 Storage Lens 存储统计管理工具访问存储活动和使用情况。有关指标的完整列表，请参阅 S3 Storage Lens 存储统计管理工具指标词汇表。

要审计为 SSE-KMS 加密数据使用 Amazon KMS 密钥的情况，您可以使用 Amazon CloudTrail 日志。您可以深入了解自己的加密操作，例如 GenerateDataKey 和 Decrypt。CloudTrail 支持多种属性值来筛选您的搜索，包括事件名称、用户名和事件源。

### Amazon S3 存储桶密钥

当您配置使用 Amazon KMS 的服务器端加密（SSE-KMS）时，您可以将存储桶配置为使用 S3 存储桶密钥实现 SSE-KMS。使用 SSE-KMS 的存储桶级别密钥可以通过减少从 Amazon S3 到 Amazon KMS 的流量请求，从而使您可以将 Amazon KMS 请求成本最高降低 99%。

当您将存储桶配置为使用 S3 存储桶密钥对新对象实现 SSE-KMS 时，Amazon KMS 会生成存储桶级别密钥，该密钥用于为存储桶中的对象创建唯一的数据密钥。此 S3 存储桶密钥在 Amazon S3 内限时使用，从而进一步减少了 Amazon S3 向 Amazon KMS 发出请求以完成加密操作的需求。有关使用 S3 存储桶密钥的更多信息，请参阅 使用 Amazon S3 存储桶密钥降低 SSE-KMS 的成本。

### 需要服务器端加密

如果要求对特定 Amazon S3 存储桶中的所有对象进行服务器端加密，请使用存储桶策略。例如，如果请求不包含用于请求服务器端加密（SSE-KMS）的 `x-amz-server-side-encryption-aws-kms-key-id` 标头，则下面的存储桶策略将拒绝所有人的上传对象（`s3:PutObject`）权限。

```
{
   "Version":"2012-10-17",
   "Id":"PutObjectPolicy",
   "Statement":[{
         "Sid":"DenyObjectsThatAreNotSSEKMS",
         "Effect":"Deny",
         "Principal":"*",
         "Action":"s3:PutObject",
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/*",
         "Condition":{
            "Null":{
               "s3:x-amz-server-side-encryption-aws-kms-key-id":"true"
            }
         }
      }
   ]
}
```

如要求使用特定 Amazon KMS key 对存储桶中的对象进行加密，可以使用 `s3:x-amz-server-side-encryption-aws-kms-key-id` 条件键。要指定 KMS 密钥，必须使用 `arn:aws:kms:region:acct-id:key/key-id` 格式的键 Amazon 资源名称（ARN）。Amazon Identity and Access Management 不验证 `s3:x-amz-server-side-encryption-aws-kms-key-id` 的字符串是否存在。

> **Note**
>
> 在上传对象时，可以使用 `x-amz-server-side-encryption-aws-kms-key-id` 标头指定 KMS 密钥，也可以依赖您的默认存储桶加密配置。如果 PutObject 请求在 `x-amz-server-side-encryption` 标头中指定 `aws:kms`，但未指定 `x-amz-server-side-encryption-aws-kms-key-id` 标头，则 Amazon S3 会假定您要使用 Amazon 托管式密钥。无论如何，Amazon S3 用于对象加密的 Amazon KMS 密钥 ID 必须与策略中的 Amazon KMS 密钥 ID 匹配，否则 Amazon S3 会拒绝请求。

要查看 Amazon S3 特定条件键的列表，请参阅《Service Authorization Reference》中的 Condition keys for Amazon S3。

### 加密上下文

加密上下文是一组键值对，其中包含有关数据的其他上下文信息。加密上下文没有加密。在为加密操作指定加密上下文时，Amazon S3 必须指定与解密操作相同的加密上下文。否则，解密将失败。Amazon KMS 会将加密上下文用作其他已经过验证的数据 (AAD) 以支持经过身份验证的加密。有关加密上下文的更多信息，请参阅 Amazon Key Management Service 开发人员指南中的加密上下文。

默认情况下，Amazon S3 使用对象或存储桶 Amazon 资源名称（ARN）作为加密上下文对：

- 如果您在不启用 S3 存储桶密钥的情况下使用 SSE-KMS，则将对象 ARN 用作加密上下文。

```
arn:aws:s3:::object_ARN
```

- 如果您使用 SSE-KMS 并启用 S3 存储桶密钥，则将存储桶 ARN 用作加密上下文。有关 S3 存储桶的更多信息，请参阅 使用 Amazon S3 存储桶密钥降低 SSE-KMS 的成本。

```
arn:aws:s3:::bucket_ARN
```

您可以选择使用 s3:PutObject 请求中的 `x-amz-server-side-encryption-context` 标头提供其他的加密上下文对。但是，由于加密上下文未加密，请确保它不包含敏感信息。Amazon S3 将此额外的密钥对与默认加密上下文一起存储。当处理 PUT 请求时，Amazon S3 会将 `aws:s3:arn` 的默认加密上下文附加到您提供的上下文中。

您可以使用加密上下文来标识和分类加密操作。您还可以使用默认的加密上下文 ARN 值来跟踪 Amazon CloudTrail 中的相关请求，方法是通过查看哪个 Amazon S3 ARN 与哪个加密密钥一起使用。

在 CloudTrail 日志文件的 `requestParameters` 字段中，加密上下文与以下内容类似。

```
"encryptionContext": {
    "aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-bucket1/file_name"
}
```

在将 SSE-KMS 与可选的 S3 存储桶密钥特征一起使用时，加密上下文值是存储桶的 ARN。

```
"encryptionContext": {
    "aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-bucket1"
}
```

发送对 Amazon KMS 加密对象的请求

> **Important**
>
> 对 Amazon KMS 加密对象的所有 GET 和 PUT 请求必须使用安全套接字层协议（SSL）和传输层安全性协议（TLS）发出。还必须使用有效的凭证对请求进行签名，例如 Amazon 签名版本 4（或 Amazon 签名版本 2）。

Amazon 签名版本 4 是将身份验证信息添加到通过 HTTP 发送的 Amazon 请求的过程。出于安全考虑，大多数 Amazon 请求都必须使用访问密钥（包括访问密钥 ID 和秘密访问密钥）进行签名。这两个密钥通常称为您的安全凭证。有关更多信息，请参阅对请求进行身份验证（Amazon Signature Version 4）和 Signature Version 4 签名过程。

> **Important**
>
> 如果对象使用 SSE-KMS，则不应对 GET 请求和 HEAD 请求发送加密请求标头。否则，您会收到 HTTP 400 错误请求错误。

主题

- 使用 Amazon KMS (SSE-KMS) 指定服务器端加密
- 使用 Amazon S3 存储桶密钥降低 SSE-KMS 的成本

使用 Amazon KMS (SSE-KMS) 指定服务器端加密

默认情况下，所有 Amazon S3 存储桶都配置了加密，所有上传到 S3 存储桶的新对象都会自动静态加密。具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）是 Amazon S3 中每个存储桶的默认加密配置。要使用其他类型的加密，您可以指定要在 S3 PUT 请求中使用的服务器端加密类型，也可以在目标存储桶中设置默认加密配置。

如果您想在 PUT 请求中指定不同的加密类型，则可以使用具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）、具有 Amazon KMS 密钥的双层服务器端加密（DSSE-KMS）或具有客户提供的密钥的服务器端加密（SSE-C）。如果您想在目标存储桶中设置不同的默认加密配置，则可以使用 SSE-KMS 或 DSSE-KMS。

当您上传新对象或复制现有对象时，您可以应用加密。

您可以使用 Amazon S3 控制台、REST API 操作、Amazon SDK 和 Amazon Command Line Interface（Amazon CLI）指定 SSE-KMS。有关更多信息，请参阅以下主题。

> **Note**
>
> 您可以在 Amazon S3 中使用多区域 Amazon KMS keys。但是，Amazon S3 目前将多区域密钥视为单区域密钥，且不使用密钥的多区域特征。有关更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的 Using multi-Region keys。

> **Note**
>
> 如果您希望使用其它账户拥有的 KMS 密钥，您必须有权使用该密钥。有关 KMS 密钥的跨账户权限的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的创建其他账户可以使用的 KMS 密钥。

使用 S3 控制台

本主题描述如何使用 Amazon S3 控制台，将对象的加密类型设置或更改为使用具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）。

> **Note**
>
> - 如果对象小于 5 GB，则可以更改对象的加密。如果对象大于 5GB，必须使用 Amazon CLI 或 Amazon SDK 来更改对象的加密。
> - 有关更改对象的加密所需的其它权限的列表，请参阅 the section called “S3 API 操作所需的权限”。有关授予此权限的示例策略，请参阅the section called “基于身份的策略示例”。
> - 如果更改对象的加密，则会创建一个新对象来替换旧对象。如果启用 S3 版本控制，则会创建对象的新版本，而现有对象将变为旧版本。更改属性的角色也会成为新对象（或对象版本）的拥有者。

添加或更改对象的加密

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。

2. 在导航窗格中，选择存储桶，然后选择通用存储桶选项卡。导航到包含要更改的对象的 Amazon S3 存储桶或文件夹。
3. 选中要更改的对象所对应的复选框。
4. 在操作菜单上，从显示的选项列表中选择编辑服务器端加密。
5. 滚动到服务器端加密部分。
6. 在加密设置下，选择使用默认加密的存储桶设置或覆盖默认加密的存储桶设置。

> **Important**
>
> 如果您将 SSE-KMS 选项用于默认加密配置，则您将受到 Amazon KMS 的每秒请求数（RPS）限额限制。有关 Amazon KMS 限额以及如何请求增加限额的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的限额。

7. 如果您选择覆盖默认加密的存储桶设置，请配置以下加密设置。

   a. 在加密类型下，选择具有 Amazon Key Management Service 密钥的服务器端加密（SSE-KMS）。

   b. 在 Amazon KMS 密钥下，执行以下操作以选择您的 KMS 密钥：

   - 要从可用的 KMS 密钥列表中进行选择，请选择从您的 Amazon KMS keys 中进行选择，然后从可用密钥的列表中选择您的 KMS 密钥。

     Amazon 托管式密钥（aws/s3）和您的客户自主管理型密钥都显示在此列表中。有关客户自主管理型密钥的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的客户密钥和 Amazon 密钥。
   - 要输入 KMS 密钥 ARN，请选择输入 Amazon KMS key ARN，然后在显示的字段中输入您的 KMS 密钥 ARN。
   - 要在 Amazon KMS 控制台中创建新的客户自主管理型密钥，请选择创建 KMS 密钥。

     有关创建 Amazon KMS key 的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的创建密钥。

> **Important**
>
> 您只能使用与存储桶所在相同的 Amazon Web Services 区域中可用的 KMS 密钥。Amazon S3 控制台仅列出与存储桶位于同一区域中的前 100 个 KMS 密钥。要使

用未列出的 KMS 密钥，您必须输入 KMS 密钥 ARN。如果您希望使用其他账户拥有的 KMS 密钥，则必须首先有权使用该密钥，然后必须输入相应的 KMS 密钥 ARN。Amazon S3 仅支持对称加密 KMS 密钥，不支持非对称 KMS 密钥。有关更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的确定对称和非对称 KMS 密钥。

8. 在其它复制设置下，选择是要复制源设置、请勿指定设置还是指定设置。复制源设置是默认选项。如果您只想复制不带源设置属性的对象，请选择请勿指定设置。选择指定设置，来指定存储类、ACL、对象标签、元数据、服务器端加密和其它校验和的设置。
9. 选择保存更改。

> **Note**
>
> 此操作将加密应用于所有指定的对象。加密文件夹时，请等待保存操作完成，然后再将新对象添加到文件夹。

使用 REST API

创建对象时（即上传新对象或复制现有对象时），您可以指定使用具有 Amazon KMS keys 的服务器端加密（SSE-KMS）来加密数据。为此，请将 `x-amz-server-side-encryption` 标头添加到请求。将标头的值设置为加密算法 `aws:kms`。Amazon S3 通过返回响应标头 `x-amz-server-side-encryption` 来确认已使用 SSE-KMS 存储您的对象。

如果您指定值为 `aws:kms` 的 `x-amz-server-side-encryption` 标头，则还可以使用以下请求标头：

- `x-amz-server-side-encryption-aws-kms-key-id`
- `x-amz-server-side-encryption-context`
- `x-amz-server-side-encryption-bucket-key-enabled`

主题

- 支持 SSE-KMS 的 Amazon S3 REST API 操作
- 加密上下文（x-amz-server-side-encryption-context）
- Amazon KMS 密钥 ID（x-amz-server-side-encryption-aws-kms-key-id）
- S3 桶密钥（x-amz-server-side-encryption-aws-bucket-key-enabled）

### 支持 SSE-KMS 的 Amazon S3 REST API 操作

以下 REST API 操作接受 `x-amz-server-side-encryption`、`x-amz-server-side-encryption-aws-kms-key-id` 和 `x-amz-server-side-encryption-context` 请求标头。

- PutObject – 使用 PUT API 操作上传数据时，您可以指定这些请求标头。
- CopyObject – 复制对象时，您同时具有源对象和目标对象。如果使用 `CopyObject` 操作传递 SSE-KMS 标头，这些标头仅应用于目标对象。复制现有对象时，不论源对象是否已加密，都不会对目标对象加密，除非您显式请求服务器端加密。
- POST Object – 使用 `POST` 操作上传对象时，可在表单字段（而不是在请求标头）中提供相同的信息。
- CreateMultipartUpload – 使用分段上传 API 操作上传大型对象时，可以指定这些标头。您可以在 `CreateMultipartUpload` 请求中指定这些标头。

使用服务器端加密存储对象时，以下 REST API 操作的响应标头将返回 `x-amz-server-side-encryption` 标头。

- PutObject
- CopyObject
- POST Object
- CreateMultipartUpload
- UploadPart
- UploadPartCopy
- CompleteMultipartUpload
- GetObject
- HeadObject

> **Important**
>
> - 如果您不让使用安全套接字协议（SSL）、传输层安全性协议（TLS）或签名版本 4 针对受 Amazon KMS 保护的对象发出所有 `GET` 和 `PUT` 请求，则这些请求都将失败。
> - 如果对象使用 SSE-KMS，则不应对 `GET` 请求和 `HEAD` 请求发送加密请求标头，否则将显示 HTTP 400 BadRequest 错误。

加密上下文（**x-amz-server-side-encryption-context**）

如果您指定 x-amz-server-side-encryption:aws:kms，Amazon S3 API 将支持带有 x-amz-server-side-encryption-context 标头的加密上下文。加密上下文是一组键值对，其中包含有关数据的其他上下文信息。

Amazon S3 会自动使用对象或存储桶 Amazon Resource Name（ARN）作为加密上下文对。如果您在不启用 S3 存储桶密钥的情况下使用 SSE-KMS，则将对象 ARN 用作加密上下文；例如 arn:aws:s3:::*object_ARN*。但是，如果您使用 SSE-KMS 并启用 S3 存储桶密钥，则将存储桶 ARN 用于加密上下文；例如 arn:aws:s3:::*bucket_ARN*。

您可以选择使用 x-amz-server-side-encryption-context 标头提供其他的加密上下文对。但是，由于加密上下文未加密，请确保其中不包含敏感信息。Amazon S3 将此额外的密钥对与默认加密上下文一起存储。

有关 Amazon S3 中加密上下文的信息，请参阅 加密上下文。有关加密上下文的一般信息，请参阅 Amazon Key Management Service 开发人员指南中的 Amazon Key Management Service 概念 - 加密上下文。

Amazon KMS 密钥 ID（**x-amz-server-side-encryption-aws-kms-key-id**）

您可以使用 x-amz-server-side-encryption-aws-kms-key-id 标头指定用于保护数据的客户自主管理型密钥的 ID。如果您指定 x-amz-server-side-encryption:aws:kms 标头但未提供 x-amz-server-side-encryption-aws-kms-key-id 标头，Amazon S3 将使用 Amazon 托管式密钥（aws/s3）来保护数据。如果要使用客户托管密钥，则必须提供客户托管密钥的 x-amz-server-side-encryption-aws-kms-key-id 标头。

> **Important**
>
> 在 Amazon S3 中使用 Amazon KMS key 进行服务器端加密时，您必须选择对称加密 KMS 密钥。Amazon S3 仅支持对称加密 KMS 密钥。有关这些密钥的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的对称加密 KMS 密钥。

S3 桶密钥（**x-amz-server-side-encryption-aws-bucket-key-enabled**）

您可以使用 x-amz-server-side-encryption-aws-bucket-key-enabled 请求标头在对象级别启用或禁用 S3 存储桶密钥。S3 存储桶密钥通过减少从 Amazon S3 到 Amazon KMS 的请求流量来降低您的 Amazon KMS 请求成本。有关更多信息，请参阅 使用 Amazon S3 存储桶密钥降低 SSE-KMS 的成本。

如果您指定 x-amz-server-side-encryption:aws:kms 标头但未提供 x-amz-server-side-encryption-aws-bucket-key-enabled 标头，则您的对象将使用目标存储桶的 S3 存储桶密钥设置来加密对象。有关更多信息，请参阅 在对象级别配置 S3 存储桶密钥。

使用 Amazon CLI

要使用以下示例 Amazon CLI 命令，请将 *user input placeholders* 替换为您自己的信息。

当您上传新对象或复制现有对象时，可以指定使用具有 Amazon KMS 密钥的服务器端加密来加密数据。为此，请将 --server-side-encryption aws:kms 标头添加到请求。使用 --ssekms-key-id *example-key-id* 添加您创建的客户托管式 Amazon KMS 密钥。如果您指定 --server-side-encryption aws:kms，但未提供 Amazon KMS 密钥 ID，Amazon S3 将使用 Amazon 托管式密钥。

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key example-object-key --server-
side-encryption aws:kms --ssekms-key-id example-key-id --body filepath
```

此外，您还可以通过添加 --bucket-key-enabled 或 --no-bucket-key-enabled 在 PUT 或 COPY 操作中启用或禁用 Amazon S3 存储桶密钥。Amazon S3 存储桶密钥可以通过减少从 Amazon S3 到 Amazon KMS 的请求流量来降低您的 Amazon KMS 请求成本。有关更多信息，请参阅使用 Amazon S3 存储桶密钥降低 SSE-KMS 的成本。

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key example-object-key --server-
side-encryption aws:kms --bucket-key-enabled --body filepath
```

您可以通过将未加密的对象复制回原位来加密该对象以使用 SSE-KMS。

```
aws s3api copy-object --bucket amzn-s3-demo-bucket --key example-object-key --
body filepath --bucket amzn-s3-demo-bucket --key example-object-key --sse aws:kms --
sse-kms-key-id example-key-id --body filepath
```

使用 Amazon SDK

使用 Amazon SDK 时，您可以请求 Amazon S3 使用 Amazon KMS keys 进行服务器端加密。以下示例展示了如何将 SSE-KMS 与适用于 Java 和 .NET 的 Amazon SDK 结合使用。有关其它 SDK 的信息，请参阅 Amazon 开发人员中心上的示例代码和库。

> **Important**
>
> 在 Amazon S3 中使用 Amazon KMS key 进行服务器端加密时，您必须选择对称加密 KMS 密钥。Amazon S3 仅支持对称加密 KMS 密钥。有关这些密钥的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的对称加密 KMS 密钥。

**`CopyObject` 操作**

在复制对象时，您添加相同的请求属性（`ServerSideEncryptionMethod` 和 `ServerSideEncryptionKeyManagementServiceKeyId`）来请求 Amazon S3 使用 Amazon KMS key。有关复制对象的更多信息，请参阅 复制、移动和重命名对象。

**`PUT` 操作**

Java

当使用适用于 Java 的 Amazon SDK 上传对象时，您可以通过添加 `SSEAwsKeyManagementParams` 属性来请求 Amazon S3 使用 Amazon KMS key，如以下请求所示：

```
PutObjectRequest putRequest = new PutObjectRequest(bucketName,
   keyName, file).withSSEAwsKeyManagementParams(new SSEAwsKeyManagementParams());
```

在这种情况下，Amazon S3 使用 Amazon 托管式密钥（`aws/s3`）。有关更多信息，请参阅 使用具有 Amazon KMS 密钥的服务器端加密（SSE-KMS）。您可以选择创建对称加密 KMS 密钥，并在请求中指定该密钥，如以下示例所示：

```
PutObjectRequest putRequest = new PutObjectRequest(bucketName,
   keyName, file).withSSEAwsKeyManagementParams(new
 SSEAwsKeyManagementParams(keyID));
```

有关创建客户托管密钥的更多信息，请参阅 Amazon Key Management Service 开发人员指南中的对 Amazon KMS API 进行编程。

有关上传对象的工作代码示例，请参阅以下主题。要使用这些示例，您必须更新这些代码示例并提供加密信息，如上述代码片段所示。

- 有关在单个操作中上传对象，请参阅 上传对象。

- 有关使用高级或低级分段上传 API 操作的分段上传，请参阅使用分段上传操作上传对象。

.NET

当使用适用于 .NET 的 Amazon SDK 上传对象时，您可以通过添加 `ServerSideEncryptionMethod` 属性来请求 Amazon S3 使用 Amazon KMS key，如以下请求所示：

```
PutObjectRequest putRequest = new PutObjectRequest
 {
     BucketName = amzn-s3-demo-bucket,
     Key = keyName,
     // other properties
     ServerSideEncryptionMethod = ServerSideEncryptionMethod.AWSKMS
 };
```

在这种情况下，Amazon S3 使用 Amazon 托管式密钥。有关更多信息，请参阅 使用具有 Amazon KMS 密钥的服务器端加密（SSE-KMS）。您可以选择创建自己的对称加密客户自主管理型密钥，并在请求中指定该密钥，如以下示例所示：

```
PutObjectRequest putRequest1 = new PutObjectRequest
{
  BucketName = amzn-s3-demo-bucket,
  Key = keyName,
  // other properties
  ServerSideEncryptionMethod = ServerSideEncryptionMethod.AWSKMS,
  ServerSideEncryptionKeyManagementServiceKeyId = keyId
};
```

有关创建客户托管密钥的更多信息，请参阅 Amazon Key Management Service 开发人员指南中的对 Amazon KMS API 进行编程。

有关上传对象的工作代码示例，请参阅以下主题。要使用这些示例，您必须更新这些代码示例并提供加密信息，如上述代码片段所示。

- 有关在单个操作中上传对象，请参阅 上传对象。
- 有关使用高级或低级分段上传 API 操作的分段上传，请参阅使用分段上传操作上传对象。

预签名 URL

Java

在为使用 Amazon KMS key加密的对象创建预签名 URL 时，您必须显式指定签名版本 4，如以下示例所示：

```
ClientConfiguration clientConfiguration = new ClientConfiguration();
clientConfiguration.setSignerOverride("AWSS3V4SignerType");
AmazonS3Client s3client = new AmazonS3Client(
        new ProfileCredentialsProvider(), clientConfiguration);
...
```

有关代码示例，请参阅 使用预签名 URL 共享对象。

.NET

在为使用 Amazon KMS key加密的对象创建预签名 URL 时，您必须显式指定签名版本 4，如以下示例所示：

```
AWSConfigs.S3Config.UseSignatureVersion4 = true;
```

有关代码示例，请参阅 使用预签名 URL 共享对象。

使用 Amazon S3 存储桶密钥降低 SSE-KMS 的成本

Amazon S3 存储桶密钥降低了具有 Amazon Key Management Service（Amazon KMS）密钥的 Amazon S3 服务器端加密（SSE-KMS）的成本。使用 SSE-KMS 的存储桶级别密钥可以通过减少从 Amazon S3 到 Amazon KMS 的请求流量，从而使您可以将 Amazon KMS 请求成本最高降低 99%。只需在 Amazon Web Services Management Console中单击几下，无需对客户端应用程序进行任何更改，您就可以将存储桶配置为使用 S3 存储桶密钥对新对象进行 SSE-KMS 加密。

> **Note**
>
> 使用 Amazon Key Management Service（Amazon KMS）密钥的双层服务器端加密（DSSE-KMS）不支持 S3 存储桶密钥。

SSE-KMS 的 S3 存储桶密钥

访问使用 SSE-KMS 加密的数百万或数十亿个对象的工作负载可以生成大量到 Amazon KMS 的请求。当您在没有 S3 存储桶密钥的情况下使用 SSE-KMS 保护数据时，Amazon S3 会为每个对象使用单独的 Amazon KMS 数据密钥。在这种情况下，每次对 KMS 加密的对象发出请求时，Amazon S3 都会调用 Amazon KMS。有关 SSE-KMS 工作原理的信息，请参阅 使用具有 Amazon KMS 密钥的服务器端加密（SSE-KMS）。

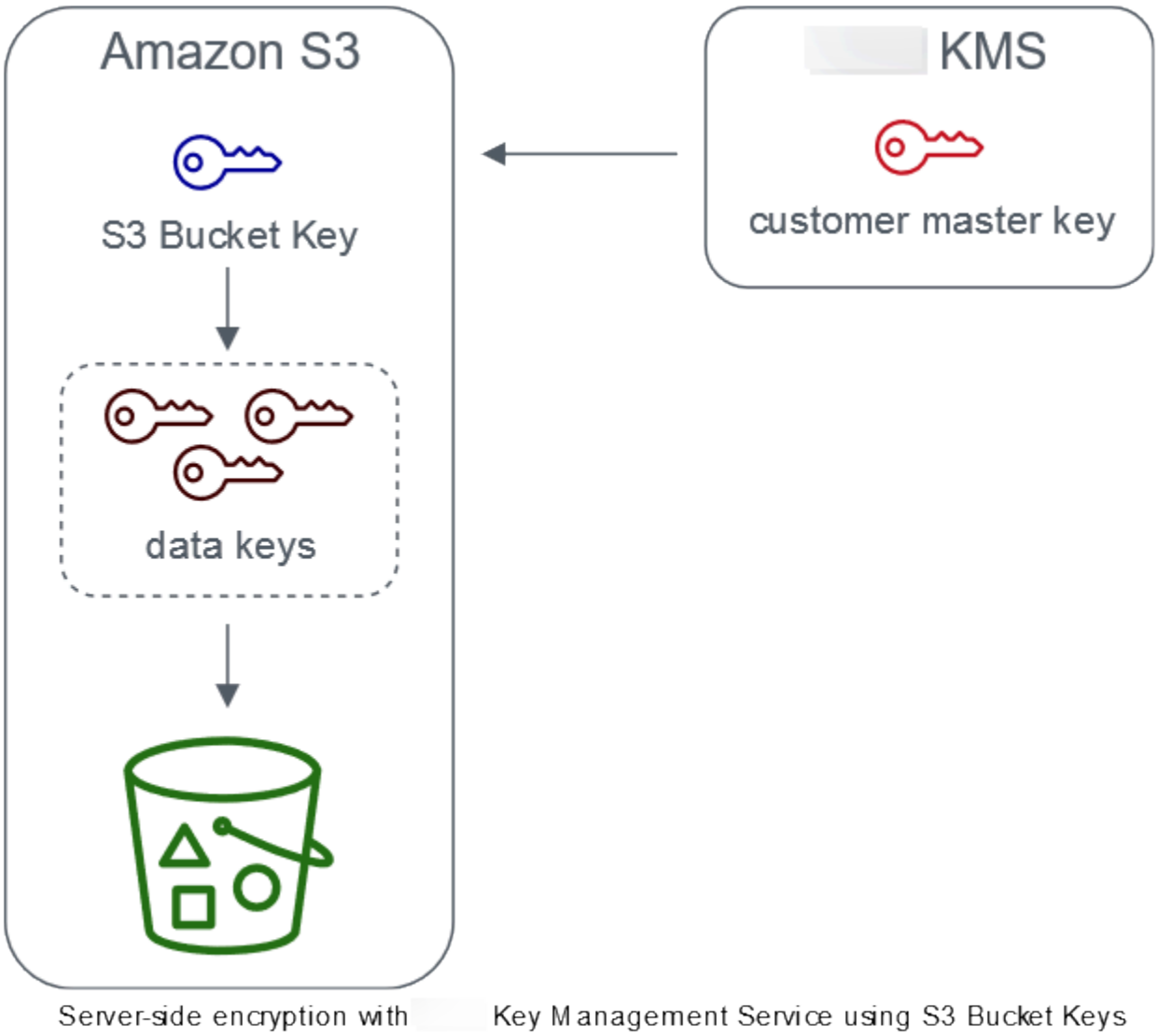
当您将存储桶配置为使用 S3 存储桶密钥进行 SSE-KMS 加密时，Amazon 会从 Amazon KMS 生成生存期较短的存储桶级密钥，然后暂时将其保留在 S3 中。此存储桶级密钥将在新对象的生命周期中为其创建数据密钥。S3 存储桶密钥在 Amazon S3 内限时使用，从而减少了 S3 向 Amazon KMS 发出请求以完成加密操作的需求。这样可以减少从 S3 到 Amazon KMS 的流量，使您能够在 Amazon S3 中访问 Amazon KMS 加密的对象，所需成本仅为以前的一小部分。

每个请求者至少获取一次唯一存储桶级密钥，以确保在 Amazon KMS CloudTrail 事件中捕获请求者对密钥的访问权限。当调用方使用不同的角色或账户，或使用具有不同范围限定策略的相同角色时，Amazon S3 会将其视为不同的请求者。Amazon KMS 节省的请求反映了请求者的数量、请求模式和所请求对象的相对年限。例如，减少请求者数量，在有限的时间窗口内请求多个对象，并使用相同的存储桶级密钥进行加密，可以节省更多费用。

> **Note**
>
> 利用 S3 存储桶密钥，可通过使用桶级密钥减少向 Amazon KMS 发出的面向 `Encrypt`、`GenerateDataKey` 和 `Decrypt` 操作的请求数，从而节省 Amazon KMS 请求成本。根据设计，利用此存储桶级密钥的后续请求不会产生 Amazon KMS API 请求或根据 Amazon KMS 密钥策略验证访问权限。

配置 S3 存储桶密钥时，存储桶中已存在的对象不使用 S3 存储桶密钥。要为现有对象配置 S3 存储桶密钥，可以使用 `CopyObject` 操作。有关更多信息，请参阅 在对象级别配置 S3 存储桶密钥。

Amazon S3 将仅为由同一 Amazon KMS key 加密的对象共享 S3 存储桶密钥。S3 存储桶密钥与 Amazon KMS 创建的 KMS 密钥、导入的密钥材料以及由自定义密钥存储库支持的密钥材料兼容。




Server-side encryption with Key Management Service using S3 Bucket Keys

配置 S3 存储桶密钥

您可以通过 Amazon S3 控制台、Amazon SDK、Amazon CLI 或 REST API 将存储桶配置为使用 S3 存储桶密钥对新对象进行 SSE-KMS 加密。在您的存储桶上启用 S3 存储桶密钥后，使用其他指定 SSE-KMS 密钥上传的对象将使用其自己的 S3 存储桶密钥。无论您的 S3 存储桶密钥设置如何，您都可以在请求中包含带 `true` 或 `false` 值的 `x-amz-server-side-encryption-bucket-key-enabled` 标头，以覆盖存储桶设置。

在将存储桶配置为使用 S3 存储桶密钥之前，请查看 启用 S3 存储桶密钥之前需要注意的更改。

使用 Amazon S3 控制台配置 S3 存储桶密钥

创建新存储桶时，您可以将存储桶配置为使用 S3 存储桶密钥对新对象进行 SSE-KMS 加密。您还可以通过更新存储桶属性，从而将现有存储桶配置为使用 S3 存储桶密钥对新对象进行 SSE-KMS 加密。

有关更多信息，请参阅 将存储桶配置为将 S3 存储桶密钥与 SSE-KMS 结合使用于新对象。

REST API、Amazon CLI 和 Amazon SDK 支持 S3 存储桶密钥

您可以使用 REST API、Amazon CLI 或 Amazon SDK 将存储桶配置为使用 S3 存储桶密钥对新对象进行 SSE-KMS 加密。您还可以在对象级别启用 S3 存储桶密钥。

有关更多信息，请参阅下列内容：

- 在对象级别配置 S3 存储桶密钥
- 将存储桶配置为将 S3 存储桶密钥与 SSE-KMS 结合使用于新对象

以下 API 操作对于 SSE-KMS 支持 S3 存储桶密钥：

- PutBucketEncryption
  - `ServerSideEncryptionRule` 接受用于启用和禁用 S3 存储桶密钥的 `BucketKeyEnabled` 参数。
- GetBucketEncryption
  - `ServerSideEncryptionRule` 返回 `BucketKeyEnabled` 的设置。
- PutObject、CopyObject、CreateMultipartUpload 和 POST 对象
  - `x-amz-server-side-encryption-bucket-key-enabled` 请求标头在对象级别启用或禁用 S3 存储桶密钥。
- HeadObject、GetObject、UploadPartCopy、UploadPart 和 CompleteMultipartUpload
  - `x-amz-server-side-encryption-bucket-key-enabled` 响应标头指示是否为对象启用或禁用了 S3 存储桶密钥。

使用 Amazon CloudFormation

在 Amazon CloudFormation 中，`AWS::S3::Bucket` 资源包括名为 `BucketKeyEnabled` 的加密属性，您可以使用该属性来启用或禁用 S3 存储桶密钥。

有关更多信息，请参阅 使用 Amazon CloudFormation。

启用 S3 存储桶密钥之前需要注意的更改

在启用 S3 存储桶密钥之前，请注意以下相关更改：

IAM 或 Amazon KMS 密钥策略

如果您现有的 Amazon Identity and Access Management（IAM）策略或 Amazon KMS 密钥策略使用您的对象 Amazon 资源名称（ARN）作为加密上下文来优化或限制对 KMS 密钥的访问，则这些策略将不使用 S3 存储桶密钥。S3 存储桶密钥使用存储桶 ARN 作为加密上下文。在启用 S3 存储桶密钥之前，请更新 IAM 策略或 Amazon KMS 密钥策略，以将存储桶 ARN 用作加密上下文。

有关加密上下文和 S3 存储桶密钥的更多信息，请参阅加密上下文。

Amazon KMS 的 CloudTrail 事件

启用 S3 存储桶密钥后，Amazon KMS CloudTrail 事件会记录存储桶 ARN 而不是对象 ARN。此外，您在日志中看到的 SSE-KMS 对象的 KMS CloudTrail 事件较少。因为 Amazon S3 中的密钥材料是有时间限制的，所以对 Amazon KMS 的请求减少。

将 S3 存储桶密钥与复制功能结合使用

您可以将 S3 存储桶密钥与同区域复制（SRR）和跨区域复制（CRR）结合使用。

当 Amazon S3 复制加密对象时，它通常会在目标存储桶中保留副本对象的加密设置。但是，如果源对象未加密且目标存储桶使用默认加密或 S3 存储桶密钥，则 Amazon S3 会使用目标存储桶的配置加密对象。

以下示例说明了 S3 存储桶密钥如何与复制结合使用。有关更多信息，请参阅 复制加密对象（SSE-S3、SSE-KMS、DSSE-KMS、SSE-C）。

Example 示例 1 – 源对象使用 S3 存储桶密钥；目标存储桶使用默认加密

如果源对象使用 S3 存储桶密钥，但目标存储桶将默认加密与 SSE-KMS 结合使用，则副本对象将在目标存储桶中维护其 S3 存储桶密钥加密设置。目标存储桶仍将默认加密与 SSE-KMS 结合使用。

Example 示例 2 – 源对象未加密；目标存储桶将 S3 存储桶密钥与 SSE-KMS 结合使用

如果源对象未加密，而目标存储桶将 S3 存储桶密钥与 SSE-KMS 结合使用，则将通过在目标存储桶中将 S3 存储桶密钥与 SSE-KMS 结合使用来加密复制的对象。这将导致源对象的 ETag 与副本对象的 ETag 不同。您必须更新使用 ETag 的应用程序以应对这种差异。

使用 S3 存储桶密钥

有关启用和使用 S3 存储桶密钥的更多信息，请参阅以下各部分：

- 将存储桶配置为将 S3 存储桶密钥与 SSE-KMS 结合使用于新对象

- 在对象级别配置 S3 存储桶密钥
- 查看 S3 存储桶密钥的设置

将存储桶配置为将 S3 存储桶密钥与 SSE-KMS 结合使用于新对象

当您配置具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）时，您可以将存储桶配置为使用 S3 存储桶密钥对新对象进行 SSE-KMS 加密。S3 存储桶密钥可减少从 Amazon S3 到 Amazon KMS 的请求流量，从而降低 SSE-KMS 的成本。有关更多信息，请参阅 使用 Amazon S3 存储桶密钥降低 SSE-KMS 的成本。

您可以使用 Amazon S3 控制台、REST API、Amazon SDK、Amazon Command Line Interface（Amazon CLI）或 Amazon CloudFormation 将存储桶配置为使用 S3 存储桶密钥对新对象进行 SSE-KMS 加密。如果要为现有对象启用或禁用 S3 存储桶密钥，则可以使用 `CopyObject` 操作。有关更多信息，请参阅在对象级别配置 S3 存储桶密钥和使用批量操作为 SSE-KMS 启用 S3 存储桶密钥。

当为源存储桶或目标存储桶启用 S3 存储桶密钥时，加密上下文将是存储桶 Amazon Resource Name（ARN），而不是对象 ARN，例如 `arn:aws:s3:::`*`bucket_ARN`*。您需要更新 IAM 策略才能将存储桶 ARN 用于加密上下文。有关更多信息，请参阅 S3 存储桶密钥和复制。

以下示例说明了 S3 存储桶密钥如何与复制结合使用。有关更多信息，请参阅 复制加密对象（SSE-S3、SSE-KMS、DSSE-KMS、SSE-C）。

先决条件

在将存储桶配置为使用 S3 存储桶密钥之前，请查看 启用 S3 存储桶密钥之前需要注意的更改。

使用 S3 控制台

在 S3 控制台中，您可以为新存储桶或现有存储桶启用或禁用 S3 存储桶密钥。S3 控制台中的对象从存储桶配置中继承其 S3 存储桶密钥设置。当您为存储桶启用 S3 存储桶密钥时，您上传到存储桶的新对象将利用 S3 存储桶密钥进行 SSE-KMS 加密。

在启用了 S3 存储桶密钥的存储桶中上传，复制或修改对象

如果您在启用了 S3 存储桶密钥的存储桶中上传、修改或复制对象，则该对象的 S3 存储桶密钥设置可能会更新以与存储桶配置保持一致。

如果对象已启用 S3 存储桶密钥，则在复制或修改对象时，该对象的 S3 存储桶密钥设置不会更改。但是，如果您修改或复制未启用 S3 存储桶密钥的对象，并且目标存储桶具有 S3 存储桶密钥配置，则该

对象将继承目标存储桶的 S3 存储桶密钥设置。例如，如果源对象尚未启用 S3 存储桶密钥，但目标存储桶已启用 S3 存储桶密钥，则为该对象启用 S3 存储桶密钥。

在创建新存储桶时启用 S3 存储桶密钥

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 请选择 Create bucket（创建存储桶）。
4. 输入存储桶名称，然后选择您的 Amazon Web Services 区域。
5. 在默认加密下，对于加密密钥类型，选择 Amazon Key Management Service 密钥（SSE-KMS）。
6. 在 Amazon KMS 密钥下，执行以下操作以选择您的 KMS 密钥：

   - 要从可用的 KMS 密钥列表中进行选择，请选择从您的 Amazon KMS keys 中进行选择，然后从可用密钥的列表中选择您的 KMS 密钥。

     Amazon 托管式密钥（aws/s3）和您的客户自主管理型密钥都显示在此列表中。有关客户自主管理型密钥的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的客户密钥和 Amazon 密钥。
   - 要输入 KMS 密钥 ARN，请选择输入 Amazon KMS key ARN，然后在显示的字段中输入您的 KMS 密钥 ARN。
   - 要在 Amazon KMS 控制台中创建新的客户自主管理型密钥，请选择创建 KMS 密钥。

     有关创建 Amazon KMS key 的更多信息，请参阅 Amazon Key Management Service 开发人员指南中的创建密钥。
7. 在 Bucket Key（存储桶密钥）下，请选择 Enable（启用）。
8. 请选择 Create bucket（创建存储桶）。

   Amazon S3 创建启用了 S3 存储桶密钥的存储桶。您上传到存储桶的新对象将使用 S3 存储桶密钥。

   要禁用 S3 存储桶密钥，请按照前面的步骤操作，然后选择 Disable（禁用）。

为现有存储桶启用 S3 存储桶密钥

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。

2. 在左侧导航窗格中，选择存储桶。
3. 在 Buckets（存储桶）列表中，请选择要为其启用 S3 存储桶密钥的存储桶。
4. 选择属性选项卡。
5. 在默认加密下，选择编辑。
6. 在默认加密下，对于加密密钥类型，选择 Amazon Key Management Service 密钥（SSE-KMS）。
7. 在 Amazon KMS 密钥下，执行以下操作以选择您的 KMS 密钥：

   - 要从可用的 KMS 密钥列表中进行选择，请选择从您的 Amazon KMS keys 中进行选择，然后从可用密钥的列表中选择您的 KMS 密钥。

     Amazon 托管式密钥（aws/s3）和您的客户自主管理型密钥都显示在此列表中。有关客户自主管理型密钥的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的客户密钥和 Amazon 密钥。
   - 要输入 KMS 密钥 ARN，请选择输入 Amazon KMS key ARN，然后在显示的字段中输入您的 KMS 密钥 ARN。
   - 要在 Amazon KMS 控制台中创建新的客户自主管理型密钥，请选择创建 KMS 密钥。

     有关创建 Amazon KMS key 的更多信息，请参阅 Amazon Key Management Service 开发人员指南中的创建密钥。
8. 在 Bucket Key（存储桶密钥）下，请选择 Enable（启用）。
9. 选择 Save Changes（保存更改）。

   Amazon S3 为添加到存储桶中的新对象启用 S3 存储桶密钥。现有对象未使用 S3 存储桶密钥。要为现有对象配置 S3 存储桶密钥，可以使用 `CopyObject` 操作。有关更多信息，请参阅 在对象级别配置 S3 存储桶密钥。

   要禁用 S3 存储桶密钥，请按照前面的步骤操作，然后选择 Disable（禁用）。

### 使用 REST API

您可以使用 PutBucketEncryption 为存储桶启用或禁用 S3 存储桶密钥。要使用 `PutBucketEncryption` 配置 S3 存储桶密钥，请使用 ServerSideEncryptionRule 数据类型，其中包括使用 SSE-KMS 进行的默认加密。您还可以通过客户托管密钥的 KMS 密钥 ID 来选择使用客户托管密钥。

有关更多信息和示例语法，请参阅 putbucKetenCryption 。

使用适用于 Java 的 Amazon 软件开发工具包

以下示例使用 适用于 Java 的 Amazon SDK，通过 SSE-KMS 和 S3 存储桶密钥启用默认存储桶加密。

Java

```
AmazonS3 s3client = AmazonS3ClientBuilder.standard()
    .withRegion(Regions.DEFAULT_REGION)
    .build();

ServerSideEncryptionByDefault serverSideEncryptionByDefault = new
 ServerSideEncryptionByDefault()
    .withSSEAlgorithm(SSEAlgorithm.KMS);
ServerSideEncryptionRule rule = new ServerSideEncryptionRule()
    .withApplyServerSideEncryptionByDefault(serverSideEncryptionByDefault)
    .withBucketKeyEnabled(true);
ServerSideEncryptionConfiguration serverSideEncryptionConfiguration =
    new ServerSideEncryptionConfiguration().withRules(Collections.singleton(rule));

SetBucketEncryptionRequest setBucketEncryptionRequest = new
 SetBucketEncryptionRequest()
    .withServerSideEncryptionConfiguration(serverSideEncryptionConfiguration)
    .withBucketName(bucketName);

s3client.setBucketEncryption(setBucketEncryptionRequest);
```

使用 Amazon CLI

以下示例使用 Amazon CLI，通过 SSE-KMS 和 S3 存储桶密钥启用默认存储桶加密。将 *user input placeholders* 替换为您自己的信息。

```
aws s3api put-bucket-encryption --bucket amzn-s3-demo-bucket --server-side-encryption-
configuration '{
        "Rules": [
            {
                "ApplyServerSideEncryptionByDefault": {
                    "SSEAlgorithm": "aws:kms",
                    "KMSMasterKeyID": "KMS-Key-ARN"
                },
                "BucketKeyEnabled": true
            }
```

```
        ]
    }'
```

使用 Amazon CloudFormation

有关使用 Amazon CloudFormation 配置 S3 存储桶密钥的更多信息，请参阅《Amazon CloudFormation 用户指南》中的 AWS::S3::Bucket ServerSideEncryptionRule。

在对象级别配置 S3 存储桶密钥

当您使用 REST API、Amazon SDK 或 Amazon CLI 执行 PUT 或 COPY 操作时，您可以通过添加带有 `true` 或 `false` 值的 `x-amz-server-side-encryption-bucket-key-enabled` 请求标头在对象级别启用或禁用 S3 存储桶密钥。S3 存储桶密钥通过减少从 Amazon S3 到 Amazon KMS 的请求流量，降低了使用 Amazon Key Management Service（Amazon KMS）（SSE-KMS）进行服务器端加密的成本。有关更多信息，请参阅 使用 Amazon S3 存储桶密钥降低 SSE-KMS 的成本。

当您使用 PUT 或 COPY 操作为对象配置 S3 存储桶密钥时，Amazon S3 仅更新该对象的设置。目标存储桶的 S3 存储桶密钥设置不会更改。如果您在启用了 S3 存储桶密钥的存储桶中提交对于 KMS 加密对象的 PUT 或 COPY 请求，则除非您禁用了请求标头中的密钥，否则您的对象级操作将自动使用 S3 存储桶密钥。如果您未为对象指定 S3 存储桶密钥，则 Amazon S3 会将目标存储桶的 S3 存储桶密钥设置应用于该对象。

先决条件：

在将对象配置为使用 S3 存储桶密钥之前，请查看 启用 S3 存储桶密钥之前需要注意的更改。

主题

- Amazon S3 批量操作
- 使用 REST API
- 使用适用于 Java 的 Amazon SDK（PutObject）
- 使用 Amazon CLI (PutObject)

Amazon S3 批量操作

要加密现有 Amazon S3 对象，可以使用 Amazon S3 批量操作。您为 S3 批量操作提供了要操作的对象列表，而批量操作调用相应的 API 来执行指定的操作。

您可以使用 S3 批量操作复制操作复制现有的未加密对象，并将其作为加密对象写回同一存储桶。单个批量操作作业可对数十亿个对象执行指定操作。有关更多信息，请参阅 使用批量操作批量执行对象操作 和 使用 Amazon S3 批量操作加密对象。

使用 REST API

使用 SSE-KMS 时，您可以使用以下 API 操作为对象启用 S3 存储桶密钥：

- PutObject – 上传对象时，您可以指定 `x-amz-server-side-encryption-bucket-key-enabled` 请求标头以在对象级别启用或禁用 S3 存储桶密钥。
- CopyObject – 当您复制对象并配置 SSE-KMS 时，您可以指定 `x-amz-server-side-encryption-bucket-key-enabled` 请求标头以为对象启用或禁用 S3 存储桶密钥。
- POST 对象 – 当您使用 POST 操作上传对象并配置 SSE-KMS 时，您可以使用 `x-amz-server-side-encryption-bucket-key-enabled` 表单字段为对象启用或禁用 S3 存储桶密钥。
- CreateMultipartUpload – 当您使用 `CreateMultipartUpload` API 操作上传大型对象并配置 SSE-KMS 时，您可以使用 `x-amz-server-side-encryption-bucket-key-enabled` 请求标头为对象启用或禁用 S3 存储桶密钥。

要在对象级别启用 S3 存储桶密钥，请包含 `x-amz-server-side-encryption-bucket-key-enabled` 请求标头。有关 SSE-KMS 和 REST API 的更多信息，请参阅 使用 REST API。

使用适用于 Java 的 Amazon SDK（PutObject）

您可以使用以下示例通过 适用于 Java 的 Amazon SDK 在对象级别配置 S3 存储桶密钥。

Java

```
AmazonS3 s3client = AmazonS3ClientBuilder.standard()
    .withRegion(Regions.DEFAULT_REGION)
    .build();

String bucketName = "amzn-s3-demo-bucket1";
String keyName = "key name for object";
String contents = "file contents";

PutObjectRequest putObjectRequest = new PutObjectRequest(bucketName, keyName,
 contents)
    .withBucketKeyEnabled(true);

s3client.putObject(putObjectRequest);
```

使用 Amazon CLI (PutObject)

您可以使用以下 Amazon CLI 示例作为 PutObject 请求的一部分在对象级别配置 S3 存储桶密钥。

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key object key name --server-side-encryption aws:kms --bucket-key-enabled --body filepath
```

查看 S3 存储桶密钥的设置

您可以使用 Amazon S3 控制台、REST API、Amazon Command Line Interface（Amazon CLI）或 Amazon SDK 在存储桶或对象级别查看 S3 存储桶密钥的设置。

S3 存储桶密钥减少了从 Amazon S3 到 Amazon KMS 的请求流量，从而降低了使用 Amazon Key Management Service（SSE-KMS）进行服务器端加密的成本。有关更多信息，请参阅 使用 Amazon S3 存储桶密钥降低 SSE-KMS 的成本。

要查看存储桶或已从存储桶配置继承了 S3 存储桶密钥设置的对象的 S3 存储桶密钥设置，您需要获得执行 s3:GetEncryptionConfiguration 操作的权限。有关更多信息，请参阅 Amazon Simple Storage Service API 参考中的 GetBucketEncryption。

使用 S3 控制台

在 S3 控制台中，您可以查看存储桶或对象的 S3 存储桶密钥设置。S3 存储桶密钥设置继承自存储桶配置，除非源对象已配置 S3 存储桶密钥。

同一存储桶中的对象和文件夹可以具有不同的 S3 存储桶密钥设置。例如，如果您使用 REST API 上传对象并为该对象启用了 S3 存储桶密钥，则即使在目标存储桶中禁用了 S3 存储桶密钥，该对象仍会在目标存储桶中保留其 S3 存储桶密钥设置。另一个示例是，如果您为现有存储桶启用 S3 存储桶密钥，则存储桶中已存在的对象将不使用 S3 存储桶密钥。但是，新对象已启用 S3 存储桶密钥。

查看存储桶的 S3 存储桶密钥设置

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 在 Buckets（存储桶）列表中，请选择要为其启用 S3 存储桶密钥的存储桶。
4. 选择 Properties (属性)。
5. 在默认加密部分的存储桶密钥下，您可以看到存储桶的 S3 存储桶密钥设置。

如果您看不到 S3 存储桶密钥设置，则可能没有执行 `s3:GetEncryptionConfiguration` 操作的权限。有关更多信息，请参阅 Amazon Simple Storage Service API 参考 中的 GetBucketEncryption。

查看对象的 S3 存储桶密钥设置

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets（存储桶）列表中，请选择要为其启用 S3 存储桶密钥的存储桶。
3. 在 Objects（对象）列表中，请选择对象名称。
4. 在 Details (详细信息) 选项卡上，Server-side encryption settings (服务器端加密设置) 下，请选择 Edit (编辑)。

   在存储桶密钥下，您可以看到对象的 S3 存储桶密钥设置。您无法编辑此设置。

使用 Amazon CLI

返回存储桶级别 S3 存储桶密钥设置

要使用此示例，请将每个 *user input placeholder* 替换为您自己的信息。

```
aws s3api get-bucket-encryption --bucket amzn-s3-demo-bucket1
```

有关更多信息，请参阅《Amazon CLI 命令参考》中的 get-bucket-encryption。

返回对象级别 S3 存储桶密钥设置

要使用此示例，请将每个 *user input placeholder* 替换为您自己的信息。

```
aws s3api head-object --bucket amzn-s3-demo-bucket1 --key my_images.tar.bz2
```

有关更多信息，请参阅《Amazon CLI 命令参考》中的 head-object。

使用 REST API

返回存储桶级别 S3 存储桶密钥设置

要返回存储桶的加密信息，包括 S3 存储桶密钥的设置，请使用 `GetBucketEncryption` 操作。S3 存储桶密钥设置将在 `ServerSideEncryptionConfiguration` 元素中的响应正文

中与 BucketKeyEnabled 设置一起返回。有关更多信息，请参阅 Amazon S3 API 参考中的 GetBucketEncryption。

返回 S3 存储桶密钥的对象级别设置

要返回对象的 S3 存储桶密钥状态，请使用 HeadObject 操作。HeadObject 返回 x-amz-server-side-encryption-bucket-key-enabled 响应标头，以显示是否为对象启用或禁用了 S3 存储桶密钥。有关更多信息，请参阅 Amazon S3 API 参考中的 HeadObject。

如果为对象配置了 S3 存储桶密钥，则以下 API 操作还会返回 x-amz-server-side-encryption-bucket-key-enabled 响应标头：

- PutObject
- PostObject
- CopyObject
- CreateMultipartUpload
- UploadPartCopy
- UploadPart
- CompleteMultipartUpload
- GetObject

## 使用具有 Amazon KMS 密钥的双层服务器端加密（DSSE-KMS）

在将对象上传到 Amazon S3 时，使用具有 Amazon Key Management Service（Amazon KMS）密钥的双层服务器端加密（DSSE-KMS）将会对于对象应用两层加密。DSSE-KMS 可帮助您更轻松地满足合规性标准，这些标准要求您对数据应用多层加密并完全控制您的加密密钥。

将 DSSE-KMS 加密用于 Amazon S3 存储桶时，Amazon KMS 密钥必须位于该存储桶所在的同一区域中。此外，当为对象请求 DSSE-KMS 时，作为对象元数据一部分的 S3 校验和将以加密形式存储。有关校验和的更多信息，请参阅在 Amazon S3 中检查对象完整性。

使用 DSSE-KMS 和 Amazon KMS keys 密钥需要支付额外费用。有关 DSSE-KMS 定价的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的 Amazon KMS key 概念以及 Amazon KMS 定价。

> **Note**
>
> DSSE-KMS 不支持 S3 存储桶密钥。

### 要求使用具有 Amazon KMS keys 的双层服务器端加密（DSSE-KMS）

如果要求对特定 Amazon S3 存储桶中的所有对象进行双层服务器端加密，则可以使用存储桶策略。例如，如果请求不包含用于请求服务器端加密（DSSE-KMS）的 `x-amz-server-side-encryption` 标头，则下面的存储桶策略将拒绝所有人的上传对象（`s3:PutObject`）权限。

```
{
            "Version":"2012-10-17",
            "Id":"PutObjectPolicy",
            "Statement":[{
                  "Sid":"DenyUnEncryptedObjectUploads",
                  "Effect":"Deny",
                  "Principal":"*",
                  "Action":"s3:PutObject",
                  "Resource":"arn:aws:s3:::amzn-s3-demo-bucket/*",
                  "Condition":{
                     "StringNotEquals":{
                        "s3:x-amz-server-side-encryption":"aws:kms:dsse"
                     }
                  }
               }
            ]
         }
```

主题

- 指定具有 Amazon KMS 密钥的双层服务器端加密（DSSE-KMS）

### 指定具有 Amazon KMS 密钥的双层服务器端加密（DSSE-KMS）

当您上传新对象或复制现有对象时，您可以应用加密。

您可以使用 Amazon S3 控制台、Amazon S3 REST API 和 Amazon Command Line Interface（Amazon CLI）指定 DSSE-KMS。有关更多信息，请参阅以下主题。

> **Note**
>
> 您可以在 Amazon S3 中使用多区域 Amazon KMS keys。但是，Amazon S3 目前将多区域密钥视为单区域密钥，且不使用密钥的多区域特征。有关更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的 Using multi-Region keys。

> **Note**
>
> 如果您希望使用其他账户拥有的 KMS 密钥，则您必须有权使用该密钥。有关 KMS 密钥的跨账户权限的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的创建其他账户可以使用的 KMS 密钥。

使用 S3 控制台

本节介绍如何使用 Amazon S3 控制台，将对象的加密类型设置或更改为使用具有 Amazon Key Management Service（Amazon KMS）密钥的双层服务器端加密（DSSE-KMS）。

> **Note**
>
> - 如果对象小于 5 GB，则可以更改对象的加密。如果对象大于 5GB，必须使用 Amazon CLI 或 Amazon SDK 来更改对象的加密。
> - 有关更改对象的加密所需的其它权限的列表，请参阅 the section called “S3 API 操作所需的权限”。有关授予此权限的示例策略，请参阅the section called “基于身份的策略示例”。
> - 如果更改对象的加密，则会创建一个新对象来替换旧对象。如果启用 S3 版本控制，则会创建对象的新版本，而现有对象将变为旧版本。更改属性的角色也会成为新对象（或对象版本）的拥有者。

添加或更改对象的加密

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在导航窗格中，选择存储桶，然后选择通用存储桶选项卡。导航到包含要更改的对象的 Amazon S3 存储桶或文件夹。
3. 选中要更改的对象所对应的复选框。
4. 在操作菜单上，从显示的选项列表中选择编辑服务器端加密。
5. 滚动到服务器端加密部分。
6. 在加密设置下，选择使用默认加密的存储桶设置或覆盖默认加密的存储桶设置。
7. 如果您选择覆盖默认加密的存储桶设置，请配置以下加密设置。

a. 在加密类型下，选择具有 Amazon Key Management Service 密钥的双层服务器端加密（DSSE-KMS）。

b. 在 Amazon KMS 密钥下，执行以下操作以选择您的 KMS 密钥：

- 要从可用的 KMS 密钥列表中进行选择，请选择从您的 Amazon KMS keys 中进行选择，然后从可用密钥的列表中选择您的 KMS 密钥。

  Amazon 托管式密钥（aws/s3）和您的客户自主管理型密钥都显示在此列表中。有关客户自主管理型密钥的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的客户密钥和 Amazon 密钥。

- 要输入 KMS 密钥 ARN，请选择输入 Amazon KMS key ARN，然后在显示的字段中输入您的 KMS 密钥 ARN。

- 要在 Amazon KMS 控制台中创建新的客户自主管理型密钥，请选择创建 KMS 密钥。

  有关创建 Amazon KMS key 的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的创建密钥。

> **Important**
>
> 您只能使用与存储桶所在相同的 Amazon Web Services 区域中可用的 KMS 密钥。Amazon S3 控制台仅列出与存储桶位于同一区域中的前 100 个 KMS 密钥。要使用未列出的 KMS 密钥，您必须输入 KMS 密钥 ARN。如果您希望使用其他账户拥有的 KMS 密钥，则必须首先有权使用该密钥，然后必须输入相应的 KMS 密钥 ARN。Amazon S3 仅支持对称加密 KMS 密钥，不支持非对称 KMS 密钥。有关更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的确定非对称 KMS 密钥。

8. 对于存储桶密钥，选择禁用。DSSE-KMS 不支持 S3 存储桶密钥。
9. 在其它复制设置下，选择是要复制源设置、请勿指定设置还是指定设置。复制源设置是默认选项。如果您只想复制不带源设置属性的对象，请选择请勿指定设置。选择指定设置，来指定存储类、ACL、对象标签、元数据、服务器端加密和其它校验和的设置。
10. 选择保存更改。

> **Note**
>
> 此操作将加密应用于所有指定的对象。加密文件夹时，请等待保存操作完成，然后再将新对象添加到文件夹。

### 使用 REST API

创建对象时（即上传新对象或复制现有对象时），您可以指定使用具有 Amazon KMS keys 的双层服务器端加密（DSSE-KMS）来加密数据。为此，请将 `x-amz-server-side-encryption` 标头添加到请求。将标头的值设置为加密算法 `aws:kms:dsse`。Amazon S3 通过返回响应标头 `x-amz-server-side-encryption` 来确认已使用 DSSE-KMS 加密来存储对象。

如果您指定值为 `aws:kms:dsse` 的 `x-amz-server-side-encryption` 标头，则还可以使用以下请求标头：

- `x-amz-server-side-encryption-aws-kms-key-id: SSEKMSKeyId`
- `x-amz-server-side-encryption-context: SSEKMSEncryptionContext`

### 主题

- 支持 DSSE-KMS 的 Amazon S3 REST API 操作
- 加密上下文（x-amz-server-side-encryption-context）
- Amazon KMS 密钥 ID（x-amz-server-side-encryption-aws-kms-key-id）

### 支持 DSSE-KMS 的 Amazon S3 REST API 操作

以下 REST API 操作接受 `x-amz-server-side-encryption`、`x-amz-server-side-encryption-aws-kms-key-id` 和 `x-amz-server-side-encryption-context` 请求标头。

- PutObject – 使用 PUT API 操作上传数据时，您可以指定这些请求标头。
- CopyObject – 复制对象时，您同时具有源对象和目标对象。如果使用 `CopyObject` 操作传递 DSSE-KMS 标头，它们仅应用于目标对象。复制现有对象时，不论源对象是否已经加密，都不会加密目标对象，除非您显式请求服务器端加密。
- POST Object – 使用 `POST` 操作上传对象时，可在表单字段（而不是在请求标头）中提供相同的信息。
- CreateMultipartUpload – 使用分段上传来上传大型对象时，可以在 `CreateMultipartUpload` 请求中指定这些标头。

使用服务器端加密存储对象时，以下 REST API 操作的响应标头将返回 `x-amz-server-side-encryption` 标头。

- PutObject
- CopyObject
- POST 对象
- CreateMultipartUpload
- UploadPart
- UploadPartCopy
- CompleteMultipartUpload
- GetObject
- HeadObject

> **Important**
>
> - 如果您不让使用安全套接字层（SSL）、传输层安全性协议（TLS）或签名版本 4 发出针对受 Amazon KMS 保护的对象的所有 GET 和 PUT 请求，则这些请求都将失败。
> - 如果对象使用 DSSE-KMS，则不应对 GET 请求和 HEAD 请求发送加密请求标头，否则您将得到 HTTP 400（错误请求）错误。

加密上下文（**`x-amz-server-side-encryption-context`**）

如果您指定 `x-amz-server-side-encryption:aws:kms:dsse`，Amazon S3 API 将支持带有 `x-amz-server-side-encryption-context` 标头的加密上下文。加密上下文是一组键值对，其中包含有关数据的其他上下文信息。

Amazon S3 自动使用对象的 Amazon 资源名称（ARN）作为加密上下文对；例如 `arn:aws:s3:::`*`object_ARN`*。

您可以选择使用 `x-amz-server-side-encryption-context` 标头提供其他的加密上下文对。但是，由于加密上下文未加密，请确保它不包含敏感信息。Amazon S3 将此额外的密钥对与默认加密上下文一起存储。

有关 Amazon S3 中加密上下文的信息，请参阅 加密上下文。有关加密上下文的一般信息，请参阅 Amazon Key Management Service 开发人员指南中的 Amazon Key Management Service 概念 - 加密上下文。

Amazon KMS 密钥 ID（**`x-amz-server-side-encryption-aws-kms-key-id`**）

您可以使用 `x-amz-server-side-encryption-aws-kms-key-id` 标头指定用于保护数据的客户自主管理型密钥的 ID。如果您指定 `x-amz-server-side-encryption:aws:kms:dsse` 标头但未提供 `x-amz-server-side-encryption-aws-kms-key-id` 标头，Amazon S3 将使用 Amazon 托管式密钥（`aws/s3`）来保护数据。如果要使用客户托管密钥，则必须提供客户托管密钥的 `x-amz-server-side-encryption-aws-kms-key-id` 标头。

> **Important**
>
> 在 Amazon S3 中使用 Amazon KMS key 进行服务器端加密时，您必须选择对称加密 KMS 密钥。Amazon S3 仅支持对称加密 KMS 密钥。有关这些密钥的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的对称加密 KMS 密钥。

使用 Amazon CLI

当您上传新对象或复制现有对象时，可以指定使用 DSSE-KMS 来加密数据。为此，请将 `--server-side-encryption aws:kms:dsse` 参数添加到请求。使用 `--ssekms-key-id` *`example-key-id`* 参数添加您创建的客户自主管理型 Amazon KMS 密钥。如果您指定 `--server-side-encryption aws:kms:dsse`，但未提供 Amazon KMS 密钥 ID，则 Amazon S3 将使用 Amazon 托管式密钥（`aws/s3`）。

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key example-object-key --server-
side-encryption aws:kms:dsse --ssekms-key-id example-key-id --body filepath
```

您可以通过将未加密的对象复制回原位来加密该对象以使用 DSSE-KMS。

```
aws s3api copy-object --bucket amzn-s3-demo-bucket --key example-object-key --
body filepath --bucket amzn-s3-demo-bucket --key example-object-key --sse aws:kms:dsse
 --sse-kms-key-id example-key-id --body filepath
```

## 使用具有客户提供的密钥的服务器端加密（SSE-C）

服务器端加密是为了保护静态数据。服务器端加密仅加密对象数据而非加密对象元数据。使用具有客户提供的密钥的服务器端加密（SSE-C），您可以存储使用自己的加密密钥加密的数据。使用您作为请

求的一部分提供的加密密钥，Amazon S3 在其写入磁盘时管理数据加密，并在您访问对象时管理数据解密。因此，您不需要维护任何代码来执行数据加密和解密。您只需管理您提供的加密密钥。

在您上传对象时，Amazon S3 将使用您提供的加密密钥对您的数据应用 AES-256 加密。然后，Amazon S3 从内存中删除此加密密钥。在检索对象时，必须提供相同的加密密钥作为您请求的一部分。Amazon S3 在将对象数据返回给您之前，会首先验证您提供的加密密钥是否匹配，然后再解密对象。

使用 SSE-C 没有额外费用。但是，配置和使用 SSE-C 的请求会产生标准的 Amazon S3 请求费用。有关定价的信息，请参阅 Amazon S3 定价。

> **Note**
>
> Amazon S3 不存储您提供的加密密钥，而是存储加密密钥的添加了随机数据的 HMAC 散列消息认证码（HMAC）值，以验证将来的请求。无法使用添加了随机数据的 HMAC 值来推导出加密密钥的值或解密加密对象的内容。这意味着，如果您丢失加密密钥，则会失去该对象。

S3 复制支持使用 SSE-C 加密的对象。有关复制加密对象的更多信息，请参阅the section called “复制加密对象”。

有关 SSE-C 的更多信息，请参阅以下主题。

主题

- SSE-C 概览
- 要求和限制 SSE-C
- 预签名 URL 和 SSE-C
- 指定使用客户提供的密钥的服务器端加密 (SSE-C)。

SSE-C 概览

本部分提供 SSE-C 的概述。使用 SSE-C 时，请记住以下注意事项。

- 您必须使用 HTTPS。

> **Important**
>
> 在使用 SSE-C 时，Amazon S3 会拒绝通过 HTTP 发出的所有请求。出于安全原因，我们建议您考虑您错误地通过 HTTP 发送的任何密钥都会遭泄露。丢弃该密钥，并根据需要轮换密钥。

- 响应中的实体标签（ETag）不是对象数据的 MD5 哈希。
- 您管理哪个加密密钥用于加密哪个对象的映射。Amazon S3 不存储加密密钥。您负责跟踪为哪个对象提供了哪个加密密钥。
  - 如果您的存储桶启用了版本控制，则您使用此特征上传的每个对象版本可能都具有自己的加密密钥。您负责跟踪哪个加密密钥用于哪个对象版本。
  - 因为您在客户端管理加密密钥，所以也要在客户端管理所有额外的保护措施，例如密钥轮换。

> **Warning**
>
> 如果您丢失加密密钥，则在没有加密密钥的情况下对于对象的任何 GET 请求都会失败，并且您将丢失该对象。

### 要求和限制 SSE-C

如果要求对特定 Amazon S3 存储桶中的所有对象执行 SSE-C，请使用存储桶策略。

例如，如果请求不包括用于请求 SSE-C 的 `x-amz-server-side-encryption-customer-algorithm` 标头，以下存储桶策略将拒绝针对所有此类请求的上传对象（`s3:PutObject`）权限。

```
{
    "Version": "2012-10-17",
    "Id": "PutObjectPolicy",
    "Statement": [
        {
            "Sid": "RequireSSECObjectUploads",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "Null": {
                    "s3:x-amz-server-side-encryption-customer-algorithm": "true"
```

```
                }
            }
        }
    ]
}
```

也可以使用策略，以限制对特定 Amazon S3 存储桶中的所有对象进行服务器端加密。例如，如果请求包含用于请求 SSE-C 的 `x-amz-server-side-encryption-customer-algorithm` 标头，则下面的存储桶策略将对所有人拒绝上传对象（`s3:PutObject`）权限。

```
{
    "Version": "2012-10-17",
    "Id": "PutObjectPolicy",
    "Statement": [
        {
            "Sid": "RestrictSSECObjectUploads",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "Null": {
                    "s3:x-amz-server-side-encryption-customer-algorithm": "false"
                }
            }
        }
    ]
}
```

> **Important**
>
> 如果您使用存储桶策略在 `s3:PutObject` 上请求 SSE-C，则必须在所有分段上传请求中（CreateMultipartUpload、UploadPart 和 CompleteMultipartUpload）包括 `x-amz-server-side-encryption-customer-algorithm` 标头。

### 预签名 URL 和 SSE-C

您可以生成可用于上传新对象、检索现有对象或检索对象元数据等操作的预签名 URL。预签名 URL 支持 SSE-C，如下所示：

- 在创建预签名 URL 时，您必须在签名计算中使用 `x-amz-server-side-encryption-customer-algorithm` 标头指定算法。
- 在使用预签名 URL 上传新对象、检索现有对象或仅检索对象元数据时，您必须在您的客户端应用程序的请求中提供所有加密标头。

> **Note**
>
> 对于非 SSE-C 对象，您可以生成预签名 URL，并将该 URL 直接复制到浏览器中以访问数据。
> 但是，不能对 SSE-C 对象执行此操作，因为除了预签名 URL 外，还必须包含 SSE-C 对象特定的 HTTP 标头。因此，您只能以编程方式将预签名 URL 用于 SSE-C 对象。

有关预签名 URL 的更多信息，请参阅the section called “使用预签名 URL 下载和上传对象”。

指定使用客户提供的密钥的服务器端加密 (SSE-C)。

在使用 REST API 创建对象时，您可以使用客户提供的密钥（SSE-C）指定服务器端加密。使用 SSE-C 时，必须使用以下请求标头提供加密密钥信息。

| 名称 | 描述 |
| --- | --- |
| `x-amz-server-side-encryption-customer-algorithm` | 使用此标头来指定加密算法。标头值必须为 AES256。 |
| `x-amz-server-side-encryption-customer-key` | 使用此标头来提供 256 位的 base64 编码的加密密钥以供 Amazon S3 用于加密或解密您的数据。 |
| `x-amz-server-side-encryption-customer-key-MD5` | 使用此标头根据 RFC 1321 提供加密密钥的 base64 编码的 128 位 MD5 摘要。Amazon S3 使用此标头进行消息完整性检查以确保加密密钥的传输无误。 |

您可以使用 Amazon SDK 包装库将这些标头添加到您的请求中。如果需要，您可以直接在应用程序中调用 Amazon S3 REST API。

> **Note**
>
> 您不能使用 Amazon S3 控制台上传对象并请求 SSE-C。也不能使用控制台来更新使用 SSE-C 存储的现有对象（例如，更改存储类或添加元数据）。

使用 REST API

支持 SSE-C 的 Amazon S3 REST API

以下 Amazon S3 API 支持使用客户提供的加密密钥进行服务器端加密 (SSE-C)。

- GET 操作 – 在使用 GET API 检索对象（请参阅 GET Object）时，您可以指定请求标头。
- HEAD 操作 – 要使用 HEAD API 检索对象元数据（请参阅 HEAD Object），可以指定这些请求标头。
- PUT 操作 – 使用 PUT Object API 上传数据（请参阅 PUT Object）时，可以指定这些请求标头。
- 分段上传 – 在使用分段上传 API 上传大对象时，可以指定这些标头。您可以在以下请求中指定这些标头：启动请求（请参阅启动分段上传）和每个后续分段上传请求（请参阅上传分段或上传分段 - 复制）。对于每个分段上传请求，加密信息必须与您在启动分段上传请求中提供的信息相同。
- POST 操作 – 使用 POST 操作上传对象（请参阅 POST 对象）时，可在表单字段而不是请求标头中提供相同的信息。
- 复制操作 – 复制对象（请参阅 PUT Object - 复制）时，您同时具有源对象和目标对象：
  - 如果您希望使用具有 Amazon 托管式密钥的服务器端加密对目标对象加密，则必须提供 `x-amz-server-side-encryption` 请求标头。
  - 如果您希望使用 SSE-C 对目标对象加密，则必须使用上表中描述的三个标头提供加密信息。
  - 如果源对象是使用 SSE-C 加密的，则您必须使用以下标头提供加密密钥信息，以便 Amazon S3 可以解密对象以进行复制。

| 名称 | 描述 |
| --- | --- |
| `x-amz-copy-source-server-side-encryption-customer-algorithm` | 包括此标头以指定 Amazon S3 用于解密源对象的算法。此值必须是 AES256。 |

| 名称 | 描述 |
| --- | --- |
| `x-amz-copy-source-server-side-encryption-customer-key` | 包括此标头以提供 base64 编码的加密密钥，供 Amazon S3 用于解密源对象。此加密密钥必须是您在创建源对象时为 Amazon S3 提供的加密密钥。否则，Amazon S3 无法解密对象。 |
| `x-amz-copy-source-server-side-encryption-customer-key-MD5` | 包括此标头以根据 RFC 1321 提供加密密钥的 base64 编码的 128 位 MD5 摘要。 |

使用 Amazon SDK 为 PUT、GET、Head 和 Copy 操作指定 SSE-C

以下示例演示如何为对象请求使用客户提供的密钥的服务器端加密 (SSE-C)。这些示例执行以下操作。每个操作均演示了如何在请求中指定 SSE-C 相关标头：

- 放置对象 – 上传对象，并请求使用客户提供的加密密钥的服务器端加密。
- 获取对象 – 下载上一步中上传的对象。在请求中，应提供上传对象时提供的同一加密信息。Amazon S3 需要此信息来解密对象，以便将对象返回给您。
- 获取对象元数据 – 检索对象的元数据。提供创建对象时使用的同一加密信息。
- 复制对象 – 复制之前上传的对象的副本。因为源对象是使用 SSE-C 存储的，因此必须在复制请求中提供其加密信息。默认情况下，仅当您显式请求加密时，Amazon S3 才会为对象的副本加密。此示例指示 Amazon S3 存储对象的加密副本。

Java

> **Note**
>
> 本示例显示如何在单个操作中上传对象。当使用分段上传 API 上传大型对象时，应按照此示例中所示的方式提供加密信息。有关使用 适用于 Java 的 Amazon SDK 的分段上传的示例，请参阅 使用分段上传操作上传对象。

要添加必需的加密信息，请在请求中包含 SSECustomerKey。有关该 SSECustomerKey 课程的更多信息，请参阅 REST API 部分。

有关 SSE-C 的信息，请参阅 使用具有客户提供的密钥的服务器端加密（SSE-C）。有关创建和测试有效示例的说明，请参阅《适用于 Java 的 Amazon SDK 开发人员指南》中的入门。

Example

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import javax.crypto.KeyGenerator;
import java.io.BufferedReader;
import java.io.File;
import java.io.IOException;
import java.io.InputStreamReader;
import java.security.NoSuchAlgorithmException;
import java.security.SecureRandom;

public class ServerSideEncryptionUsingClientSideEncryptionKey {
    private static SSECustomerKey SSE_KEY;
    private static AmazonS3 S3_CLIENT;
    private static KeyGenerator KEY_GENERATOR;

    public static void main(String[] args) throws IOException,
 NoSuchAlgorithmException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String keyName = "*** Key name ***";
        String uploadFileName = "*** File path ***";
        String targetKeyName = "*** Target key name ***";

        // Create an encryption key.
        KEY_GENERATOR = KeyGenerator.getInstance("AES");
        KEY_GENERATOR.init(256, new SecureRandom());
        SSE_KEY = new SSECustomerKey(KEY_GENERATOR.generateKey());
```

```
        try {
            S3_CLIENT = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Upload an object.
            uploadObject(bucketName, keyName, new File(uploadFileName));

            // Download the object.
            downloadObject(bucketName, keyName);

            // Verify that the object is properly encrypted by attempting to
retrieve it
            // using the encryption key.
            retrieveObjectMetadata(bucketName, keyName);

            // Copy the object into a new object that also uses SSE-C.
            copyObject(bucketName, keyName, targetKeyName);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }

    private static void uploadObject(String bucketName, String keyName, File file) {
        PutObjectRequest putRequest = new PutObjectRequest(bucketName, keyName,
file).withSSECustomerKey(SSE_KEY);
        S3_CLIENT.putObject(putRequest);
        System.out.println("Object uploaded");
    }

    private static void downloadObject(String bucketName, String keyName) throws
IOException {
        GetObjectRequest getObjectRequest = new GetObjectRequest(bucketName,
keyName).withSSECustomerKey(SSE_KEY);
        S3Object object = S3_CLIENT.getObject(getObjectRequest);

        System.out.println("Object content: ");
```

```
        displayTextInputStream(object.getObjectContent());
    }

    private static void retrieveObjectMetadata(String bucketName, String keyName) {
        GetObjectMetadataRequest getMetadataRequest = new
 GetObjectMetadataRequest(bucketName, keyName)
                .withSSECustomerKey(SSE_KEY);
        ObjectMetadata objectMetadata =
 S3_CLIENT.getObjectMetadata(getMetadataRequest);
        System.out.println("Metadata retrieved. Object size: " +
 objectMetadata.getContentLength());
    }

    private static void copyObject(String bucketName, String keyName, String
 targetKeyName)
            throws NoSuchAlgorithmException {
        // Create a new encryption key for target so that the target is saved using
        // SSE-C.
        SSECustomerKey newSSEKey = new SSECustomerKey(KEY_GENERATOR.generateKey());

        CopyObjectRequest copyRequest = new CopyObjectRequest(bucketName, keyName,
 bucketName, targetKeyName)
                .withSourceSSECustomerKey(SSE_KEY)
                .withDestinationSSECustomerKey(newSSEKey);

        S3_CLIENT.copyObject(copyRequest);
        System.out.println("Object copied");
    }

    private static void displayTextInputStream(S3ObjectInputStream input) throws
 IOException {
        // Read one line at a time from the input stream and display each line.
        BufferedReader reader = new BufferedReader(new InputStreamReader(input));
        String line;
        while ((line = reader.readLine()) != null) {
            System.out.println(line);
        }
        System.out.println();
    }
}
```

.NET

> **Note**
>
> 有关使用分段上传 API 上传大型对象的示例，请参阅 使用分段上传操作上传对象 和 使用 Amazon SDK（低级别 API）。

有关 SSE-C 的信息，请参阅 使用具有客户提供的密钥的服务器端加密（SSE-C）。有关设置和运行代码示例的信息，请参阅《适用于 .NET 的 Amazon SDK 开发人员指南》中的适用于 .NET 的 Amazon SDK 入门。

Example

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.IO;
using System.Security.Cryptography;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class SSEClientEncryptionKeyObjectOperationsTest
    {
        private const string bucketName = "*** bucket name ***";
        private const string keyName = "*** key name for new object created ***";
        private const string copyTargetKeyName = "*** key name for object copy ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;

        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            ObjectOpsUsingClientEncryptionKeyAsync().Wait();
        }
        private static async Task ObjectOpsUsingClientEncryptionKeyAsync()
        {
            try
```

```
            {
                // Create an encryption key.
                Aes aesEncryption = Aes.Create();
                aesEncryption.KeySize = 256;
                aesEncryption.GenerateKey();
                string base64Key = Convert.ToBase64String(aesEncryption.Key);

                // 1. Upload the object.
                PutObjectRequest putObjectRequest = await
UploadObjectAsync(base64Key);
                // 2. Download the object and verify that its contents matches what
you uploaded.
                await DownloadObjectAsync(base64Key, putObjectRequest);
                // 3. Get object metadata and verify that the object uses AES-256
encryption.
                await GetObjectMetadataAsync(base64Key);
                // 4. Copy both the source and target objects using server-side
encryption with
                //    a customer-provided encryption key.
                await CopyObjectAsync(aesEncryption, base64Key);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered ***. Message:'{0}' when writing
an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
        }

        private static async Task<PutObjectRequest> UploadObjectAsync(string
base64Key)
        {
            PutObjectRequest putObjectRequest = new PutObjectRequest
            {
                BucketName = bucketName,
                Key = keyName,
                ContentBody = "sample text",
                ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                ServerSideEncryptionCustomerProvidedKey = base64Key
```

```
            };
            PutObjectResponse putObjectResponse = await
client.PutObjectAsync(putObjectRequest);
            return putObjectRequest;
        }
        private static async Task DownloadObjectAsync(string base64Key,
PutObjectRequest putObjectRequest)
        {
            GetObjectRequest getObjectRequest = new GetObjectRequest
            {
                BucketName = bucketName,
                Key = keyName,
                // Provide encryption information for the object stored in Amazon
S3.
                ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                ServerSideEncryptionCustomerProvidedKey = base64Key
            };

            using (GetObjectResponse getResponse = await
client.GetObjectAsync(getObjectRequest))
            using (StreamReader reader = new
StreamReader(getResponse.ResponseStream))
            {
                string content = reader.ReadToEnd();
                if (String.Compare(putObjectRequest.ContentBody, content) == 0)
                    Console.WriteLine("Object content is same as we uploaded");
                else
                    Console.WriteLine("Error...Object content is not same.");

                if (getResponse.ServerSideEncryptionCustomerMethod ==
ServerSideEncryptionCustomerMethod.AES256)
                    Console.WriteLine("Object encryption method is AES256, same as
we set");
                else
                    Console.WriteLine("Error...Object encryption method is not the
same as AES256 we set");

                // Assert.AreEqual(putObjectRequest.ContentBody, content);
                // Assert.AreEqual(ServerSideEncryptionCustomerMethod.AES256,
getResponse.ServerSideEncryptionCustomerMethod);
            }
        }
        private static async Task GetObjectMetadataAsync(string base64Key)
```

```
        {
            GetObjectMetadataRequest getObjectMetadataRequest = new
GetObjectMetadataRequest
            {
                BucketName = bucketName,
                Key = keyName,

                // The object stored in Amazon S3 is encrypted, so provide the
necessary encryption information.
                ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                ServerSideEncryptionCustomerProvidedKey = base64Key
            };

            GetObjectMetadataResponse getObjectMetadataResponse = await
client.GetObjectMetadataAsync(getObjectMetadataRequest);
            Console.WriteLine("The object metadata show encryption method used is:
{0}", getObjectMetadataResponse.ServerSideEncryptionCustomerMethod);
            // Assert.AreEqual(ServerSideEncryptionCustomerMethod.AES256,
getObjectMetadataResponse.ServerSideEncryptionCustomerMethod);
        }
        private static async Task CopyObjectAsync(Aes aesEncryption, string
base64Key)
        {
            aesEncryption.GenerateKey();
            string copyBase64Key = Convert.ToBase64String(aesEncryption.Key);

            CopyObjectRequest copyRequest = new CopyObjectRequest
            {
                SourceBucket = bucketName,
                SourceKey = keyName,
                DestinationBucket = bucketName,
                DestinationKey = copyTargetKeyName,
                // Information about the source object's encryption.
                CopySourceServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                CopySourceServerSideEncryptionCustomerProvidedKey = base64Key,
                // Information about the target object's encryption.
                ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                ServerSideEncryptionCustomerProvidedKey = copyBase64Key
            };
            await client.CopyObjectAsync(copyRequest);
        }
```

```
    }
}
```

### 使用 Amazon SDK 为分段上传指定 SSE-C

上一部分中的示例显示了如何在 PUT、GET、Head 和 Copy 操作中请求使用客户提供的密钥的服务器端加密 (SSE-C)。本节介绍支持 SSE-C 的其他 Amazon S3 API。

Java

要上传大型对象，您可以使用分段上传 API（请参阅在 Amazon S3 中使用分段上传来上传和复制对象）。可以使用高级或低级 API 上传大型对象。这些 API 支持在请求中使用与加密相关的标头。

- 当使用高级别 `TransferManager` API 时，应在 `PutObjectRequest` 中提供特定于加密的标头 (请参阅 使用分段上传操作上传对象)。
- 当使用低级别 API 时，应提供 `InitiateMultipartUploadRequest` 中的加密相关信息，后跟每个 `UploadPartRequest` 中的相同加密信息。不需要在 `CompleteMultipartUploadRequest` 中提供任何特定于加密的标头。有关示例，请参阅 使用 Amazon SDK（低级别 API）。

以下示例使用 `TransferManager` 创建对象并显示如何提供 SSE-C 相关信息。本示例执行以下操作：

- 使用 `TransferManager.upload()` 方法创建对象。在 `PutObjectRequest` 实例中，应提供要请求的加密密钥信息。Amazon S3 将使用客户提供的密钥对于对象进行加密。
- 通过调用 `TransferManager.copy()` 方法创建对象的副本。该示例指示 Amazon S3 使用新的 `SSECustomerKey` 对对象副本进行加密。由于源对象使用 SSE-C 加密，因此 `CopyObjectRequest` 还提供了源对象的加密密钥，以便 Amazon S3 可以在复制对象之前解密对象。

Example

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
```

```
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.CopyObjectRequest;
import com.amazonaws.services.s3.model.PutObjectRequest;
import com.amazonaws.services.s3.model.SSECustomerKey;
import com.amazonaws.services.s3.transfer.Copy;
import com.amazonaws.services.s3.transfer.TransferManager;
import com.amazonaws.services.s3.transfer.TransferManagerBuilder;
import com.amazonaws.services.s3.transfer.Upload;

import javax.crypto.KeyGenerator;
import java.io.File;
import java.security.SecureRandom;

public class ServerSideEncryptionCopyObjectUsingHLwithSSEC {

    public static void main(String[] args) throws Exception {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String fileToUpload = "*** File path ***";
        String keyName = "*** New object key name ***";
        String targetKeyName = "*** Key name for object copy ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withRegion(clientRegion)
                    .withCredentials(new ProfileCredentialsProvider())
                    .build();
            TransferManager tm = TransferManagerBuilder.standard()
                    .withS3Client(s3Client)
                    .build();

            // Create an object from a file.
            PutObjectRequest putObjectRequest = new PutObjectRequest(bucketName,
 keyName, new File(fileToUpload));

            // Create an encryption key.
            KeyGenerator keyGenerator = KeyGenerator.getInstance("AES");
            keyGenerator.init(256, new SecureRandom());
            SSECustomerKey sseCustomerEncryptionKey = new
 SSECustomerKey(keyGenerator.generateKey());

            // Upload the object. TransferManager uploads asynchronously, so this
 call
            // returns immediately.
```

```
            putObjectRequest.setSSECustomerKey(sseCustomerEncryptionKey);
            Upload upload = tm.upload(putObjectRequest);

            // Optionally, wait for the upload to finish before continuing.
            upload.waitForCompletion();
            System.out.println("Object created.");

            // Copy the object and store the copy using SSE-C with a new key.
            CopyObjectRequest copyObjectRequest = new CopyObjectRequest(bucketName,
 keyName, bucketName, targetKeyName);
            SSECustomerKey sseTargetObjectEncryptionKey = new
 SSECustomerKey(keyGenerator.generateKey());
            copyObjectRequest.setSourceSSECustomerKey(sseCustomerEncryptionKey);

 copyObjectRequest.setDestinationSSECustomerKey(sseTargetObjectEncryptionKey);

            // Copy the object. TransferManager copies asynchronously, so this call
 returns
            // immediately.
            Copy copy = tm.copy(copyObjectRequest);

            // Optionally, wait for the upload to finish before continuing.
            copy.waitForCompletion();
            System.out.println("Copy complete.");
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

要上传大型对象，您可以使用分段上传 API（请参阅[在 Amazon S3 中使用分段上传来上传和复制对象](#)）。Amazon适用于 .NET 的 SDK 提供了高级或低级 API 来上传大型对象。这些 API 支持在请求中使用与加密相关的标头。

- 当使用高级 Transfer-Utility API 时，可以在 TransferUtilityUploadRequest 中提供特定于加密的标头，如下所示。有关代码示例，请参阅 使用分段上传操作上传对象。

```
TransferUtilityUploadRequest request = new TransferUtilityUploadRequest()
{
    FilePath = filePath,
    BucketName = existingBucketName,
    Key = keyName,
    // Provide encryption information.
    ServerSideEncryptionCustomerMethod =
 ServerSideEncryptionCustomerMethod.AES256,
    ServerSideEncryptionCustomerProvidedKey = base64Key,
};
```

- 当使用低级 API 时，可以在启动分段上传请求中提供加密相关的信息，并在后续的分段上传请求中提供相同加密信息。不需要在完成的分段上传请求中提供任何特定于加密的标头。有关示例，请参阅 使用 Amazon SDK（低级别 API）。

  下面是一个低级分段上传示例，该示例复制一个现有大型对象。在本示例中，要复制的对象使用 SSE-C 存储在 Amazon S3 中，并且您希望使用 SSE-C 保存目标对象。在本例中，您可以执行以下操作：

  - 通过提供加密密钥和相关信息启动分段上传请求。
  - 在 CopyPartRequest 中提供源和目标对象加密密钥及相关信息。
  - 通过检索对象元数据获取要复制的源对象的大小。
  - 以 5 MB 大小的分段上传对象。

  Example

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.IO;
using System.Security.Cryptography;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class SSECLowLevelMPUcopyObjectTest
```

```
   {
        private const string existingBucketName = "*** bucket name ***";
        private const string sourceKeyName      = "*** source object key name
***";
        private const string targetKeyName      = "*** key name for the target
object ***";
        private const string filePath           = @"*** file path ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;
        static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            CopyObjClientEncryptionKeyAsync().Wait();
        }

        private static async Task CopyObjClientEncryptionKeyAsync()
        {
            Aes aesEncryption = Aes.Create();
            aesEncryption.KeySize = 256;
            aesEncryption.GenerateKey();
            string base64Key = Convert.ToBase64String(aesEncryption.Key);

            await CreateSampleObjUsingClientEncryptionKeyAsync(base64Key,
s3Client);

            await CopyObjectAsync(s3Client, base64Key);
        }
        private static async Task CopyObjectAsync(IAmazonS3 s3Client, string
base64Key)
        {
            List<CopyPartResponse> uploadResponses = new List<CopyPartResponse>();

            // 1. Initialize.
            InitiateMultipartUploadRequest initiateRequest = new
InitiateMultipartUploadRequest
            {
                BucketName = existingBucketName,
                Key = targetKeyName,
                ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                ServerSideEncryptionCustomerProvidedKey = base64Key,
            };
```

```
            InitiateMultipartUploadResponse initResponse =
                await s3Client.InitiateMultipartUploadAsync(initiateRequest);

            // 2. Upload Parts.
            long partSize = 5 * (long)Math.Pow(2, 20); // 5 MB
            long firstByte = 0;
            long lastByte = partSize;

            try
            {
                // First find source object size. Because object is stored
encrypted with
                // customer provided key you need to provide encryption
information in your request.
                GetObjectMetadataRequest getObjectMetadataRequest = new
GetObjectMetadataRequest()
                {
                    BucketName = existingBucketName,
                    Key = sourceKeyName,
                    ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                    ServerSideEncryptionCustomerProvidedKey = base64Key // " *
**source object encryption key ***"
                };

                GetObjectMetadataResponse getObjectMetadataResponse = await
s3Client.GetObjectMetadataAsync(getObjectMetadataRequest);

                long filePosition = 0;
                for (int i = 1; filePosition <
getObjectMetadataResponse.ContentLength; i++)
                {
                    CopyPartRequest copyPartRequest = new CopyPartRequest
                    {
                        UploadId = initResponse.UploadId,
                        // Source.
                        SourceBucket = existingBucketName,
                        SourceKey = sourceKeyName,
                        // Source object is stored using SSE-C. Provide encryption
information.
                        CopySourceServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
```

```
                        CopySourceServerSideEncryptionCustomerProvidedKey =
base64Key, //"***source object encryption key ***",
                        FirstByte = firstByte,
                        // If the last part is smaller then our normal part size
then use the remaining size.
                        LastByte = lastByte >
getObjectMetadataResponse.ContentLength ?
                            getObjectMetadataResponse.ContentLength - 1 :
lastByte,

                        // Target.
                        DestinationBucket = existingBucketName,
                        DestinationKey = targetKeyName,
                        PartNumber = i,
                        // Encryption information for the target object.
                        ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                        ServerSideEncryptionCustomerProvidedKey = base64Key
                    };
                    uploadResponses.Add(await
s3Client.CopyPartAsync(copyPartRequest));
                    filePosition += partSize;
                    firstByte += partSize;
                    lastByte += partSize;
                }

                // Step 3: complete.
                CompleteMultipartUploadRequest completeRequest = new
CompleteMultipartUploadRequest
                {
                    BucketName = existingBucketName,
                    Key = targetKeyName,
                    UploadId = initResponse.UploadId,
                };
                completeRequest.AddPartETags(uploadResponses);

                CompleteMultipartUploadResponse completeUploadResponse =
                    await s3Client.CompleteMultipartUploadAsync(completeRequest);
            }
            catch (Exception exception)
            {
                Console.WriteLine("Exception occurred: {0}", exception.Message);
                AbortMultipartUploadRequest abortMPURequest = new
AbortMultipartUploadRequest
```

```
                {
                    BucketName = existingBucketName,
                    Key = targetKeyName,
                    UploadId = initResponse.UploadId
                };
                s3Client.AbortMultipartUpload(abortMPURequest);
            }
        }
        private static async Task
CreateSampleObjUsingClientEncryptionKeyAsync(string base64Key, IAmazonS3
s3Client)
        {
            // List to store upload part responses.
            List<UploadPartResponse> uploadResponses = new
List<UploadPartResponse>();

            // 1. Initialize.
            InitiateMultipartUploadRequest initiateRequest = new
InitiateMultipartUploadRequest
            {
                BucketName = existingBucketName,
                Key = sourceKeyName,
                ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                ServerSideEncryptionCustomerProvidedKey = base64Key
            };

            InitiateMultipartUploadResponse initResponse =
               await s3Client.InitiateMultipartUploadAsync(initiateRequest);

            // 2. Upload Parts.
            long contentLength = new FileInfo(filePath).Length;
            long partSize = 5 * (long)Math.Pow(2, 20); // 5 MB

            try
            {
                long filePosition = 0;
                for (int i = 1; filePosition < contentLength; i++)
                {
                    UploadPartRequest uploadRequest = new UploadPartRequest
                    {
                        BucketName = existingBucketName,
                        Key = sourceKeyName,
                        UploadId = initResponse.UploadId,
```

```
                        PartNumber = i,
                        PartSize = partSize,
                        FilePosition = filePosition,
                        FilePath = filePath,
                        ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                        ServerSideEncryptionCustomerProvidedKey = base64Key
                    };

                    // Upload part and add response to our list.
                    uploadResponses.Add(await
s3Client.UploadPartAsync(uploadRequest));

                    filePosition += partSize;
                }

                // Step 3: complete.
                CompleteMultipartUploadRequest completeRequest = new
CompleteMultipartUploadRequest
                {
                    BucketName = existingBucketName,
                    Key = sourceKeyName,
                    UploadId = initResponse.UploadId,
                    //PartETags = new List<PartETag>(uploadResponses)

                };
                completeRequest.AddPartETags(uploadResponses);

                CompleteMultipartUploadResponse completeUploadResponse =
                    await s3Client.CompleteMultipartUploadAsync(completeRequest);

            }
            catch (Exception exception)
            {
                Console.WriteLine("Exception occurred: {0}", exception.Message);
                AbortMultipartUploadRequest abortMPURequest = new
AbortMultipartUploadRequest
                {
                    BucketName = existingBucketName,
                    Key = sourceKeyName,
                    UploadId = initResponse.UploadId
                };
                await s3Client.AbortMultipartUploadAsync(abortMPURequest);
            }
```

```
        }
    }
}
```

## 使用客户端加密保护数据

客户端加密是在本地加密数据，以帮助确保数据在传输中和静态时的安全性的行为。要在将对象发送到 Amazon S3 之前对其进行加密，请使用 Amazon S3 加密客户端。当您的对象以这种方式加密时，您的对象不会泄露给任何第三方，包括 Amazon。Amazon S3 接收已经加密的对象；Amazon S3 在加密或解密对象方面不起作用。您可以使用 Amazon S3 加密客户端和服务器端加密来加密您的数据。当您向 Amazon S3 发送加密对象时，Amazon S3 无法将这些对象识别为已加密，它只会检测典型的对象。

Amazon S3 加密客户端充当您与 Amazon S3 之间的中介。在您实例化 Amazon S3 加密客户端后，您的对象将作为 Amazon S3 `PutObject` 和 `GetObject` 请求的一部分自动加密和解密。您的对象全部使用唯一的数据密钥加密。即使您将 KMS 密钥指定为包装密钥，Amazon S3 加密客户端也不会使用存储桶密钥或与存储桶密钥交互。

《Amazon S3 Encryption Client Developer Guide》侧重于 3.0 及更高版本的 Amazon S3 加密客户端。有关更多信息，请参阅《Amazon S3 加密客户端开发人员指南》中的什么是 Amazon S3 加密客户端？

有关早期版本的 Amazon S3 加密客户端的更多信息，请参阅适用于您的编程语言的《Amazon SDK Developer Guide》。

- 适用于 Java 的 Amazon SDK
- 适用于 .NET 的 Amazon SDK
- 适用于 Go 的 Amazon SDK
- 适用于 PHP 的 Amazon SDK
- 适用于 Ruby 的 Amazon SDK
- 适用于 C++ 的 Amazon SDK

# 互联网络流量隐私

此主题介绍 Amazon S3 如何保护从服务到其他位置的连接。

## 服务与本地客户端和应用之间的流量

以下连接可以和 Amazon PrivateLink 合并使用，以提供私有联网和 Amazon 之间的连接性：

- 一个 Amazon Site-to-Site VPN 连接。有关更多信息，请参阅什么是 Amazon Site-to-Site VPN？
- Amazon Direct Connect 连接。有关更多信息，请参阅什么是 Amazon Direct Connect？

通过网络访问 Amazon S3 是通过 Amazon 发布的 API 进行的。客户端必须支持传输层安全性（TLS）1.2。我们建议使用 TLS 1.3。客户端还必须支持具有完全向前保密 (PFS) 的密码套件，例如 Ephemeral Diffie-Hellman (DHE) 或 Elliptic Curve Diffie-Hellman Ephemeral (ECDHE)。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。此外，必须使用与 IAM 主体关联的访问密钥 ID 和秘密访问密钥签名请求，或者可以使用 Amazon Security Token Service（STS）生成临时安全证书来签名请求。

## 同一区域中 Amazon 资源之间的流量

Amazon S3 的 Virtual Private Cloud (VPC) 端点是 VPC 内的逻辑实体，仅允许连接到 Amazon S3。VPC 将请求路由到 Amazon S3 并将响应路由回 VPC。有关更多信息，请参阅 VPC 用户指南中的 VPC 端点。有关您可用来从 VPC 端点控制 S3 存储桶访问的示例存储桶策略，请参阅使用存储桶策略控制从 VPC 端点的访问。

## Amazon PrivateLink：表示 Amazon S3

借助适用于 Amazon S3 的 Amazon PrivateLink，您可以在 Virtual Private Cloud (VPC) 中预置接口 VPC 端点（接口端点）。这些端点可从本地（通过 VPN 及 Amazon Direct Connect）或其他 Amazon Web Services 区域（通过 VPC 对等连接）中的应用程序直接访问。

接口端点由一个或多个弹性网络接口 (ENI) 代表，这些接口是从 VPC 中的子网分配的私有 IP 地址。通过接口端点向 Amazon S3 发出的请求仍留在 Amazon 网络上。您还可以通过 Amazon Direct Connect 或 Amazon Virtual Private Network (Amazon VPN) 从本地部署应用程序访问 VPC 中的接口端点。有关如何将 VPC 与本地网络连接的更多信息，请参阅 Amazon Direct Connect 用户指南和 Amazon Site-to-Site VPN 用户指南。

有关接口端点的一般信息，请参阅 Amazon PrivateLink 指南中的接口 VPC 端点 (Amazon PrivateLink)。

主题

- 适用于 Amazon S3 的 VPC 端点类型

- 适用于 Amazon S3 的 Amazon PrivateLink 的限制和局限性
- 创建 VPC 端点
- 访问 Amazon S3 接口端点
- 私有 DNS
- 从 S3 接口端点访问存储桶、接入点和 Amazon S3 控制 API 操作
- 更新本地 DNS 配置
- 为 Amazon S3 创建 VPC 端点策略

## 适用于 Amazon S3 的 VPC 端点类型

您可以使用两种类型的 VPC 端点访问 Amazon S3：网关端点和接口端点（使用 Amazon PrivateLink）。网关端点是您在路由表中指定的网关，用于通过 Amazon 网络从 VPC 访问 Amazon S3。接口端点通过私有 IP 地址，使用 VPC 对等连接或 Amazon Transit Gateway 将请求从您的 VPC 内、本地或其它 Amazon Web Services 区域中的 VPC 路由到 Amazon S3，从而扩展网关端点的功能。有关更多信息，请参阅什么是 VPC 对等连接?和 Transit Gateway 与 VPC 对等连接。

接口端点与网关端点兼容。如果您在 VPC 中有现有网关端点，则可以在同一 VPC 中使用这两种类型的端点。

| 适用于 Amazon S3 的网关端点 | 适用于 Amazon S3 的接口端点 |
| --- | --- |
| 在这两种情况下，您的网络流量仍保留在 Amazon 网络中。 | |
| 使用 Amazon S3 公有 IP 地址 | 使用 VPC 中的私有 IP 地址访问 Amazon S3 |
| 使用相同的 Simple Storage Service (Amazon S3) DNS 名称 | 需要特定于端点的 Simple Storage Service (Amazon S3) DNS 名称 |
| 不允许从本地访问 | 允许从本地访问 |
| 不允许从其他 Amazon Web Services 区域访问 | 允许从另一个 Amazon Web Services 区域使用 VPC 对等连接或 Amazon Transit Gateway 进行访问 |
| 不计费 | 已计费 |

有关网关端点的更多信息，请参阅 Amazon PrivateLink 指南中的网关 VPC 端点。

## 适用于 Amazon S3 的 Amazon PrivateLink 的限制和局限性

VPC 限制应用于适用于 Amazon S3 的 Amazon PrivateLink。有关更多信息，请参阅《Amazon PrivateLink 指南》中的接口端点注意事项和 Amazon PrivateLink 限额。此外，以下限制将适用：

适用于 Amazon S3 的 Amazon PrivateLink 不支持以下各项：

- 美国联邦信息处理标准 (FIPS) 端点
- 网站端点
- 传统全局端点
- S3 短划线区域端点
- Dual-stack endpoints
- 在不同 Amazon Web Services 区域中的存储桶之间使用 CopyObject 或 UploadPartCopy
- 传输层安全性协议（TLS）1.1

## 创建 VPC 端点

要创建 VPC 接口端点，请参阅《Amazon PrivateLink 指南》中的创建 VPC 端点。

## 访问 Amazon S3 接口端点

创建接口端点时，Amazon S3 会生成两种特定于端点的 S3 DNS 名称：区域和地区。

- 区域 DNS 名称包括唯一的 VPC 端点 ID、服务标识符、Amazon Web Services 区域和以其命名的 `vpce.amazonaws.com`。例如，对于 VPC 端点 ID *`vpce-1a2b3c4d`*，生成的 DNS 名称可能类似于 *`vpce-1a2b3c4d-5e6f`*`.s3.us-east-1.vpce.amazonaws.com`。
- 区域 DNS 名称包括可用区 – 例如 *`vpce-1a2b3c4d-5e6f`*`-us-east-1a.s3.us-east-1.vpce.amazonaws.com`。如果您的架构隔离了可用区，则可以使用此选项。例如，您可以将其用于故障控制或降低区域数据传输成本。

可以从 S3 公有 DNS 域解析特定于端点的 S3 DNS 名称。

## 私有 DNS

VPC 接口端点的私有 DNS 选项简化了通过 VPC 端点路由 S3 流量的过程，并帮助您充分利用应用程序可用的最低成本网络路径。您可以使用私有 DNS 选项来路由区域 S3 流量，而无需更新 S3 客户端以使用接口端点的端点特定 DNS 名称，也无需管理 DNS 基础设施。启用私有 DNS 名称后，对于以下端点，区域 S3 DNS 查询将解析为 Amazon PrivateLink 的私有 IP 地址：

- 区域存储桶端点（例如 `s3.us-east-1.amazonaws.com`）
- 控制端点（例如 `s3-control.us-east-1.amazonaws.com`）
- 接入点端点（例如 `s3-accesspoint.us-east-1.amazonaws.com`）

适用于 Amazon S3 的 Amazon PrivateLink 不支持 Using Amazon S3 dual-stack endpoints。如果您使用 S3 双堆栈 DNS 名称作为私有 DNS 名称，则 IPv6 流量将被丢弃，或者，如果虚拟私有云（VPC）有互联网网关，则 IPv6 流量将通过 VPC 中的互联网网关路由。

如果您的 VPC 中有网关端点，则可以通过现有 S3 网关端点自动路由 VPC 内请求，并通过接口端点自动路由本地请求。此方法允许您使用 VPC 内流量不计费的网关端点来优化网络成本。您的本地应用程序可以在入站解析器端点的帮助下使用 Amazon PrivateLink。Amazon 为您的 VPC 提供 DNS 服务器，称为 Route 53 Resolver。入站解析器端点将来自本地网络的 DNS 查询转发到 Route 53 Resolver。

> **Important**
>
> 要在使用仅对入站端点启用私有 DNS 时充分利用成本最低的网络路径，您的 VPC 中必须存在网关端点。当选择仅对入站端点启用私有 DNS 选项时，网关端点的存在有助于确保 VPC 内流量始终通过 Amazon 私有网络路由。当选择仅对入站端点启用私有 DNS 选项时，必须维护此网关端点。如果要删除网关端点，则必须先清除仅对入站端点启用私有 DNS。
> 如果您想要将现有接口端点更新为仅对入站端点启用私有 DNS，请先确认您的 VPC 具有 S3 网关端点。有关网关端点和管理私有 DNS 名称的更多信息，请分别参阅《Amazon PrivateLink 指南》中的网关 VPC 端点和管理 DNS 名称。

仅对入站端点启用私有 DNS 选项仅适用于支持网关端点的服务。

有关创建使用仅对入站端点启用私有 DNS 的 VPC 端点的更多信息，请参阅《Amazon PrivateLink 指南》中的创建接口端点。

使用 VPC 控制台

在控制台中，您有两个选项：启用 DNS 名称和仅对入站端点启用私有 DNS。启用 DNS 名称是 Amazon PrivateLink 支持的选项。通过使用启用 DNS 名称选项，您可以使用 Amazon 的与 Amazon S3 的私有连接，同时向默认公有端点 DNS 名称发出请求。启用此选项后，客户可以利用其应用程序可用的成本最低的网络路径。

当您在 Amazon S3 的现有或新的 VPC 接口端点上启用私有 DNS 名称时，默认情况下会选择仅对入站端点启用私有 DNS 选项。如果选择此选项，则您的应用程序仅对本地流量使用接口端点。这种 VPC

内流量会自动使用成本较低的网关端点。或者，您可以清除仅对入站端点启用私有 DNS，以通过您的接口端点路由所有 S3 请求。

使用 Amazon CLI

如果不指定 `PrivateDnsOnlyForInboundResolverEndpoint` 的值，则它默认为 `true`。但是，在您的 VPC 应用设置之前，它会进行检查以确保 VPC 中存在网关端点。如果 VPC 中存在网关端点，则调用成功。否则，您将看到以下错误消息：

要将 PrivateDnsOnlyForInboundResolverEndpoint 设置为 true，VPC *vpce_id* 必须具有该服务的网关端点。

对于新的接口 VPC 端点

使用 `private-dns-enabled` 和 `dns-options` 属性通过命令行启用私有 DNS。`dns-options` 属性中的 `PrivateDnsOnlyForInboundResolverEndpoint` 选项必须设置为 `true`。将 *user input placeholders* 替换为您自己的信息。

```
aws ec2 create-vpc-endpoint \
--region us-east-1 \
--service-name s3-service-name \
--vpc-id client-vpc-id \
--subnet-ids client-subnet-id \
--vpc-endpoint-type Interface  \
--private-dns-enabled  \
--ip-address-type ip-address-type \
--dns-options PrivateDnsOnlyForInboundResolverEndpoint=true \
--security-group-ids client-sg-id
```

对于现有 VPC 端点

如果您想对现有 VPC 端点使用私有 DNS，请使用以下示例命令并将 *user input placeholders* 替换为您自己的信息。

```
aws ec2 modify-vpc-endpoint \
--region us-east-1 \
--vpc-endpoint-id client-vpc-id \
--private-dns-enabled \
--dns-options PrivateDnsOnlyForInboundResolverEndpoint=false
```

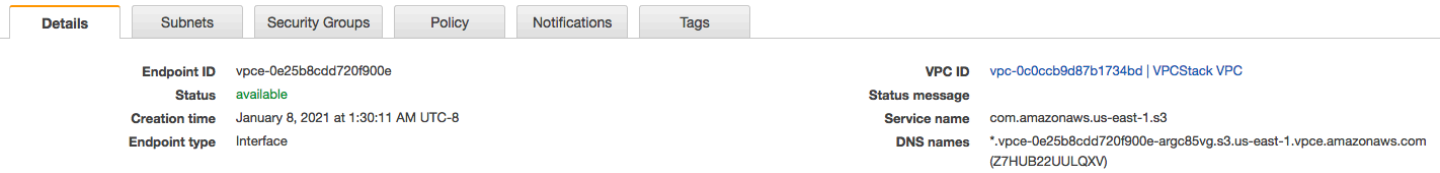
如果您想更新现有 VPC 端点以仅对入站解析器启用私有 DNS，请使用以下示例并将示例值替换为您自己的值。

```
aws ec2 modify-vpc-endpoint \
--region us-east-1 \
--vpc-endpoint-id client-vpc-id \
--private-dns-enabled \
--dns-options PrivateDnsOnlyForInboundResolverEndpoint=true
```

## 从 S3 接口端点访问存储桶、接入点和 Amazon S3 控制 API 操作

您可以使用 Amazon CLI 或 Amazon SDK 通过 S3 接口端点访问存储桶、S3 接入点和 Amazon S3 控制 API 操作。

下图显示了 VPC 控制台详细信息选项卡，您可以在其中找到 VPC 端点的 DNS 名称。在此示例中，VPC 端点 ID (vpce-id) 为 `vpce-0e25b8cdd720f900e`，DNS 名称为 `*.vpce-0e25b8cdd720f900e-argc85vg.s3.us-east-1.vpce.amazonaws.com`。




使用 DNS 名称访问资源时，将 * 替换为相应的值。用来代替 * 的相应值如下所示：

- `bucket`
- `accesspoint`
- `control`

例如，要访问存储桶，请使用如下所示的 DNS 名称。

`bucket.vpce-0e25b8cdd720f900e-argc85vg.s3.us-east-1.vpce.amazonaws.com`

有关如何使用 DNS 名称访问存储桶、接入点和 Amazon S3 控制 API 操作的示例，请参阅下面的章节：Amazon CLI 示例和Amazon SDK 示例。

有关如何查看端点特定 DNS 名称的更多信息，请参阅《VPC 用户指南》中的查看端点服务私有 DNS 名称配置。

Amazon CLI 示例

要在 Amazon CLI 命令中通过 S3 接口端点访问 S3 存储桶、S3 接入点或 Amazon S3 控制 API操作，请使用 `--region` 和 `--endpoint-url` 参数。

示例：使用端点 URL 列出存储桶中的对象

在以下示例中，将存储桶名称 *my-bucket*、区域 *us-east-1* 和 VPC 端点 ID 的 DNS 名称 *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* 替换为您自己的信息。

```
aws s3 ls s3://my-bucket/ --region us-east-1 --endpoint-url
 https://bucket.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com
```

示例：使用端点 URL 列出接入点中的对象

- 方法 1 – 将接入点的 Amazon 资源名称（ARN）与接入点端点结合使用

  将 ARN *us-east-1:123456789012:accesspoint/accesspointexamplename*、区域 *us-east-1* 和 VPC 端点 ID *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* 替换为您自己的信息。

  ```
  aws s3api list-objects-v2 --bucket arn:aws:s3:us-east-1:123456789012:accesspoint/
  accesspointexamplename --region us-east-1 --endpoint-url
   https://accesspoint.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com
  ```

  如果您无法成功运行该命令，请将 Amazon CLI 更新为最新版本，然后重试。有关更新说明的更多信息，请参阅《Amazon Command Line Interface 用户指南》中的安装或更新 Amazon CLI 的最新版本。
- 方法 2 – 将接入点的别名与区域存储桶端点结合使用

  在以下示例中，将接入点别名 *accesspointexamplename-8tyekmigicmhun8n9kwpfur39dnw4use1a-s3alias*、区域 *us-east-1* 和 VPC 端点 ID *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* 替换为您自己的信息。

  ```
  aws s3api list-objects-v2 --
  bucket accesspointexamplename-8tyekmigicmhun8n9kwpfur39dnw4use1a-s3alias
  ```

```
 --region us-east-1 --endpoint-url https://bucket.vpce-1a2b3c4d-5e6f.s3.us-
east-1.vpce.amazonaws.com
```

- 方法 3 – 将接入点的别名与接入点端点结合使用

  首先，要构造一个包含存储桶作为主机名一部分的 S3 端点，请将寻址样式设置为 `virtual` 以供 `aws s3api` 使用。有关 `AWS configure` 的更多信息，请参阅《Amazon Command Line Interface 用户指南》中的配置和凭证文件设置。

  ```
  aws configure set default.s3.addressing_style virtual
  ```

  然后，在以下示例中，将接入点别名 *accesspointexamplename-8tyekmigicmhun8n9kwpfur39dnw4use1a-s3alias*、区域 *us-east-1* 和 VPC 端点 ID *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* 替换为您自己的信息。有关接入点别名的更多信息，请参阅通用存储桶的接入点别名

  ```
  aws s3api list-objects-v2 --
  bucket accesspointexamplename-8tyekmigicmhun8n9kwpfur39dnw4use1a-s3alias --
  region us-east-1 --endpoint-url https://accesspoint.vpce-1a2b3c4d-5e6f.s3.us-
  east-1.vpce.amazonaws.com
  ```

示例：使用端点 URL 通过 S3 控制 API 操作列出任务

在以下示例中，将区域 *us-east-1*、VPC 端点 ID *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* 和账户 ID *12345678* 替换为您自己的信息。

```
aws s3control --region us-east-1 --endpoint-url
 https://control.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com list-jobs --
account-id 12345678
```

Amazon SDK 示例

要在使用 Amazon SDK 时通过 S3 接口端点访问 S3 存储桶、S3 接入点、Amazon S3 控制 API 操作，请将 SDK 更新到最新版本。然后，将客户端配置为使用端点 URL 通过 S3 接口端点访问存储桶、接入点或 Amazon S3 控制 API 操作。

SDK for Python (Boto3)

示例：使用端点 URL 访问 S3 存储桶

在以下示例中，将区域 *us-east-1* 和 VPC 端点 ID *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* 替换为您自己的信息。

```
s3_client = session.client(
service_name='s3',
region_name='us-east-1',
endpoint_url='https://bucket.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com'
)
```

示例：使用端点 URL 访问 S3 接入点

在以下示例中，将区域 *us-east-1* 和 VPC 端点 ID *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* 替换为您自己的信息。

```
ap_client = session.client(
service_name='s3',
region_name='us-east-1',
endpoint_url='https://accesspoint.vpce-1a2b3c4d-5e6f.s3.us-
east-1.vpce.amazonaws.com'
)
```

示例：使用端点 URL 访问 Amazon S3 控制 API

在以下示例中，将区域 *us-east-1* 和 VPC 端点 ID *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* 替换为您自己的信息。

```
control_client = session.client(
service_name='s3control',
region_name='us-east-1',
endpoint_url='https://control.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com'
)
```

SDK for Java 1.x

示例：使用端点 URL 访问 S3 存储桶

在以下示例中，将 VPC 端点 ID *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* 替换为您自己的信息。

```
// bucket client
```

```
final AmazonS3 s3 = AmazonS3ClientBuilder.standard().withEndpointConfiguration(
        new AwsClientBuilder.EndpointConfiguration(
                "https://bucket.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com",
                Regions.DEFAULT_REGION.getName()
        )
).build();
List<Bucket> buckets = s3.listBuckets();
```

示例：使用端点 URL 访问 S3 接入点

在以下示例中，将 VPC 端点 ID *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* 和 ARN *us-east-1:123456789012:accesspoint/prod* 替换为您自己的信息。

```
// accesspoint client
final AmazonS3 s3accesspoint =
 AmazonS3ClientBuilder.standard().withEndpointConfiguration(
        new AwsClientBuilder.EndpointConfiguration(
                "https://accesspoint.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com",
                Regions.DEFAULT_REGION.getName()
        )
).build();
ObjectListing objects = s3accesspoint.listObjects("arn:aws:s3:us-east-1:123456789012:accesspoint/prod");
```

示例：使用端点 URL 访问 Amazon S3 控制 API 操作

在以下示例中，将 VPC 端点 ID *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* 替换为您自己的信息。

```
// control client
final AWSS3Control s3control =
 AWSS3ControlClient.builder().withEndpointConfiguration(
        new AwsClientBuilder.EndpointConfiguration(
                "https://control.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com",
                Regions.DEFAULT_REGION.getName()
        )
).build();
final ListJobsResult jobs = s3control.listJobs(new ListJobsRequest());
```

SDK for Java 2.x

示例：使用端点 URL 访问 S3 存储桶

在以下示例中，将 VPC 端点 ID *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* 和区域 *Region.US_EAST_1* 替换为您自己的信息。

```
// bucket client
Region region = Region.US_EAST_1;
s3Client = S3Client.builder().region(region)

 .endpointOverride(URI.create("https://bucket.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com"))
                    .build()
```

示例：使用端点 URL 访问 S3 接入点

在以下示例中，将 VPC 端点 ID *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* 和区域 *Region.US_EAST_1* 替换为您自己的信息。

```
// accesspoint client
Region region = Region.US_EAST_1;
s3Client = S3Client.builder().region(region)

 .endpointOverride(URI.create("https://accesspoint.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com"))
                    .build()
```

示例：使用端点 URL 访问 Amazon S3 控制 API

在以下示例中，将 VPC 端点 ID *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* 和区域 *Region.US_EAST_1* 替换为您自己的信息。

```
// control client
Region region = Region.US_EAST_1;
s3ControlClient = S3ControlClient.builder().region(region)

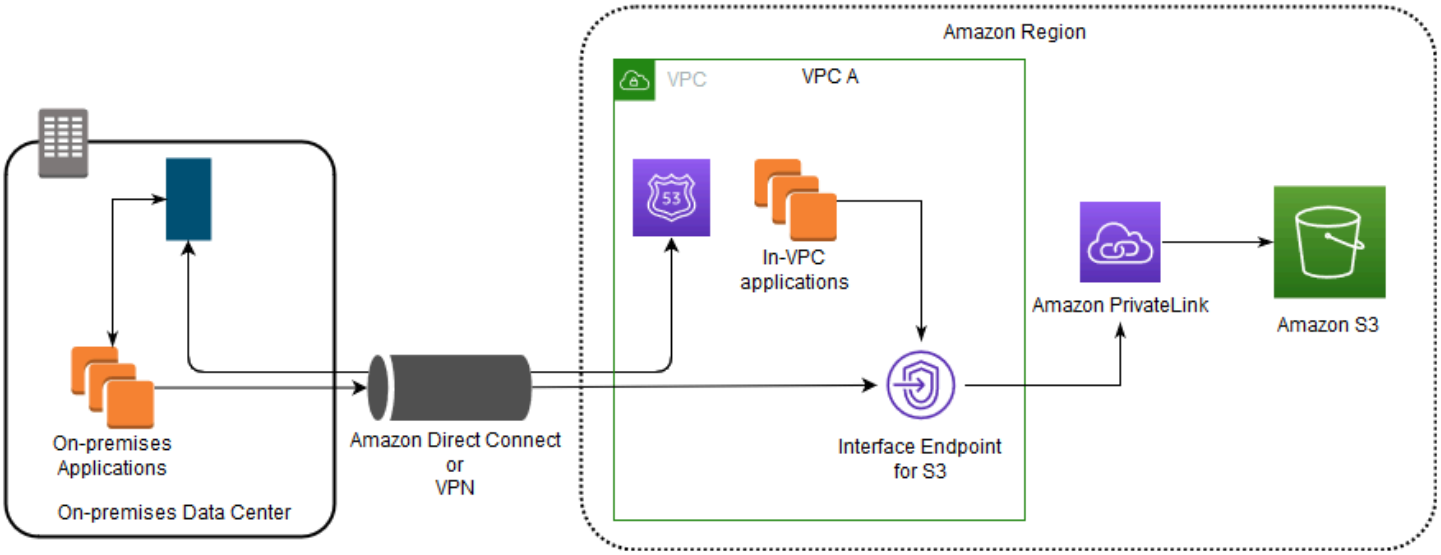
 .endpointOverride(URI.create("https://control.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com"))
                                  .build()
```

## 更新本地 DNS 配置

使用特定于端点的 DNS 名称访问适用于 Amazon S3 的接口端点时，您无需更新本地 DNS 解析程序。您可以使用来自公有 Amazon S3 DNS 域的接口端点的私有 IP 地址解析特定于端点的 DNS 名称。

使用接口端点访问 Amazon S3，无需 VPC 中的网关端点和互联网网关

VPC 中的接口端点可以通过 Amazon 网络将 VPC 内的应用程序和本地应用程序路由到 Amazon S3，如下图所示。

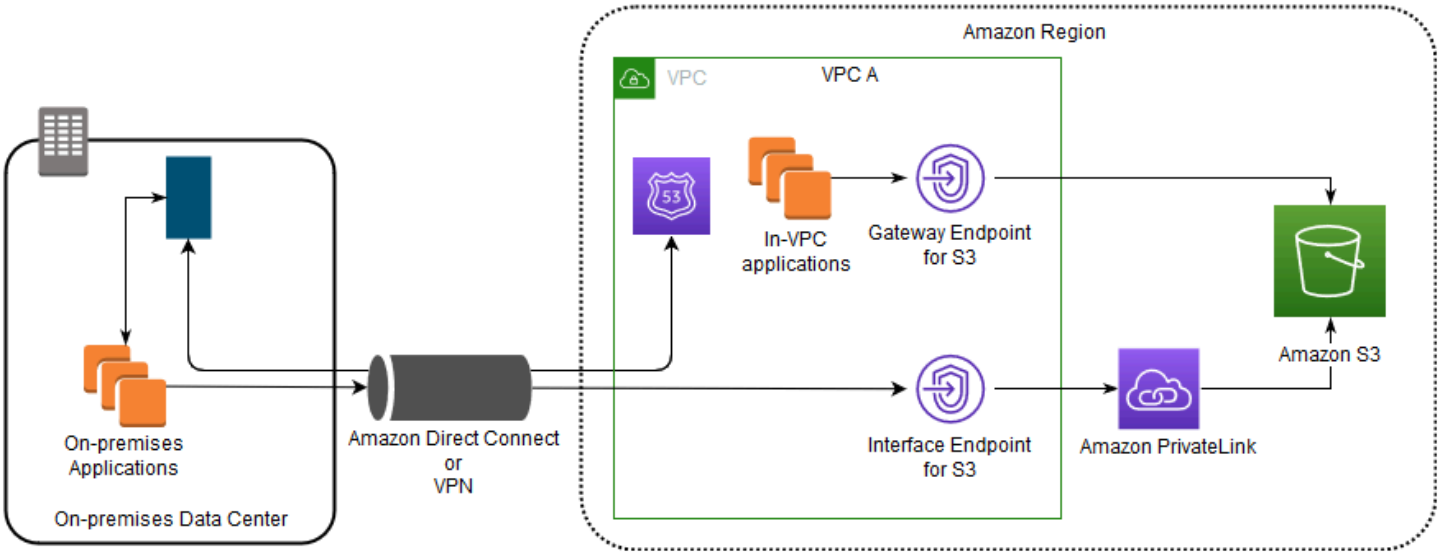



该图阐释了以下内容：

- 您的本地部署网络使用 Amazon Direct Connect 或者 Amazon VPN 连接到 VPC A。
- 本地和 VPC A 中的应用程序使用特定于端点的 DNS 名称通过 S3 接口端点访问 Amazon S3。
- 本地部署应用程序通过 Amazon Direct Connect（或 Amazon VPN）将数据发送到 VPC 中的接口端点。Amazon PrivateLink 通过 Amazon 网络将数据从接口端点移动到 Amazon S3。
- VPC 中的应用程序还向接口端点发送通信。Amazon PrivateLink 通过 Amazon 网络将数据从接口端点移动到 Amazon S3。

在同一 VPC 中同时使用网关端点和接口端点来访问 Amazon S3

您可以创建接口端点并将现有网关端点保留在同一 VPC 中，如下图所示。通过这种方法，您可以允许 VPC 内应用程序继续通过网关端点访问 Amazon S3，而无需付费。然后，只有您的本地应用程序才会使用接口端点访问 Amazon S3。要通过这种方式访问 Amazon S3，您必须更新本地应用程序，以使用适用于 Amazon S3 的特定于端点的 DNS 名称。




该图阐释了以下内容：

- 本地部署应用程序使用特定于端点的 DNS 名称通过 Amazon Direct Connect（或 Amazon VPN）将数据发送到 VPC 中的接口端点。Amazon PrivateLink 通过 Amazon 网络将数据从接口端点移动到 Amazon S3。
- 使用默认的区域 Amazon S3 名称，VPC 内应用程序会将数据发送到通过 Amazon 网络连接到 Amazon S3 的网关端点。

有关网关端点的更多信息，请参阅 VPC 用户指南中的网关 VPC 端点。

## 为 Amazon S3 创建 VPC 端点策略

您可以为 VPC 端点附加控制对 Amazon S3 的访问的端点策略。该策略指定以下信息：

- 可执行操作的 Amazon Identity and Access Management (IAM) 主体
- 可执行的操作
- 可对其执行操作的资源

您还可以使用 Amazon S3 存储桶策略，通过使用存储桶策略中的 `aws:sourceVpce` 条件限制从特定 VPC 端点访问特定存储桶。以下示例显示了限制对存储桶或端点的访问的策略。

主题

- 示例：限制从 VPC 端点对特定存储桶的访问
- 示例：限制从 VPC 端点对特定账户中存储桶的访问

- 示例：限制对 S3 存储桶策略中特定 VPC 端点的访问

### 示例：限制从 VPC 端点对特定存储桶的访问

您可以创建一个端点策略来仅允许访问特定的 Amazon S3 存储桶。如果您的 VPC 中有使用存储桶的其他 Amazon Web Services 服务，这种策略会非常有用。以下存储桶策略限制为仅可访问 *amzn-s3-demo-bucket1*。要使用此端点策略，请将 *amzn-s3-demo-bucket1* 替换为您的存储桶名称。

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909151",
  "Statement": [
    { "Sid": "Access-to-specific-bucket-only",
      "Principal": "*",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket1",
                   "arn:aws:s3:::amzn-s3-demo-bucket1/*"]
    }
  ]
}
```

### 示例：限制从 VPC 端点对特定账户中存储桶的访问

您可以创建一个端点策略，以限制仅访问特定 Amazon Web Services 账户中的 S3 存储桶。要防止 VPC 内的客户端访问并非您拥有的存储桶，请在端点策略中使用以下语句。以下示例语句创建了一个策略，此策略将访问限制为由单个 Amazon Web Services 账户 ID *111122223333* 拥有的资源。

```
{
  "Statement": [
    {
      "Sid": "Access-to-bucket-in-specific-account-only",
      "Principal": "*",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Effect": "Deny",
```

```
      "Resource": "arn:aws:s3:::*",
      "Condition": {
        "StringNotEquals": {
          "aws:ResourceAccount": "111122223333"
        }
      }
    }
  ]
}
```

> **Note**
>
> 要指定要访问的资源的 Amazon Web Services 账户 ID，可以在 IAM 策略中使用 `aws:ResourceAccount` 或 `s3:ResourceAccount` 键。但请注意，有些 Amazon Web Services 服务依赖于访问 Amazon 托管式存储桶。因此，在 IAM 策略中使用 `aws:ResourceAccount` 或 `s3:ResourceAccount` 键也可能会影响对这些资源的访问。

示例：限制对 S3 存储桶策略中特定 VPC 端点的访问

示例：限制对 S3 存储桶策略中特定 VPC 端点的访问

以下 Amazon S3 存储桶策略仅允许从 VPC 端点 *vpce-1a2b3c4d* 访问特定的存储桶 *amzn-s3-demo-bucket2*。如果未使用指定的端点，则该策略拒绝对存储桶的所有访问。`aws:sourceVpce` 条件指定端点，而不需要 VPC 端点资源的 Amazon 资源名称（ARN），只需要端点 ID。要使用此存储桶策略，请将 *amzn-s3-demo-bucket2* 和 *vpce-1a2b3c4d* 替换为您的存储桶名称和端点。

> **Important**
>
> - 当应用以下 Amazon S3 存储桶策略来限制仅可访问特定的 VPC 端点时，您可能会无意中屏蔽对存储桶的访问。存储桶策略旨在专门限制存储桶访问源自 VPC 端点的连接，而这可能会屏蔽到存储桶的所有连接。有关如何修复此问题的信息，请参阅我的存储桶策略有错误的 VPC 或 VPC 端点 ID。Amazon Web Services 支持 知识中心内的如何修复策略才能访问存储桶？。
> - 在使用以下示例策略之前，将 VPC 端点 ID 替换为适合您的使用案例的值。否则，您将无法访问您的存储桶。
> - 此策略禁用控制台访问指定的存储桶，因为控制台请求不是来自指定的 VPC 端点。

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
    { "Sid": "Access-to-specific-VPCE-only",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket2",
                   "arn:aws:s3:::amzn-s3-demo-bucket2/*"],
      "Condition": {"StringNotEquals": {"aws:sourceVpce": "vpce-1a2b3c4d"}}
    }
  ]
}
```

有关更多策略示例，请参阅 VPC 用户指南中的 Amazon S3 端点。

有关 VPC 连接的更多信息，请参阅 Amazon 白皮书 Amazon Virtual Private Cloud 连接性选项中的 Network-to-VPC connectivity options（从网络到 VPC 的连接性选项）。

# Amazon S3 的合规性验证

作为多个 Amazon 合规性计划的一部分，第三方审计员将评估 Amazon S3 的安全性和合规性，包括以下内容：

- 系统和组织控制 (SOC)
- 支付卡行业数据安全标准 (PCI DSS)
- 联邦风险与授权管理项目 (FedRAMP)
- 健康保险流通与责任法案 (HIPAA)

Amazon 在合规性计划范围内的 Amazon 服务中提供特定合规性计划范围内经常更新的 Amazon 服务列表。

提供第三方审计报告，可使用 Amazon Artifact 下载。有关更多信息，请参阅下载 Amazon Artifact 中的报告。

有关 Amazon 合规性计划的更多信息，请参阅 Amazon 合规性计划。

您在使用 Amazon S3 时的合规性责任由您数据的敏感性、您组织的合规性目标以及适用的法律法规决定。如果您对 Amazon S3 的使用需遵守 HIPAA、PCI 或 FedRAMP 等标准，Amazon 提供了以下实用资源：

- 安全性和合规性快速入门指南，介绍了架构注意事项，以及在 Amazon 上部署侧重于安全性和合规性的基准环境的步骤。
- 设计符合 HIPAA 安全性和合规性要求的架构概述了公司如何使用 Amazon 来帮助自己满足 HIPAA 要求。
- Amazon 合规性资源提供了可能适用于您的行业和位置的多个不同业务手册和指南。
- Amazon Config 可用于评估您的资源配置对内部实践、行业指南和法规的遵循情况。
- Amazon Security Hub 提供了 Amazon 中安全状态的全面视图，可帮助您检查是否符合安全行业标准和最佳实践。
- 使用对象锁定以锁定对象 可以帮助您满足金融服务监管机构（如SEC、FINRA 和 CFTC）的技术要求，这些监管机构对于某些类型的账簿和记录信息要求编写一次、多次读取 (WORM) 数据存储。
- 使用 S3 清单对数据进行编目和分析 可帮助您出于业务、合规性和法规要求，使用它来审核和报告对象的复制和加密状态。

# Amazon S3 中的恢复能力

Amazon 全球基础设施围绕区域和可用区构建。Amazon Web Services 区域提供多个在物理上独立且隔离的可用区，这些可用区通过延迟低、吞吐量高且冗余性高的网络连接在一起。这些可用区为您提供了高效的方法来设计和操作应用程序和数据库。与传统的单个数据中心基础设施或多个数据中心基础设施相比，它们具有更高的可用性、容错性和可扩展性。如果您尤其需要跨更长地理距离复制您的数据，您可以使用在区域内和跨区域复制对象，它允许跨不同 Amazon Web Services 区域中的存储桶自动异步复制对象。

每个 Amazon Web Services 区域都有多个可用区。您可以跨一个区域中的多个可用区部署您的应用来获得容错性和低延迟。可用区通过快速、私密的光纤网络来互相连接，使您能够轻松构建可在可用区之间无中断地自动实现故障转移的应用程序。

有关 Amazon Web Services 区域 和可用区的更多信息，请参阅 Amazon 全球基础设施。

除了 Amazon 全球基础设施之外，Amazon S3 还提供多种特征，以帮助支持您的数据恢复能力和备份需求。

生命周期配置

生命周期配置是一组规则，用于定义 Amazon S3 对一组对象应用的操作。利用生命周期配置规则，您可以指示 Amazon S3 将对象转换为较低成本的存储类，或者归档或删除它们。有关更多信息，请参阅 管理对象的生命周期。

版本控制

版本控制是在相同的存储桶中保留对象的多个变量的方法。对于 Amazon S3 存储桶中存储的每个对象，您可以使用版本控制功能来保存、检索和还原它们的各个版本。使用版本控制能够轻松从用户意外操作和应用程序故障中恢复数据。有关更多信息，请参阅 使用 S3 版本控制保留对象的多个版本。

S3 对象锁定

您可以使用 S3 对象锁定通过一次写入、多次读取 (WORM) 模式存储对象。使用 S3 对象锁定时，您可以在固定的时间段内或无限期地阻止删除或覆盖对象。S3 对象锁定让您可以满足需要 WORM 存储的法规要求，或只是添加一个额外的保护层来防止对象被更改和删除。有关更多信息，请参阅使用对象锁定以锁定对象。

存储类

Amazon S3 提供一系列存储类，可供选择，具体取决于您的工作负载要求。S3 Standard-IA 和 S3 One Zone-IA 存储类用于大约每月访问一次且需要毫秒访问的数据。S3 Glacier Instant Retrieval

存储类专为长期归档数据而设计，您可以访问几毫秒的访问权限，大约每季度访问一次。对于不需要立即访问的归档数据，例如备份，您可以使用 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储类。有关更多信息，请参阅 了解和管理 Amazon S3 存储类。

下面的安全最佳实践也处理弹性：

- Enable versioning
- Consider Amazon S3 cross-region replication
- Identify and audit all your Amazon S3 buckets

# Amazon S3 备份的加密

如果您使用 Amazon S3 存储备份，则备份的加密取决于这些存储桶的配置。Amazon S3 提供了一种方法来设置 S3 存储桶的默认加密行为。您可以对存储桶设置默认加密，以便在存储桶中存储所有对象时对这些对象进行加密。默认加密支持存储在 Amazon KMS 中的密钥（SSE-KMS）。有关更多信息，请参阅 为 Amazon S3 存储桶设置默认服务器端加密行为。

有关版本控制和对象锁定的详细信息，请参阅以下主题：使用 S3 版本控制保留对象的多个版本 使用对象锁定以锁定对象

# Amazon S3 中的基础设施安全性

作为一个受管理的服务，Amazon S3 受到 Amazon 全局网络安全过程的保护，这些过程在 Amazon Well-Architected 框架的安全支柱中进行了描述。

通过网络访问 Amazon S3 是通过 Amazon 发布的 API 进行的。客户端必须支持传输层安全性（TLS）1.2。我们建议还支持 TLS 1.3。（有关此建议的更多信息，请参阅《Amazon 安全博客》上的使用 TLS 1.3 加快 Amazon 云连接）。客户端还必须支持具有完全向前保密 (PFS) 的密码套件，例如 Ephemeral Diffie-Hellman (DHE) 或 Elliptic Curve Diffie-Hellman Ephemeral (ECDHE)。另外，请求必须使用 Amazon 签名 V4 或 Amazon 签名 V2 进行签名，同时要求提供有效凭证。

这些 API 可以从任何网络位置调用。然而，Amazon S3 的确支持基于资源的访问策略，其中可以包含基于源 IP 地址的限制。您还可以使用 Amazon S3 存储桶策略控制从特定 Virtual Private Cloud（VPC）端点或特定 VPC 对存储桶的访问。事实上，这隔离了在 Amazon 网络中仅从特定 VPC 到给定 Amazon S3 存储桶的网络访问。有关更多信息，请参阅 使用存储桶策略控制从 VPC 端点的访问。

下面的安全最佳实践也处理 Amazon S3 中的基础设施安全性：

- Consider VPC endpoints for Amazon S3 access
- Identify and audit all your Amazon S3 buckets

# Amazon S3 中的配置和漏洞分析

Amazon 负责处理基本安全任务，如来宾操作系统（OS）和数据库补丁、防火墙配置和灾难恢复等。这些流程已通过相应第三方审核和认证。有关更多详细信息，请参阅以下资源：

- Amazon S3 的合规性验证
- 责任共担模式
- Amazon Web Services：安全过程概述

以下安全最佳实践还处理 Amazon S3 中的配置和漏洞分析：

- Identify and audit all your Amazon S3 buckets
- Enable Amazon Config（启用 Gem）

# 访问权限管理

Amazon S3 提供了各种访问管理工具。以下是这些功能和工具的列表。您并不需要所有这些访问管理工具，但必须使用一个或多个工具来授予对 Amazon S3 存储桶、对象和其它 S3 资源的访问权限。正确应用这些工具有助于确保只有目标用户才能访问您的资源。

最常用的访问管理工具是访问策略。访问策略可以是附加到 Amazon 资源的基于资源的策略，例如存储桶的存储桶策略。访问策略也可以是附加到 Amazon Identity and Access Management（IAM）身份（如 IAM 用户、组或角色）的基于身份的策略。访问策略描述了谁可以访问哪些内容。编写访问策略来向 Amazon Web Services 账户和 IAM 用户、组和角色授予对资源执行操作的权限。例如，您可以向另一个 Amazon Web Services 账户授予 `PUT Object` 权限，以使该账户可以向您的存储桶上传对象。

以下是 Amazon S3 中提供的访问管理工具。有关 Amazon S3 访问控制的更全面指南，请参阅 Amazon S3 中的访问控制。

存储桶策略

Amazon S3 存储桶策略是采用 JSON 格式的 Amazon Identity and Access Management（IAM）基于资源的策略，该策略附加到特定的存储桶。使用存储桶策略来向其它 Amazon Web Services 账户或 IAM 身份授予对相应存储桶及其中对象的权限。使用存储桶策略可以满足许多 S3 访问管理使用案例的要求。通过存储桶策略，您可以对存储桶访问权限进行个性化设置，以协助确保只有您已批准的身份才能访问资源并在其中执行操作。有关更多信息，请参阅 Amazon S3 的存储桶策略。

基于身份的策略

基于身份的策略或 IAM 用户策略是一种 Amazon Identity and Access Management（IAM）策略。基于身份的策略是采用 JSON 格式的策略，该策略附加到您的 Amazon 账户中的 IAM 用户、组或角色。您可以使用基于身份的策略，来向 IAM 身份授予对您的存储桶或对象的访问权限。您可以在您的账户中创建 IAM 用户、组和角色，并为其附加访问策略。然后，您可以授予对 Amazon 资源（包括 Amazon S3 资源）的访问权限。有关更多信息，请参阅 Amazon S3 基于身份的策略。

S3 访问权限管控

使用 S3 Access Grants 为企业身份目录（例如 Active Directory）中的身份以及 Amazon Identity and Access Management（IAM）身份创建对您的 Amazon S3 数据的访问授权。S3 Access Grants 可协助您大规模管理数据权限。此外，S3 Access Grants 还会记录最终用户身份以及用于访问 Amazon CloudTrail 中 S3 数据的应用程序。这提供了详细的审计历史记录，细至与 S3 存储桶中数据的所有访问权限对应的最终用户身份。有关更多信息，请参阅 使用 S3 Access Grants 管理访问权限。

访问点

对于使用 S3 上的共享数据集的应用程序，Amazon S3 接入点可简化大规模管理数据访问的事宜。接入点是附加到存储桶的命名网络端点。您可以使用接入点来大规模执行 S3 对象操作，例如上传和检索对象。一个存储桶最多可附加 10000 个接入点，对于每个接入点，您可以强制实施不同的权限和网络控制，从而让您可以详细控制对于 S3 对象的访问权限。S3 接入点可以与同一个账户或其它可信账户中的存储桶相关联。接入点策略是与底层存储桶策略一起进行评估的基于资源的策略。有关更多信息，请参阅 通过接入点管理对通用存储桶中共享数据集的访问。

访问控制列表 (ACL)

ACL 是用于确定被授权者和所授予权限的授权列表。ACL 向其它 Amazon Web Services 账户授予基本的读取或写入权限。ACL 使用特定于 Amazon S3 的 XML 架构。ACL 是一种 Amazon Identity and Access Management（IAM）策略。对象 ACL 用于管理对于对象的访问权限，而存储桶 ACL 用于管理对存储桶的访问权限。使用存储桶策略，整个存储桶只有单个策略，但可以为每个对象指定对象 ACL。我们建议您将 ACL 保持为关闭状态，除非有必须单独控制每个对象的访问权限的特殊情况。有关 ACL 的更多信息，请参阅 为您的存储桶控制对象所有权和禁用 ACL。。

> **Warning**
>
> Amazon S3 中的大多数现代使用案例不需要使用 ACL。

对象所有权

要管理对于对象的访问权限，您必须是该对象的拥有者。您可以使用对象所有权存储桶级别设置，来控制上传到存储桶的对象的所有权。此外，使用对象所有权来开启 ACL。默认情况下，对象所有权设为强制存储桶拥有者设置，并且所有 ACL 均处于关闭状态。关闭 ACL 后，存储桶拥有者拥有存储桶中的所有对象，并独占管理对数据的访问权限。为了管理访问权限，存储桶拥有者使用策略或其它访问管理工具（ACL 除外）。有关更多信息，请参阅 为您的存储桶控制对象所有权和禁用 ACL。。

有关 Amazon S3 访问控制的更全面指南和其它最佳实践，请参阅 Amazon S3 中的访问控制。

# Amazon S3 中的数据保护

除了 Amazon 全球基础设施提供的恢复能力之外，Amazon S3 还提供了多种功能，有助于保护数据免遭意外删除或区域故障影响。

S3 复制

可以使用实时复制来启用跨 Amazon S3 存储桶自动以异步方式复制对象。为对象复制配置的存储桶可由相同 Amazon Web Services 账户 或不同账户拥有。您可以将对象复制到单个目标存储桶或多个目标存储桶。目标存储桶可以位于不同的 Amazon Web Services 区域，也可以与源存储桶位于同一区域内。要启用失效转移控制，可以将复制配置为双向，以便在区域故障期间源存储桶和目标存储桶可以保持同步。有关更多信息，请参阅 the section called “在区域内和跨区域复制对象”。

多区域接入点和失效转移控制

Amazon S3 多区域接入点提供了一个全局端点，应用程序可以使用该端点来满足来自位于多个 Amazon Web Services 区域中的 S3 桶的请求。您可以使用多区域接入点通过单个区域中使用的相同架构构建多区域应用程序，然后在世界任何地方运行这些应用程序。多区域接入点不是通过拥挤的公共互联网发送请求，而是提供内置的网络恢复能力，加速向 Amazon S3 发送基于互联网的请求。向多区域接入点全局端点发出的应用程序请求使用 Amazon Global Accelerator，以自动通过 Amazon 全局网络路由到具有活动的路由状态且距离最近的 S3 桶。有关多区域接入点的更多信息，请参阅the section called “管理多区域流量 ”。

借助 Amazon S3 多区域接入点失效转移控制，您可以在区域流量中断期间保持业务连续性，同时还可以为您的应用程序提供多区域架构以满足合规性和冗余需求。如果您的区域流量中断，您可以使用多区域接入点失效转移控制来选择 Amazon S3 多区域接入点后面的哪个 Amazon Web Services 区域将处理数据访问和存储请求。

要支持失效转移，您可以将多区域接入点设置为主动-被动配置，在正常情况下流量流向主动区域，而被动区域处于备用状态以用于失效转移。如果您通过双向复制规则启用 S3 跨区域复制（CRR），则可以在失效转移期间保持桶同步。有关失效转移控制的更多信息，请参阅the section called “失效转移配置”。

S3 版本控制

版本控制是在相同的存储桶中保留对象的多个变量的方法。对于 Amazon S3 存储桶中存储的每个对象，您可以使用版本控制功能来保存、检索和还原它们的各个版本。使用版本控制能够轻松从用户意外操作和应用程序故障中恢复数据。有关更多信息，请参阅 使用 S3 版本控制保留对象的多个版本。

S3 对象锁定

您可以使用 S3 对象锁定通过一次写入、多次读取 (WORM) 模式存储对象。使用 S3 对象锁定时，您可以在固定的时间段内或无限期地阻止删除或覆盖对象。S3 对象锁定让您可以满足需要 WORM 存储的法规要求，或只是添加一个额外的保护层来防止对象被更改和删除。有关更多信息，请参阅使用对象锁定以锁定对象。

Amazon Backup

Amazon S3 与 Amazon Backup 本机集成，后者是一项完全托管式、基于策略的服务，您可以使用它来集中定义备份策略，以保护 Amazon S3 中的数据。在定义备份策略并将 Amazon S3 资源分配给策略之后，Amazon Backup 自动创建 Amazon S3 备份，并将备份安全存储在备份计划中指定的加密备份文件库中。有关更多信息，请参阅 the section called “备份数据”。

有关如何结合使用其中某些功能来保护数据的教程，请参阅教程：使用 S3 版本控制、S3 对象锁定和 S3 复制保护 Amazon S3 上的数据免遭意外删除或应用程序错误。

> **Important**
>
> 除使用上述功能保护数据之外，我们还建议您查看 the section called “安全最佳实践”中的建议。

主题


- 在区域内和跨区域复制对象
- 使用多区域接入点管理多区域流量
- 使用 S3 版本控制保留对象的多个版本
- 使用对象锁定以锁定对象
- 备份 Amazon S3 数据


# 在区域内和跨区域复制对象

您可以使用复制来启用跨 Amazon S3 存储桶自动以异步方式复制对象。为对象复制配置的存储桶可由相同 Amazon Web Services 账户 或不同账户拥有。您可以将对象复制到单个目标存储桶或多个目标存储桶。目标存储桶可以位于不同的 Amazon Web Services 区域，也可以与源存储桶位于同一区域内。

复制有两种类型：实时复制 和按需复制。

- 实时复制：想要在向源存储桶写入新的和更新的对象的同时，自动复制这些对象，请使用实时复制。实时复制不会复制在设置复制之前就存在于存储桶中的任何对象。想要复制在设置复制之前就存在的对象，请使用按需复制。
- 按需复制：想要按需从源存储桶中复制现有对象到一个或多个目标存储桶，请使用 S3 批量复制。有关复制现有对象的更多信息，请参阅 何时使用 S3 分批复制。

实时复制有两种形式：跨区域复制（CRR）和同区域复制（SRR）。

- 跨区域复制（CRR）：可以使用 CRR 跨不同 Amazon Web Services 区域中的 S3 存储桶复制对象。有关 CRR 的更多信息，请参阅the section called “何时使用跨区域复制”。
- 同区域复制（SRR）– 可以使用 SRR 跨同一 Amazon Web Services 区域中的 Amazon S3 存储桶复制对象。有关 SRR 的更多信息，请参阅the section called “何时使用同区域复制”。

主题


- 为什么使用复制？
- 何时使用跨区域复制
- 何时使用同区域复制
- 何时使用双向复制
- 何时使用 S3 分批复制
- 工作负载要求和实时复制
- Amazon S3 复制什么内容？
- 复制的要求和注意事项
- 设置实时复制概述
- 管理或暂停实时复制
- 使用批量复制以复制现有对象
- 对复制进行问题排查
- 使用指标、事件通知和状态监控复制


## 为什么使用复制？

复制可帮助您实现以下功能：

- 复制对象，同时保留元数据 – 您可以使用复制来制作对象的副本，并保留所有元数据（例如原始对象创建时间和版本 ID）。如果您必须确保副本与源对象完全相同，则此功能非常重要。
- 将对象复制到不同的存储类 – 您可以使用复制直接将对象置于目标存储桶中的 S3 Glacier Flexible Retrieval、S3 Glacier Deep Archive 或其他存储类中。您还可以将数据复制到相同的存储类，并在目标存储桶上使用生命周期配置，以在对象老化时将其移动到较冷的存储类。
- 在不同的所有权下维护对象副本 – 无论谁拥有源对象，您都可以指示 Amazon S3 将副本的所有权更改为拥有目标存储桶的 Amazon Web Services 账户。这称为拥有者覆盖 选项。您可以使用此选项来要限制对对象副本的访问权限。
- 将对象存储在多个 Amazon Web Services 区域 – 要确保数据保存位置的地理差异，您可以在不同的 Amazon Web Services 区域 中设置多个目标存储桶。此功能可能会帮助您满足某些合规性要求。
- 在 15 分钟内复制对象 – 要在可预测的时间范围内在同一 Amazon Web Services 区域 或跨不同区域复制您的数据，您可以使用 S3 Replication Time Control（S3 RTC）。S3 RTC 在 15 分钟内复制 Amazon S3 中存储的 99.99% 的新对象（由服务等级协议提供支持）。有关更多信息，请参阅 the section called “使用 S3 Replication Time Control”。

  > **Note**
  >
  > S3 RTC 不适用于分批复制。分批复制是一项按需复制任务，可以使用 S3 批量操作进行跟踪。有关更多信息，请参阅 跟踪任务状态和完成报告。

- 同步存储桶、复制现有对象以及之前无法复制或已复制的对象 – 要同步存储桶和复制现有对象，请使用分批复制作为按需复制操作。有关何时使用分批复制的更多信息，请参阅 何时使用 S3 分批复制。
- 复制对象并失效转移到另一个 Amazon Web Services 区域中的存储桶 - 要在数据复制期间使所有元数据和对象在存储桶之间保持同步，请在配置 Amazon S3 多区域接入点失效转移控制之前使用双向复制规则。双向复制规则有助于确保在将数据写入流量失效转移到的 S3 存储桶时，该数据随后被复制回源存储桶。

## 何时使用跨区域复制

S3 跨区域复制（CRR）用于在不同 Amazon Web Services 区域中跨 Amazon S3 存储桶复制对象。CRR 可帮助您：

- 满足合规性要求 – 虽然 Amazon S3 默认跨多个地理位置较远的可用区存储数据，但是合规性要求所规定的数据存储距离可能更远。为满足这些要求，可以使用跨区域复制在远距离 Amazon Web Services 区域 之间复制数据。

- 最大限度减少延迟 – 如果客户处于两个地理位置，您可以在地理位置与用户较近的Amazon Web Services 区域中维护对象副本，从而最大限度缩短访问对象时的延迟。
- 提高操作效率 – 如果您在两个不同 Amazon Web Services 区域 中具有分析同一组对象的计算集群，则可以选择在这些区域中维护对象副本。

## 何时使用同区域复制

同区域复制（SRR）用于在同一 Amazon Web Services 区域中跨 Amazon S3 存储桶复制对象。SRR 可帮助您：

- 将日志聚合到单个存储桶 – 如果您在多个存储桶中或者跨多个账户存储日志，则可以轻松地将日志复制到区域中的单个存储桶。这样做实现了在单个位置更简单地处理日志。
- 在生产账户和测试账户之间配置实时复制 – 如果您或您的客户有使用相同数据的生产账户和测试账户，您可以在那些账户之间复制对象，同时保留对象元数据。
- 遵守数据主权法律 – 您可能需要将数据的多个副本存储在特定区域内的单独 Amazon Web Services 账户 中。当合规性法规不允许数据离开您的国家/地区时，同区域复制可帮助您自动复制关键数据。

## 何时使用双向复制

- 跨多个 Amazon Web Services 区域构建共享数据集 – 通过副本修改同步功能，您可以轻松地对于复制对象复制元数据更改，例如对象访问控制列表（ACL)、对象标签或对象锁定。如果要使所有对象和对象元数据更改保持同步，这种双向复制非常重要。在相同或不同 Amazon Web Services 区域中的两个或更多存储桶之间执行双向复制时，您可以对新的或现有的复制规则启用副本修改同步。
- 在失效转移期间跨区域保持数据同步 – 您可以直接从多区域接入点通过 S3 跨区域复制（CRR）配置双向复制规则，在 Amazon Web Services 区域中的存储桶之间同步数据。要就何时启动失效转移做出明智的决定，您还可以启用 S3 复制指标，以便监控 Amazon CloudWatch、S3 Replication Time Control（S3 RTC）或多区域接入点中的复制。
- 使应用程序具有高可用性 - 即使在区域流量中断的情况下，您也可以使用双向复制规则在数据复制期间跨存储桶保持所有元数据和对象同步。

## 何时使用 S3 分批复制

作为按需选项，分批复制将现有对象复制到不同的存储桶。与实时复制不同，这些任务可以根据需要运行。分批复制可帮助您实现以下功能：

- 复制现有对象 – 您可以使用分批复制来复制在配置同区域复制或跨区域复制之前添加到存储桶中的对象。
- 复制之前无法复制的对象 – 您可以筛选分批复制任务以尝试复制状态为 FAILED 的对象。
- 复制已经复制的对象 – 您可能需要将数据的多个副本存储在单独的 Amazon Web Services 账户 或 Amazon Web Services 区域 中。分批复制可以将现有对象复制到新添加的目标。
- 复制根据复制规则创建的对象的副本 – 复制配置在目标存储桶中创建对象的副本。对象的副本只能通过分批复制进行复制。

## 工作负载要求和实时复制

根据工作负载要求，某些类型的实时复制将比其它类型的复制更适合您的应用场景。使用下表来确定针对您的场景应该使用哪种类型的复制，以及是否需要对您的工作负载使用 S3 Replication Time Control（S3 RTC）。S3 RTC 在 15 分钟内复制 Amazon S3 中存储的 99.99% 的新对象 [由服务等级协议（SLA）提供支持]。有关更多信息，请参阅 the section called “使用 S3 Replication Time Control”。

| 工作负载要求 | S3 RTC（15 分钟 SLA） | 跨区域复制 (CRR) | 同区域复制（SRR） |
|---|---|---|---|
| 在不同 Amazon Web Services 账户之间复制对象 | 支持 | 是 | 是 |
| 在 24-48 小时内，在同一 Amazon Web Services 区域中复制对象（不受 SLA 支持） | 否 | 否 | 是 |
| 在 24-48 小时内，在不同 Amazon Web Services 区域之间复制对象（不受 SLA 支持） | 否 | 是 | 否 |
| 可预测的复制时间：由 SLA 提供支持， | 是 | 否 | 否 |

| 工作负载要求 | S3 RTC（15 分钟 SLA） | 跨区域复制 (CRR) | 同区域复制（SRR） |
| --- | --- | --- | --- |
| 可在 15 分钟内复制 99.9% 的对象 | | | |

# Amazon S3 复制什么内容？

Amazon S3 仅复制为复制配置的存储桶中的特定项目。

主题


- 使用复制配置会复制什么？
- 使用复制配置不会复制什么？


## 使用复制配置会复制什么？

默认情况下，Amazon S3 会复制以下内容：

- 添加复制配置之后创建的对象。
- 未加密的对象。
- 使用客户提供密钥（SSE-C）加密的对象，使用 Amazon S3 托管密钥（SSE-S3）或存储在 Amazon Key Management Service 中的 KMS 密钥（SSE-KMS）静态加密的对象。有关更多信息，请参阅 the section called “复制加密对象”。
- 从源对象到副本的对象元数据。有关将元数据从副本复制到源对象的信息，请参阅 使用副本修改同步复制元数据更改。
- 仅限存储桶拥有者有权读取其对象和访问控制列表（ACL）的源存储存储桶中的对象。

  有关资源所有权的更多信息，请参阅 Amazon S3 存储桶和对象所有权。
- 对象 ACL 更新（但源存储桶和目标存储桶不是由相同账户拥有时指示 Amazon S3 更改副本所有权的情况除外）。

  有关更多信息，请参阅 更改副本拥有者。

  在 Amazon S3 能够使两个 ACL 同步之前，可能需要花一些时间。这一所有权变更仅适用于在向存储桶添加复制配置之后创建的对象。
- 对象标签（如果有）。

- S3 对象锁定保留信息（如果有）。

  如果 Amazon S3 复制应用了保留信息的对象，它会将相同的保留控制功能应用于您的副本，从而替换在目标存储桶上配置的默认保留期。如果未对您源存储桶中的对象应用保留控制功能，并且您复制到设置了默认保留期的目标存储桶，则目标存储桶的默认保留期将应用于对象副本。有关更多信息，请参阅 使用对象锁定以锁定对象。

删除操作对复制操作有何影响

如果您从源存储桶中删除对象，则默认情况下会执行以下操作：

- 如果您发出 DELETE 请求而未指定对象版本 ID，Amazon S3 会添加一个删除标记。Amazon S3 将按如下所示处理该删除标记：
  - 如果您使用的是最新版本的复制配置（即在复制配置规则中指定 `Filter` 元素），Amazon S3 默认不会复制该删除标记。但是，您可以将删除标记复制添加到非基于标记的规则。有关更多信息，请参阅 在存储桶之间复制删除标记。
  - 如果您未指定 `Filter` 元素，则 Amazon S3 将假定复制配置为版本 V1，并复制用户操作产生的删除标记。但是，如果 Amazon S3 因生命周期操作删除了对象，则删除标记不会复制到目标存储桶。
- 如果您在 `DELETE` 请求中指定一个要删除的对象版本 ID，Amazon S3 会在源存储桶中删除该对象版本。但不会将删除操作复制到目标存储桶中。换句话说，它不会从目标存储桶中删除同一对象版本。这会防止恶意删除数据。

## 使用复制配置不会复制什么？

默认情况下，Amazon S3 不复制以下内容：

- 源存储桶中作为另一个复制规则所建副本的对象。例如，假设您配置的复制中，存储桶 A 是源，存储桶 B 是目标。现在假设您添加另一个复制配置，其中存储桶 B 是源，而存储桶 C 是目标。在这种情况下，存储桶 B 中作为存储桶 A 中对象的副本的对象不会复制到存储桶 C。

  要复制属于副本的对象，请使用分批复制。请通过 复制现有对象 了解有关配置分批复制的更多信息。
- 源存储桶中已复制到其他目标的对象。例如，如果您在现有复制配置中更改目标存储桶，则 Amazon S3 不会再次复制对象。

要复制之前已复制的对象，请使用分批复制。请通过 复制现有对象 了解有关配置分批复制的更多信息。

- 批处理复制不支持重新复制从目标存储桶中使用对象的版本 ID 删除的对象。要重新复制这些对象，您可以使用分批复制任务将源对象复制到位。将这些对象复制到位会在源存储桶中创建对象的新版本，并自动启动到目标的复制。有关如何使用分批复制的更多信息，请参阅使用分批操作复制对象的示例。
- 默认情况下，从不同的 Amazon Web Services 账户 进行复制时，添加到源存储桶的删除标记不会被复制。

  有关如何复制删除标记的更多信息，请参阅 在存储桶之间复制删除标记。
- 存储在 S3 Glacier Flexible Retrieval、S3 Glacier Deep Archive、S3 Intelligent-Tiering Archive Access 或 S3 Intelligent-Tiering Deep Archive Access 存储类或层中的对象。在还原这些对象并将它们复制到不同的存储类之前，您无法复制它们。

  要了解有关 S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 的更多信息，请参阅极少访问的对象的存储类。

  有关 S3 Intelligent-Tiering 的更多信息，请参阅使用 Amazon S3 Intelligent-Tiering 管理存储成本。
- 源存储存储桶中存储桶拥有者没有足够权限进行复制的对象。

  有关对象拥有者如何向存储桶拥有者授予权限的信息，请参阅在授予上传对象的跨账户权限的同时，确保存储桶拥有者拥有完全控制权。
- 对存储桶级别子资源进行的更新。

  例如，如果您更改生命周期配置或向源存储桶添加通知配置，则这些更改不会应用于目标存储桶。此功能使您可以在源存储桶和目标存储桶中具有不同的配置。
- 由生命周期配置执行的操作。

  例如，如果仅对源存储桶启用了生命周期配置，则 Amazon S3 会为过期对象创建删除标记，但不会复制这些标记。如果您希望对源存储桶和目标存储桶应用相同的生命周期配置，请对这两个存储桶启用相同的生命周期配置。有关生命周期配置的更多信息，请参阅 管理对象的生命周期。
- 当您在实时复制中使用基于标签的复制规则时，必须在 `PutObject` 操作中使用匹配的复制规则标签来标记新对象。否则，将不会复制对象。如果在 `PutObject` 操作后标记了对象，也不会复制这些对象。

  要复制在 `PutObject` 操作之后标记的对象，您必须使用 S3 批量复制。有关分批复制的更多信息，请参阅 复制现有对象。

# 复制的要求和注意事项

Amazon S3 复制具有以下要求：

- 源存储桶拥有者必须已为其账户启用源和目标 Amazon Web Services 区域。目标存储桶拥有者必须已为其账户启用目标区域。

  有关启用和禁用 Amazon Web Services 区域的更多信息，请参阅《Amazon 账户管理 参考指南》中的 Specify which Amazon Web Services 区域 your account can use。
- 源存储桶和目标存储桶必须均已启用版本控制。有关版本控制的更多信息，请参阅 使用 S3 版本控制保留对象的多个版本。
- Amazon S3 必须有权代表您将对象从源存储桶复制到目标存储桶。有关这些权限的更多信息，请参阅 为实时复制设置权限。
- 如果源存储桶的拥有者不拥有该存储桶中的对象，则对象拥有者必须使用对象访问控制列表（ACL）对该存储桶拥有者授予 READ 和 READ_ACP 权限。有关更多信息，请参阅 访问控制列表 (ACL) 概述。
- 如果源存储桶已启用 S3 对象锁定，目标存储桶也必须启用 S3 对象锁定。

  要在启用了对象锁定的存储桶上启用复制，您必须使用 Amazon Command Line Interface、REST API 或 Amazon SDK。有关更多一般信息，请参阅 使用对象锁定以锁定对象。

  > **Note**
  >
  > 您必须在用于设置复制的 Amazon Identity and Access Management (IAM) 角色中授予对源 S3 存储桶的两项新权限。这两项新权限是 `s3:GetObjectRetention` 和 `s3:GetObjectLegalHold`。如果这个角色有 `s3:Get*` 权限，则它已经满足要求了。有关更多信息，请参阅 为实时复制设置权限。

有关更多信息，请参阅 设置实时复制概述。

如果您要在跨账户方案（其中，源存储桶和目标存储桶由不同的 Amazon Web Services 账户拥有）中设置复制配置，则需要满足以下附加要求：

- 目标存储桶的拥有者必须使用存储桶策略向源存储桶的拥有者授予复制对象的权限。有关更多信息，请参阅 在源存储桶和目标存储桶由不同的 Amazon Web Services 账户 拥有时授予权限。
- 目标存储桶不能配置为申请方付款存储桶。有关更多信息，请参阅 使用申请方付款通用存储桶进行存储传输和使用。

# 复制的注意事项

在创建复制配置之前，请注意以下注意事项。

主题


- 生命周期配置和对象副本
- 版本控制配置和复制配置
- 将 S3 复制与 S3 Intelligent-Tiering 结合使用
- 日志记录配置和复制配置
- CRR 和目标区域
- S3 批量复制
- S3 Replication Time Control


## 生命周期配置和对象副本

Amazon S3 复制对象所需的时间取决于对象大小。对于大型对象，可能需要几个小时。虽然可能需要一段时间之后副本才能出现在目标存储桶中，但创建副本所需的时间与创建源存储桶中的对应对象所需的时间相同。如果您对目标存储桶启用了生命周期配置，生命周期规则遵循对象的原始创建时间，而不是副本在目标存储桶中可用的时间。

复制配置需要启用版本控制的存储桶。在存储桶上启用版本控制时，请注意以下几点：

- 如果您具有对象过期生命周期配置，在启用版本控制后，请添加 `NonCurrentVersionExpiration` 策略以保持与启用版本控制之前相同的永久删除行为。
- 如果具有转换生命周期配置，则在启用版本控制后，考虑添加 `NonCurrentVersionTransition` 策略。

## 版本控制配置和复制配置

对存储桶配置复制时，源存储桶和目标存储桶都必须启用版本控制。对源存储桶和目标存储桶启用版本控制并对源存储桶配置复制后，您会遇到以下问题：

- 如果您尝试对源存储桶禁用版本控制，则 Amazon S3 会返回错误。您必须先删除复制配置，然后才能对源存储桶禁用版本控制。
- 如果您对目标存储桶禁用版本控制，则复制会失败。源对象的复制状态为 `FAILED`。

### 将 S3 复制与 S3 Intelligent-Tiering 结合使用

S3 Intelligent-Tiering 是一种存储类，旨在通过自动将数据移动到最具成本效益的访问层来优化存储成本。每月只需支付少量的对象监控和自动化费用，S3 Intelligent-Tiering 即可监控访问模式并将未访问的对象移动到成本较低的访问层。

使用 S3 批量复制来复制存储在 S3 Intelligent-Tiering 中的对象或调用 CopyObject 或 UploadPartCopy 将构成访问。在这些情况下，复制操作的源对象是分层的。

有关 S3 Intelligent-Tiering 的更多信息，请参阅使用 Amazon S3 Intelligent-Tiering 管理存储成本。

### 日志记录配置和复制配置

如果 Amazon S3 将日志传送到已启用复制的存储桶，它将复制日志对象。

如果对源存储桶或目标存储桶启用了服务器访问日志或 Amazon CloudTrail 日志，Amazon S3 将在这些日志中包含复制相关的请求。例如，Amazon S3 将记录它复制的每个对象。

### CRR 和目标区域

Amazon S3 跨区域复制（CRR）用于在不同 Amazon Web Services 区域 中跨 S3 存储桶复制对象。根据您的业务需求或成本考虑，您可能选择了区域作为目标存储桶。例如，区域间数据传输费用因您所选的区域而异。

假设您选择了美国东部（弗吉尼亚州北部）(us-east-1) 作为源存储桶的区域。如果您选择了美国西部（俄勒冈州）(us-west-2) 作为目标存储桶的区域，则您支付的费用将比选择美国东部（俄亥俄州）(us-east-2) 区域时更多。有关定价信息，请参阅 Amazon S3 定价中的“数据传输定价”。

同区域复制 (SRR) 不会产生相关的数据传输费用。

### S3 批量复制

有关批量复制的注意事项的信息，请参阅 S3 分批复制注意事项。

### S3 Replication Time Control

有关 S3 Replication Time Control（S3 RTC）的最佳实践和注意事项的信息，请参阅 S3 RTC 的最佳实践和准则。

# 设置实时复制概述

> **Note**
>
> 在您设置复制之前就存在的对象将不会自动复制。换句话说，Amazon S3 不以回溯方式复制对象。要复制在复制配置之前创建的对象，请使用 S3 分批复制。有关配置批量复制的更多信息，请参阅复制现有对象。

要启用实时复制，即同区域复制（SRR）或跨区域复制（CRR），请向源存储桶添加复制配置。该配置会指示 Amazon S3 按照指定的方式复制对象。在复制配置中，您必须提供以下内容：

- 目标存储桶 – 您希望 Amazon S3 将对象复制到的存储桶。
- 要复制的对象 – 可以复制源存储桶中的所有对象或对象的子集。通过在配置中提供一个键名前缀和/或一个或多个对象标签，可标识子集。

  例如，如果您配置复制规则，仅复制键名前缀为 `Tax/` 的对象，则 Amazon S3 仅复制键为 `Tax/doc1` 或 `Tax/doc2` 之类的对象。但它不复制具有键 `Legal/doc3` 的对象。如果您同时指定前缀和一个或多个标签，则 Amazon S3 仅复制具有特定键前缀和这些标签的对象。
- Amazon Identity and Access Management（IAM）角色 – Amazon S3 代入此 IAM 角色以代表您复制对象。有关创建此 IAM 角色和管理权限的更多信息，请参阅为实时复制设置权限。

除了这些最低要求，您还可以选择以下选项：

- 副本存储类 – 默认情况下，Amazon S3 使用与源对象相同的存储类来存储对象副本。您可以为副本指定其他存储类。
- 副本所有权 – Amazon S3 假定对象副本继续由源对象的拥有者拥有。因此，在复制对象时，它还会复制对应的对象访问控制列表 (ACL) 或 S3 对象拥有权设置。如果源存储桶和目标存储桶由不同的 Amazon Web Services 账户拥有，您可以配置复制以将副本的拥有者更改为拥有目标存储桶的 Amazon Web Services 账户。有关更多信息，请参阅 the section called “更改副本拥有者”。

可以使用 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 Amazon S3 REST API 配置复制。有关如何设置复制的详细演练，请参阅the section called “复制演练”。

Amazon S3 提供了 REST API 操作来支持设置复制规则。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的以下主题：

- PutBucketReplication
- GetBucketReplication
- DeleteBucketReplication

主题

- 复制配置文件元素
- 为实时复制设置权限
- 配置实时复制的示例

## 复制配置文件元素

Amazon S3 以 XML 形式存储复制配置。如果您通过 Amazon S3 REST API 以编程方式配置复制，则可以在此 XML 文件中指定复制配置的不同元素。如果您通过 Amazon Command Line Interface（Amazon CLI）配置复制，则可以使用 JSON 格式指定复制配置。有关 JSON 示例，请参阅the section called “复制演练”中的演练。

> **Note**
>
> 复制配置 XML 格式的最新版本为 V2。XML V2 复制配置是那些包含规则的 `<Filter>` 元素和指定 S3 Replication Time Control（S3 RTC）的规则的配置。
> 要查看复制配置版本，您可以使用 `GetBucketReplication` API 操作。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 GetBucketReplication。
> 为了向后兼容，Amazon S3 继续支持 XML V1 复制配置格式。如果您已使用 XML V1 复制配置格式，请参阅向后兼容性注意事项来了解向后兼容性注意事项。

在复制配置 XML 文件中，必须指定一个 Amazon Identity and Access Management（IAM）角色以及一个或多个规则，如下面的示例所示：

```
<ReplicationConfiguration>
    <Role>IAM-role-ARN</Role>
    <Rule>
        ...
    </Rule>
    <Rule>
         ...
    </Rule>
```

```
    ...
</ReplicationConfiguration>
```

Amazon S3 无法在未经您的权限的情况下复制对象。可以使用在复制配置中指定的 IAM 角色向 Amazon S3 授予权限。Amazon S3 担任此 IAM 角色以代表您复制对象。您必须先向 IAM 角色授予必要的权限。有关管理权限的更多信息，请参阅 为实时复制设置权限。

在以下场景下，只在复制配置中添加一个规则：

- 您希望复制所有对象。
- 您希望只复制对象的一个子集。通过在规则中添加一个筛选条件，可标识对象子级。在该筛选条件中，指定对象键前缀、标签或二者的组合，来标识要向其应用规则的对象子集。筛选条件指向与您指定的确切值相匹配的对象。

如果要复制不同的对象子集，请在复制配置中添加多个规则。在每个规则中，指定一个用于选择不同子集的筛选条件。例如，您可能选择了键前缀为 `tax/` 或 `document/` 的复制对象。要做到这一点，您需要添加两个规则，一个规则指定 `tax/` 键前缀筛选条件，另一个指定 `document/` 键前缀。有关对象键前缀的更多信息，请参阅使用前缀组织对象。

以下各节提供了更多信息。

主题

- 基本规则配置
- 可选：指定筛选条件
- 其他目标配置
- 复制配置示例
- 向后兼容性注意事项

### 基本规则配置

每个规则必须包含规则的状态和优先级。规则还必须指示是否复制删除标记。

- `<Status>` 元素通过使用值 `Enabled` 或 `Disabled` 来指示是启用还是禁用规则。如果规则处于禁用状态，则 Amazon S3 不会执行规则中指定的操作。
- `<Priority>` 元素指示当两个或更多复制规则冲突时哪个规则优先。Amazon S3 将尝试根据所有复制规则复制对象。但是，如果同一目标存储桶有两个或更多规则，则将根据具有最高优先级的规则复制对象。数字越大，优先级越高。

- <DeleteMarkerReplication> 元素通过使用值 Enabled 或 Disabled 来指示是否复制删除标记。

在 <Destination> 元素配置中，必须提供您希望 Amazon S3 将对象复制到其中的一个或多个目标存储桶的名称。

以下示例显示针对 V2 规则的最低要求。为了向后兼容，Amazon S3 仍继续支持 XML V1 格式。有关更多信息，请参阅 向后兼容性注意事项。

```
...
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled-or-Disabled</Status>
        <Filter>
            <Prefix></Prefix>
        </Filter>
        <Priority>integer</Priority>
        <DeleteMarkerReplication>
           <Status>Enabled-or-Disabled</Status>
        </DeleteMarkerReplication>
        <Destination>
           <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
        </Destination>
    </Rule>
    <Rule>
         ...
    </Rule>
     ...
...
```

您也可以指定其他配置选项。例如，您可能选择了将一个存储类用于对象副本，将另一个存储类用于源对象。

可选：指定筛选条件

要选择规则应用于的对象子集，请添加一个可选筛选条件。可按对象键前缀、对象标签或二者的组合进行筛选。如果您同时按键前缀和对象标签进行筛选，Amazon S3 会使用逻辑 AND 运算符组合这些筛选条件。换句话说，规则会应用于同时具有特定键前缀和特定标签的对象子集。

根据对象键前缀进行筛选

要指定具有基于对象键前缀的筛选条件的规则，请使用以下 XML。对于每个规则，只能指定一个前缀。

```
<Rule>
    ...
    <Filter>
        <Prefix>key-prefix</Prefix>
    </Filter>
    ...
</Rule>
...
```

根据对象标签进行筛选

要指定具有基于对象标签的筛选条件的规则，请使用以下 XML。可以指定一个或多个对象标签。

```
<Rule>
    ...
    <Filter>
        <And>
            <Tag>
                <Key>key1</Key>
                <Value>value1</Value>
            </Tag>
            <Tag>
                <Key>key2</Key>
                <Value>value2</Value>
            </Tag>
             ...
        </And>
    </Filter>
    ...
</Rule>
...
```

使用键前缀和对象标签进行筛选

要指定组合了键前缀和对象标签的规则筛选条件，请使用以下 XML。您需要将这些筛选条件包含在 <And> 父元素中。Amazon S3 会执行逻辑 AND 运算以组合这些筛选条件。换句话说，规则会应用于同时具有特定键前缀和特定标签的对象子集。

```
<Rule>
```

```
    ...
    <Filter>
        <And>
            <Prefix>key-prefix</Prefix>
            <Tag>
                <Key>key1</Key>
                <Value>value1</Value>
            </Tag>
            <Tag>
                <Key>key2</Key>
                <Value>value2</Value>
            </Tag>
             ...
    </Filter>
    ...
</Rule>
...
```

> **Note**
>
> - 如果您指定了一条带有空 <Filter> 元素的规则，则该规则将应用于您存储桶中的所有对象。
> - 当您在实时复制中使用基于标签的复制规则时，必须在 PutObject 操作中使用匹配的复制规则标签来标记新对象。否则，将不会复制对象。如果在 PutObject 操作后标记了对象，也不会复制这些对象。
>
>   要复制在 PutObject 操作之后标记的对象，您必须使用 S3 批量复制。有关分批复制的更多信息，请参阅 复制现有对象。

### 其他目标配置

在目标配置中，指定您希望 Amazon S3 将对象复制到其中的存储桶。您可以设置配置以将对象从一个源存储桶复制到一个或更多个目标存储桶。

```
...
<Destination>
    <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
</Destination>
...
```

您可在 <Destination> 元素中添加以下选项。

主题

- 指定存储类
- 添加多个目标存储桶
- 为涉及多个目标存储桶的每个复制规则指定不同的参数
- 更改副本所有权
- 启用 S3 Replication Time Control
- 复制使用 Amazon KMS 通过服务器端加密所创建的对象

### 指定存储类

您可以为对象副本指定存储类。默认情况下，Amazon S3 使用源对象的存储类来创建对象副本，如以下示例所示。

```
...
<Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
       <StorageClass>storage-class</StorageClass>
</Destination>
...
```

### 添加多个目标存储桶

您可以在单个复制配置中添加多个目标存储桶，如下所示。

```
...
<Rule>
    <ID>Rule-1</ID>
    <Status>Enabled-or-Disabled</Status>
    <Priority>integer</Priority>
    <DeleteMarkerReplication>
       <Status>Enabled-or-Disabled</Status>
    </DeleteMarkerReplication>
    <Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket1</Bucket>
    </Destination>
</Rule>
<Rule>
    <ID>Rule-2</ID>
```

```
    <Status>Enabled-or-Disabled</Status>
    <Priority>integer</Priority>
    <DeleteMarkerReplication>
       <Status>Enabled-or-Disabled</Status>
    </DeleteMarkerReplication>
    <Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket2</Bucket>
    </Destination>
</Rule>
...
```

为涉及多个目标存储桶的每个复制规则指定不同的参数

在单个复制配置中添加多个目标存储桶时，可以为每个复制规则指定不同的参数，如下所示。

```
...
<Rule>
    <ID>Rule-1</ID>
    <Status>Enabled-or-Disabled</Status>
    <Priority>integer</Priority>
    <DeleteMarkerReplication>
       <Status>Disabled</Status>
    </DeleteMarkerReplication>
      <Metrics>
    <Status>Enabled</Status>
    <EventThreshold>
      <Minutes>15</Minutes>
    </EventThreshold>
  </Metrics>
    <Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket1</Bucket>
    </Destination>
</Rule>
<Rule>
    <ID>Rule-2</ID>
    <Status>Enabled-or-Disabled</Status>
    <Priority>integer</Priority>
    <DeleteMarkerReplication>
       <Status>Enabled</Status>
    </DeleteMarkerReplication>
      <Metrics>
    <Status>Enabled</Status>
    <EventThreshold>
      <Minutes>15</Minutes>
```

```
    </EventThreshold>
  </Metrics>
  <ReplicationTime>
    <Status>Enabled</Status>
    <Time>
      <Minutes>15</Minutes>
    </Time>
  </ReplicationTime>
    <Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket2</Bucket>
    </Destination>
</Rule>
...
```

更改副本所有权

当源存储桶和目标存储桶由不同账户拥有时，您可以将副本的所有权更改为拥有目标存储桶的 Amazon Web Services 账户。为此，请添加 <AccessControlTranslation> 元素。这个元素将获取值 Destination。

```
...
<Destination>
   <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
   <Account>destination-bucket-owner-account-id</Account>
   <AccessControlTranslation>
       <Owner>Destination</Owner>
   </AccessControlTranslation>
</Destination>
...
```

如果您没有将 <AccessControlTranslation> 元素添加到复制配置中，则副本由拥有源对象的同一 Amazon Web Services 账户 拥有。有关更多信息，请参阅 更改副本拥有者。

启用 S3 Replication Time Control

您可以在复制配置中启用 S3 Replication Time Control（S3 RTC）。S3 RTC 在几秒钟内复制大多数对象，并在 15 分钟内复制 99.99% 的对象（由服务等级协议提供支持）。

> **Note**
>
> <EventThreshold> 和 <Time> 元素只接受值 <Minutes>15</Minutes>。

```
...
<Destination>
  <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
  <Metrics>
    <Status>Enabled</Status>
    <EventThreshold>
      <Minutes>15</Minutes>
    </EventThreshold>
  </Metrics>
  <ReplicationTime>
    <Status>Enabled</Status>
    <Time>
      <Minutes>15</Minutes>
    </Time>
  </ReplicationTime>
</Destination>
...
```

有关更多信息，请参阅 使用 S3 Replication Time Control 满足合规性要求。有关 API 示例，请参阅《Amazon Simple Storage Service API 参考》中的 PutBucketReplication。

复制使用 Amazon KMS 通过服务器端加密所创建的对象

您的源存储桶可能包含一些对象，它们是使用 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）创建的。默认情况下，Amazon S3 不复制这些对象。您可以有选择地指示 Amazon S3 复制这些对象。要做到这一点，首先通过添加 <SourceSelectionCriteria> 元素显式选择此功能。然后提供 Amazon KMS key（对于目标存储桶的 Amazon Web Services 区域），用于加密对象副本。以下示例显示了如何指定这些元素。

```
...
<SourceSelectionCriteria>
  <SseKmsEncryptedObjects>
    <Status>Enabled</Status>
  </SseKmsEncryptedObjects>
</SourceSelectionCriteria>
<Destination>
  <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
  <EncryptionConfiguration>
    <ReplicaKmsKeyID>Amazon KMS key ID to use for encrypting object replicas</
ReplicaKmsKeyID>
  </EncryptionConfiguration>
</Destination>
```

```
...
```

有关更多信息，请参阅 复制加密对象（SSE-S3、SSE-KMS、DSSE-KMS、SSE-C）。

复制配置示例

首先，您可以根据需要将以下复制配置示例添加到存储桶。

> **Important**
>
> 要向存储桶添加复制配置，您必须具有 `iam:PassRole` 权限。此权限允许您传递向 Amazon S3 授予复制权限的 IAM 角色。通过提供复制配置 XML 中 `<Role>` 元素中使用的 Amazon 资源名称（ARN），可指定 IAM 角色。有关更多信息，请参阅《IAM 用户指南》中的向用户授予将角色传递给 Amazon Web Services 服务的权限。

Example 1：包含一个规则的复制配置

以下基本复制配置指定一个规则。该规则指定 Amazon S3 可担任的一个 IAM 角色以及用于对象副本的目标存储桶。`<Status>` 的元素值 `Enabled` 指示该规则是有效的。

```
<?xml version="1.0" encoding="UTF-8"?>
<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Role>arn:aws:iam::account-id:role/role-name</Role>
  <Rule>
    <Status>Enabled</Status>

    <Destination>
      <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>
  </Rule>
</ReplicationConfiguration>
```

要选择要复制的对象子集，可添加一个筛选条件。在以下配置中，该筛选条件指定一个对象键前缀。此规则将应用于其键名中带有前缀 *Tax/* 的对象。

```
<?xml version="1.0" encoding="UTF-8"?>
<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Role>arn:aws:iam::account-id:role/role-name</Role>
  <Rule>
```

```
    <Status>Enabled</Status>
    <Priority>1</Priority>
    <DeleteMarkerReplication>
       <Status>string</Status>
    </DeleteMarkerReplication>

    <Filter>
       <Prefix>Tax/</Prefix>
    </Filter>

    <Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>

  </Rule>
</ReplicationConfiguration>
```

如果您指定 <Filter> 元素，则还必须包含 <Priority> 和 <DeleteMarkerReplication> 元素。在此示例中，由于只有一个规则，因此您为 <Priority> 元素设置的值无关紧要。

在以下配置中，筛选条件指定一个前缀和两个标签。规则将应用于具有指定键前缀和标签的对象子级。具体来说，规则将应用于在键名称中具有 *Tax/* 前缀并具有两个指定对象标签的对象。在此示例中，由于只有一个规则，因此您为 <Priority> 元素设置的值无关紧要。

```
<?xml version="1.0" encoding="UTF-8"?>
<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Role>arn:aws:iam::account-id:role/role-name</Role>
  <Rule>
    <Status>Enabled</Status>
    <Priority>1</Priority>
    <DeleteMarkerReplication>
       <Status>string</Status>
    </DeleteMarkerReplication>

    <Filter>
        <And>
          <Prefix>Tax/</Prefix>
          <Tag>
             <Tag>
                <Key>tagA</Key>
                <Value>valueA</Value>
             </Tag>
          </Tag>
```

```
            <Tag>
               <Tag>
                  <Key>tagB</Key>
                  <Value>valueB</Value>
               </Tag>
            </Tag>
         </And>

    </Filter>

    <Destination>
        <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>

  </Rule>
</ReplicationConfiguration>
```

可以为对象副本指定存储类，如下所示：

```
<?xml version="1.0" encoding="UTF-8"?>

<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Role>arn:aws:iam::account-id:role/role-name</Role>
  <Rule>
    <Status>Enabled</Status>
    <Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
       <StorageClass>storage-class</StorageClass>
    </Destination>
  </Rule>
</ReplicationConfiguration>
```

您可以指定 Amazon S3 支持的任何存储类。

Example 2：包含两个规则的复制配置

Example

在以下复制配置中，规则指定以下内容：

- 每个规则按不同的键前缀进行筛选，以便每个规则应用于不同的对象子集。在此示例中，Amazon S3 复制键名为 *Tax/doc1.pdf* 和 *Project/project1.txt* 的对象，但是它不复制键名为 *PersonalDoc/documentA* 的对象。

- 尽管两个规则都指定 <Priority> 元素的值，但由于规则应用于两个不同的对象集，因此规则优先级无关紧要。下一示例将说明应用规则优先级时会发生的情况。
- 第二个规则为对象副本指定 S3 Standard-IA 存储类。Amazon S3 对这些对象副本使用指定的存储类。

```
<?xml version="1.0" encoding="UTF-8"?>

<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Role>arn:aws:iam::account-id:role/role-name</Role>
  <Rule>
    <Status>Enabled</Status>
    <Priority>1</Priority>
    <DeleteMarkerReplication>
       <Status>string</Status>
    </DeleteMarkerReplication>
    <Filter>
        <Prefix>Tax</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Destination>
      <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>
     ...
  </Rule>
 <Rule>
    <Status>Enabled</Status>
    <Priority>2</Priority>
    <DeleteMarkerReplication>
       <Status>string</Status>
    </DeleteMarkerReplication>
    <Filter>
        <Prefix>Project</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Destination>
      <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
     <StorageClass>STANDARD_IA</StorageClass>
    </Destination>
     ...
  </Rule>
```

```
</ReplicationConfiguration>
```

Example 3：包含两个具有重叠前缀的规则的复制配置

在此配置中，两个规则指定具有重叠键前缀 *star/* 和 *starship/* 的筛选条件。两个规则应用于键名称为 *starship-x* 的对象。在此示例中，Amazon S3 使用规则优先级确定要应用哪个规则。数字越大，优先级越高。

```
<ReplicationConfiguration>

  <Role>arn:aws:iam::account-id:role/role-name</Role>

  <Rule>
    <Status>Enabled</Status>
    <Priority>1</Priority>
    <DeleteMarkerReplication>
       <Status>string</Status>
    </DeleteMarkerReplication>
    <Filter>
        <Prefix>star</Prefix>
    </Filter>
    <Destination>
      <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>
  </Rule>
  <Rule>
    <Status>Enabled</Status>
    <Priority>2</Priority>
    <DeleteMarkerReplication>
       <Status>string</Status>
    </DeleteMarkerReplication>
    <Filter>
        <Prefix>starship</Prefix>
    </Filter>
    <Destination>
      <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>
  </Rule>
</ReplicationConfiguration>
```

Example 4：示例演练

有关演练示例，请参阅 配置实时复制的示例。

有关复制配置的 XML 结构的更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 PutBucketReplication。

向后兼容性注意事项

复制配置 XML 格式的最新版本为 V2。XML V2 复制配置是那些包含规则的 <Filter> 元素和指定 S3 Replication Time Control（S3 RTC）的规则的配置。

要查看复制配置版本，您可以使用 GetBucketReplication API 操作。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 GetBucketReplication。

为了向后兼容，Amazon S3 继续支持 XML V1 复制配置格式。如果您已使用 XML V1 复制配置格式，请考虑以下影响向后兼容性的问题：

- 复制配置 XML V2 格式包含规则的 <Filter> 元素。通过 <Filter> 元素，您可以指定基于对象键前缀和/或标签的对象筛选条件，以确定规则要应用于的范围。复制配置 XML V1 格式支持仅基于键前缀的筛选。在这种情况下，您直接添加 <Prefix> 元素作为 <Rule> 元素的子元素，如以下示例所示：

```
<?xml version="1.0" encoding="UTF-8"?>
<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Role>arn:aws:iam::account-id:role/role-name</Role>
  <Rule>
    <Status>Enabled</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>

  </Rule>
</ReplicationConfiguration>
```

- 当您从源存储桶中删除对象而不指定对象版本 ID 时，Amazon S3 会添加一个删除标记。如果使用复制配置 XML V1 格式，Amazon S3 仅复制因用户操作产生的删除标记。换句话说，Amazon S3 仅在用户删除对象时才复制删除标记。如果 Amazon S3 移除到期的对象（作为生命周期操作的一部分），Amazon S3 不会复制删除标记。

在复制配置 XML V2 格式中，可以为非基于标签的规则启用删除标记复制。有关更多信息，请参阅在存储桶之间复制删除标记。

## 为实时复制设置权限

在 Amazon S3 中设置实时复制时，您必须获取必要的权限，如下所示：

- Amazon S3 需要代表您复制对象的权限。您通过创建一个 Amazon Identity and Access Management（IAM）角色，然后在复制配置中指定该角色，来授予这些权限。
- 当源存储桶与目标存储桶不是由相同账户拥有时，目标存储桶的拥有者还必须向源存储桶拥有者授予存储副本的权限。

主题

- 设置创建复制规则的权限
- 创建 IAM 角色
- 在源存储桶和目标存储桶由不同的 Amazon Web Services 账户 拥有时授予权限
- 更改副本所有权
- 授予 S3 批量操作的权限

### 设置创建复制规则的权限

您将用于创建复制规则的 IAM 用户或角色需要相应的权限，才能为单向或双向复制创建复制规则。如果用户或角色没有这些权限，您将无法创建复制规则。有关更多信息，请参阅《IAM 用户指南》中的 IAM 身份。

用户或角色需要执行以下操作：

- `iam:AttachRolePolicy`
- `iam:CreatePolicy`
- `iam:CreateServiceLinkedRole`
- `iam:PassRole`
- `iam:PutRolePolicy`
- `s3:GetBucketVersioning`
- `s3:GetObjectVersionAcl`

- s3:GetObjectVersionForReplication
- s3:GetReplicationConfiguration
- s3:PutReplicationConfiguration

以下是包含这些操作的示例 IAM 策略。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetAccessPoint",
                "s3:GetAccountPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:ListAccessPoints",
                "s3:ListAllMyBuckets",
                "s3:PutReplicationConfiguration",
                "s3:GetReplicationConfiguration",
                "s3:GetBucketVersioning",
                "s3:GetObjectVersionForReplication",
                "s3:GetObjectVersionAcl",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetObjectVersion",
                "s3:GetBucketOwnershipControls",
                "s3:PutBucketOwnershipControls",
                "s3:GetObjectLegalHold",
                "s3:GetObjectRetention",
                "s3:GetBucketObjectLockConfiguration"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket1-*",
                "arn:aws:s3:::amzn-s3-demo-bucket2-*/*"
            ]
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "s3:List*AccessPoint*",
                "s3:GetMultiRegion*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:Get*",
                "iam:CreateServiceLinkedRole",
                "iam:CreateRole",
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::*:role/service-role/s3*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:List*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:PutRolePolicy",
                "iam:CreatePolicy"
              ],
            "Resource": [
                "arn:aws:iam::*:policy/service-role/s3*",
                "arn:aws:iam::*:role/service-role/s3*"
            ]
        }
    ]
}
```

## 创建 IAM 角色

默认情况下，所有 Amazon S3 资源（存储桶、对象和相关子资源）都是私有的，只有资源拥有者可以访问相应的资源。Amazon S3 需要权限才能从源存储桶读取和复制对象。您通过创建一个 IAM 角色，并在复制配置中指定该角色，来授予这些权限。

本节解释了附加到此 IAM 角色的信任策略和最低所需权限策略。示例演练提供创建 IAM 角色的分步说明。有关更多信息，请参阅 配置实时复制的示例。

信任策略确定哪些主体身份可以担任此 IAM 角色。权限策略指定 IAM 角色可在什么条件下对哪些资源执行哪些操作。

- 以下示例显示了一个信任策略，您在其中将 Amazon S3 标识为可担任此角色的 Amazon Web Services 服务主体。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

- 以下示例显示了一个信任策略，您在其中将 Amazon S3 和 S3 批量操作标识为可担任此角色的服务主体。如果您正在创建批量复制任务，则使用此方法。有关更多信息，请参阅 为新的复制规则或目标创建批量复制任务。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service": [
              "s3.amazonaws.com",
              "batchoperations.s3.amazonaws.com"
            ]
         },
         "Action":"sts:AssumeRole"
```

```
      }
   ]
}
```

有关 IAM 角色的更多信息，请参阅《IAM 用户指南》中的 IAM 角色。

- 以下示例显示了权限策略，您在其中向 IAM 角色授予代表您执行复制任务的权限。当 Amazon S3 担任角色时，它将具有您在此策略中指定的权限。在此策略中，*amzn-s3-demo-source-bucket* 是源存储桶，*amzn-s3-demo-destination-bucket* 是目标存储桶。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetReplicationConfiguration",
            "s3:ListBucket"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObjectVersionForReplication",
            "s3:GetObjectVersionAcl",
            "s3:GetObjectVersionTagging"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:ReplicateObject",
            "s3:ReplicateDelete",
            "s3:ReplicateTags"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      }
```

```
    ]
}
```

此权限策略授予执行以下操作的权限：

- `s3:GetReplicationConfiguration` 和 `s3:ListBucket` – 对 *amzn-s3-demo-source-bucket* 存储桶执行这些操作的权限可让 Amazon S3 检索复制配置和列出存储桶内容。（当前权限模型需要 `s3:ListBucket` 权限来访问删除标记）。
- `s3:GetObjectVersionForReplication` 和 `s3:GetObjectVersionAcl` – 针对所有对象授予的这些操作的权限允许 Amazon S3 获取特定对象版本和对象关联的访问控制列表 (ACL)。
- `s3:ReplicateObject` 和 `s3:ReplicateDelete` – *amzn-s3-demo-destination-bucket* 存储桶中所有对象上的这些操作的权限允许 Amazon S3 将对象或删除标记复制到目标存储桶。有关删除标记的信息，请参阅 删除操作对复制操作有何影响。

  > **Note**
  >
  > 对 *amzn-s3-demo-destination-bucket* 存储桶执行 `s3:ReplicateObject` 操作的权限还支持复制元数据，例如对象标签和 ACL。因此，您无需显式授予执行 `s3:ReplicateTags` 操作的权限。

- `s3:GetObjectVersionTagging` – 对 *amzn-s3-demo-source-bucket* 存储桶中的对象执行此操作的权限可让 Amazon S3 读取用于复制的对象标签。有关对象标签的更多信息，请参阅 使用标签对存储进行分类。如果 Amazon S3 没有 `s3:GetObjectVersionTagging` 权限，它将复制对象，而不是对象标签。

有关 Amazon S3 操作的列表，请参阅《Service Authorization Reference》中的 Actions, resources, and condition keys for Amazon S3。

有关按 S3 资源类型对 S3 API 操作的权限的更多信息，请参阅 Amazon S3 API 操作所需的权限。

> **Important**
>
> 拥有 IAM 角色的 Amazon Web Services 账户 必须拥有其向 IAM 角色授予的操作的权限。例如，假定源存储桶包含由另一个 Amazon Web Services 账户 拥有的对象。对象的拥有者必须通过对象的访问控制列表（ACL），向拥有 IAM 角色的 Amazon Web Services 账户显式授予必要的权限。否则，Amazon S3 无法访问这些对象，因而这些对象的复制将失败。有关 ACL 权限的信息，请参阅 访问控制列表 (ACL) 概述。

此处介绍的权限与最低复制配置相关。如果您选择添加可选复制配置，则必须向 Amazon S3 授予其它权限：

- 要复制加密的对象，还需要授予必要的 Amazon Key Management Service（Amazon KMS）密钥权限。有关更多信息，请参阅 the section called “复制加密对象”。
- 要将对象锁定与复制功能结合使用，您必须在用于设置复制的 Amazon Identity and Access Management（IAM）角色中，授予对源 S3 存储桶的两项额外的权限。这两项额外的权限是 `s3:GetObjectRetention` 和 `s3:GetObjectLegalHold`。如果角色已有 `s3:Get*` 权限声明，则该声明已满足要求。有关更多信息，请参阅 the section called “将对象锁定与 S3 复制结合使用”。

在源存储桶和目标存储桶由不同的 Amazon Web Services 账户 拥有时授予权限

当源存储桶和目标存储桶不是由相同的账户拥有时，目标存储桶的拥有者还必须添加一个存储桶策略，来向源存储桶的拥有者授予执行复制操作的权限，如下面的示例所示。在此示例策略中，*amzn-s3-demo-destination-bucket* 是目标存储桶。

还可以使用 Amazon S3 控制台来自动为您生成此存储桶策略。有关更多信息，请参阅启用从源存储桶接收复制的对象。

> **Note**
>
> 角色的 ARN 格式可能看起来不同。如果使用控制台创建角色，则 ARN 格式为 `arn:aws:iam::`*account-ID*`:role/service-role/`*role-name*。如果使用 Amazon CLI 创建角色，则 ARN 格式为 `arn:aws:iam::`*account-ID*`:role/`*role-name*。有关更多信息，请参阅《IAM 用户指南》中的 IAM 角色。

```
{
   "Version":"2012-10-17",
   "Id":"PolicyForDestinationBucket",
   "Statement":[
      {
         "Sid":"Permissions on objects",
         "Effect":"Allow",
         "Principal":{
            "AWS":"arn:aws:iam::source-bucket-account-ID:role/service-role/source-account-IAM-role"
         },
```

```
         "Action":[
            "s3:ReplicateDelete",
            "s3:ReplicateObject"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      },
      {
         "Sid":"Permissions on bucket",
         "Effect":"Allow",
         "Principal":{
            "AWS":"arn:aws:iam::source-bucket-account-ID:role/service-role/source-
account-IAM-role"
         },
         "Action": [
            "s3:List*",
            "s3:GetBucketVersioning",
            "s3:PutBucketVersioning"
         ],
         "Resource":"arn:aws:s3::amzn-s3-demo-destination-bucket"
      }
   ]
}
```

有关示例，请参阅针对不同账户中的存储桶配置复制。

如果向源存储桶中的对象添加标签，请注意以下事项：

- 如果源存储桶拥有者向 Amazon S3 授予 `s3:GetObjectVersionTagging` 和 `s3:ReplicateTags` 操作的权限来复制对象标签（通过 IAM 角色），则 Amazon S3 将复制标签以及对象。有关 IAM 角色的信息，请参阅 创建 IAM 角色。
- 如果目标存储桶的所有者不希望复制标签，则他们可以向目标存储桶策略添加以下语句来显式拒绝 `s3:ReplicateTags` 操作的权限。在此策略中，*amzn-s3-demo-destination-bucket* 是目标存储桶。

```
...
   "Statement":[
      {
         "Effect":"Deny",
         "Principal":{
            "AWS":"arn:aws:iam::source-bucket-account-id:role/service-role/source-
account-IAM-role"
         },
```

```
        "Action":"s3:ReplicateTags",
        "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      }
   ]
...
```

> **Note**
>
> - 如果要复制加密的对象，还必须授予必要的 Amazon Key Management Service（Amazon KMS）密钥权限。有关更多信息，请参阅 the section called “复制加密对象”。
> - 要将对象锁定与复制功能结合使用，您必须在用于设置复制的 Amazon Identity and Access Management（IAM）角色中，授予对源 S3 存储桶的两项额外的权限。这两项额外的权限是 `s3:GetObjectRetention` 和 `s3:GetObjectLegalHold`。如果角色已有 `s3:Get*` 权限声明，则该声明已满足要求。有关更多信息，请参阅 the section called “将对象锁定与 S3 复制结合使用”。

启用从源存储桶接收复制的对象

您可以快速生成所需的策略，以便启用通过 Amazon S3 控制台从源存储桶接收复制的对象，而不是手动将上述策略添加到目标存储桶中。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 在存储桶列表中，选择要用作目标存储桶的存储桶。
4. 选择 Management（管理）选项卡，然后向下滚动到 Replication rules（复制规则）。
5. 对于 Actions（操作），选择 Receive replicated objects（接收复制的对象）。

   按照提示进行操作并输入源存储桶账户的 Amazon Web Services 账户 ID，然后选择生成策略。控制台将生成 Amazon S3 存储桶策略和 KMS 密钥策略。
6. 要将此策略添加到现有存储桶策略中，请选择 Apply settings（应用设置），或者选择 Copy（复制）以手动复制更改。
7. （可选）在 Amazon Key Management Service 控制台中将 Amazon KMS 策略复制到所需的 KMS 密钥策略。

更改副本所有权

当源存储桶和目标存储桶由不同的 Amazon Web Services 账户 拥有时，您可以指示 Amazon S3 将副本的所有权更改为拥有目标存储桶的 Amazon Web Services 账户。有关拥有者覆盖的更多信息，请参阅更改副本拥有者。

授予 S3 批量操作的权限

S3 批量复制为您提供了一种复制以下对象的方法：

- 在复制配置设立之前已经存在的对象
- 以前已复制的对象
- 复制失败的对象

当在新的复制配置中创建第一个规则时，或者通过 Amazon S3 控制台将新目标添加到现有配置时，您可以创建一次性批量复制任务。也可以通过创建批量操作任务来启动现有复制配置的批量复制。

有关批量复制 IAM 角色和策略示例，请参阅配置 IAM 角色以进行 S3 批量复制。

## 配置实时复制的示例

以下各示例提供的分步演练介绍了如何为常见使用案例配置实时复制。

> **Note**
>
> 实时复制指同区域复制 (SRR) 和跨区域复制 (CRR)。实时复制不会复制在设置复制之前就存在于存储桶中的任何对象。想要复制在设置复制之前就存在的对象，请使用按需复制。要同步存储桶和按需复制现有对象，请参阅复制现有对象。

这些示例演示了如何使用 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）和 Amazon SDK（展示了适用于 Java 的 Amazon SDK 和适用于 .NET 的 Amazon SDK 示例）创建复制配置。

有关安装和配置 Amazon CLI 的信息，请参阅《Amazon Command Line Interface 用户指南》中的以下主题：

- 开始使用 Amazon CLI
- Configure the Amazon CLI – 必须设置至少一个配置文件。如果要探讨跨账户方案，请设置两个配置文件。

有关 Amazon SDK 的更多信息，请参阅适用于 Java 的 Amazon SDK 和适用于 .NET 的 Amazon SDK。

> **Tip**
>
> 有关演示如何使用实时复制来复制数据的分步教程，请参阅教程：使用 S3 复制在 Amazon Web Services 区域内和区域之间复制数据。

主题


- 针对同一账户中的存储桶配置复制
- 针对不同账户中的存储桶配置复制
- 使用 S3 Replication Time Control 满足合规性要求
- 复制加密对象（SSE-S3、SSE-KMS、DSSE-KMS、SSE-C）
- 使用副本修改同步复制元数据更改
- 在存储桶之间复制删除标记


## 针对同一账户中的存储桶配置复制

实时复制是跨相同或不同 Amazon Web Services 区域中的通用存储桶自动、异步复制对象。实时复制会将源存储桶中新创建的对象和对象更新复制到一个或多个目标存储桶。有关更多信息，请参阅 在区域内和跨区域复制对象。

配置复制时，需要向源存储桶添加复制规则。复制规则定义要复制的源存储桶对象和存储已复制对象的目标存储桶。您可以创建一条规则，以复制存储桶中的所有对象或具有特定键名前缀和/或一个或多个对象标签的对象子集。目标存储桶与源存储桶可以位于同一 Amazon Web Services 账户 中，也可以位于不同的账户中。

如果您指定要删除的对象版本 ID，Amazon S3 会在源存储桶中删除该对象版本。但不会将删除操作复制到目标存储桶中。换句话说，它不会从目标存储桶中删除同一对象版本。这会防止恶意删除数据。

当您将复制规则添加到存储桶后，默认情况下将启用复制规则，使该规则在您保存它后立即启动。

在此示例中，您为由同一 Amazon Web Services 账户拥有的源存储桶和目标存储桶设置实时复制。提供了使用 Amazon S3 控制台、Amazon Command Line Interface (Amazon CLI) 以及 适用于 Java 的 Amazon SDK 和 适用于 .NET 的 Amazon SDK 的示例。

先决条件

在使用以下过程之前，请确保您已设置了复制所需的权限，具体取决于源存储桶和目标存储桶是由相同的账户还是不同的账户拥有。有关更多信息，请参阅 the section called “设置权限”。

> **Note**
>
> - 如果要复制加密的对象，还必须授予必要的 Amazon Key Management Service（Amazon KMS）密钥权限。有关更多信息，请参阅 the section called “复制加密对象”。
> - 要将对象锁定与复制功能结合使用，您必须在用于设置复制的 Amazon Identity and Access Management（IAM）角色中，授予对源 S3 存储桶的两项额外的权限。这两项额外的权限是 `s3:GetObjectRetention` 和 `s3:GetObjectLegalHold`。如果角色已有 `s3:Get*` 权限声明，则该声明已满足要求。有关更多信息，请参阅 the section called “将对象锁定与 S3 复制结合使用”。

使用 S3 控制台

要在目标存储桶与源存储桶位于同一 Amazon Web Services 账户中时配置复制规则，请按照以下步骤操作。

如果目标存储桶与源存储桶位于不同的账户中，您必须向目标存储桶添加存储桶策略以便为源存储桶账户的所有者授予复制目标存储桶中的对象的权利。有关更多信息，请参阅 在源存储桶和目标存储桶由不同的 Amazon Web Services 账户 拥有时授予权限。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在存储桶列表中，选择您想要的存储桶的名称。
4. 选择管理选项卡，向下滚动到复制规则，然后选择创建复制规则。
5. 在复制规则配置部分的复制规则名称下，输入规则的名称，以帮助以后识别该规则。该名称是必填项，并且它在存储桶内必须是唯一的。
6. 在状态下，已启用默认情况下处于选中状态。已启用的规则将在您保存它后立即开始工作。如果您想以后再启用该规则，请选择已禁用。
7. 如果存储桶具有现有的复制规则，系统会指示您为规则设置优先级。必须为规则设置优先级，以避免因在多个规则的范围内包含对象而引起冲突。如果规则重叠，Amazon S3 会使用规则优先级确

定要应用哪个规则。数字越大，优先级越高。有关规则优先级的更多信息，请参阅 复制配置文件元素。

8. 在源存储桶下，您可以通过以下选项设置复制源：

   - 要复制整个存储桶，请选择应用到存储桶中的所有对象。
   - 要复制具有相同前缀的所有对象，请选择 Limit the scope of this rule using one or more filters (使用一个或多个筛选条件限制此规则的范围)。这会将复制限制为名称以您指定的前缀（例如 `pictures`）开头的所有对象。在前缀框中输入前缀。

     > **Note**
     >
     > 如果您输入的前缀是文件夹名称，则必须使用 /（正斜杠）作为最后一个字符（例如，`pictures/`）。

   - 要复制具有一个或多个对象标签的所有对象，请选择添加标签，然后在框中输入键值对。重复上述过程以添加其他标签。您可以组合前缀和标签。有关对象标签的更多信息，请参阅 使用标签对存储进行分类。

   新的复制配置 XML 模式支持前缀和标签筛选以及规则优先级划分。有关新架构的更多信息，请参阅 向后兼容性注意事项。如需详细了解在用户界面后台工作的 Amazon S3 API 所使用的 XML，请参阅 复制配置文件元素。新架构被描述为复制配置 XML V2。

9. 在目标下，选择您希望 Amazon S3 将对象复制到的存储桶。

   > **Note**
   >
   > 目标存储桶的数量仅限于给定分区中的 Amazon Web Services 区域 的数量。分区是一组区域。Amazon 目前有三个分区：`aws`（标准区域）、`aws-cn`（中国区域）和 `aws-us-gov`（Amazon GovCloud (US) 区域）。要请求提高目标存储桶限额，您可以使用服务限额。

   - 要复制到您的账户中的一个或多个存储桶，请选取选择此账户中的存储桶，然后输入或浏览目标存储桶。
   - 要复制到其他 Amazon Web Services 账户中的一个或多个存储存储桶，请选择指定另一个账户中的存储存储桶，然后输入目标存储存储桶账户 ID 和存储桶名称。

如果目标存储桶与源存储桶位于不同的账户中，您必须向目标存储桶添加存储桶策略以便为源存储桶账户的所有者授予复制对象的权限。有关更多信息，请参阅 在源存储桶和目标存储桶由不同的 Amazon Web Services 账户 拥有时授予权限。

（可选）如果要帮助标准化目标存储桶中的新对象的所有权，请选择将对象所有权更改为目标存储桶拥有者。有关此选项的更多信息，请参阅 为您的存储桶控制对象所有权和禁用 ACL。。

> **Note**
>
> 如果未对目标存储桶启用版本控制，您将收到包含 Enable versioning（启用版本控制）按钮的警告。请选择此按钮可对存储桶启用版本控制。

10. 设置 Amazon Identity and Access Management (IAM) 角色，Amazon S3 可以代入该角色以代表您复制对象。

    要设置 IAM 角色，请在 IAM 角色部分中，从 IAM 角色下拉列表中选择以下任一选项：

    - 我们强烈建议您选择 Create new role (创建新角色)，让 Amazon S3 为您创建一个新的 IAM 角色。当您保存该规则后，将为 IAM 角色生成一个与您选择的源和目标存储桶匹配的新策略。
    - 您可以选择使用现有的 IAM 角色。在这种情况下，您必须选择一个角色，该角色会授予 Amazon S3 必要的权限以进行复制。如果该角色未按照您的复制规则授予 Amazon S3 足够的权限，复制会失败。

    > **Important**
    >
    > 将复制规则添加到存储桶时，您必须具有 `iam:PassRole` 权限才能传递授予 Amazon S3 复制权限的 IAM 角色。有关更多信息，请参阅《IAM 用户指南》中的向用户授予将角色传递给 Amazon Web Services 服务的权限。

11. 要复制源存储桶中使用具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）进行加密的对象，请在加密下选择复制已使用 Amazon KMS 加密的对象。在用于加密目标对象的 Amazon KMS 密钥下，是您允许复制使用的源密钥。预设情况下，所有源 KMS 密钥都包含在内。要缩小 KMS 密钥选择范围，可以选择别名或密钥 ID。

    使用您未选择的 Amazon KMS keys 加密的对象不会进行复制。系统为您选择一个 KMS 密钥或一组 KMS 密钥，您可以自行选择 KMS 密钥。有关将 Amazon KMS 用于复制的信息，请参阅 复制加密对象（SSE-S3、SSE-KMS、DSSE-KMS、SSE-C）。

> **Important**
>
> 在复制使用 Amazon KMS 加密的对象时，Amazon KMS 请求速率会在源区域中加倍并在目标区域中增加相同的量。之所以对 Amazon KMS 的调用率会增加，是因为数据是使用您为复制目标区域定义的 KMS 密钥进行重新加密的。对于每个区域的每个调用账户，Amazon KMS 设定了一个请求速率限额。有关限额默认值的信息，请参阅《Amazon Key Management Service 开发人员指南》中的 Amazon KMS 限额 – 每秒请求数：因情况而异。
>
> 如果您在复制期间的当前 Amazon S3 PUT 对象请求速率超过您账户的默认 Amazon KMS 速率限制的一半，则建议您请求提高您的 Amazon KMS 请求速率限额。要请求提高，请在联系我们处的 Amazon Web Services 支持 中心内创建一个案例。例如，假设您当前的 PUT 对象请求速率为每秒 1000 个请求并且您使用 Amazon KMS 加密对象。在此情况下，建议您让 Amazon Web Services 支持 将您在源区域和目标区域中的 Amazon KMS 速率限制提高到每秒 2500 个请求（如果不同），以确保不受 Amazon KMS 的限制。
>
> 要查看源存储桶中的 PUT 对象请求速率，请查看 Amazon S3 的 Amazon CloudWatch 请求指标中的 `PutRequests`。有关查看 CloudWatch 指标的信息，请参阅使用 S3 控制台

如果选择复制使用 Amazon KMS 加密的对象，请执行以下操作：

- 在用于加密目标对象的 Amazon KMS key 下，通过以下方式之一指定您的 KMS 密钥：
  - 要从可用的 KMS 密钥列表中进行选择，请选择从您的 Amazon KMS keys 密钥中进行选择，并从可用密钥的列表中选择您的 KMS 密钥。

    Amazon 托管式密钥 (`aws/s3`) 和您的客户自主管理型密钥都显示在此列表中。有关客户自主管理型密钥的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的客户密钥和 Amazon 密钥。
  - 要输入 KMS 密钥 Amazon 资源名称（ARN），请选择输入 Amazon KMS key ARN，然后在显示的字段中输入您的 KMS 密钥 ARN。这会加密目标存储桶中的副本。您可以在 IAM 控制台中的加密密钥下方找到您的 KMS 密钥的 ARN。
  - 要在 Amazon KMS 控制台中创建新的客户自主管理型密钥，请选择创建 KMS 密钥。

    有关创建 Amazon KMS key 的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的创建密钥。

> **Important**
>
> 您只能使用与存储桶所在相同 Amazon Web Services 区域 中启用的 KMS 密钥。选择从您的 KMS 密钥中选择时，S3 控制台对于每个区域仅列出 100 个 KMS 密钥。如果您在同一区域中有超过 100 个 KMS 密钥，您只会在 S3 控制台中看到前 100 个 KMS 密钥。要使用控制台中未列出的 KMS 密钥，请选择输入 Amazon KMS key ARN，然后输入您的 KMS 密钥 ARN。
>
> 在 Amazon S3 中使用 Amazon KMS key 进行服务器端加密时，您必须选择对称加密 KMS 密钥。Amazon S3 仅支持对称加密 KMS 密钥，而不支持非对称 KMS 密钥。有关更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的确定对称和非对称 KMS 密钥。

有关创建 Amazon KMS key 的更多信息，请参阅 Amazon Key Management Service 开发人员指南中的创建密钥。有关将 Amazon KMS 与 Amazon S3 结合使用的更多信息，请参阅使用具有 Amazon KMS 密钥的服务器端加密（SSE-KMS）。

12. 在目标存储类下，如果要将数据复制到目标中的特定存储类，请选择更改复制对象的存储类。然后选择要用于目标中的已复制对象的存储类。如果您不选择此选项，已复制对象的存储类将与原始对象的类相同。
13. 设置其他复制选项时，您具有以下附加选项：

    - 如果要在复制配置中启用 S3 Replication Time Control（S3 RTC），请选择复制时间控制（RTC）。有关此选项的更多信息，请参阅 使用 S3 Replication Time Control 满足合规性要求。
    - 如果要在复制配置中启用 S3 复制指标，请选择 Replication metrics and events（复制指标和事件）。有关更多信息，请参阅使用指标、事件通知和状态监控复制。
    - 如果要在复制配置中启用删除标记复制，请选择 Delete marker replication (删除标记复制)。有关更多信息，请参阅在存储桶之间复制删除标记。
    - 如果要在复制配置中启用 Amazon S3 副本修改同步，请选择 Replica modification sync (副本修改同步)。有关更多信息，请参阅使用副本修改同步复制元数据更改。

> **Note**
>
> 使用 S3 RTC 或 S3 复制指标时，需要支付额外费用。

14. 要完成，请选择 Save (保存)。
15. 在您保存规则之后，可以通过选择您的规则并选择 Edit rule (编辑规则) 来编辑、启用、禁用或删除您的规则。

使用 Amazon CLI

要使用 Amazon CLI 在源存储桶和目标存储桶由同一 Amazon Web Services 账户 拥有时设置复制，请执行以下操作：

- 创建源存储桶和目标存储桶。
- 对存储桶启用版本控制。
- 创建 Amazon Identity and Access Management（IAM）角色来向 Amazon S3 授予复制对象的权限。
- 将复制配置添加到源存储桶。

要验证您的设置，请对其进行测试。

当源存储桶和目标存储桶由同一 Amazon Web Services 账户拥有时设置复制

1. 为 Amazon CLI 设置凭证配置文件。此示例使用配置文件名称 `acctA`。有关设置凭证配置文件和使用命名配置文件的信息，请参阅《Amazon Command Line Interface 用户指南》中的 Configuration and credential file settings。

> **Important**
>
> 用于此示例的配置文件必须具有必要的权限。例如，在复制配置中，指定 Amazon S3 可担任的 IAM 角色。仅当您使用的配置文件具有 `iam:PassRole` 权限时，才能执行此操作。有关更多信息，请参阅《IAM 用户指南》中的向用户授予权限以将角色传递给 Amazon Web Services 服务。如果您使用管理员凭证创建命名配置文件，则可执行所有任务。

2. 使用以下 Amazon CLI 命令创建一个源存储桶，并对其启用版本控制。要使用这些命令，请将 *user input placeholders* 替换为您自己的信息。

   以下 create-bucket 命令在美国东部（弗吉尼亚州北部）(us-east-1) 区域中创建一个名为 *amzn-s3-demo-source-bucket* 的源存储桶。

   ```
   aws s3api create-bucket \
   --bucket amzn-s3-demo-source-bucket \
   --region us-east-1 \
   --profile acctA
   ```

   以下 put-bucket-versioning 命令对于 *amzn-s3-demo-source-bucket* 存储桶启用 S3 版本控制：

   ```
   aws s3api put-bucket-versioning \
   --bucket amzn-s3-demo-source-bucket \
   --versioning-configuration Status=Enabled \
   --profile acctA
   ```

3. 使用以下 Amazon CLI 命令创建一个目标存储桶，并对其启用版本控制。要使用这些命令，请将 *user input placeholders* 替换为您自己的信息。

   > **Note**
   >
   > 要在源存储桶和目标存储桶位于同一 Amazon Web Services 账户中时设置复制配置，请对源存储桶和目标存储桶使用相同的配置文件。此示例使用 acctA。
   > 要在这些存储桶由不同 Amazon Web Services 账户拥有时对复制配置进行测试，请为每个账户指定不同的配置文件。例如，对目标存储桶使用 acctB 配置文件。

   以下 create-bucket 命令在美国西部（俄勒冈州）(us-west-2) 区域中创建一个名为 *amzn-s3-demo-destination-bucket* 的目标存储桶。

   ```
   aws s3api create-bucket \
   --bucket amzn-s3-demo-destination-bucket \
   --region us-west-2 \
   --create-bucket-configuration LocationConstraint=us-west-2 \
   --profile acctA
   ```

以下 put-bucket-versioning 命令对于 *amzn-s3-demo-destination-bucket* 存储桶启用 S3 版本控制：

```
aws s3api put-bucket-versioning \
--bucket amzn-s3-demo-destination-bucket \
--versioning-configuration Status=Enabled \
--profile acctA
```

4. 创建一个 IAM 角色。您将在稍后添加到源存储桶的复制配置中指定此角色。Amazon S3 担任此角色以代表您复制对象。分两个步骤创建 IAM 角色：

   - 创建角色。
   - 将权限策略附加到角色。

   a. 创建 IAM 角色。

      i. 复制以下信任策略，并将其保存到本地计算机上当前目录中一个名为 s3-role-trust-policy.json 的文件。此策略向 Amazon S3 服务主体授予担任该角色的权限。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

      ii. 运行以下命令以创建角色。

```
$ aws iam create-role \
--role-name replicationRole \
--assume-role-policy-document file://s3-role-trust-policy.json  \
--profile acctA
```

   b. 将权限策略附加到角色。

i. 复制以下权限策略，并将其保存到本地计算机上当前目录中一个名为 `s3-role-permissions-policy.json` 的文件。此策略授予对各种 Amazon S3 存储桶和对象操作的权限。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObjectVersionForReplication",
            "s3:GetObjectVersionAcl",
            "s3:GetObjectVersionTagging"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket",
            "s3:GetReplicationConfiguration"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:ReplicateObject",
            "s3:ReplicateDelete",
            "s3:ReplicateTags"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      }
   ]
}
```

> **Note**
>
> - 如果要复制加密的对象，还必须授予必要的 Amazon Key Management Service（Amazon KMS）密钥权限。有关更多信息，请参阅 the section called “复制加密对象”。
> - 要将对象锁定与复制功能结合使用，您必须在用于设置复制的 Amazon Identity and Access Management（IAM）角色中，授予对源 S3 存储桶的两项额外的权限。这两项额外的权限是 `s3:GetObjectRetention` 和 `s3:GetObjectLegalHold`。如果角色已有 `s3:Get*` 权限声明，则该声明已满足要求。有关更多信息，请参阅 the section called “将对象锁定与 S3 复制结合使用”。

ii. 运行以下命令以创建策略并将其附加到角色。将 *user input placeholders* 替换为您自己的信息。

```
$ aws iam put-role-policy \
--role-name replicationRole \
--policy-document file://s3-role-permissions-policy.json \
--policy-name replicationRolePolicy \
--profile acctA
```

5. 将复制配置添加到源存储桶。

a. 尽管 Amazon S3 API 要求您将复制配置指定为 XML 形式，但 Amazon CLI 要求您将复制配置指定为 JSON 形式。将以下 JSON 保存到计算机上本地目录中一个名为 `replication.json` 文件。

```
{
  "Role": "IAM-role-ARN",
  "Rules": [
    {
      "Status": "Enabled",
      "Priority": 1,
      "DeleteMarkerReplication": { "Status": "Disabled" },
      "Filter" : { "Prefix": "Tax"},
      "Destination": {
        "Bucket": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
      }
    }
```

```
  ]
}
```

b. 通过使用您自己的信息替换 *amzn-s3-demo-destination-bucket* 和 *IAM-role-ARN* 的值来更新 JSON。保存更改。

c. 运行以下 put-bucket-replication 命令来将复制配置添加到源存储桶。请务必提供源存储桶名称：

```
$ aws s3api put-bucket-replication \
--replication-configuration file://replication.json \
--bucket amzn-s3-demo-source-bucket \
--profile acctA
```

要检索复制配置，请使用 get-bucket-replication 命令：

```
$ aws s3api get-bucket-replication \
--bucket amzn-s3-demo-source-bucket \
--profile acctA
```

6. 通过执行以下步骤，在 Amazon S3 控制台中测试设置：

a. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。

b. 在左侧导航窗格中，选择存储桶。在通用存储桶列表中，选择源存储桶。

c. 在源存储桶中，创建一个名为 *Tax* 的文件夹。

d. 将示例对象添加到源存储桶中的 *Tax* 文件夹。

> **Note**
>
> Amazon S3 复制对象所需的时间量取决于对象的大小。有关如何查看复制状态的信息，请参阅获取复制状态信息。

在##存储桶中，确认以下几点：

- 该 Amazon S3 已复制对象。
- 这些对象是副本。在对象的属性选项卡上，向下滚动至对象管理概述部分。在管理配置下，查看复制状态下的值。确保此值设置为 REPLICA。

- 副本归源存储桶账户拥有。可以在对象的权限选项卡上验证对象所有权。

  如果源存储桶和目标存储桶由不同的账户拥有，则可以添加可选配置，来指示 Amazon S3 将副本所有权更改为目标账户。有关示例，请参阅如何更改副本拥有者。

### 使用 Amazon SDK

以下代码示例分别使用 适用于 Java 的 Amazon SDK 和 适用于 .NET 的 Amazon SDK 向存储桶添加复制配置。

> **Note**
>
> - 如果要复制加密的对象，还必须授予必要的 Amazon Key Management Service（Amazon KMS）密钥权限。有关更多信息，请参阅 the section called “复制加密对象”。
> - 要将对象锁定与复制功能结合使用，您必须在用于设置复制的 Amazon Identity and Access Management（IAM）角色中，授予对源 S3 存储桶的两项额外的权限。这两项额外的权限是 `s3:GetObjectRetention` 和 `s3:GetObjectLegalHold`。如果角色已有 `s3:Get*` 权限声明，则该声明已满足要求。有关更多信息，请参阅 the section called “将对象锁定与 S3 复制结合使用”。

#### Java

以下示例向存储桶添加复制配置，然后检索并验证该配置。有关创建和测试有效示例的说明，请参阅《适用于 Java 的 Amazon SDK 开发人员指南》中的 Getting Started。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.identitymanagement.AmazonIdentityManagement;
import
 com.amazonaws.services.identitymanagement.AmazonIdentityManagementClientBuilder;
import com.amazonaws.services.identitymanagement.model.CreateRoleRequest;
import com.amazonaws.services.identitymanagement.model.PutRolePolicyRequest;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3Client;
import com.amazonaws.services.s3.model.BucketReplicationConfiguration;
import com.amazonaws.services.s3.model.BucketVersioningConfiguration;
```

```
import com.amazonaws.services.s3.model.CreateBucketRequest;
import com.amazonaws.services.s3.model.DeleteMarkerReplication;
import com.amazonaws.services.s3.model.DeleteMarkerReplicationStatus;
import com.amazonaws.services.s3.model.ReplicationDestinationConfig;
import com.amazonaws.services.s3.model.ReplicationRule;
import com.amazonaws.services.s3.model.ReplicationRuleStatus;
import com.amazonaws.services.s3.model.SetBucketVersioningConfigurationRequest;
import com.amazonaws.services.s3.model.StorageClass;
import com.amazonaws.services.s3.model.replication.ReplicationFilter;
import com.amazonaws.services.s3.model.replication.ReplicationFilterPredicate;
import com.amazonaws.services.s3.model.replication.ReplicationPrefixPredicate;

import java.io.IOException;
import java.util.ArrayList;
import java.util.HashMap;
import java.util.List;
import java.util.Map;

public class CrossRegionReplication {

        public static void main(String[] args) throws IOException {
                Regions clientRegion = Regions.DEFAULT_REGION;
                String accountId = "*** Account ID ***";
                String roleName = "*** Role name ***";
                String sourceBucketName = "*** Source bucket name ***";
                String destBucketName = "*** Destination bucket name ***";
                String prefix = "Tax/";

                String roleARN = String.format("arn:aws:iam::%s:%s", accountId,
 roleName);
                String destinationBucketARN = "arn:aws:s3:::" + destBucketName;

                AmazonS3 s3Client = AmazonS3Client.builder()
                                .withCredentials(new ProfileCredentialsProvider())
                                .withRegion(clientRegion)
                                .build();

                createBucket(s3Client, clientRegion, sourceBucketName);
                createBucket(s3Client, clientRegion, destBucketName);
                assignRole(roleName, clientRegion, sourceBucketName,
 destBucketName);

                try {
```

```
                        // Create the replication rule.
                        List<ReplicationFilterPredicate> andOperands = new
ArrayList<ReplicationFilterPredicate>();
                        andOperands.add(new ReplicationPrefixPredicate(prefix));

                        Map<String, ReplicationRule> replicationRules = new
HashMap<String, ReplicationRule>();
                        replicationRules.put("ReplicationRule1",
                                        new ReplicationRule()
                                                        .withPriority(0)

.withStatus(ReplicationRuleStatus.Enabled)

.withDeleteMarkerReplication(
                                                                        new
DeleteMarkerReplication().withStatus(

   DeleteMarkerReplicationStatus.DISABLED))
                                                        .withFilter(new
ReplicationFilter().withPredicate(
                                                                        new
ReplicationPrefixPredicate(prefix)))
                                                        .withDestinationConfig(new
ReplicationDestinationConfig()

.withBucketARN(destinationBucketARN)

.withStorageClass(StorageClass.Standard)));

                        // Save the replication rule to the source bucket.
                        s3Client.setBucketReplicationConfiguration(sourceBucketName,
                                        new BucketReplicationConfiguration()
                                                        .withRoleARN(roleARN)

.withRules(replicationRules));

                        // Retrieve the replication configuration and verify that
the configuration
                        // matches the rule we just set.
                        BucketReplicationConfiguration replicationConfig = s3Client

.getBucketReplicationConfiguration(sourceBucketName);
                        ReplicationRule rule =
replicationConfig.getRule("ReplicationRule1");
```

```
                        System.out.println("Retrieved destination bucket ARN: "
                                           +
rule.getDestinationConfig().getBucketARN());
                        System.out.println("Retrieved priority: " +
rule.getPriority());
                        System.out.println("Retrieved source-bucket replication rule
status: " + rule.getStatus());
                } catch (AmazonServiceException e) {
                        // The call was transmitted successfully, but Amazon S3
couldn't process
                        // it, so it returned an error response.
                        e.printStackTrace();
                } catch (SdkClientException e) {
                        // Amazon S3 couldn't be contacted for a response, or the
client
                        // couldn't parse the response from Amazon S3.
                        e.printStackTrace();
                }
        }

        private static void createBucket(AmazonS3 s3Client, Regions region, String
bucketName) {
                CreateBucketRequest request = new CreateBucketRequest(bucketName,
region.getName());
                s3Client.createBucket(request);
                BucketVersioningConfiguration configuration = new
BucketVersioningConfiguration()
                                .withStatus(BucketVersioningConfiguration.ENABLED);

                SetBucketVersioningConfigurationRequest enableVersioningRequest =
new SetBucketVersioningConfigurationRequest(
                                bucketName, configuration);
                s3Client.setBucketVersioningConfiguration(enableVersioningRequest);

        }

        private static void assignRole(String roleName, Regions region, String
sourceBucket, String destinationBucket) {
                AmazonIdentityManagement iamClient =
AmazonIdentityManagementClientBuilder.standard()
                                .withRegion(region)
                                .withCredentials(new ProfileCredentialsProvider())
                                .build();
                StringBuilder trustPolicy = new StringBuilder();
```

```
                trustPolicy.append("{\\r\\n   ");
                trustPolicy.append("\\\"Version\\\":\\\"2012-10-17\\\",\\r\\n   ");
                trustPolicy.append("\\\"Statement\\\":[\\r\\n      {\\r\\n
 ");
                trustPolicy.append("\\\"Effect\\\":\\\"Allow\\\",\\r\\n        \\
\"Principal\\\":{\\r\\n            ");
                trustPolicy.append("\\\"Service\\\":\\\"s3.amazonaws.com\\\"\\r\\n
      },\\r\\n         ");
                trustPolicy.append("\\\"Action\\\":\\\"sts:AssumeRole\\\"\\r\\n
  }\\r\\n   ]\\r\\n}");

                CreateRoleRequest createRoleRequest = new CreateRoleRequest()
                                .withRoleName(roleName)

 .withAssumeRolePolicyDocument(trustPolicy.toString());

                iamClient.createRole(createRoleRequest);

                StringBuilder permissionPolicy = new StringBuilder();
                permissionPolicy.append(
                                "{\\r\\n   \\\"Version\\\":\\\"2012-10-17\\\",\\r\\n
   \\\"Statement\\\":[\\r\\n      {\\r\\n         ");
                permissionPolicy.append(
                                "\\\"Effect\\\":\\\"Allow\\\",\\r\\n        \\
\"Action\\\":[\\r\\n             ");
                permissionPolicy.append("\\\"s3:GetObjectVersionForReplication\\\",\
\r\\n            ");
                permissionPolicy.append(
                                "\\\"s3:GetObjectVersionAcl\\\"\\r\\n         ],\\r\
\n         \\\"Resource\\\":[\\r\\n            ");
                permissionPolicy.append("\\\"arn:aws:s3:::");
                permissionPolicy.append(sourceBucket);
                permissionPolicy.append("/*\\\"\\r\\n         ]\\r\\n      },\\r\\n
     {\\r\\n         ");
                permissionPolicy.append(
                                "\\\"Effect\\\":\\\"Allow\\\",\\r\\n        \\
\"Action\\\":[\\r\\n            ");
                permissionPolicy.append(
                                "\\\"s3:ListBucket\\\",\\r\\n           \\
\"s3:GetReplicationConfiguration\\\"\\r\\n         ");
                permissionPolicy.append("],\\r\\n         \\\"Resource\\\":[\\r\\n
          \\\"arn:aws:s3:::");
                permissionPolicy.append(sourceBucket);
                permissionPolicy.append("\\r\\n         ");
```

```
                permissionPolicy
                                .append("]\\r\\n      },\\r\\n      {\\r\\n
 \\\"Effect\\\":\\\"Allow\\\",\\r\\n         ");
                permissionPolicy.append(
                                "\\\"Action\\\":[\\r\\n            \\
\"s3:ReplicateObject\\\",\\r\\n            ");
                permissionPolicy
                                .append("\\\"s3:ReplicateDelete\\\",\\r\\n
  \\\"s3:ReplicateTags\\\",\\r\\n            ");
                permissionPolicy.append("\\\"s3:GetObjectVersionTagging\\\"\\r\\n\\r
\\n         ],\\r\\n         ");
                permissionPolicy.append("\\\"Resource\\\":\\\"arn:aws:s3:::");
                permissionPolicy.append(destinationBucket);
                permissionPolicy.append("/*\\\"\\r\\n      }\\r\\n   ]\\r\\n}");

                PutRolePolicyRequest putRolePolicyRequest = new
 PutRolePolicyRequest()
                                .withRoleName(roleName)
                                .withPolicyDocument(permissionPolicy.toString())
                                .withPolicyName("crrRolePolicy");

                iamClient.putRolePolicy(putRolePolicyRequest);

        }
}
```

C#

以下 适用于 .NET 的 Amazon SDK 代码示例向存储桶添加复制配置，然后检索该配置。要使用此代码，请为存储桶提供名称，并为 IAM 角色提供 Amazon 资源名称（ARN）。有关设置和运行代码示例的信息，请参阅《适用于 .NET 的 Amazon SDK 开发人员指南》中的 Getting Started with the 适用于 .NET 的 Amazon SDK。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class CrossRegionReplicationTest
```

```
   {
       private const string sourceBucket = "*** source bucket ***";
       // Bucket ARN example - arn:aws:s3:::destinationbucket
       private const string destinationBucketArn = "*** destination bucket ARN
***";
       private const string roleArn = "*** IAM Role ARN ***";
       // Specify your bucket region (an example region is shown).
       private static readonly RegionEndpoint sourceBucketRegion =
RegionEndpoint.USWest2;
       private static IAmazonS3 s3Client;
       public static void Main()
       {
           s3Client = new AmazonS3Client(sourceBucketRegion);
           EnableReplicationAsync().Wait();
       }
       static async Task EnableReplicationAsync()
       {
           try
           {
               ReplicationConfiguration replConfig = new ReplicationConfiguration
               {
                   Role = roleArn,
                   Rules =
                       {
                           new ReplicationRule
                           {
                               Prefix = "Tax",
                               Status = ReplicationRuleStatus.Enabled,
                               Destination = new ReplicationDestination
                               {
                                   BucketArn = destinationBucketArn
                               }
                           }
                       }
               };

               PutBucketReplicationRequest putRequest = new
PutBucketReplicationRequest
               {
                   BucketName = sourceBucket,
                   Configuration = replConfig
               };
```

```
                PutBucketReplicationResponse putResponse = await
 s3Client.PutBucketReplicationAsync(putRequest);

                // Verify configuration by retrieving it.
                await RetrieveReplicationConfigurationAsync(s3Client);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
        }
        private static async Task RetrieveReplicationConfigurationAsync(IAmazonS3
 client)
        {
            // Retrieve the configuration.
            GetBucketReplicationRequest getRequest = new GetBucketReplicationRequest
            {
                BucketName = sourceBucket
            };
            GetBucketReplicationResponse getResponse = await
 client.GetBucketReplicationAsync(getRequest);
            // Print.
            Console.WriteLine("Printing replication configuration information...");
            Console.WriteLine("Role ARN: {0}", getResponse.Configuration.Role);
            foreach (var rule in getResponse.Configuration.Rules)
            {
                Console.WriteLine("ID: {0}", rule.Id);
                Console.WriteLine("Prefix: {0}", rule.Prefix);
                Console.WriteLine("Status: {0}", rule.Status);
            }
        }
    }
}
```

## 针对不同账户中的存储桶配置复制

实时复制是跨相同或不同 Amazon Web Services 区域中的存储桶自动、异步复制对象。实时复制会将源存储桶中新创建的对象和对象更新复制到一个或多个目标存储桶。有关更多信息，请参阅 在区域内和跨区域复制对象。

配置复制时，需要向源存储桶添加复制规则。复制规则定义要复制的源存储桶对象和存储已复制对象的目标存储桶。您可以创建一条规则，以复制存储桶中的所有对象或具有特定键名前缀和/或一个或多个对象标签的对象子集。目标存储桶与源存储桶可以位于同一 Amazon Web Services 账户 中，也可以位于不同的账户中。

如果您指定要删除的对象版本 ID，Amazon S3 会在源存储桶中删除该对象版本。但不会将删除操作复制到目标存储桶中。换句话说，它不会从目标存储桶中删除同一对象版本。这会防止恶意删除数据。

当您将复制规则添加到存储桶后，默认情况下将启用复制规则，使该规则在您保存它后立即启动。

当源存储桶和目标存储桶由不同 Amazon Web Services 账户拥有时设置实时复制的过程，与这两个存储桶由相同账户拥有时设置复制的过程类似。但是，当您在跨账户场景中配置复制时，会有一些区别：

- 目标存储桶拥有者必须在目标存储桶策略中，向源存储桶拥有者授予复制对象的权限。
- 如果在跨账户场景中，您要复制的对象使用了具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）进行加密，则 KMS 密钥的拥有者必须向源存储桶拥有者授予使用 KMS 密钥的权限。有关更多信息，请参阅 为跨账户方案授予其他权限。
- 默认情况下，复制的对象归源存储桶拥有者所有。在跨账户场景中，您可能希望配置复制，来将复制对象的所有权更改为目标存储桶的拥有者。有关更多信息，请参阅 更改副本拥有者。

### 当源存储桶和目标存储桶由不同 Amazon Web Services 账户 拥有时配置复制

1. 在此示例中，您将在两个不同的 Amazon Web Services 账户中创建源存储桶和目标存储桶。您必须为 Amazon CLI 设置两个凭证配置文件。此示例使用 `acctA` 和 `acctB` 作为这些配置文件名称。有关设置凭证配置文件和使用命名配置文件的信息，请参阅《Amazon Command Line Interface 用户指南》中的 Configuration and credential file settings。
2. 按照 针对同一账户中的存储桶配置复制 中的分步说明操作，进行以下更改：
   - 对于与源存储桶活动相关的所有 Amazon CLI 命令（例如，创建源存储桶、启用版本控制和创建 IAM 角色），请使用 `acctA` 配置文件。使用 `acctB` 配置文件创建目标存储桶。
   - 确保 IAM 角色的权限策略指定您为此示例创建的源存储桶和目标存储桶。

3. 在控制台中，在目标存储存储桶上添加以下存储桶策略，以允许源存储存储桶的拥有者复制对象。有关说明，请参阅使用 Amazon S3 控制台添加存储桶策略。请务必编辑该策略，即提供源存储桶拥有者的 Amazon Web Services 账户 ID、IAM 角色名称和目标存储桶名称。

> **Note**
>
> 要使用以下示例，请将 *user input placeholders* 替换为您自己的信息。将 *amzn-s3-demo-destination-bucket* 替换为目标存储桶名称。将 IAM Amazon 资源名称（ARN）中的 *source-bucket-account-ID*:role/service-role/*source-account-IAM-role* 替换为您用于此复制配置的 IAM 角色。
>
> 如果您手动创建了 IAM 服务角色，请将 IAM ARN 中的角色路径设置为 `role/service-role/`，如以下策略示例所示。有关更多信息，请参阅《IAM 用户指南》中的 IAM ARN。

```
{
   "Version":"2012-10-17",
   "Id":"",
   "Statement":[
      {
         "Sid":"Set-permissions-for-objects",
         "Effect":"Allow",
         "Principal":{
            "AWS":"arn:aws:iam::source-bucket-account-ID:role/service-role/source-account-IAM-role"
         },
         "Action":["s3:ReplicateObject", "s3:ReplicateDelete"],
         "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      },
      {
         "Sid":"Set permissions on bucket",
         "Effect":"Allow",
         "Principal":{
            "AWS":"arn:aws:iam::source-bucket-account-ID:role/service-role/source-account-IAM-role"
         },
         "Action":["s3:GetBucketVersioning", "s3:PutBucketVersioning"],
         "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket"
      }
   ]
}
```

4. （可选）如果您要复制的对象使用了 SSE-KMS 进行加密，则 KMS 密钥的拥有者必须向源存储桶拥有者授予使用 KMS 密钥的权限。有关更多信息，请参阅 为跨账户方案授予其他权限。
5. （可选）在复制中，默认情况下，源对象的拥有者拥有副本。当源存储桶和目标存储桶由不同的 Amazon Web Services 账户拥有时，您可以添加可选的配置设置，来将副本所有权更改为拥有目标存储桶的 Amazon Web Services 账户。这包括授予 `ObjectOwnerOverrideToBucketOwner` 权限。有关更多信息，请参阅 更改副本拥有者。

更改副本拥有者

在复制中，默认情况下，源对象的拥有者也拥有副本。但是，当源存储桶和目标存储桶由不同的 Amazon Web Services 账户拥有时，您可能想要更改副本所有权。例如，您可能想要更改所有权，来限制对于对象副本的访问权限。在复制配置中，可以添加可选的配置设置，来将副本所有权更改为拥有目标存储桶的 Amazon Web Services 账户。

要更改副本拥有者，请执行以下操作：

- 将拥有者覆盖 选项添加到复制配置，来指示 Amazon S3 更改副本所有权。
- 向 Amazon S3 授予更改副本所有权的 `s3:ObjectOwnerOverrideToBucketOwner` 权限。
- 在目标存储桶策略中添加支持更改副本所有权的 `s3:ObjectOwnerOverrideToBucketOwner` 权限。`s3:ObjectOwnerOverrideToBucketOwner` 权限可让目标存储桶的拥有者接受对象副本的所有权。

有关更多信息，请参阅the section called “所有权覆盖选项的注意事项”和向复制配置添加拥有者覆盖选项。有关带分步说明的有效示例，请参阅如何更改副本拥有者。

> **Important**
>
> 您可以为对象所有权使用“强制存储桶拥有者”设置，而不是使用拥有者覆盖选项。当您使用复制且源存储桶和目标存储桶由不同的 Amazon Web Services 账户拥有时，目标存储桶的存储桶拥有者可以为对象所有权使用“强制存储桶拥有者”设置，来将副本所有权更改为拥有目标存储桶的 Amazon Web Services 账户。此设置将禁用对象访问控制列表（ACL）。
> “强制存储桶拥有者”设置模拟现有的拥有者覆盖行为，而无需 `s3:ObjectOwnerOverrideToBucketOwner` 权限。在桶拥有者强制设置的情况下已复制到目标桶的所有对象都归目标桶拥有者所有。有关对象所有权的更多信息，请参阅为您的存储桶控制对象所有权和禁用 ACL。。

### 所有权覆盖选项的注意事项

当您配置所有权覆盖选项时，请注意以下几点：

- 默认情况下，源对象的拥有者也拥有副本。Amazon S3 复制对象版本及其关联的 ACL。

  如果您向复制配置中添加拥有者覆盖选项，Amazon S3 将仅复制对象版本，而不复制 ACL。此外，Amazon S3 不会复制对源对象 ACL 的任何后续更改。Amazon S3 在副本上设置 ACL，将完全控制权限授予目标存储桶拥有者。
- 当您更新复制配置来启用或禁用拥有者覆盖时，会发生以下行为：
  - 如果向复制配置添加拥有者覆盖选项：

    当 Amazon S3 复制对象版本时，它会放弃与源对象关联的 ACL。而是 Amazon S3 改为在副本上设置 ACL，将完全控制权限授予目标存储桶的拥有者。Amazon S3 不会复制对源对象 ACL 的任何后续更改。但是，此 ACL 更改不会应用于设置拥有者覆盖选项之前已复制的对象版本。设置拥有者覆盖之前所复制的源对象 ACL 上的任何更新仍将继续复制（因为对象及其副本继续具有相同的拥有者）。
  - 如果从复制配置中删除拥有者覆盖选项：

    Amazon S3 将源存储桶中出现的新对象及其关联的 ACL 复制到目标存储桶。对于删除拥有者覆盖之前已复制的对象，Amazon S3 不会复制其 ACL，因为 Amazon S3 进行的对象所有权更改仍保持有效。也就是说，对于在您设置了拥有者覆盖的情况下所复制的对象版本上的 ACL，接下来不会进行复制。

### 向复制配置添加拥有者覆盖选项

> **Warning**
>
> 仅在源存储桶和目标存储桶由不同 Amazon Web Services 账户拥有时添加拥有者覆盖选项。Amazon S3 不会检查存储桶由相同账户还是不同账户拥有。如果您在两个存储桶均由同一 Amazon Web Services 账户拥有时添加拥有者覆盖，Amazon S3 会应用拥有者覆盖。此选项向目标存储桶的拥有者授予完全权限，并且不会将后续更新复制到源对象的访问控制列表（ACL）。副本拥有者可以使用 `PutObjectAcl` 请求直接更改与副本关联的 ACL，但不能通过复制进行更改。

要指定拥有者覆盖选项，请向每个 `Destination` 元素添加以下元素：

- AccessControlTranslation 元素，指示 Amazon S3 更改副本所有权
- Account 元素，指定目标存储桶拥有者的 Amazon Web Services 账户

```
<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    ...
    <Destination>
      ...
      <AccessControlTranslation>
           <Owner>Destination</Owner>
       </AccessControlTranslation>
      <Account>destination-bucket-owner-account-id</Account>
    </Destination>
  </Rule>
</ReplicationConfiguration>
```

以下复制配置示例指示 Amazon S3 将键前缀为 *Tax* 的对象复制到 *amzn-s3-demo-destination-bucket* 目标存储桶，并更改副本的所有权。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
<?xml version="1.0" encoding="UTF-8"?>
<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
   <Role>arn:aws:iam::account-id:role/role-name</Role>
   <Rule>
      <ID>Rule-1</ID>
      <Priority>1</Priority>
      <Status>Enabled</Status>
      <DeleteMarkerReplication>
         <Status>Disabled</Status>
      </DeleteMarkerReplication>
      <Filter>
         <Prefix>Tax</Prefix>
      </Filter>
      <Destination>
         <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
         <Account>destination-bucket-owner-account-id</Account>
         <AccessControlTranslation>
            <Owner>Destination</Owner>
         </AccessControlTranslation>
      </Destination>
   </Rule>
</ReplicationConfiguration>
```

向 Amazon S3 授予更改副本所有权的权限

通过在与 Amazon Identity and Access Management（IAM）角色关联的权限策略中添加 `s3:ObjectOwnerOverrideToBucketOwner` 操作的权限，可向 Amazon S3 授予更改副本所有权的权限。此角色是在复制配置中指定的 IAM 角色，可让 Amazon S3 担任该角色并代表您复制对象。要使用以下示例，请将 *amzn-s3-demo-destination-bucket* 替换为目标存储桶的名称。

```
...
{
    "Effect":"Allow",
         "Action":[
       "s3:ObjectOwnerOverrideToBucketOwner"
    ],
    "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}
...
```

在目标存储桶策略中添加允许更改副本所有权的权限

目标存储桶的拥有者必须向源存储桶的拥有者授予更改副本所有权的权限。目标存储桶的拥有者向源存储桶的拥有者授予 `s3:ObjectOwnerOverrideToBucketOwner` 操作的权限。此权限可让目标存储桶拥有者接受对象副本的所有权。以下示例存储桶策略语句说明如何执行此操作。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
...
{
    "Sid":"1",
    "Effect":"Allow",
    "Principal":{"AWS":"source-bucket-account-id"},
    "Action":["s3:ObjectOwnerOverrideToBucketOwner"],
    "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}
...
```

如何更改副本拥有者

当复制配置中的源存储桶和目标存储桶由不同的 Amazon Web Services 账户拥有时，可以指示 Amazon S3 将副本所有权更改为拥有目标存储桶的 Amazon Web Services 账户。以下示例显示如何使用 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）和 Amazon SDK 来更改副本所有权。

使用 S3 控制台

如需分步指导，请参阅 针对同一账户中的存储桶配置复制。本主题提供了在源存储桶和目标存储桶由相同和不同的 Amazon Web Services 账户拥有时设置复制配置的说明。

使用 Amazon CLI

以下过程介绍如何使用 Amazon CLI 更改副本所有权。在此过程中，您将执行以下操作：

- 创建源存储桶和目标存储桶。
- 对存储桶启用版本控制。
- 创建 Amazon Identity and Access Management（IAM）角色来向 Amazon S3 授予复制对象的权限。
- 将复制配置添加到源存储桶。
- 在复制配置中，指示 Amazon S3 更改副本所有权。
- 您需要测试复制配置。

当源存储桶和目标存储桶由不同的 Amazon Web Services 账户拥有时更改副本所有权（Amazon CLI）

要在此过程中使用示例 Amazon CLI 命令，请将 *user input placeholders* 替换为您自己的信息。

1. 在此示例中，您将在两个不同的 Amazon Web Services 账户中创建源存储桶和目标存储桶。要使用这两个账户，请使用两个命名配置文件配置 Amazon CLI。此示例分别使用名为 *acctA* 和 *acctB* 的配置文件。有关设置凭证配置文件和使用命名配置文件的信息，请参阅《Amazon Command Line Interface 用户指南》中的 Configuration and credential file settings。

   > **Important**
   >
   > 用于此过程的配置文件必须具有必要的权限。例如，在复制配置中，指定 Amazon S3 可担任的 IAM 角色。仅当您使用的配置文件具有 `iam:PassRole` 权限时，才能执行此操作。如果您使用管理员用户凭证来创建命名配置文件，则可以执行此过程中的所有任务。有关更多信息，请参阅《IAM 用户指南》中的向用户授予将角色传递给 Amazon Web Services 服务的权限。

2. 创建源存储桶，并启用版本控制。此示例在美国东部（弗吉尼亚州北部）(`us-east-1`) 区域中创建名为 *amzn-s3-demo-source-bucket* 的源存储桶。

```
aws s3api create-bucket \
--bucket amzn-s3-demo-source-bucket \
--region us-east-1 \
--profile acctA
```

```
aws s3api put-bucket-versioning \
--bucket amzn-s3-demo-source-bucket \
--versioning-configuration Status=Enabled \
--profile acctA
```

3. 创建一个目标存储桶，并启用版本控制。此示例在美国西部（俄勒冈州）(us-west-2) 区域中创建名为 *amzn-s3-demo-destination-bucket* 的目标存储桶。使用的 Amazon Web Services 账户配置文件应与您用于源存储桶的配置文件不同。

```
aws s3api create-bucket \
--bucket amzn-s3-demo-destination-bucket \
--region us-west-2 \
--create-bucket-configuration LocationConstraint=us-west-2 \
--profile acctB
```

```
aws s3api put-bucket-versioning \
--bucket amzn-s3-demo-destination-bucket \
--versioning-configuration Status=Enabled \
--profile acctB
```

4. 您必须添加权限到目标存储桶策略以允许更改副本所有权。

   a. 将以下策略保存到名为 *destination-bucket-policy*.json 的文件中。确保将 *user input placeholders* 替换为您自己的信息。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "destination_bucket_policy_sid",
      "Principal": {
        "AWS": "source-bucket-owner-account-id"
      },
      "Action": [
        "s3:ReplicateObject",
```

```
        "s3:ReplicateDelete",
        "s3:ObjectOwnerOverrideToBucketOwner",
        "s3:ReplicateTags",
        "s3:GetObjectVersionTagging"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      ]
    }
  ]
}
```

b. 使用以下 put-bucket-policy 命令将上述策略添加到目标存储桶：

```
aws s3api put-bucket-policy --region $ {destination-region} --bucket $ {amzn-s3-demo-destination-bucket} --policy file://destination_bucket_policy.json
```

5. 创建一个 IAM 角色。您将在稍后添加到源存储桶的复制配置中指定此角色。Amazon S3 担任此角色以代表您复制对象。分两个步骤创建 IAM 角色：

   - 创建角色。
   - 将权限策略附加到角色。

   a. 创建 IAM 角色。

      i. 复制以下信任策略，并将其保存到本地计算机上当前目录中一个名为 *s3-role-trust-policy*.json 的文件。此策略会向 Amazon S3 授予担任该角色的权限。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
```

```
}
```

ii. 运行以下 Amazon CLI `create-role` 命令来创建 IAM 角色：

```
$ aws iam create-role \
--role-name replicationRole \
--assume-role-policy-document file://s3-role-trust-policy.json  \
--profile acctA
```

记下您创建的 IAM 角色的 Amazon 资源名称（ARN）。您将在后面的步骤中用到此 ARN。

b. 将权限策略附加到角色。

i. 复制以下权限策略，并将其保存到本地计算机上当前目录中一个名为 *s3-role-perm-pol-changeowner*.json 的文件。此策略授予对各种 Amazon S3 存储桶和对象操作的权限。在下面的步骤中，您将此策略附加到之前创建的 IAM 角色。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObjectVersionForReplication",
            "s3:GetObjectVersionAcl"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket",
            "s3:GetReplicationConfiguration"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket"
         ]
      },
      {
         "Effect":"Allow",
```

```
            "Action":[
               "s3:ReplicateObject",
               "s3:ReplicateDelete",
               "s3:ObjectOwnerOverrideToBucketOwner",
               "s3:ReplicateTags",
               "s3:GetObjectVersionTagging"
            ],
            "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
         }
      ]
}
```

ii. 要将前面的权限策略附加到该角色，请运行以下 put-role-policy 命令：

```
$ aws iam put-role-policy \
--role-name replicationRole \
--policy-document file://s3-role-perm-pol-changeowner.json \
--policy-name replicationRolechangeownerPolicy \
--profile acctA
```

6. 向源存储桶添加复制配置。

a. Amazon CLI 要求以 JSON 形式指定复制配置。将以下 JSON 保存到本地计算机上当前目录中一个名为 *replication*.json 的文件。在配置中，AccessControlTranslation 指定副本所有权从源存储桶拥有者更改为目标存储桶拥有者。

```
{
   "Role":"IAM-role-ARN",
   "Rules":[
      {
         "Status":"Enabled",
         "Priority":1,
         "DeleteMarkerReplication":{
            "Status":"Disabled"
         },
         "Filter":{
         },
         "Status":"Enabled",
         "Destination":{
            "Bucket":"arn:aws:s3:::amzn-s3-demo-destination-bucket",
            "Account":"destination-bucket-owner-account-id",
            "AccessControlTranslation":{
               "Owner":"Destination"
```

```
            }
         }
      }
   ]
}
```

b. 编辑 JSON，即提供目标存储桶名称、目标存储桶拥有者账户 ID 和 *IAM-role-ARN* 的值。将 *IAM-role-ARN* 替换为您之前创建的 IAM 角色的 ARN。保存更改。

c. 要向源存储桶添加复制配置，请运行以下命令：

```
$ aws s3api put-bucket-replication \
--replication-configuration file://replication.json \
--bucket amzn-s3-demo-source-bucket \
--profile acctA
```

7. 通过在 Amazon S3 控制台中检查副本所有权，来测试复制配置。

a. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。

b. 将对象添加到源存储桶。验证目标存储桶包含对象副本，并且该副本的所有权已更改为拥有目标存储桶的 Amazon Web Services 账户。

使用 Amazon SDK

有关添加复制配置的代码示例，请参阅使用 Amazon SDK。您必须适当地修改复制配置。有关概念性信息，请参阅 更改副本拥有者。

使用 S3 Replication Time Control 满足合规性要求

S3 Replication Time Control（S3 RTC）可以帮助您满足数据复制的合规性要求或业务要求，并提供对 Amazon S3 复制时间的可见性。S3 RTC 会在几秒钟内复制您上传到 Amazon S3 的大多数对象，并在 15 分钟内复制 99.9% 的对象。

默认情况下，S3 RTC 包括两种跟踪复制进度的方法：

- S3 复制指标 – 可以使用 S3 复制指标，来监控待复制的 S3 API 操作的总数、待复制的对象的总大小、到目标区域的最长复制时间以及复制失败的操作总数。然后，您可以监控单独复制的每个数据集。也可以独立于 S3 RTC 启用 S3 复制指标。有关更多信息，请参阅 the section called “使用 S3 复制指标”。

启用了 S3 Replication Time Control（S3 RTC）的复制规则可发布 S3 复制指标。复制指标在启用 S3 RTC 之后的 15 分钟内可用。复制指标可通过 Amazon S3 控制台、Amazon S3 API、Amazon SDK、Amazon Command Line Interface（Amazon CLI）和 Amazon CloudWatch 提供。有关 CloudWatch 指标的更多信息，请参阅使用 Amazon CloudWatch 监控指标。有关通过 Amazon S3 控制台查看复制指标的更多信息，请参阅查看复制指标。

S3 复制指标的费率与 Amazon CloudWatch 自定义指标费率相同。有关信息，请参阅 Amazon CloudWatch 定价。

- Amazon S3 事件通知 – S3 RTC 提供 `OperationMissedThreshold` 和 `OperationReplicatedAfterThreshold` 事件，如果对象复制超过 15 分钟阈值或在 15 分钟阈值后发生，这些事件会通知存储桶拥有者。借助 S3 RTC，当对象在 15 分钟内未复制（这种情况很罕见）以及当这些对象在 15 分钟阈值之后复制时，Amazon S3 事件通知可以通知您。

  复制事件在启用 S3 RTC 之后的 15 分钟内可用。Amazon S3 事件通知可通过 Amazon SQS、Amazon SNS 或 Amazon Lambda 提供。有关更多信息，请参阅 the section called “接收复制失败事件”。

## S3 RTC 的最佳实践和准则

在 Amazon S3 中在启用 S3 Replication Time Control（S3 RTC）的情况下复制数据时，请遵循这些最佳实践准则，来为您的工作负载优化复制性能。

主题

- Amazon S3 复制和请求速率性能准则
- 估算您的复制请求速率
- 超过 S3 RTC 数据传输速率配额
- Amazon KMS 加密对象复制请求速率

### Amazon S3 复制和请求速率性能准则

当从 Amazon S3 上传和检索存储时，您的应用程序可以实现每秒数千个事务的请求性能。例如，应用程序在 S3 存储桶中对于每个前缀每秒可实现至少 3500 个 PUT/COPY/POST/DELETE 请求或 5500 个 GET/HEAD 请求，包括 S3 复制代表您发出的请求。对存储桶中的前缀数量没有限制。您可以通过并行读取来增加读取或写入性能。例如，如果您在 S3 存储桶中创建 10 个前缀来并行处理读取，则可以将读取性能扩展到每秒 55000 个读取请求。

Amazon S3 根据高于这些准则的持续请求速率或与 LIST 请求并行的持续请求速率自动扩展。尽管 Amazon S3 在内部针对新的请求速率进行优化，但您可能暂时会收到 HTTP 503 请求响应，直至优化完成。随着每秒请求速率增大，或者当您首次启用 S3 RTC 时，可能会发生这种行为。在这些期间，您的复制延迟可能会增加。S3 RTC 服务等级协议 (SLA) 不适用于超出 Amazon S3 每秒请求性能准则的时间段。

在复制数据传输速率超过默认 1 千兆位/秒（Gbps）配额的时间段内，S3 RTC SLA 也不适用。如果您预计复制传输速率超过 1 Gbps，则可以联系 Amazon Web Services 支持 中心或使用 Service Quotas 来请求提高复制传输速率配额。

估算您的复制请求速率

总请求速率（包括 Amazon S3 复制代表您发出的请求）不得超出复制源存储桶和目标存储桶的 Amazon S3 请求速率准则。对于每个已复制的对象，Amazon S3 复制向源存储桶发出最多五个 GET/HEAD 请求和一个 PUT 请求，并向每个目标存储桶发出一个 PUT 请求。

例如，如果您预期每秒复制 100 个对象，则 Amazon S3 复制可能会代表您执行额外 100 个 PUT 请求，每秒总计向源 S3 存储桶发出 200 个 PUT 请求。Amazon S3 复制也可能最多执行 500 个 GET/HEAD 请求（每个已复制的对象有 5 个 GET/HEAD 请求）。

> **Note**
>
> 每个已复制的对象只会产生一个 PUT 请求的费用。有关更多信息，请参阅 Amazon S3 有关复制的常见问题中的定价信息。

超过 S3 RTC 数据传输速率配额

如果您预期 S3 RTC 数据传输速率会超过默认的 1 Gbps 配额，请联系 Amazon Web Services 支持 中心或使用 Service Quotas 来请求提高复制传输速率配额。

Amazon KMS 加密对象复制请求速率

当您复制通过具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）来加密的对象时，每秒 Amazon KMS 请求配额适用。因为请求速率超过了每秒请求数的配额，所以 Amazon KMS 可能会拒绝其它有效的请求。如果请求受到限制，Amazon KMS 将返回 ThrottlingException 错误。Amazon KMS 请求速率配额适用于您直接发出的请求和 Amazon S3 复制代表您发出的请求。

例如，如果您预期每秒复制 1000 个对象，则可以从 Amazon KMS 请求速率配额中减去 2000 个请求。生成的每秒请求速率可用于除复制之外的 Amazon KMS 工作负载。您可以使用 Amazon

CloudWatch 中的 Amazon KMS 请求指标来监控Amazon Web Services 账户的总 Amazon KMS 请求速率。

要申请增加每秒 Amazon KMS 请求配额，请联系 Amazon Web Services 支持 中心或使用服务配额。

启用 S3 Replication Time Control

您可以基于新的或现有的复制规则开始使用 S3 Replication Time Control（S3 RTC）。可以选择将复制规则应用于整个存储桶，或应用于具有特定前缀或标签的对象。启用 S3 RTC 时，也会在复制规则上启用 S3 复制指标。

还可以使用 Amazon S3 控制台、Amazon S3 API、Amazon SDK 和 Amazon Command Line Interface（Amazon CLI）配置 S3 RTC。

使用 S3 控制台

如需分步指导，请参阅 针对同一账户中的存储桶配置复制。本主题提供了在源存储桶和目标存储桶由相同和不同的 Amazon Web Services 账户拥有时，在复制配置中启用 S3 RTC 的说明。

使用 Amazon CLI

要在启用 S3 RTC 的情况下使用 Amazon CLI 复制对象，您需要创建存储桶，对存储桶启用版本控制，创建一个 IAM 角色（该角色向 Amazon S3 赋予复制对象的权限），并将复制配置添加到源存储桶。复制配置必须启用了 S3 RTC，如以下示例所示。

有关使用 Amazon CLI 设置复制配置的分步说明，请参阅针对同一账户中的存储桶配置复制。

以下示例复制配置启用并设置复制规则的 `ReplicationTime` 和 `EventThreshold` 值。启用和设置这些值可以对规则启用 S3 RTC。

```
{
    "Rules": [
        {
            "Status": "Enabled",
            "Filter": {
                "Prefix": "Tax"
            },
            "DeleteMarkerReplication": {
                "Status": "Disabled"
            },
            "Destination": {
                "Bucket": "arn:aws:s3:::amzn-s3-demo-destination-bucket",
                "Metrics": {
                    "Status": "Enabled",
```

```
                    "EventThreshold": {
                        "Minutes": 15
                    }
                },
                "ReplicationTime": {
                    "Status": "Enabled",
                    "Time": {
                        "Minutes": 15
                    }
                }
            },
            "Priority": 1
        }
    ],
    "Role": "IAM-Role-ARN"
}
```

> **Important**
>
> `Metrics:EventThreshold:Minutes` 和 `ReplicationTime:Time:Minutes` 只能将 15 作为有效值。

使用适用于 Java 的 Amazon SDK

以下 Java 示例在启用 S3 Replication Time Control（S3 RTC）的情况下添加复制配置。

```
import software.amazon.awssdk.auth.credentials.AwsBasicCredentials;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3.model.DeleteMarkerReplication;
import software.amazon.awssdk.services.s3.model.Destination;
import software.amazon.awssdk.services.s3.model.Metrics;
import software.amazon.awssdk.services.s3.model.MetricsStatus;
import software.amazon.awssdk.services.s3.model.PutBucketReplicationRequest;
import software.amazon.awssdk.services.s3.model.ReplicationConfiguration;
import software.amazon.awssdk.services.s3.model.ReplicationRule;
import software.amazon.awssdk.services.s3.model.ReplicationRuleFilter;
import software.amazon.awssdk.services.s3.model.ReplicationTime;
import software.amazon.awssdk.services.s3.model.ReplicationTimeStatus;
import software.amazon.awssdk.services.s3.model.ReplicationTimeValue;

public class Main {
```

```
public static void main(String[] args) {
  S3Client s3 = S3Client.builder()
    .region(Region.US_EAST_1)
    .credentialsProvider(() -> AwsBasicCredentials.create(
        "AWS_ACCESS_KEY_ID",
        "AWS_SECRET_ACCESS_KEY")
    )
    .build();

  ReplicationConfiguration replicationConfig = ReplicationConfiguration
    .builder()
    .rules(
        ReplicationRule
          .builder()
          .status("Enabled")
          .priority(1)
          .deleteMarkerReplication(
              DeleteMarkerReplication
                  .builder()
                  .status("Disabled")
                  .build()
          )
          .destination(
              Destination
                  .builder()
                  .bucket("destination_bucket_arn")
                  .replicationTime(
                      ReplicationTime.builder().time(
                          ReplicationTimeValue.builder().minutes(15).build()
                      ).status(
                          ReplicationTimeStatus.ENABLED
                      ).build()
                  )
                  .metrics(
                      Metrics.builder().eventThreshold(
                          ReplicationTimeValue.builder().minutes(15).build()
                      ).status(
                          MetricsStatus.ENABLED
                      ).build()
                  )
                  .build()
          )
          .filter(
```

```
                ReplicationRuleFilter
                    .builder()
                    .prefix("testtest")
                    .build()
            )
        .build())
        .role("role_arn")
        .build();

    // Put replication configuration
    PutBucketReplicationRequest putBucketReplicationRequest =
 PutBucketReplicationRequest
      .builder()
      .bucket("source_bucket")
      .replicationConfiguration(replicationConfig)
      .build();

    s3.putBucketReplication(putBucketReplicationRequest);
  }
}
```

复制加密对象（SSE-S3、SSE-KMS、DSSE-KMS、SSE-C）

> **Important**
>
> Amazon S3 现在将具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）作为 Amazon S3 中每个存储桶的基本加密级别。从 2023 年 1 月 5 日起，上传到 Amazon S3 的所有新对象都将自动加密，不会产生额外费用，也不会影响性能。S3 存储桶默认加密配置和上传的新对象的自动加密状态可在 Amazon CloudTrail 日志、S3 清单、S3 Storage Lens 存储统计管理工具、Amazon S3 控制台中获得，并可用作 Amazon Command Line Interface 和 Amazon SDK 中的附加 Amazon S3 API 响应标头。有关更多信息，请参阅默认加密常见问题解答。

在复制已使用服务器端加密进行加密的对象时，有一些特殊注意事项。Amazon S3 支持以下服务器端加密类型：

- 具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）
- 具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）
- 具有 Amazon KMS 密钥的双层服务器端加密（DSSE-KMS）

- 具有客户提供密钥的服务器端加密（SSE-C）

有关服务器端加密的更多信息，请参阅 the section called “服务器端加密”。

本主题介绍指示 Amazon S3 复制已使用服务器端加密进行加密的对象所需的权限。本主题还提供了您可以添加的其他配置元素以及授予复制加密对象所需权限的示例 Amazon Identity and Access Management（IAM）策略。

有关带分步说明的示例，请参阅为加密对象启用复制。有关创建复制配置的信息，请参阅在区域内和跨区域复制对象。

> **Note**
>
> 您可以在 Amazon S3 中使用多区域 Amazon KMS keys。但是，Amazon S3 目前将多区域密钥视为单区域密钥，且不使用密钥的多区域特征。有关更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的 Using multi-Region keys。

主题


- 默认存储桶加密如何影响复制
- 复制使用 SSE-C 加密的对象
- 复制使用 SSE-S3、SSE-KMS 或 DSSE-KMS 加密的对象
- 为加密对象启用复制


## 默认存储桶加密如何影响复制

在为复制目标存储桶启用默认加密后，将应用以下加密行为：

- 如果未对源存储桶中的对象进行加密，则将使用目标存储桶的默认加密设置对目标存储桶中的副本对象进行加密。因此，源对象的实体标签（ETag）与副本对象的 ETag 不同。如果您有使用 ETag 的应用程序，则必须更新这些应用程序以弥补这种差异。
- 如果使用具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）、具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）或具有 Amazon KMS 密钥的双层服务器端加密（DSSE-KMS）来加密源存储桶中的对象，则目标存储桶中的副本对象使用与源对象相同类型的加密。不会使用目标存储桶的默认加密设置。

复制使用 SSE-C 加密的对象

使用具有客户提供密钥的服务器端加密（SSE-C），您可以管理您自己的专有加密密钥。使用 SSE-C，您可以管理密钥，而 Amazon S3 管理加密和解密过程。您必须在请求中提供加密密钥，但无需编写任何代码即可执行对象加密或解密。在上传对象时，Amazon S3 将使用您提供的密钥加密对象。然后，Amazon S3 将该密钥从内存中清除。在检索对象时，必须提供相同的加密密钥作为您请求的一部分。有关更多信息，请参阅 the section called “客户提供的加密密钥（SSE-C）”。

S3 复制支持使用 SSE-C 加密的对象。您可以在 Amazon S3 控制台中或使用 Amazon SDK 配置 SSE-C 对象复制，方法与为未加密对象配置复制的方法相同。除了复制当前所需的权限外，没有其他的 SSE-C 权限。

根据在 S3 复制配置中指定的内容，如果符合条件，S3 复制会自动复制新上传的 SSE-C 加密对象。要复制存储桶中的现有对象，请使用 S3 批量复制。有关复制对象的更多信息，请参阅the section called “设置实时复制”和the section called “复制现有对象”。

复制 SSE-C 对象不会产生额外的费用。有关复制定价的详细信息，请参阅 Amazon S3 定价。

复制使用 SSE-S3、SSE-KMS 或 DSSE-KMS 加密的对象

默认情况下，Amazon S3 不会复制使用 SSE-KMS 或 DSSE-KMS 加密的对象。本节介绍您可以添加的其他配置元素以指示 Amazon S3 复制这些对象。

有关带分步说明的示例，请参阅为加密对象启用复制。有关创建复制配置的信息，请参阅在区域内和跨区域复制对象。

在复制配置中指定其他信息

在复制配置中，您需要执行以下操作：

- 在复制配置的 `Destination` 元素中，添加您希望 Amazon S3 用来加密对象副本的对称 Amazon KMS 客户托管密钥的 ID，如下面的复制配置示例所示。
- 明确选择支持复制使用 KMS 密钥（SSE-KMS 或 DSSE-KMS）加密的对象。要选择加入，请添加 `SourceSelectionCriteria` 元素，如以下复制配置示例所示。

```
<ReplicationConfiguration>
   <Rule>
      ...
      <SourceSelectionCriteria>
         <SseKmsEncryptedObjects>
```

```
            <Status>Enabled</Status>
         </SseKmsEncryptedObjects>
      </SourceSelectionCriteria>

      <Destination>
          ...
          <EncryptionConfiguration>
             <ReplicaKmsKeyID>Amazon KMS key ARN or Key Alias ARN that's in the same
 Amazon Web Services ## as the destination bucket.</ReplicaKmsKeyID>
          </EncryptionConfiguration>
       </Destination>
      ...
   </Rule>
</ReplicationConfiguration>
```

> **Important**
>
> - 必须已在目标存储桶所在的同一 Amazon Web Services 区域中创建 KMS 密钥。
> - KMS 密钥必须有效。PutBucketReplication API 操作不检查 KMS 密钥的有效性。如果使用的 KMS 密钥无效，您将在响应中收到 HTTP 200 OK 状态代码，但复制将失败。

以下示例显示了一个包含可选配置元素的复制配置。此复制配置包含一个规则。该规则应用于键前缀为 *Tax* 的对象。Amazon S3 使用指定的 Amazon KMS key ID 来加密这些对象副本。

```
<?xml version="1.0" encoding="UTF-8"?>
<ReplicationConfiguration>
   <Role>arn:aws:iam::account-id:role/role-name</Role>
   <Rule>
      <ID>Rule-1</ID>
      <Priority>1</Priority>
      <Status>Enabled</Status>
      <DeleteMarkerReplication>
         <Status>Disabled</Status>
      </DeleteMarkerReplication>
      <Filter>
         <Prefix>Tax</Prefix>
      </Filter>
      <Destination>
         <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
         <EncryptionConfiguration>
```

```
            <ReplicaKmsKeyID>Amazon KMS key ARN or Key Alias ARN that's in the same
 Amazon Web Services ## as the destination bucket.</ReplicaKmsKeyID>
         </EncryptionConfiguration>
      </Destination>
      <SourceSelectionCriteria>
         <SseKmsEncryptedObjects>
            <Status>Enabled</Status>
         </SseKmsEncryptedObjects>
      </SourceSelectionCriteria>
   </Rule>
</ReplicationConfiguration>
```

为 IAM 角色授予额外权限

要复制使用 SSE-S3、SSE-KMS 或 DSSE-KMS 静态加密的对象，请向您在复制配置中指定的 Amazon Identity and Access Management（IAM）角色授予以下其他权限。通过更新与 IAM 角色关联的权限策略，可授予这些权限。

- 针对源对象的 **`s3:GetObjectVersionForReplication`** 操作 – 此操作允许 Amazon S3 复制未加密的对象，以及通过使用 SSE-S3、SSE-KMS 或 DSSE-KMS 的服务器端加密创建的对象。

  > **Note**
  >
  > 我们建议您使用 `s3:GetObjectVersionForReplication` 操作而不是 `s3:GetObjectVersion` 操作，因为 `s3:GetObjectVersionForReplication` 仅向 Amazon S3 提供进行复制所需的最低权限。此外，`s3:GetObjectVersion` 操作允许复制未加密的对象和 SSE-S3 加密的对象，但不允许复制使用 KMS 密钥（SSE-KMS 或 DSSE-KMS）加密的对象。

- 针对 KMS 密钥的 **`kms:Decrypt`** 和 **`kms:Encrypt`** Amazon KMS 操作
  - 您必须授予对 Amazon KMS key（用于解密源对象）的 `kms:Decrypt` 权限。
  - 您必须授予对 `kms:Encrypt`（用于加密对象副本）的 Amazon KMS key 权限。
- 用于复制明文对象的 **`kms:GenerateDataKey`** 操作 – 如果将明文对象复制到默认情况下启用 SSE-KMS 或 DSSE-KMS 加密的存储桶中，则必须在 IAM 策略中包含目标加密上下文的 `kms:GenerateDataKey` 权限和 KMS 密钥。

我们建议您通过使用 Amazon KMS 条件键将这些权限仅限于目标存储桶和对象。对于策略中列出的 KMS 密钥，拥有 IAM 角色的 Amazon Web Services 账户必须具有执行 `kms:Encrypt` 和 `kms:Decrypt` 操作的权限。如果 KMS 密钥由另一个 Amazon Web Services 账户拥有，则 KMS 密

钥的拥有者必须向拥有 IAM 角色的 Amazon Web Services 账户授予这些权限。有关管理对这些 KMS 密钥的访问权限的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的 Using IAM policies with Amazon KMS。

S3 存储桶密钥和复制

要将复制与 S3 存储桶密钥结合使用，用于加密对象副本的 KMS 密钥的 Amazon KMS key 策略必须包含发出调用的主体的 `kms:Decrypt` 权限。对 `kms:Decrypt` 的调用会在使用 S3 存储桶密钥之前验证 S3 存储桶密钥的完整性。有关更多信息，请参阅 将 S3 存储桶密钥与复制功能结合使用。

当为源存储桶或目标存储桶启用 S3 存储桶密钥时，加密上下文将是存储桶的 Amazon 资源名称（ARN），而不是对象的 ARN（例如 `arn:aws:s3:::bucket_ARN`）。您必须更新 IAM 策略才能将存储桶 ARN 用于加密上下文：

```
"kms:EncryptionContext:aws:s3:arn": [
"arn:aws:s3:::bucket_ARN"
]
```

有关更多信息，请参阅加密上下文（x-amz-server-side-encryption-context）（在“使用 REST API”一节中）和启用 S3 存储桶密钥之前需要注意的更改。

示例策略：将 SSE-S3 和 SSE-KMS 与复制结合使用

以下 IAM 策略示例显示了将 SSE-S3 和 SSE-KMS 与复制结合使用的语句。

Example – 将 SSE-KMS 用于单独的目标存储桶

以下示例策略显示了将 SSE-KMS 与单独的目标存储桶结合使用的语句。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action": ["kms:Decrypt"],
         "Effect": "Allow",
         "Condition": {
             "StringLike": {
                  "kms:ViaService": "s3.source-bucket-region.amazonaws.com",
                  "kms:EncryptionContext:aws:s3:arn": [
                      "arn:aws:s3:::amzn-s3-demo-source-bucket/key-prefix1*"
                  ]
             }
          },
```

```
            "Resource": [
               "List of Amazon KMS key ARNs that are used to encrypt source objects."
            ]
         },
         {
            "Action": ["kms:Encrypt"],
            "Effect": "Allow",
            "Condition": {
               "StringLike": {
                  "kms:ViaService": "s3.destination-bucket-1-region.amazonaws.com",
                  "kms:EncryptionContext:aws:s3:arn": [
                     "arn:aws:s3:::amzn-s3-demo-destination-bucket1/key-prefix1*"
                  ]
            }
            },
            "Resource": [
               "Amazon KMS key ARNs (in the same Amazon Web Services ## as destination
  bucket 1). Used to encrypt object replicas created in destination bucket 1."
            ]
         },
         {
            "Action": ["kms:Encrypt"],
            "Effect": "Allow",
            "Condition": {
               "StringLike": {
                  "kms:ViaService": "s3.destination-bucket-2-region.amazonaws.com",
                  "kms:EncryptionContext:aws:s3:arn": [
                     "arn:aws:s3:::amzn-s3-demo-destination-bucket2/key-prefix1*"
                  ]
            }
            },
            "Resource": [
               "Amazon KMS key ARNs (in the same Amazon Web Services ## as destination
  bucket 2). Used to encrypt object replicas created in destination bucket 2."
            ]
         }
      ]
}
```

Example – 复制使用 SSE-S3 和 SSE-KMS 创建的对象

以下是一个完整的 IAM 策略，它授予所需的权限以复制未加密的对象、使用 SSE-S3 创建的对象以及使用 SSE-KMS 创建的对象。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetReplicationConfiguration",
            "s3:ListBucket"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObjectVersionForReplication",
            "s3:GetObjectVersionAcl"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/key-prefix1*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:ReplicateObject",
            "s3:ReplicateDelete"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/key-prefix1*"
      },
      {
         "Action":[
            "kms:Decrypt"
         ],
         "Effect":"Allow",
         "Condition":{
            "StringLike":{
               "kms:ViaService":"s3.source-bucket-region.amazonaws.com",
               "kms:EncryptionContext:aws:s3:arn":[
                  "arn:aws:s3:::amzn-s3-demo-source-bucket/key-prefix1*"
               ]
            }
```

```
         },
         "Resource":[
           "List of the Amazon KMS key ARNs that are used to encrypt source objects."
         ]
      },
      {
         "Action":[
            "kms:Encrypt"
         ],
         "Effect":"Allow",
         "Condition":{
            "StringLike":{
               "kms:ViaService":"s3.destination-bucket-region.amazonaws.com",
               "kms:EncryptionContext:aws:s3:arn":[
                  "arn:aws:s3:::amzn-s3-demo-destination-bucket/prefix1*"
               ]
            }
         },
         "Resource":[
            "Amazon KMS key ARNs (in the same Amazon Web Services ## as the destination
 bucket) to use for encrypting object replicas"
         ]
      }
   ]
}
```

Example – 使用 S3 存储桶密钥复制对象

以下是一个完整的 IAM 策略，它授予复制具有 S3 存储桶密钥的对象所必需的权限。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetReplicationConfiguration",
            "s3:ListBucket"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket"
         ]
      },
      {
```

```
         "Effect":"Allow",
         "Action":[
            "s3:GetObjectVersionForReplication",
            "s3:GetObjectVersionAcl"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/key-prefix1*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:ReplicateObject",
            "s3:ReplicateDelete"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/key-prefix1*"
      },
      {
         "Action":[
            "kms:Decrypt"
         ],
         "Effect":"Allow",
         "Condition":{
            "StringLike":{
               "kms:ViaService":"s3.source-bucket-region.amazonaws.com",
               "kms:EncryptionContext:aws:s3:arn":[
                  "arn:aws:s3:::amzn-s3-demo-source-bucket"
               ]
            }
         },
         "Resource":[
           "List of the Amazon KMS key ARNs that are used to encrypt source objects."
         ]
      },
      {
         "Action":[
            "kms:Encrypt"
         ],
         "Effect":"Allow",
         "Condition":{
            "StringLike":{
               "kms:ViaService":"s3.destination-bucket-region.amazonaws.com",
               "kms:EncryptionContext:aws:s3:arn":[
                  "arn:aws:s3:::amzn-s3-demo-destination-bucket"
```

```
                ]
            }
        },
        "Resource":[
            "Amazon KMS key ARNs (in the same Amazon Web Services ## as the destination
 bucket) to use for encrypting object replicas"
        ]
      }
   ]
}
```

为跨账户方案授予其他权限

在跨账户方案中（其中源存储桶和目标存储桶由不同的 Amazon Web Services 账户拥有），您可以使用 KMS 密钥加密对象副本。但是，KMS 密钥拥有者必须向源存储桶拥有者授予使用 KMS 密钥的权限。

> **Note**
>
> 如果您需要跨账户复制 SSE-KMS 数据，则复制规则必须指定来自目标账户 Amazon KMS 的客户托管式密钥。Amazon 托管式密钥不支持跨账户使用，因此不能用于执行跨账户复制。

向源存储桶拥有者授予使用 KMS 密钥的权限（Amazon KMS 控制台）

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon KMS 控制台：https://console.aws.amazon.com/kms。
2. 要更改 Amazon Web Services 区域，请使用页面右上角的区域选择器。
3. 要查看您账户中自己所创建和管理的密钥，请在导航窗格中选择 Customer managed keys (客户托管密钥)。
4. 请选择 KMS 密钥。
5. 在一般配置部分下，选择密钥策略选项卡。
6. 向下滚动到其他 Amazon Web Services 账户。
7. 选择添加其他 Amazon Web Services 账户。

   将显示其它 Amazon Web Services 账户对话框。
8. 在此对话框中，选择添加其他 Amazon Web Services 账户。对于 arn:aws:iam::，输入源存储桶账户 ID。

9. 选择 Save changes（保存更改）。

向源存储桶拥有者授予使用 KMS 密钥的权限 (Amazon CLI)

- 有关 `put-key-policy` Amazon Command Line Interface（Amazon CLI）命令的信息，请参阅《Amazon CLI 命令参考》中的 put-key-policy。有关基础 `PutKeyPolicy` API 操作的信息，请参阅《Amazon Key Management Service API 参考》https://docs.amazonaws.cn/kms/latest/APIReference/中的 PutKeyPolicy。

Amazon KMS 事务限额注意事项

在启用跨区域复制（CRR）后使用 Amazon KMS 加密添加许多新对象时，您可能会遇到节流（HTTP `503 Service Unavailable` 错误）。如果每秒 Amazon KMS 事务数超出当前限额，则会发生节流。有关更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的配额。

要请求增加限额，您可以使用服务限额。有关更多信息，请参阅 Requesting a quota increase（请求增加限额）。如果您所在区域不支持服务配额，请创建一个 Amazon Web Services 支持 案例。

为加密对象启用复制

默认情况下，Amazon S3 不会复制使用具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）或具有 Amazon KMS 密钥的双层服务器端加密（DSSE-KMS）加密的对象。要复制用 SSE-KMS 或 DSS-KMS 加密的对象，必须修改存储桶复制配置，以指示 Amazon S3 复制这些对象。此示例介绍如何使用 Amazon S3 控制台和 Amazon Command Line Interface（Amazon CLI）更改存储桶复制配置以允许复制加密对象。

> **Note**
>
> 当为源或目标存储桶启用 S3 存储桶密钥时，加密上下文将是存储桶的 Amazon 资源名称 (ARN)，而不是对象的 ARN。您必须更新 IAM 策略才能将存储桶 ARN 用于加密上下文。有关更多信息，请参阅 S3 存储桶密钥和复制。

> **Note**
>
> 您可以在 Amazon S3 中使用多区域 Amazon KMS keys。但是，Amazon S3 目前将多区域密钥视为单区域密钥，且不使用密钥的多区域特征。有关更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的 Using multi-Region keys。

使用 S3 控制台

如需分步指导，请参阅 针对同一账户中的存储桶配置复制。本主题提供了在源存储桶和目标存储桶由相同和不同的 Amazon Web Services 账户拥有时设置复制配置的说明。

使用 Amazon CLI

要使用 Amazon CLI 复制加密的对象，请执行以下操作：

- 创建源存储桶和目标存储桶，并对这些存储桶启用版本控制。
- 创建向 Amazon S3 授予复制对象的权限的 Amazon Identity and Access Management（IAM）服务角色。IAM 角色的权限包含复制这些加密对象所需的权限。
- 将复制配置添加到源存储桶。复制配置提供与复制使用 KMS 密钥加密的对象相关的信息。
- 将加密的对象添加到源存储桶。
- 测试设置，以确认加密的对象正在复制到目标存储桶。

以下过程指导您完成此过程。

复制服务器端加密对象 (Amazon CLI)

要在此过程中使用这些示例，请将 *user input placeholders* 替换为您自己的信息。

1. 在此示例中，您在同一个 Amazon Web Services 账户中创建源存储桶 (*amzn-s3-demo-source-bucket*) 和目标存储桶 (*amzn-s3-demo-destination-bucket*)。还可以为 Amazon CLI 设置凭证配置文件。此示例使用配置文件名称 *acctA*。

   有关设置凭证配置文件和使用命名配置文件的信息，请参阅《Amazon Command Line Interface 用户指南》中的 Configuration and credential file settings。
2. 使用以下命令创建 *amzn-s3-demo-source-bucket* 存储桶并对该存储桶启用版本控制。以下示例命令在美国东部（弗吉尼亚州北部）（us-east-1）区域中创建 *amzn-s3-demo-source-bucket* 存储桶。

```
aws s3api create-bucket \
--bucket amzn-s3-demo-source-bucket \
--region us-east-1 \
--profile acctA
```

```
aws s3api put-bucket-versioning \
```

```
--bucket amzn-s3-demo-source-bucket \
--versioning-configuration Status=Enabled \
--profile acctA
```

3. 使用以下命令创建 *amzn-s3-demo-destination-bucket* 存储桶并对该存储桶启用版本控制。以下示例命令在美国西部（俄勒冈州）（us-west-2）区域中创建 *amzn-s3-demo-destination-bucket* 存储桶。

> **Note**
>
> 要在 *amzn-s3-demo-source-bucket* 存储桶和 *amzn-s3-demo-destination-bucket* 存储桶均位于同一 Amazon Web Services 账户中时设置复制配置，请使用同一配置文件。此示例使用 *acctA*。要在两个存储桶由不同 Amazon Web Services 账户拥有时配置复制，您需要为每个存储桶指定不同的配置文件。

```
aws s3api create-bucket \
--bucket amzn-s3-demo-destination-bucket \
--region us-west-2 \
--create-bucket-configuration LocationConstraint=us-west-2 \
--profile acctA
```

```
aws s3api put-bucket-versioning \
--bucket amzn-s3-demo-destination-bucket \
--versioning-configuration Status=Enabled \
--profile acctA
```

4. 接下来，创建 IAM 服务角色。您将在稍后添加到 *amzn-s3-demo-source-bucket* 存储桶的复制配置中指定此角色。Amazon S3 担任此角色以代表您复制对象。分两个步骤创建 IAM 角色：

   - 创建服务角色。
   - 将权限策略附加到角色。

   a. 要创建 IAM 服务角色，请执行以下操作：

      i. 复制以下信任策略，并将其保存到本地计算机上当前目录中一个名为 *s3-role-trust-policy-kmsobj*.json 的文件。此策略授予 Amazon S3 服务主体担任该角色的权限，以便 Amazon S3 可代表您执行任务。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

ii. 使用以下命令创建角色：

```
$ aws iam create-role \
--role-name replicationRolekmsobj \
--assume-role-policy-document file://s3-role-trust-policy-kmsobj.json  \
--profile acctA
```

b. 接下来，将权限策略附加到角色。此策略授予对各种 Amazon S3 存储桶和对象操作的权限。

i. 复制以下权限策略，并将其保存到本地计算机上当前目录中一个名为 *s3-role-permissions-policykmsobj*.json 的文件。您将创建一个 IAM 角色，稍后将策略附加到该角色。

> **Important**
>
> 在权限策略中，您可以指定将用于加密 *amzn-s3-demo-source-bucket* 和 *amzn-s3-demo-destination-bucket* 存储桶的 Amazon KMS 密钥 ID。您必须为 *amzn-s3-demo-source-bucket* 和 *amzn-s3-demo-destination-bucket* 存储桶创建两个单独的 KMS 密钥。Amazon KMS keys不会在创建它们的 Amazon Web Services 区域之外共享。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[
```

```
            "s3:ListBucket",
            "s3:GetReplicationConfiguration",
            "s3:GetObjectVersionForReplication",
            "s3:GetObjectVersionAcl",
            "s3:GetObjectVersionTagging"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket",
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
         ]
      },
      {
         "Action":[
            "s3:ReplicateObject",
            "s3:ReplicateDelete",
            "s3:ReplicateTags"
         ],
         "Effect":"Allow",
         "Condition":{
            "StringLikeIfExists":{
               "s3:x-amz-server-side-encryption":[
                  "aws:kms",
                  "AES256",
                  "aws:kms:dsse"
               ],
               "s3:x-amz-server-side-encryption-aws-kms-key-id":[
                  "Amazon KMS key IDs(in ARN format) to use for encrypting
object replicas"
               ]
            }
         },
         "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      },
      {
         "Action":[
            "kms:Decrypt"
         ],
         "Effect":"Allow",
         "Condition":{
            "StringLike":{
               "kms:ViaService":"s3.us-east-1.amazonaws.com",
               "kms:EncryptionContext:aws:s3:arn":[
                  "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
```

```
                ]
             }
          },
          "Resource":[
             "Amazon KMS key IDs(in ARN format) used to encrypt source
 objects."
          ]
       },
       {
          "Action":[
             "kms:Encrypt"
          ],
          "Effect":"Allow",
          "Condition":{
             "StringLike":{
                "kms:ViaService":"s3.us-west-2.amazonaws.com",
                "kms:EncryptionContext:aws:s3:arn":[
                   "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
                ]
             }
          },
          "Resource":[
             "Amazon KMS key IDs (in ARN format) to use for encrypting
 object replicas"
          ]
       }
    ]
}
```

ii. 创建一个策略并将其附加到角色。

```
$ aws iam put-role-policy \
--role-name replicationRolekmsobj \
--policy-document file://s3-role-permissions-policykmsobj.json \
--policy-name replicationRolechangeownerPolicy \
--profile acctA
```

5. 接下来，将以下复制配置添加到 *amzn-s3-demo-source-bucket* 存储桶。它指示 Amazon S3 将前缀为 *Tax/* 的对象复制到 *amzn-s3-demo-destination-bucket* 存储桶。

> **Important**
>
> 在复制配置中，指定 Amazon S3 可代入的 IAM 角色。仅当您具有 `iam:PassRole` 权限时，才能执行此操作。您在 CLI 命令中指定的配置文件必须具有此权限。有关更多信息，请参阅《IAM 用户指南》中的向用户授予将角色传递给 Amazon Web Services 服务的权限。

```
<ReplicationConfiguration>
 <Role>IAM-Role-ARN</Role>
 <Rule>
   <Priority>1</Priority>
   <DeleteMarkerReplication>
      <Status>Disabled</Status>
   </DeleteMarkerReplication>
   <Filter>
      <Prefix>Tax</Prefix>
   </Filter>
   <Status>Enabled</Status>
   <SourceSelectionCriteria>
     <SseKmsEncryptedObjects>
       <Status>Enabled</Status>
     </SseKmsEncryptedObjects>
   </SourceSelectionCriteria>
   <Destination>
     <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
     <EncryptionConfiguration>
       <ReplicaKmsKeyID>Amazon KMS key IDs to use for encrypting object replicas</
ReplicaKmsKeyID>
     </EncryptionConfiguration>
   </Destination>
  </Rule>
</ReplicationConfiguration>
```

要将复制配置添加到 *amzn-s3-demo-source-bucket* 存储桶，请执行以下操作：

a. Amazon CLI 要求以 JSON 形式指定复制配置。将以下 JSON 保存到本地计算机上当前目录中的一个文件 (*replication*.json)。

```
{
```

```
   "Role":"IAM-Role-ARN",
   "Rules":[
      {
         "Status":"Enabled",
         "Priority":1,
         "DeleteMarkerReplication":{
            "Status":"Disabled"
         },
         "Filter":{
            "Prefix":"Tax"
         },
         "Destination":{
            "Bucket":"arn:aws:s3:::amzn-s3-demo-destination-bucket",
            "EncryptionConfiguration":{
               "ReplicaKmsKeyID":"Amazon KMS key IDs (in ARN format) to use for
 encrypting object replicas"
            }
         },
         "SourceSelectionCriteria":{
            "SseKmsEncryptedObjects":{
               "Status":"Enabled"
            }
         }
      }
   ]
}
```

b. 编辑 JSON 以提供 *amzn-s3-demo-destination-bucket* 存储桶、*Amazon KMS key IDs (in ARN format)* 和 *IAM-role-ARN* 的值。保存更改。

c. 使用以下命令以将复制配置添加到 *amzn-s3-demo-source-bucket* 存储桶中。请务必提供 *amzn-s3-demo-source-bucket* 存储桶名称。

```
$ aws s3api put-bucket-replication \
--replication-configuration file://replication.json \
--bucket amzn-s3-demo-source-bucket \
--profile acctA
```

6. 测试该配置以确认已经复制了加密对象。在 Amazon S3 控制台中，执行以下操作：

a. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。

b. 在 *amzn-s3-demo-source-bucket* 存储桶中，创建一个名为 *Tax* 的文件夹。

c. 将示例对象添加到文件夹。请务必选择加密选项并指定用于加密对象的 KMS 密钥。

d. 确认 *amzn-s3-demo-destination-bucket* 存储桶包含对象副本，并且它们已使用在配置中指定的 KMS 密钥进行了加密。有关更多信息，请参阅 the section called “获取复制状态”。

使用 Amazon SDK

有关显示如何添加复制配置的代码示例，请参阅使用 Amazon SDK。您必须适当地修改复制配置。

使用副本修改同步复制元数据更改

Amazon S3 副本修改同步可以协助您保留在副本和源对象之间复制的对象元数据，例如标签、访问控制列表（ACL）和对象锁定设置。默认情况下，Amazon S3 仅会从源对象向副本复制元数据。启用副本修改同步后，Amazon S3 会将对副本所做的元数据更改复制回源对象，使复制成为双向复制。

启用副本修改同步

您可以将 Amazon S3 副本修改同步与新的或现有的复制规则一起使用。可以将它应用于整个存储桶或具有特定前缀的对象。

要使用 Amazon S3 控制台启用副本修改同步，请参阅配置实时复制的示例。本主题提供了在源存储桶和目标存储桶由相同或不同的 Amazon Web Services 账户拥有时，在复制配置中启用副本修改同步的说明。

要使用 Amazon Command Line Interface（Amazon CLI）启用副本修改同步，必须向包含已启用 `ReplicaModifications` 的副本的存储桶添加复制配置。要设置双向复制，请创建从源存储桶（*amzn-s3-demo-source-bucket*）到包含副本的存储桶（*amzn-s3-demo-destination-bucket*）的复制规则。然后，创建从包含副本的存储桶（*amzn-s3-demo-destination-bucket*）到源存储桶（*amzn-s3-demo-source-bucket*）的第二个复制规则。源存储桶和目标存储桶可以位于相同或不同的 Amazon Web Services 区域中。

> **Note**
>
> 必须同时在源存储桶和目标存储桶上启用副本修改同步，才能复制副本元数据更改，例如已复制对象上的对象访问控制列表（ACL）、对象标签或对象锁定设置。与所有复制规则一样，可以将这些规则应用于整个存储桶，也可以应用于按前缀或对象标签筛选的对象子集。

在以下示例配置中，Amazon S3 将以 *Tax* 为前缀的元数据更改复制到存储桶 *amzn-s3-demo-source-bucket*，该存储桶包含源对象。

```
{
    "Rules": [
        {
            "Status": "Enabled",
            "Filter": {
                "Prefix": "Tax"
            },
            "SourceSelectionCriteria": {
                "ReplicaModifications":{
                    "Status": "Enabled"
                }
            },
            "Destination": {
                "Bucket": "arn:aws:s3:::amzn-s3-demo-source-bucket"
            },
            "Priority": 1
        }
    ],
    "Role": "IAM-Role-ARN"
}
```

有关使用 Amazon CLI 创建复制规则的完整说明，请参阅针对同一账户中的存储桶配置复制。

在存储桶之间复制删除标记

默认情况下，当启用 S3 复制且源存储桶中的对象被删除时，Amazon S3 仅在源存储桶中添加删除标记。此操作有助于保护目标存储桶中的数据免遭意外删除或恶意删除。如果您启用了删除标记复制，则这些标记将复制到目标存储桶，Amazon S3 的行为就像对象在源存储桶和目标存储桶中都被删除了一样。有关删除标记工作原理的更多信息，请参阅使用删除标记。

> **Note**
>
> - 基于标签的复制规则不支持删除标记复制。删除标记复制也不符合您使用 S3 Replication Time Control（S3 RTC）时授予的 15 分钟服务水平协议（SLA）。
> - 如果您没在使用最新的复制配置 XML 版本，则删除操作会对复制产生不同的影响。有关更多信息，请参阅 删除操作对复制操作有何影响。

- 如果您启用删除标记复制，并且源存储桶具有 S3 生命周期到期规则，则 S3 生命周期到期规则添加的删除标记将不会复制到目标存储桶。

### 启用删除标记复制

您可以开始将删除标记复制与新的或现有的复制规则结合使用。可以将删除标记复制应用于整个存储桶或具有特定前缀的对象。

要使用 Amazon S3 控制台启用删除标记复制，请参阅使用 S3 控制台。本主题提供了在源存储桶和目标存储桶由相同或不同的 Amazon Web Services 账户拥有时，在复制配置中启用删除标记复制的说明。

要使用 Amazon Command Line Interface（Amazon CLI）启用删除标记复制，必须向已启用 `DeleteMarkerReplication` 的源存储桶添加复制配置，如下面的示例配置所示。

在以下示例复制配置中，对于以 *Tax* 为前缀的对象，删除标记将复制到目标存储桶 *amzn-s3-demo-destination-bucket*。

```
{
    "Rules": [
        {
            "Status": "Enabled",
            "Filter": {
                "Prefix": "Tax"
            },
            "DeleteMarkerReplication": {
                "Status": "Enabled"
            },
            "Destination": {
                "Bucket": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
            },
            "Priority": 1
        }
    ],
    "Role": "IAM-Role-ARN"
}
```

有关通过 Amazon CLI 创建复制规则的完整说明，请参阅针对同一账户中的存储桶配置复制。

# 管理或暂停实时复制

实时复制是跨相同或不同 Amazon Web Services 区域中的存储桶自动、异步复制对象。在您设置复制配置后，Amazon S3 会将源存储桶中新创建的对象和对象更新复制到一个或多个指定的目标存储桶。

您使用 Amazon S3 控制台向源存储桶添加复制规则。复制规则定义了要复制的源存储桶对象和存储已复制对象的目标存储桶。有关复制的更多信息，请参阅 在区域内和跨区域复制对象。

可以在 Amazon S3 控制台中的复制页面上管理复制规则。可以添加、查看、编辑、启用、禁用或删除复制规则。也可以更改复制规则的优先级。有关向存储桶添加复制规则的信息，请参阅 使用 S3 控制台。

使用 Amazon S3 控制台管理存储桶的复制规则

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 在通用存储桶选项卡上，选择您想要的存储桶的名称。
4. 选择管理选项卡，然后向下滚动到复制规则。
5. 可以通过以下方式更改复制规则：
   - 要启用或禁用复制规则，请选择规则左侧的选项按钮。在操作菜单上，选择启用规则或禁用规则。还可从操作菜单中禁用、启用或删除存储桶中的所有规则。

     > **Note**
     >
     > 如果您禁用复制规则，之后又重新启用该规则，那么在禁用规则期间未复制的任何新对象或更改的对象在重新启用该规则后均不会 自动复制。要复制这些对象，必须使用 S3 批量复制。有关更多信息，请参阅 the section called “复制现有对象”。

   - 要更改规则的优先级，请选择规则左侧的选项按钮，然后选择编辑规则。

     您需要设置规则优先级，以避免因在多个规则的范围内包含对象而引起冲突。如果规则重叠，Amazon S3 会使用规则优先级确定要应用哪个规则。数字越大，优先级越高。有关规则优先级的更多信息，请参阅 复制配置文件元素。

### 暂停或停止复制

要临时暂停复制并在以后自动恢复，您可以使用 Amazon Fault Injection Service 中的 `aws:s3:bucket-pause-replication` 操作。有关更多信息，请参阅《Amazon Fault Injection Service 用户指南》中的 aws:s3:bucket-pause-replication 和 Pause S3 Replication。

要在 Amazon S3 中停止复制，我们建议您禁用复制规则。如果您禁用复制规则，之后又重新启用该规则，那么在禁用规则期间未复制的任何新对象或更改的对象在重新启用该规则后均不会 自动复制。要复制这些对象，必须使用 S3 批量复制。有关更多信息，请参阅 the section called “复制现有对象”。

如果您移除向 Amazon S3 授予所需权限的 Amazon Identity and Access Management（IAM）角色、Amazon Key Management Service（Amazon KMS）权限或存储桶策略权限，复制也将停止。但是，我们建议您不要使用这些方法，因为它们会导致复制失败。Amazon S3 会将受影响对象的复制状态报告为 `FAILED`。如果稍后权限恢复，则标记为 `FAILED` 的对象不会 自动复制。要复制这些对象，必须使用 S3 批量复制。

## 使用批量复制以复制现有对象

S3 批量复制与实时复制不同，后者连续自动跨 Amazon S3 存储桶复制新对象。相反，S3 批量复制是按需对现有对象进行的。可以使用 S3 批量复制来复制以下类型的对象：

- 在复制配置设立之前已经存在的对象
- 以前已复制的对象
- 复制失败的对象

您可以使用批量操作任务来按需复制这些对象。

要开始使用批量复制，您可以：

- 为新的复制规则或目标启动批量复制 – 可以在新的复制配置中创建第一条规则时，或通过 Amazon S3 控制台向现有配置添加新的目标存储桶时，创建一次性批量复制任务。
- 为现有复制配置启动批量复制 – 可以通过 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 Amazon S3 REST API，使用 S3 批量操作创建新的批量复制任务。

分批复制任务完成后，您将收到完成报告。有关如何使用此报告检查任务的更多信息，请参阅跟踪任务状态和完成报告。

## S3 分批复制注意事项

使用 S3 批量复制之前，请查看以下注意事项列表：

- 您的源存储桶必须具有现有的复制配置。要启用复制，请参阅 设置实时复制概述 和 配置实时复制的示例。
- 如果您为存储桶配置了 S3 生命周期，我们建议在批量复制任务处于活动状态时禁用生命周期规则。这样做有助于确保源存储桶和目标存储桶的对等。否则，这些存储桶可能会出现差异，目标存储桶将不会与源存储桶完全一样。例如，考虑以下情形：
  - 您的源存储桶有某个对象的多个版本，并且对于该对象有一个删除标记。
  - 您的源存储桶和目标存储桶具有移除已过期删除标记的生命周期配置。

  在这种情况下，批量复制可能会在复制对象版本之前，将删除标记复制到目标存储桶。这种行为可能导致在复制对象版本之前，生命周期配置将删除标记标为过期，并且从目标存储桶中移除删除标记。
- 您指定用于运行批量操作任务的 Amazon Identity and Access Management（IAM）角色必须具有必要的权限，来执行基础的批量复制操作。有关创建 IAM 角色的更多信息，请参阅 配置 IAM 角色以进行 S3 批量复制。
- 批量复制需要可以由 Amazon S3 生成的清单。生成的清单必须存储在与源存储桶相同的 Amazon Web Services 区域 中。如果您选择不生成清单，则可以提供包含要复制的对象的 Amazon S3 清单报告或 CSV 文件。有关更多信息，请参阅 the section called “为分批复制任务指定清单”。
- 批量复制不支持重新复制已通过从目标存储桶中指定对象的版本 ID 删除的对象。要重新复制这些对象，您可以使用分批复制任务将源对象复制到位。将这些对象复制到位会在源存储桶中创建对象的新版本，并自动启动到目标存储桶的复制。删除和重新创建目标存储桶不会启动复制。

  有关批量复制的更多信息，请参阅使用分批操作复制对象的示例。
- 如果您在源存储桶上使用复制规则，请确保通过向附加到复制规则的 IAM 角色授予复制对象的适当权限，来更新您的复制配置。此 IAM 角色必须具有在源存储桶和目标存储桶上执行复制所需的权限。
- 如果您在短时间范围内为同一个存储桶提交多个批量复制任务，Amazon S3 会同时运行这些任务。
- 如果您为两个不同的存储桶提交多个批量复制任务，请注意 Amazon S3 可能无法同时运行所有任务。如果您超过了账户中一次可以运行的批量复制任务的数量，Amazon S3 会暂停优先级较低的任务，来处理优先级较高的任务。优先级较高的任务完成后，任何暂停的任务都会再次变为活动状态。
- 存储在 S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 存储类中的对象不支持批量复制。
- 要批量复制存储在归档访问存储层或深度归档访问存储层中的 S3 Intelligent-Tiering 对象，必须首先启动还原请求，然后等待对象移动到频繁访问层。

## 为分批复制任务指定清单

清单是一种 Amazon S3 对象，其中包含您希望 Amazon S3 采取操作的对象键。如果您希望创建批量复制任务，则必须提供用户生成的清单，或者让 Amazon S3 根据复制配置生成清单。

如果您提供用户生成的清单，清单必须采用 Amazon S3 清单报告或 CSV 文件的形式。如果清单中的对象位于受版本控制的存储桶中，则必须指定对象的版本 ID。只会复制在清单中指定了版本 ID 的对象。要了解有关指定清单的更多信息，请参阅 指定清单。

如果您选择让 Amazon S3 代表您生成清单文件，那么列出的对象会使用与源存储桶上的复制配置相同的源存储桶、前缀和标签。使用生成的清单，Amazon S3 复制所有符合条件的对象版本。

> **Note**
>
> 如果您选择让 Amazon S3 生成清单，则清单必须存储在与源存储桶相同的 Amazon Web Services 区域中。

## 分批复制任务的筛选条件

在创建批量复制任务时，您可以选择指定其它筛选条件，例如对象创建日期和复制状态，来缩小任务的范围。

您可以通过提供以下一个或多个值基于 `ObjectReplicationStatuses` 值筛选要复制的对象：

- `"NONE"` – 表示 Amazon S3 之前从未尝试过复制对象。
- `"FAILED"` – 表示 Amazon S3 之前尝试过，但未成功复制对象。
- `"COMPLETED"` – 表示 Amazon S3 之前已成功复制对象。
- `"REPLICA"` – 表示此对象是 Amazon S3 已从另一个源存储桶复制的副本。

有关复制状态的更多信息，请参阅 获取复制状态信息。

如果您不筛选批量复制任务，批量操作会尝试复制清单中与复制配置中的规则匹配的所有对象（无论其 `ObjectReplicationStatus` 如何），但默认情况下未复制的某些对象除外。有关更多信息，请参阅 the section called “使用复制配置不会复制什么？”。

根据您的目标，您可以将 `ObjectReplicationStatuses` 设置为以下一个或多个值：

- 要复制从未复制过的现有对象，请仅包括 `"NONE"`。

- 要重试复制之前未能复制的对象，请仅包括 "FAILED"。
- 要同时复制现有对象和重试复制之前未能复制的对象，请同时包括 "NONE" 和 "FAILED"。
- 要使用已复制到另一个目标的对象回填目标存储桶，请包括 "COMPLETED"。
- 要复制之前已复制的对象，请包括 "REPLICA"。

### 分批复制完成报告

在创建批量复制任务时，您可以请求 CSV 完成报告。此报告显示对象、复制成功或失败代码、输出和描述。有关任务跟踪和完成报告的更多信息，请参阅完成报告。

有关复制故障代码和描述的列表，请参阅 Amazon S3 复制失败原因。

有关排查批量复制故障的信息，请参阅批量复制错误。

### 批量复制入门

要了解有关如何使用批量复制的更多信息，请参阅教程：使用 S3 批量复制来复制 Amazon S3 存储桶中的现有对象。

### 配置 IAM 角色以进行 S3 批量复制

由于 Amazon S3 批量复制是批量操作任务的一种类型，因此您必须创建一个 Amazon Identity and Access Management（IAM）角色，用于向批量操作授予代表您执行操作的权限。您还必须将分批复制 IAM 策略附加到批量操作 IAM 角色。

使用以下过程创建策略和 IAM 角色，来向批量操作授予启动批量复制任务的权限。

创建用于批量复制的策略

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在访问管理下，选择策略。
3. 选择 Create policy (创建策略)。
4. 在指定权限页面上，选择 JSON。
5. 根据您的清单是由 Amazon S3 生成还是您自行提供清单，插入以下策略之一。有关清单的更多信息，请参阅为分批复制任务指定清单。

   在使用这些策略之前，请将以下策略中的 *user input placeholders* 替换为复制源存储桶、清单存储桶和完成报告存储桶的名称。

> **Note**
>
> 批量复制的 IAM 角色需要不同的权限，具体取决于您是生成清单还是提供清单，因此，请务必从以下示例中选择相应的策略。

使用和存储 Amazon S3 生成的清单时的策略

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[
            "s3:InitiateReplication"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
         ]
      },
      {
         "Action":[
            "s3:GetReplicationConfiguration",
            "s3:PutInventoryConfiguration"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket"
         ]
      },
      {
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
         ]
      },
      {
```

```
         "Effect":"Allow",
         "Action":[
            "s3:PutObject"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*",
            "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
         ]
      }
   ]
}
```

使用用户提供的清单时的策略

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[
            "s3:InitiateReplication"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
         ]
      },
            {
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
```

```
            ]
        }
    ]
}
```

6. 选择下一步。
7. 指定策略名称，然后选择创建策略。

创建用于批量复制的 IAM 角色

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在 Access management（访问管理）下，请选择 Roles（角色）。
3. 选择创建角色。
4. 选择 Amazon Web Services 服务作为可信实体的类型。在使用案例部分中，选择 S3 作为服务，并选择 S3 批量操作作为使用案例。
5. 选择下一步。此时将显示添加权限页面。在搜索框中，搜索您在前面的过程中创建的策略。选中策略名称旁的复选框，然后选择下一步。
6. 在命名、查看和创建页面上，输入 IAM 角色的名称。
7. 在步骤 1：信任身份部分中，验证 IAM 角色是否使用以下信任策略：

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"batchoperations.s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

8. 在步骤 2：添加权限部分中，验证 IAM 角色是否使用您之前创建的策略。
9. 选择创建角色。

## 为新的复制规则或目标创建批量复制任务

在 Amazon S3 中，实时复制不会复制在您创建复制配置之前已存在于源存储桶中的任何对象。实时复制仅自动复制在创建复制配置之后写入存储桶中的新对象和更新的对象。要复制已存在的对象，可以使用 S3 批量复制来按需复制这些对象。

在新的实时复制配置中创建第一个规则时，或通过 Amazon S3 控制台将新目标存储桶添加到现有复制配置时，可以选择创建一个批量复制任务。可以使用此批量复制任务来将源存储桶中的现有对象复制到目标存储桶。

要将批量复制用于现有配置而不添加新的目标存储桶，请参阅为现有复制规则创建分批复制任务。

先决条件

在创建批量复制任务之前，必须创建批量操作 Amazon Identity and Access Management（IAM）角色，来向 Amazon S3 授予代表您执行操作的权限。有关更多信息，请参阅 配置 IAM 角色以进行 S3 批量复制。

通过 Amazon S3 控制台将批量复制用于新的复制规则或目标

在新的复制配置中创建第一个规则时，或通过 Amazon S3 控制台将新的目标存储桶添加到现有配置时，可以选择创建批复制任务来复制源存储桶中的现有对象。

在创建或更新复制配置时创建批量复制任务

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 在通用存储桶列表中，选择包含您想要复制的对象的存储桶名称。
4. 要创建新的复制规则或编辑现有规则，请选择管理选项卡，然后向下滚动到复制规则：
   - 要创建新的复制规则，请选择 Create replication rule（创建复制规则）。有关如何设置基本复制规则的示例，请参阅配置实时复制的示例。
   - 要编辑现有复制规则，请选择规则名称旁边的选项按钮，然后选择编辑规则。
5. 创建新的复制规则或编辑现有复制规则的目标，然后选择 Save（保存）。

   在新的复制配置中创建第一个规则或编辑现有配置以添加新目标后，将显示 Replicate existing objects?（是否复制现有对象？）对话框，让您可以选择创建分批复制任务。

6. 如果要立即创建并运行此任务，请选择是，复制现有对象。

   如果要以后创建批量复制任务，请选择否，不复制现有对象。

7. 如果选择是，复制现有对象，则会出现创建批量操作任务页面。S3 批量复制任务具有以下设置：

   任务运行选项

   如果您想让 S3 批量复制任务立即运行，请选择任务准备就绪后自动运行。如果您想在以后运行任务，请选择等待任务准备就绪后再运行。

   > **Note**
   >
   > 如果选择任务准备就绪后自动运行，您将无法创建和保存批量操作清单。要保存批量操作清单，请选择等待任务准备就绪后再运行。

   批量操作清单

   如果您选择等待任务准备就绪后再运行，则会显示批量操作清单部分。清单是您希望对其运行指定操作的所有对象的列表。可以选择保存此清单。与 S3 清单文件类似，清单将另存为 CSV 文件并存储在存储桶中。要了解有关批量操作清单的更多信息，请参阅 指定清单。

   完成报告

   S3 批量操作将为在清单中指定的每个对象执行一个任务。完成报告提供了以合并格式查看任务结果的简单途径，且无需进行任何附加设置。您可以为全部任务或仅为失败的任务请求完成报告。要了解有关完成报告的更多信息，请参阅 完成报告。

   权限

   复制失败的最常见原因之一是提供的 Amazon Identity and Access Management (IAM) 角色的权限不足。有关创建此角色的信息，请参阅 配置 IAM 角色以进行 S3 批量复制。确保创建或选择拥有批量复制所需权限的 IAM 角色。

8. 选择保存。

## 为现有复制规则创建分批复制任务

在 Amazon S3 中，实时复制不会复制在您创建复制配置之前已存在于源存储桶中的任何对象。实时复制仅自动复制在创建复制配置之后写入存储桶中的新对象和更新的对象。要复制已存在的对象，可以使用 S3 批量复制来按需复制这些对象。

您可以通过使用 Amazon SDK、Amazon Command Line Interface（Amazon CLI）或 Amazon S3 控制台为现有复制配置来配置 S3 分批复制。有关批量复制的概述，请参阅使用批量复制以复制现有对象。

分批复制任务完成后，您将收到完成报告。有关如何使用报告检查任务的更多信息，请参阅 跟踪任务状态和完成报告。

先决条件

在创建批量复制任务之前，必须创建批量操作 Amazon Identity and Access Management（IAM）角色，来向 Amazon S3 授予代表您执行操作的权限。有关更多信息，请参阅 配置 IAM 角色以进行 S3 批量复制。

使用 S3 控制台

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择批量操作。
3. 选择创建任务。
4. 验证 Amazon Web Services 区域部分显示了要在其中创建任务的区域。
5. 在清单部分中，指定要使用的清单格式。清单是您希望对其运行指定操作的所有对象的列表。要了解有关批量操作清单的更多信息，请参阅 指定清单。

   - 如果您准备了清单，请选择 S3 清单报告 (manifest.json) 或 CSV。如果清单位于受版本控制的存储桶中，则可以指定清单的版本 ID。如果未指定版本 ID，批量操作会使用清单的当前版本。有关创建清单的更多信息，请参阅指定清单。

     > **Note**
     >
     > 如果清单中的对象位于受版本控制的存储桶中，则必须指定对象的版本 ID。有关更多信息，请参阅 指定清单。

   - 要根据复制配置创建清单，请选择 Create manifest using S3 Replication configuration（使用 S3 复制配置创建清单）。然后，选择复制配置的源存储桶。
6. （可选）如果您选择使用 S3 复制配置创建清单，则可以添加其它筛选条件，例如对象创建日期和复制状态。有关如何按复制状态筛选的示例，请参阅为分批复制任务指定清单。
7. （可选）如果您选择使用 S3 复制配置创建清单，则可以保存生成的清单。要保存清单，请选择保存批量操作清单。然后，为清单指定目标存储桶，并选择是否对清单进行加密。

> **Note**
>
> 生成的清单必须存储在与源存储桶相同的 Amazon Web Services 区域 中。

8. 选择下一步。
9. 在操作页上，选择复制，然后选择下一步。
10. （可选）提供 Description（说明）。
11. 必要时调整任务的 Priority（优先级）。数字越大，优先级越高。Amazon S3 尝试在优先级较低的任务之前运行优先级较高的任务。有关任务优先级的更多信息，请参阅 分配任务优先级。
12. （可选）生成完成报告。要生成此报告，请选择生成完成报告。

    如果您选择生成完成报告，则必须选择报告仅失败的任务或全部任务，并为报告提供目标存储桶。
13. 在权限部分中，请确保您选择拥有批量复制所需权限的 IAM 角色。复制失败的最常见原因之一是提供的 IAM 角色的权限不足。有关创建此角色的信息，请参阅 配置 IAM 角色以进行 S3 批量复制。
14. （可选）将任务标签添加到分批复制任务中。
15. 选择下一步。
16. 检查任务配置，然后选择创建任务。

### 通过 S3 清单使用 Amazon CLI

以下示例 `create-job` 命令通过使用 S3 为 Amazon Web Services 账户 *111122223333* 生成的清单创建 S3 批量复制任务。此示例将复制现有对象和之前复制失败的对象。有关按复制状态筛选的信息，请参阅为分批复制任务指定清单。

要使用此命令，请将 *user input placeholders* 替换为您自己的信息。将 IAM 角色 `role/`*batch-Replication-IAM-policy* 替换为您之前创建的 IAM 角色。有关更多信息，请参阅 配置 IAM 角色以进行 S3 批量复制。

```
aws s3control create-job --account-id 111122223333 \
--operation '{"S3ReplicateObject":{}}' \
--report '{"Bucket":"arn:aws:s3:::amzn-s3-demo-completion-report-bucket",\
"Prefix":"batch-replication-report", \
"Format":"Report_CSV_20180820","Enabled":true,"ReportScope":"AllTasks"}' \
--manifest-generator '{"S3JobManifestGenerator": {"ExpectedBucketOwner":
 "111122223333", \
```

```
"SourceBucket": "arn:aws:s3:::amzn-s3-demo-source-bucket", \
"EnableManifestOutput": false, "Filter": {"EligibleForReplication": true, \
"ObjectReplicationStatuses": ["NONE","FAILED"]}}}' \
--priority 1 \
--role-arn arn:aws:iam::111122223333:role/batch-Replication-IAM-policy \
--no-confirmation-required \
--region source-bucket-region
```

> **Note**
>
> 必须从与复制源存储桶相同的 Amazon Web Services 区域中启动该任务。

成功启动分批复制任务后，您会收到任务 ID 作为响应。可以使用下面的 `describe-job` 命令来监控此任务。要使用此命令，请将 *`user input placeholders`* 替换为您自己的信息。

```
aws s3control describe-job --account-id 111122223333 --job-id job-id --region source-bucket-region
```

通过用户提供的清单使用 Amazon CLI

以下示例通过使用 Amazon Web Services 账户 *`111122223333`* 的用户定义清单创建 S3 批量复制任务。如果清单中的对象位于受版本控制的存储桶中，则必须指定对象的版本 ID。只有在清单中指定了版本 ID 的对象才会复制。有关创建清单的更多信息，请参阅指定清单。

要使用此命令，请将 *`user input placeholders`* 替换为您自己的信息。将 IAM 角色 `role/`*`batch-Replication-IAM-policy`* 替换为您之前创建的 IAM 角色。有关更多信息，请参阅配置 IAM 角色以进行 S3 批量复制。

```
aws s3control create-job --account-id 111122223333 \
--operation '{"S3ReplicateObject":{}}' \
--report '{"Bucket":"arn:aws:s3:::amzn-s3-demo-completion-report-bucket",\
"Prefix":"batch-replication-report", \
"Format":"Report_CSV_20180820","Enabled":true,"ReportScope":"AllTasks"}' \
--manifest '{"Spec":{"Format":"S3BatchOperations_CSV_20180820",\
"Fields":["Bucket","Key","VersionId"]},\
"Location":{"ObjectArn":"arn:aws:s3:::amzn-s3-demo-manifest-bucket/manifest.csv",\
"ETag":"Manifest Etag"}}' \
--priority 1 \
--role-arn arn:aws:iam::111122223333:role/batch-Replication-IAM-policy \
--no-confirmation-required \
```

```
--region source-bucket-region
```

> **Note**
>
> 必须从与复制源存储桶相同的 Amazon Web Services 区域中启动该任务。

成功启动分批复制任务后，您会收到任务 ID 作为响应。可以使用下面的 `describe-job` 命令来监控此任务。

```
aws s3control describe-job --account-id 111122223333 --job-id job-id --region source-bucket-region
```

## 对复制进行问题排查

本节列出了 Amazon S3 复制的问题排查提示以及有关 S3 批量复制错误的信息。

主题


- S3 复制问题排查提示
- 批量复制错误


### S3 复制问题排查提示

如果在您配置复制之后，对象副本未出现在目标桶中，请使用以下问题排查提示确定并修复问题。

- 大多数对象会在 15 分钟内复制。Amazon S3 复制对象所需的时间取决于多个因素，包括源和目标区域对，以及对象的大小。对于大型对象，复制可能需要几个小时。要想了解复制时间，您可以使用 S3 Replication Time Control（S3 RTC）。

  如果要复制的对象较大，请稍候片刻，然后再检查它是否出现在目标桶中。还可以检查源对象的复制状态。如果对象复制状态为 `PENDING`，表示 Amazon S3 尚未完成复制。如果对象复制状态为 `FAILED`，请检查对源桶设置的复制配置。

  此外，要在复制期间接收有关失败的信息，您可以设置 Amazon S3 事件通知来接收复制失败事件。有关更多信息，请参阅使用 Amazon S3 事件通知接收复制失败事件。
- 要检查对象的复制状态，可以调用 `HeadObject` API 操作。`HeadObject` API 操作返回对象的 `PENDING`、`COMPLETED` 或 `FAILED` 复制状态。在对 `HeadObject` API 调用的响应中，复制状态将在 `x-amz-replication-status` 标头中返回。

> **Note**
>
> 要运行 HeadObject，您必须对您请求的对象拥有读取权限。HEAD 请求与 GET 请求具有相同的选项，无需执行 GET 操作。例如，要使用 Amazon Command Line Interface（Amazon CLI）运行 HeadObject 请求，可以运行以下命令。将 *user input placeholders* 替换为您自己的信息。
>
> ```
> aws s3api head-object --bucket amzn-s3-demo-source-bucket --key index.html
> ```

- 如果 HeadObject 返回复制状态为 FAILED 的对象，则可以使用 S3 批量复制来复制这些失败的对象。有关更多信息，请参阅 the section called “复制现有对象”。或者，您可以将失败的对象重新上传到源桶，这将启动新对象的复制。
- 在源桶上的复制配置中，验证以下几点：
  - 目标存储桶的 Amazon 资源名称 (ARN) 是否正确。
  - 键名前缀是否正确。例如，如果将配置设置为复制具有前缀 Tax 的对象，则仅复制具有 Tax/document1 或 Tax/document2 等键名的对象。不会复制具有键名 document3 的对象。
  - 复制规则的状态为 Enabled。
- 在复制配置中验证尚未对任何存储桶暂停版本控制。源桶和目标桶必须均已启用版本控制。
- 如果将复制规则设置为将对象所有权更改为目标桶拥有者，则用于复制的 Amazon Identity and Access Management（IAM）角色必须具有 s3:ObjectOwnerOverrideToBucketOwner 权限。此权限是对资源（在本例中为目标桶）授予的。例如，以下 Resource 语句显示如何授予对目标桶的这一权限：

```
{
  "Effect":"Allow",
  "Action":[
    "s3:ObjectOwnerOverrideToBucketOwner"
  ],
  "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}
```

- 如果目标桶由另一个账户拥有，则目标桶的拥有者还必须通过目标桶策略向源桶拥有者授予 s3:ObjectOwnerOverrideToBucketOwner 权限。要使用以下示例桶策略，请将 *user input placeholders* 替换为您自己的信息：

```
{
```

```
  "Version": "2012-10-17",
  "Id": "Policy1644945280205",
  "Statement": [
    {
      "Sid": "Stmt1644945277847",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789101:role/s3-replication-role"
      },
      "Action": [
        "s3:ReplicateObject",
        "s3:ReplicateTags",
        "s3:ObjectOwnerOverrideToBucketOwner"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    }
  ]
}
```

> **Note**
>
> 如果目标桶的对象所有权设置包括强制桶拥有者，则无需在复制规则中将此设置更新为将对象所有权更改为目标桶拥有者。原定设置情况下，对象所有权将发生变化。有关更改副本所有权的更多信息，请参阅更改副本所有权。

- 如果您要在跨账户场景（即源存储桶和目标存储桶由不同的 Amazon Web Services 账户拥有）中设置复制配置，则目标存储桶无法配置为申请方付款存储桶。有关更多信息，请参阅 使用申请方付款通用存储桶进行存储传输和使用。
- 如果存储桶的源对象使用具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）来进行加密，则必须将复制规则配置为包含 Amazon KMS 加密的对象。确保在 Amazon S3 控制台中的加密设置下选择复制使用 Amazon KMS 加密的对象。然后，选择用于加密目标对象的 Amazon KMS 密钥。

> **Note**
>
> 如果目标桶位于其他账户中，请指定目标账户拥有的 Amazon KMS 客户自主管理型密钥。不要使用原定设置的 Amazon S3 托管式密钥（aws/s3）。使用默认密钥会使用由源账户拥有的 Amazon S3 托管式密钥来加密对象，从而防止与其它账户共享对象。因此，目标账户将无法访问目标桶中的对象。

要使用属于目标账户的 Amazon KMS 密钥加密目标对象，目标账户必须在 KMS 密钥策略中向复制角色授予 kms:GenerateDataKey 和 kms:Encrypt 权限。要在 KMS 密钥策略中使用以下示例语句，请将 *user input placeholders* 替换为您自己的信息：

```
{
    "Sid": "AllowS3ReplicationSourceRoleToUseTheKey",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::123456789101:role/s3-replication-role"
    },
    "Action": ["kms:GenerateDataKey", "kms:Encrypt"],
    "Resource": "*"
}
```

如果您在 Amazon KMS 密钥策略中的 Resource 语句中使用星号（*），则该策略将使用 KMS 密钥的权限仅授予复制角色。该策略不允许复制角色提升其权限。

原定设置情况下，KMS 密钥策略向根用户授予对密钥的完全权限。这些权限可以委派给同一账户中的其他用户。除非源 KMS 密钥策略中具有 Deny 语句，否则，使用 IAM policy 向复制角色授予对源 KMS 密钥的权限就足够了。

> **Note**
>
> 将访问权限限制到特定 CIDR 范围、虚拟私有云（VPC）端点或 S3 接入点的 KMS 密钥策略可能会导致复制失败。

如果源或目标 KMS 密钥根据加密上下文授予权限，请确认对于桶开启了 Amazon S3 桶密钥。如果桶已开启了 S3 桶密钥，则加密上下文必须是桶级资源，如下所示：

```
"kms:EncryptionContext:arn:aws:arn": [
     "arn:aws:s3:::amzn-s3-demo-source-bucket"
     ]
"kms:EncryptionContext:arn:aws:arn": [
     "arn:aws:s3:::amzn-s3-demo-destination-bucket"
     ]
```

除了 KMS 密钥策略授予的权限外，源账户还必须向复制角色的 IAM policy 添加以下最低权限：

```
{
    "Effect": "Allow",
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": [
        "Source-KMS-Key-ARN"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "kms:GenerateDataKey",
        "kms:Encrypt"
    ],
    "Resource": [
        "Destination-KMS-Key-ARN"
    ]
}
```

有关如何复制使用 Amazon KMS 加密的对象的更多信息，请参阅复制加密的对象。

- 如果目标桶由另一个 Amazon Web Services 账户拥有，请验证桶拥有者是否对目标桶设置了允许源桶拥有者复制对象的桶策略。有关示例，请参阅针对不同账户中的存储桶配置复制。
- 要将对象锁定与复制功能结合使用，您必须在用于设置复制的 Amazon Identity and Access Management（IAM）角色中，授予对源 S3 存储桶的两项额外的权限。这两项额外的权限是 `s3:GetObjectRetention` 和 `s3:GetObjectLegalHold`。如果角色已有 `s3:Get*` 权限声明，则该声明已满足要求。有关更多信息，请参阅 the section called “将对象锁定与 S3 复制结合使用”。
- 如果在验证权限后您的对象仍无法复制，请检查以下位置是否存在任何显式 Deny 语句：
  - 源或目标桶策略中的 Deny 语句。如果桶策略拒绝针对以下任一操作访问复制角色，则复制将失败：

    源桶：

```
            "s3:GetReplicationConfiguration",
            "s3:ListBucket",
            "s3:GetObjectVersionForReplication",
            "s3:GetObjectVersionAcl",
            "s3:GetObjectVersionTagging"
```

目标桶：

```
            "s3:ReplicateObject",
            "s3:ReplicateDelete",
            "s3:ReplicateTags"
```

  - 附加到 IAM 角色的 Deny 语句或权限边界可能导致复制失败。
  - 附加到源账户或目标账户的 Amazon Organizations 服务控制策略（SCP）中的 Deny 语句可能导致复制失败。
  - 附加到源或目标存储桶的 Amazon Organizations 资源控制策略（RCP）中的 Deny 语句可能导致复制失败。
- 如果对象副本未出现在目标桶中，以下问题可能会禁止复制：
  - 若源桶中的某对象是另一个复制配置所创建的副本，Amazon S3 不会复制该对象。例如，如果您设置从桶 A 到桶 B 再到桶 C 的复制配置，则 Amazon S3 不会将桶 B 中的对象副本复制到桶 C。
  - 源桶拥有者可以向其他 Amazon Web Services 账户授予上载对象的权限。默认情况下，源桶拥有者对于其他账户创建的对象没有权限。复制配置仅复制源桶拥有者对其具有访问权限的对象。为避免出现此问题，源存储桶拥有者可以向其它 Amazon Web Services 账户授予有条件地创建对象的权限，从而要求针对这些对象的显式访问权限。有关策略示例，请参阅 在授予上传对象的跨账户权限的同时，确保存储桶拥有者拥有完全控制权。
- 假设在复制配置中，您添加了一个规则以复制具有特定标签的对象子集。在这种情况下，您必须在创建对象时分配特定的标签键和值，以供 Amazon S3 复制对象。如果您先创建对象，然后向现有对象添加标签，Amazon S3 将不会复制对象。
- 使用 Amazon S3 事件通知，以便您在对象未复制到其目标 Amazon Web Services 区域的情况下收到通知。Amazon S3 事件通知可以通过 Amazon Simple Queue Service（Amazon SQS）、Amazon Simple Notification Service（Amazon SNS）或 Amazon Lambda 提供。有关更多信息，请参阅 使用 Amazon S3 事件通知接收复制失败事件。

  您还可以使用 Amazon S3 事件通知查看复制失败原因。要查看失败原因的列表，请参阅 Amazon S3 复制失败原因。

## 批量复制错误

要对未复制到目标存储桶的对象进行故障排除，请检查存储桶、复制角色和用于创建批量复制任务的 IAM 角色的不同权限类型。此外，请务必检查存储桶的屏蔽公共访问权限设置和 S3 对象所有权设置。

有关使用批量复制的更多故障排除提示，请参阅the section called “排查批量操作问题”。

当使用批量复制时，可能会遇到以下错误之一：

- 生成清单时未找到符合筛选条件的密钥。

  出现此错误的原因为以下之一：

  - 当源存储桶中的对象存储在 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储类中时。

    要对这些对象使用批量复制，请先在批量操作任务中使用还原 (`S3InitiateRestoreObjectOperation`) 操作，将它们还原到 S3 Standard 存储类。有关更多信息，请参阅恢复已归档的对象和还原对象（批量操作）。还原对象后，您可以使用批量复制任务来复制它们。

  - 当提供的筛选条件与源存储桶中的任何有效对象都不匹配时。

    验证并更正筛选条件。例如，在批量复制规则中，筛选条件负责查找源存储桶中带有 `Tax/` 前缀的所有对象。如果前缀名称输入不准确，开头和结尾都有一个斜杠（即 `/Tax/`），而不是仅在结尾处有斜杠，则找不到任何 S3 对象。要解决此错误，请更正前缀，在本例中就是将复制规则中的 `/Tax/` 更改为 `Tax/`。

- 批量操作状态为失败，原因是：无法将任务报告写入报告桶。

  如果用于批量操作任务的 IAM 角色无法将完成报告放到您创建任务时指定的位置，则会出现此错误。要解决此错误，请检查 IAM 角色是否对您要保存批量操作完成报告的存储桶具有 `s3:PutObject` 权限。我们建议将报告发送到与源存储桶不同的存储桶。

  有关解决此错误的其它提示，请参阅the section called “当存在权限问题或启用了保留模式时，未交付任务报告”。

- 批量操作已完成但出现失败，并且失败总数不是 0。

  如果正在运行的批量复制任务存在对象权限不足问题，则会出现此错误。如果您对批量复制任务使用复制规则，请确保用于复制的 IAM 角色具有适当的权限，可访问源存储桶或目标存储桶中的对象。也可以检查批量复制完成报告，以查看特定的 Amazon S3 复制失败原因。

- 批量任务成功运行，但目标桶中预期的对象数量不相同。

  当批量复制任务中提供的清单中列出的对象与您在创建任务时选择的筛选条件不匹配时，就会出现此错误。当源桶中的对象与任何复制规则不匹配且未包含在生成的清单中时，您也可能会收到此消息。

向现有复制配置添加新的复制规则后，会出现批量操作失败

批量操作尝试对源桶的复制配置中的每条规则执行现有对象复制。如果任何现有复制规则出现问题，则可能会出现失败。

批量操作任务的完成报告解释了任务失败的原因。有关常见错误的列表，请参阅Amazon S3 复制失败原因。

## 使用指标、事件通知和状态监控复制

可以通过以下机制监控实时复制配置和 S3 批量复制任务：

- S3 复制指标：当您启用 S3 复制指标时，Amazon CloudWatch 会发出一些指标，可以使用这些指标在复制规则级别跟踪待处理字节、待处理操作和复制延迟。可以通过 Amazon S3 控制台和 Amazon CloudWatch 控制台查看 S3 复制指标。在 Amazon S3 控制台中，可以在源存储桶的指标选项卡中查看这些指标。有关 S3 复制指标的更多信息，请参阅the section called “使用 S3 复制指标”。
- S3 Storage Lens 存储分析功能指标：除了 S3 复制指标外，还可以使用 S3 Storage Lens 存储分析功能控制面板提供的与复制相关的数据保护指标。例如，如果使用 S3 Storage Lens 存储分析功能中的免费指标，则可以看到诸如从源存储桶复制的总字节数或从源存储桶复制的对象计数之类的指标。

  要审计总体复制状况，可以在 S3 Storage Lens 存储分析功能中启用高级指标。借助 S3 Storage Lens 存储分析功能中的高级指标，可以查看有多少不同类型的复制规则，包括复制目标无效的复制规则的计数。

  有关在 S3 Storage Lens 存储分析功能中使用复制指标的更多信息，请参阅the section called “在 S3 Storage Lens 存储分析功能控制面板中查看复制指标”。
- S3 事件通知：当对象未复制到其目标 Amazon Web Services 区域或未在特定阈值内复制对象时，在这类情况下，S3 事件通知可以在对象级别通知您。S3 事件通知提供以下复制事件类型：`s3:Replication:OperationFailedReplication`、`s3:Replication:OperationMissedTh`和 `s3:Replication:OperationNotTracked`。

  Amazon S3 事件可以通过 Amazon Simple Queue Service (Amazon SQS)、Amazon Simple Notification Service (Amazon SNS) 或 Amazon Lambda 获得。有关更多信息，请参阅 the section called “接收复制失败事件”。
- 复制状态值：还可以检索对象的复制状态。复制状态有助于您确定正在复制的对象的当前状态。源对象的复制状态将返回 `PENDING`、`COMPLETED`、或 `FAILED`。副本的复制状态将返回 `REPLICA`。

  在创建 S3 批量复制任务时，也可以使用复制状态值。例如，可以使用这些状态值来复制从未复制过或复制失败的对象。

有关检索对象的复制状态的更多信息，请参阅the section called “获取复制状态”。有关将这些值与批量复制结合使用的更多信息，请参阅the section called “分批复制任务的筛选条件”。

主题

- 使用 S3 复制指标
- 在 S3 Storage Lens 存储分析功能控制面板中查看复制指标
- 使用 Amazon S3 事件通知接收复制失败事件
- 获取复制状态信息

## 使用 S3 复制指标

S3 复制指标为复制配置中的复制规则提供了详细的指标。使用复制指标，您可以通过跟踪待复制的字节数、待复制的操作数、复制失败的操作数和复制延迟来逐分钟监控进度。

> **Note**
>
> - S3 复制指标的费率与 Amazon CloudWatch 自定义指标费率相同。有关更多信息，请参阅 Amazon CloudWatch 定价。
> - 如果您使用 S3 Replication Time Control，Amazon CloudWatch 在相应的复制规则上启用 S3 RTC 后 15 分钟开始报告复制指标。

启用 S3 Replication Time Control（S3 RTC）时，将自动开启 S3 复制指标。在创建或编辑规则时，还可以独立于 S3 RTC 启用 S3 复制指标。S3 RTC 包含其他功能，例如服务水平协议（SLA）和错过阈值的通知。有关更多信息，请参阅 使用 S3 Replication Time Control 满足合规性要求。

启用 S3 复制指标后，Amazon S3 会将以下指标发布到 Amazon CloudWatch。系统将以最大努力传输 CloudWatch 指标。

| 指标名称 | 指标描述 | 该指标适用于哪些对象？ | 该指标在哪个区域发布？ | 如果删除了目标存储桶，仍会发布该指标吗？ | 如果不进行复制，仍会发布该指标吗？ |
| --- | --- | --- | --- | --- | --- |
| 待复制的字节数 | 给定复制规则的待复制对象的总字节数。 | 此指标仅适用于通过 S3 Cross-Region Replication（S3 CRR）或 S3 Same-Region Replication（S3 SRR）复制的新对象。 | 该指标发布在目标存储桶的区域中。 | 否 | 是 |
| 复制延迟 | 对于给定的复制规则，复制目标存储桶落后于源存储桶的最大秒数。 | 此指标仅适用于使用 S3 CRR 或 S3 SRR 复制的新对象。 | 该指标发布在目标存储桶的区域中。 | 否 | 是 |
| 待复制的操作 | 给定复制规则的待复制操作的数量。此指标跟踪与对象、删除标记、标签、访问控制列表（ACL）和 S3 对象锁定相关的操作。 | 此指标仅适用于使用 S3 CRR 或 S3 SRR 复制的新对象。 | 该指标发布在目标存储桶的区域中。 | 否 | 是 |
| 复制失败的操作 | 给定复制规则的复制失败的操作数。此 | 此指标既适用于使用 S3 CRR 或 S3 | 该指标发布在源存储桶的区域中。 | 是 | 否 |

| 指标名称 | 指标描述 | 该指标适用于哪些对象？ | 该指标在哪个区域发布？ | 如果删除了目标存储桶，仍会发布该指标吗？ | 如果不进行复制，仍会发布该指标吗？ |
| --- | --- | --- | --- | --- | --- |
| | 指标跟踪与对象、删除标记、标签、访问控制列表（ACL）和对象锁定相关的操作。<br><br>复制失败的操作跟踪以一分钟为间隔汇总的 S3 复制失败。要确定复制失败的特定对象及其失败原因，请在 Amazon S3 事件通知中订阅 `OperationFailedReplication` 事件。有关更多信息，请参阅 使用 Amazon S3 事件通知接收复制失败事件。 | SRR 复制的新对象，也适用于使用 S3 批量复制所复制的现有对象。<br><br>**Note**<br>如果 S3 批量复制任务根本无法运行，则指标不会发送到 Amazon CloudWatch。例如，如果您没有运行 S3 批量复制任务 | | | |

| 指标名称 | 指标描述 | 该指标适用于哪些对象？ | 该指标在哪个区域发布？ | 如果删除了目标存储桶，仍会发布该指标吗？ | 如果不进行复制，仍会发布该指标吗？ |
| --- | --- | --- | --- | --- | --- |
| | | 所需的权限，或者复制配置中的标签或前缀不匹配，则您的任务将无法运行。 | | | |

有关使用 CloudWatch 中的这些指标的信息，请参阅 the section called “CloudWatch 中的 S3 复制指标”。

启用 S3 复制指标

您可以开始将 S3 复制指标与新的或现有的复制规则结合使用。有关创建复制规则的完整说明，请参阅针对同一账户中的存储桶配置复制。您可以选择将复制规则应用于整个 S3 存储桶，或应用于具有特定前缀或标签的 Amazon S3 对象。

本主题提供了在源和目标存储桶由相同或不同的 Amazon Web Services 账户拥有时，在复制配置中启用 S3 复制指标的说明。

要使用 Amazon Command Line Interface（Amazon CLI）启用复制指标，您必须向启用 Metrics 的源存储桶添加复制配置。在此示例配置中，以 *Tax* 为前缀的对象将复制到目标存储桶 *amzn-s3-demo-bucket*，并为这些对象生成指标。

```
{
    "Rules": [
        {
            "Status": "Enabled",
            "Filter": {
                "Prefix": "Tax"
            },
            "Destination": {
                "Bucket": "arn:aws:s3:::amzn-s3-demo-bucket",
                "Metrics": {
                    "Status": "Enabled"
                }
            },
            "Priority": 1
        }
    ],
    "Role": "IAM-Role-ARN"
}
```

查看复制指标

在 Amazon S3 控制台中，可以在源通用存储桶的指标选项卡中查看 S3 复制指标。Amazon CloudWatch 控制台中也提供了这些 Amazon CloudWatch 指标。当您启用 S3 复制指标时，Amazon CloudWatch 会发出一些指标，您可以使用这些指标在复制规则级别跟踪待处理字节、待处理操作和复制延迟。

当您通过 Amazon S3 控制台或 Amazon S3 REST API 使用 S3 Replication Time Control（S3 RTC）启用复制时，S3 复制指标将自动开启。在创建或编辑规则时，还可以独立于 S3 RTC 启用 S3 复制指标。

如果您使用 S3 Replication Time Control，Amazon CloudWatch 在相应的复制规则上启用 S3 RTC 后 15 分钟开始报告复制指标。有关更多信息，请参阅 使用 S3 复制指标。

复制指标跟踪复制配置的规则 ID。复制规则 ID 可以特定于前缀、标签或两者的组合。

有关 Amazon S3 的 CloudWatch 指标的更多信息，请参阅 使用 Amazon CloudWatch 监控指标。

先决条件

创建启用了 S3 复制指标的复制规则。有关更多信息，请参阅 the section called “查看复制指标”。

通过源存储桶的指标选项卡查看 S3 复制指标

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在存储桶列表中，选择您要获取其复制指标的对象所在的源存储桶的名称。
4. 请选择 Metrics（指标）选项卡。
5. 在复制指标下，选择要查看其指标的复制规则。
6. 请选择 Display charts (显示图表)。

   Amazon S3 会针对您选择的指标显示复制延迟、待复制的字节数、待复制的操作和复制失败的操作图表。

## 在 S3 Storage Lens 存储分析功能控制面板中查看复制指标

除了 S3 复制指标外，还可以使用 S3 Storage Lens 存储分析功能提供的与复制相关的数据保护指标。S3 Storage Lens 存储统计管理工具是一项云存储分析功能，您可以使用它在整个组织范围内了解对象存储的使用情况和活动。有关更多信息，请参阅使用 S3 Storage Lens 存储统计管理工具保护您的数据。

S3 Storage Lens 存储分析功能具有两层指标：免费指标以及高级指标和建议，您可以支付额外费用升级到高级指标和建议。借助高级指标和建议，您可以访问其他指标和功能，以深入了解您的存储。有关 S3 Storage Lens 存储统计管理工具定价的信息，请参阅 Amazon S3 定价。

如果您使用 S3 Storage Lens 存储分析功能中的免费指标，则可以看到诸如从源存储桶复制的总字节数或从源存储桶复制的对象计数之类的指标。

要审计总体复制状况，可以在 S3 Storage Lens 存储分析功能中启用高级指标。借助 S3 Storage Lens 存储分析功能中的高级指标，可以查看有多少不同类型的复制规则，包括复制目标无效的复制规则的计数。

有关 S3 Storage Lens 存储分析功能指标的完整列表，包括每个层中的复制指标，请参阅 S3 Storage Lens 存储分析功能指标词汇表。

先决条件

创建实时复制配置或 S3 批量复制任务。

在 Amazon S3 Storage Lens 存储统计管理工具中查看复制指标

1. 创建 S3 Storage Lens 存储分析功能控制面板。如需分步指导，请参阅 the section called “使用 S3 控制台”。
2. （可选）在控制面板设置过程中，如果要查看所有 S3 Storage Lens 存储分析功能复制指标，请选择高级指标和建议，然后选择高级数据保护指标。有关指标的完整列表，请参阅 S3 Storage Lens 存储统计管理工具指标词汇表。

   如果您启用高级指标和建议，则可以进一步了解您的复制配置。例如，可以使用 S3 Storage Lens 存储分析功能复制规则计数指标，来获取有关配置为进行复制的存储桶的详细信息。此信息包括桶和区域内部以及跨桶和区域的复制规则。有关更多信息，请参阅 the section called “计算每个桶的复制规则总计数”。
3. 创建控制面板后，打开控制面板，然后选择存储桶选项卡。
4. 向下滚动到 Bucket（桶）部分。在 Metrics categories（指标类别）下，选择 Data protection（数据保护）。然后清除 Summary（摘要）。
5. 要筛选存储桶列表以仅显示复制指标，请选择首选项图标（  ）。
6. 清除所有数据保护指标的切换开关，直到只有复制指标保持选中状态。
7. （可选）在 Page size（页面大小）下，选择要在列表中显示的桶数。
8. 选择继续。

## 使用 Amazon S3 事件通知接收复制失败事件

如果在复制配置中启用了 S3 复制指标，则可以设置 Amazon S3 事件通知，以便在对象未复制到目标 Amazon Web Services 区域时通知您。如果在复制配置中启用了 S3 Replication Time Control（S3 RTC），则当未在 15 分钟的 S3 RTC 复制阈值内复制对象时，您也会收到通知。

通过使用以下 `Replication` 事件类型，可以通过跟踪待处理字节数、待处理的操作和复制延迟来逐分钟监控复制事件的进度。有关 S3 复制指标的更多信息，请参阅使用 S3 复制指标。

- 当符合复制条件的对象复制失败时，`s3:Replication:OperationFailedReplication` 事件类型将通知您。
- 当符合复制（使用 S3 RTC）条件的对象超过 15 分钟的复制阈值时，`s3:Replication:OperationMissedThreshold` 事件类型将通知您。

- 当符合复制（使用 S3 RTC）条件的对象在 15 分钟阈值后复制时，`s3:Replication:OperationReplicatedAfterThreshold` 事件类型将通知您。
- 当符合实时复制（同区域复制 [SRR] 或跨区域复制 [CRR]）条件的对象不再受复制指标跟踪时，`s3:Replication:OperationNotTracked` 事件类型会通知您。

有关所有受支持的复制事件类型的完整描述，请参阅 the section called “SQS、SNS 和 Lambda 支持的事件类型”。

有关 S3 事件通知捕获的故障代码的列表，请参阅 Amazon S3 复制失败原因。

您可以通过 Amazon Simple Queue Service（Amazon SQS）、Amazon Simple Notification Service（Amazon SNS）或 Amazon Lambda 接收 S3 事件通知。有关更多信息，请参阅 the section called “Amazon S3 事件通知”。

有关如何配置 Amazon S3 事件通知的说明，请参阅 Enabling event notifications（启用事件通知）。

> **Note**
>
> 除了启用事件通知外，还要确保您也启用 S3 复制指标。有关更多信息，请参阅 the section called “查看复制指标”。

以下是 Amazon S3 发送以发布 `s3:Replication:OperationFailedReplication` 事件的消息示例。有关更多信息，请参阅 the section called “事件消息结构”。

```
{
  "Records": [
    {
      "eventVersion": "2.2",
      "eventSource": "aws:s3",
      "awsRegion": "us-east-1",
      "eventTime": "2024-09-05T21:04:32.527Z",
      "eventName": "Replication:OperationFailedReplication",
      "userIdentity": {
        "principalId": "s3.amazonaws.com"
      },
      "requestParameters": {
        "sourceIPAddress": "s3.amazonaws.com"
      },
      "responseElements": {
```

```
        "x-amz-request-id": "123bf045-2b4b-4ca8-a211-c34a63c59426",
        "x-amz-id-2":
 "12VAWNDIHnwJsRhTccqQTeAPoXQmRt22KkewMV8G3XZihAuf9CLDdmkApgZzudaIe2KlLfDqGS0="
      },
      "s3": {
        "s3SchemaVersion": "1.0",
        "configurationId": "ReplicationEventName",
        "bucket": {
          "name": "amzn-s3-demo-bucket1",
          "ownerIdentity": {
            "principalId": "111122223333"
          },
          "arn": "arn:aws:s3:::amzn-s3-demo-bucket1"
        },
        "object": {
          "key": "replication-object-put-test.png",
          "size": 520080,
          "eTag": "e12345ca7e88a38428305d3ff7fcb99f",
          "versionId": "abcdeH0Xp66ep__QDjR76LK7Gc9X4wKO",
          "sequencer": "0066DA1CBF104C0D51"
        }
      },
      "replicationEventData": {
        "replicationRuleId": "notification-test-replication-rule",
        "destinationBucket": "arn:aws:s3:::amzn-s3-demo-bucket2",
        "s3Operation": "OBJECT_PUT",
        "requestTime": "2024-09-05T21:03:59.168Z",
        "failureReason": "AssumeRoleNotPermitted"
      }
    }
  ]
}
```

### Amazon S3 复制失败原因

下表列出了 Amazon S3 复制失败原因。可以通过 Amazon S3 事件通知接收 `s3:Replication:OperationFailedReplication` 事件，然后查看 `failureReason` 值，来查看这些原因。

还可以在 S3 批量复制完成报告中查看这些失败原因。有关更多信息，请参阅 [分批复制完成报告](#)。

| 复制失败原因 | 描述 |
| --- | --- |
| AssumeRoleNotPermitted | Amazon S3 无法代入在复制配置或批量操作任务中指定的 Amazon Identity and Access Management（IAM）角色。 |
| DstBucketInvalidRegion | 目标存储桶未处于由批量操作任务指定的同一个 Amazon Web Services 区域中。此错误特定于分批复制。 |
| DstBucketNotFound | Amazon S3 找不到在复制配置中指定的目标存储桶。 |
| DstBucketObjectLockConfigMissing | 要在启用对象锁定的情况下从源存储桶复制对象，目标存储桶也必须启用对象锁定。此错误表示目标存储桶中可能未启用对象锁定。有关更多信息，请参阅 对象锁定注意事项。 |
| DstBucketUnversioned | 未为 S3 目标存储桶启用版本控制。要使用 S3 复制来复制对象，请对目标存储桶启用版本控制。 |
| DstDelObjNotPermitted | Amazon S3 无法将删除标记复制到目标存储桶。针对目标存储桶的 s3:ReplicateDelete 权限可能缺失。 |
| DstKmsKeyInvalidState | 适用于目标存储桶的 Amazon Key Management Service（Amazon KMS）密钥处于无效状态。查看并启用所需的 Amazon KMS 密钥。有关管理 Amazon KMS 密钥的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的 Amazon KMS 密钥的密钥状态。 |
| DstKmsKeyNotFound | 在复制配置中为目标存储桶配置的 Amazon KMS 密钥不存在。 |

| 复制失败原因 | 描述 |
| --- | --- |
| DstMultipartCompleteNotPermitted | Amazon S3 无法完成目标存储桶中对象的分段上传。针对目标存储桶的 s3:ReplicateObject 权限可能缺失。 |
| DstMultipartInitNotPermitted | Amazon S3 无法启动将对象分段上传到目标存储桶。针对目标存储桶的 s3:ReplicateObject 权限可能缺失。 |
| DstMultipartUploadNotPermitted | Amazon S3 无法将分段上传对象上传到目标存储桶。针对目标存储桶的 s3:ReplicateObject 权限可能缺失。 |
| DstObjectHardDeleted | S3 分批复制不支持重新复制从目标存储桶中使用对象的版本 ID 删除的对象。此错误特定于分批复制。 |
| DstPutAclNotPermitted | Amazon S3 无法将对象访问控制列表（ACL）复制到目标存储桶。针对目标存储桶的 s3:ReplicateObject 权限可能缺失。 |
| DstPutLegalHoldNotPermitted | 在复制不可变对象时，Amazon S3 无法对目标对象设置对象锁定法定保留。针对目标存储桶的 s3:PutObjectLegalHold 权限可能缺失。有关更多信息，请参阅 法定保留。 |
| DstPutObjectNotPermitted | Amazon S3 无法将对象复制到目标存储桶。针对目标存储桶的 s3:ReplicateObject 或 s3:ObjectOwnerOverrideToBucketOwner 权限可能缺失。 |
| DstPutRetentionNotPermitted | 在复制不可变对象时，Amazon S3 无法对目标对象设置保留期。针对目标存储桶的 s3:PutObjectRetention 权限可能缺失。 |

| 复制失败原因 | 描述 |
| --- | --- |
| DstPutTaggingNotPermitted | Amazon S3 无法将对象标签复制到目标存储桶。针对目标存储桶的 s3:ReplicateObject 权限可能缺失。 |
| DstVersionNotFound | Amazon S3 无法在目标存储桶中找到需要复制其元数据的所需对象版本。 |
| InitiateReplicationNotPermitted | Amazon S3 无法在对象上启动复制。批量操作任务可能缺少 s3:InitiateReplication 权限。此错误特定于分批复制。 |
| SrcBucketInvalidRegion | 源存储桶未处于批量操作任务指定的同一个 Amazon Web Services 区域中。此错误特定于分批复制。 |
| SrcBucketNotFound | Amazon S3 找不到源存储桶。 |
| SrcBucketReplicationConfigMissing | Amazon S3 找不到源存储桶的复制配置。 |
| SrcGetAclNotPermitted | Amazon S3 无法访问源存储桶中要复制的对象。针对源存储桶对象的 s3:GetObjectVersionAcl 权限可能缺失。<br><br>源存储桶中的对象必须由存储桶拥有者所有。如果启用了 ACL，则验证应将“对象所有权”设置为“首选存储桶拥有者”还是“对象编写者”。如果将“对象所有权”设置为“首选存储桶拥有者”，则源存储桶对象必须具有 bucket-owner-full-control ACL，存储桶拥有者才能成为对象拥有者。源账户可以通过将“对象所有权”设置为“强制存储桶拥有者”并禁用 ACL，从而获取其存储桶中所有对象的所有权。 |
| SrcGetLegalHoldNotPermitted | Amazon S3 无法访问 S3 对象锁定法定保留信息。 |

| 复制失败原因 | 描述 |
| --- | --- |
| SrcGetObjectNotPermitted | Amazon S3 无法访问源存储桶中要复制的对象。针对源存储桶的 s3:GetObjectVersionForReplication 权限可能缺失。 |
| SrcGetRetentionNotPermitted | Amazon S3 无法访问 S3 对象锁定保留期信息。 |
| SrcGetTaggingNotPermitted | Amazon S3 无法从源存储桶访问对象标签信息。针对源存储桶的 s3:GetObjectVersionTagging 权限可能缺失。 |
| SrcHeadObjectNotPermitted | Amazon S3 无法从源存储桶检索对象元数据。针对源存储桶的 s3:GetObjectVersionForReplication 权限可能缺失。 |
| SrcKeyNotFound | Amazon S3 找不到要复制的源对象密钥。源对象可能在复制完成之前已被删除。 |
| SrcKmsKeyInvalidState | 适用于源存储桶的 Amazon KMS 密钥处于无效状态。查看并启用所需的 Amazon KMS 密钥。有关管理 Amazon KMS 密钥的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的 Amazon KMS 密钥的密钥状态。 |
| SrcObjectNotEligible | 某些对象不符合复制条件。这可能是由于对象的存储类或对象标签与复制配置不匹配所致。 |
| SrcObjectNotFound | 源对象不存在。 |
| SrcReplicationNotPending | Amazon S3 已经复制了此对象。此对象不再处于待复制状态。 |
| SrcVersionNotFound | Amazon S3 找不到要复制的源对象版本。源对象版本可能在复制完成之前已被删除。 |

相关 主题

[为实时复制设置权限]

[对复制进行问题排查]

## 获取复制状态信息

复制状态可以帮助您确定正在复制的对象的当前状态。源对象的复制状态将返回 PENDING、COMPLETED、或 FAILED。副本的复制状态将返回 REPLICA。

在创建 S3 批量复制任务时，也可以使用复制状态值。例如，可以使用这些状态值来复制从未复制过或复制失败的对象。有关将这些值与批量复制结合使用的更多信息，请参阅the section called “将复制状态信息和批量复制任务结合使用”。

主题

- 复制状态概述
- 复制到多个目标存储桶时的复制状态
- 启用了 Amazon S3 副本修改同步时的复制状态
- 将复制状态信息和批量复制任务结合使用
- 查找复制状态

### 复制状态概述

在复制中，您有一个源存储桶（对它配置复制）和一个或多个目标存储桶（Amazon S3 将对象复制到其中）。当您请求这些存储桶中的对象（使用 GetObject）或对象元数据（使用 HeadObject）时，Amazon S3 将在响应中返回 x-amz-replication-status 标头：

- 如果请求源存储桶中的对象，Amazon S3 将返回 x-amz-replication-status 标头（如果请求中的对象符合复制条件）。

  例如，假设您在复制配置中指定了对象前缀 TaxDocs，以指示 Amazon S3 仅复制键名前缀为 TaxDocs 的对象。您上传的具有此键名前缀的任何对象（例如 TaxDocs/document1.pdf）都将复制。对于具有此键名前缀的对象请求，Amazon S3 会返回其对象复制状态为以下值之一的 x-amz-replication-status 标头：PENDING、COMPLETED 或 FAILED。

> **Note**
>
> 如果在上传对象后对象复制失败，您无法重试复制。必须再次上传该对象，或者必须使用 S3 批量复制来复制任何失败的对象。有关使用批量复制的更多信息，请参阅the section called “复制现有对象”。
>
> 对象会因缺少复制角色权限、Amazon Key Management Service（Amazon KMS）权限或存储桶权限等问题而转换为 FAILED 状态。对于临时性故障（例如，在存储桶或区域不可用的情况下），复制状态将不会转换为 FAILED，而保持 PENDING。在资源重新联机后，Amazon S3 将继续复制这些对象。

- 当请求目标存储桶中的对象时，如果请求中的对象是 Amazon S3 创建的副本，Amazon S3 会返回值为 REPLICA 的 `x-amz-replication-status` 标头。

> **Note**
>
> 在从启用了复制的源存储桶中删除对象之前，请检查该对象的复制状态，以确保已复制了该对象。
>
> 如果对源存储桶启用了 S3 生命周期配置，则 Amazon S3 将暂停生命周期操作，直到它将对象的状态标记为 COMPLETED 或 FAILED。

复制到多个目标存储桶时的复制状态

将对象复制到多个目标存储桶时，`x-amz-replication-status` 标头的作用有所不同。仅当向所有目标的复制都成功时，源对象的标头才返回 COMPLETED 值。在完成所有目标的复制之前，标头将保持 PENDING 值。如果一个或多个目标复制失败，则标头返回 FAILED。

启用了 Amazon S3 副本修改同步时的复制状态

当您的复制规则启用了 Amazon S3 副本修改同步时，副本可能报告 REPLICA 以外的状态。如果元数据更改正在复制过程中，`x-amz-replication-status` 标头返回 PENDING。如果副本修改同步无法复制元数据，则标头返回 FAILED。如果正确复制元数据，则副本将返回标头 REPLICA。

将复制状态信息和批量复制任务结合使用

在创建批量复制任务时，可以选择指定其它筛选条件，例如对象创建日期和复制状态，来缩小任务的范围。

您可以通过提供以下一个或多个值基于 `ObjectReplicationStatuses` 值筛选要复制的对象：

- `"NONE"` – 表示 Amazon S3 之前从未尝试过复制对象。
- `"FAILED"` – 表示 Amazon S3 之前尝试过，但未成功复制对象。
- `"COMPLETED"` – 表示 Amazon S3 之前已成功复制对象。
- `"REPLICA"` – 表示这是 Amazon S3 已从另一个源复制的副本对象。

有关将这些复制状态与批量复制结合使用的更多信息，请参阅the section called “分批复制任务的筛选条件”。

查找复制状态

要获取存储桶中对象的复制状态，可以使用 Amazon S3 清单工具。Amazon S3 会向目标存储桶发送一个您在清单配置中指定的 CSV 文件。您还可以使用 Amazon Athena 在清单报告中查询复制状态。有关 Amazon S3 清单的更多信息，请参阅 使用 S3 清单对数据进行编目和分析。

还可以使用 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）或 Amazon SDK 来查找对象复制状态。

使用 S3 控制台

在 Amazon S3 控制台中，可以在对象的详细信息页面上查看对象的复制状态。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 在通用存储桶列表中，选择复制源存储桶的名称。
4. 在 Objects (对象) 列表中，请选择对象名称。此时将显示对象的详细信息页面。
5. 在属性选项卡上，向下滚动至对象管理概述部分。在管理配置下，查看复制状态下的值。

使用 Amazon CLI

使用以下 Amazon Command Line Interface（Amazon CLI）`head-object` 命令检索对象元数据，如以下示例所示。将 *`amzn-s3-demo-source-bucket1`* 替换为复制源存储桶的名称，并将另一个 *`user input placeholders`* 替换为您自己的信息。

```
aws s3api head-object --bucket amzn-s3-demo-source-bucket1 --key object-key --version-id object-version-id
```

该命令会返回对象元数据（包括 ReplicationStatus），如以下示例响应所示。

```
{
   "AcceptRanges":"bytes",
   "ContentType":"image/jpeg",
   "LastModified":"Mon, 23 Mar 2015 21:02:29 GMT",
   "ContentLength":3191,
   "ReplicationStatus":"COMPLETED",
   "VersionId":"jfnW.HIMOfYiD_9rGbSkmroXsFj3fqZ.",
   "ETag":"\"6805f2cfc46c0f04559748bb039d69ae\"",
   "Metadata":{

   }
}
```

使用 Amazon SDK

以下代码段分别使用适用于 Java 的 Amazon SDK 和适用于 .NET 的 Amazon SDK 获取复制状态。

Java

```
GetObjectMetadataRequest metadataRequest = new GetObjectMetadataRequest(bucketName,
 key);
ObjectMetadata metadata = s3Client.getObjectMetadata(metadataRequest);

System.out.println("Replication Status : " +
 metadata.getRawMetadataValue(Headers.OBJECT_REPLICATION_STATUS));
```

.NET

```
GetObjectMetadataRequest getmetadataRequest = new GetObjectMetadataRequest
    {
         BucketName = sourceBucket,
         Key        = objectKey
    };

GetObjectMetadataResponse getmetadataResponse =
 client.GetObjectMetadata(getmetadataRequest);
Console.WriteLine("Object replication status: {0}",
 getmetadataResponse.ReplicationStatus);
```

# 使用多区域接入点管理多区域流量

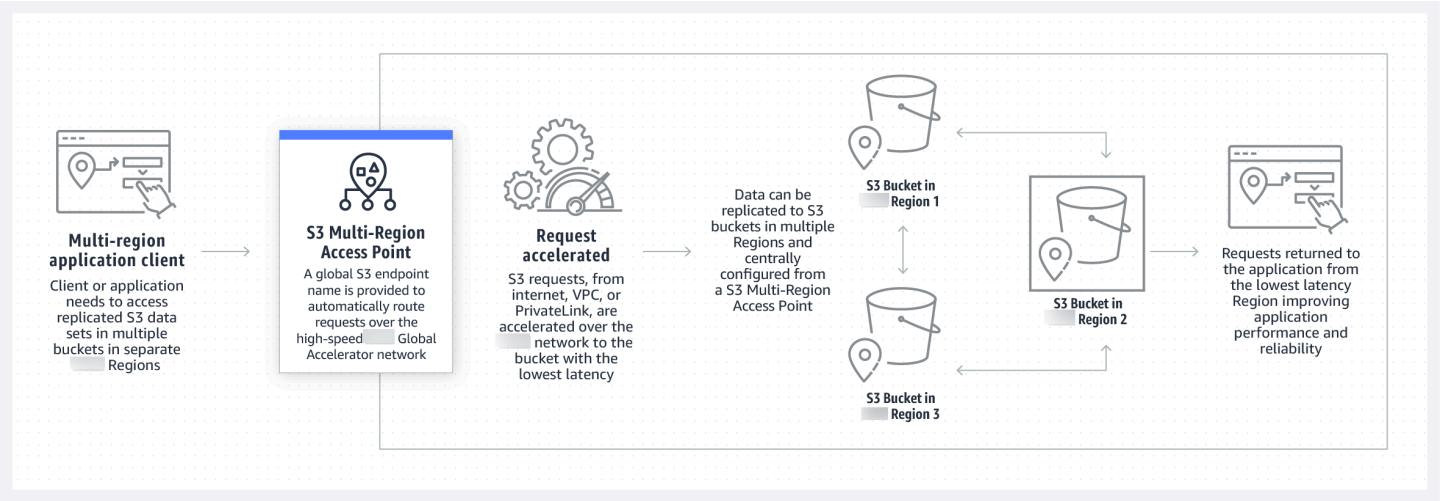
Amazon S3 多区域接入点提供了一个全局端点，应用程序可以使用该端点来满足来自位于多个 Amazon Web Services 区域中的 S3 存储桶的请求。您可以使用多区域接入点通过单个区域中使用的相同架构构建多区域应用程序，然后在世界任何地方运行这些应用程序。多区域接入点不是通过拥挤的公共互联网发送请求，而是提供内置的网络恢复能力，加速向 Amazon S3 发送基于互联网的请求。向多区域接入点全局端点发出的应用程序请求使用 Amazon Global Accelerator，以自动通过 Amazon 全局网络路由到具有活动的路由状态且距离最近的 S3 存储桶。

如果发生区域流量中断，则可以使用多区域接入点失效转移控制在 Amazon Web Services 区域之间转移 S3 数据请求流量，并在几分钟内将 S3 流量重定向到远离中断的位置。还可以针对中断测试应用程序恢复能力，来进行应用程序失效转移和执行灾难恢复模拟。如果需要从 VPC 外部连接到 S3 并加速对 S3 的请求，则可以使用 Amazon S3 多区域接入点简化应用程序和网络架构。多区域接入点请求将通过 Amazon 全球网络进行路由，然后返回到 Amazon Web Services 区域中的 S3，而无需穿越公共互联网。这样，您就可以构建可用性更高的应用程序。

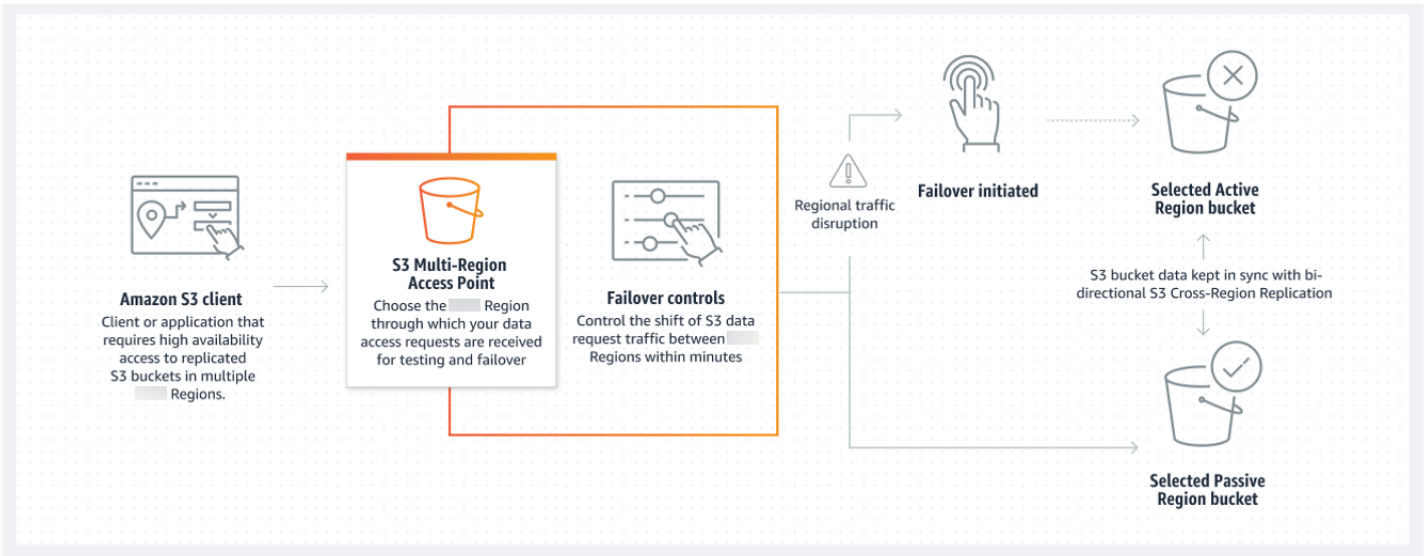
在创建和设置多区域接入点期间，您将指定一组 Amazon Web Services 区域，您希望在其中存储要通过该多区域接入点提供的数据。可以使用提供的多区域接入点端点名称来连接您的客户端。建立客户端连接后，可以选择要在其间路由多区域接入点请求的现有存储桶或新存储桶。然后，使用 S3 跨区域复制（CRR）规则在这些区域中的存储桶之间同步数据。

在设置多区域接入点后，可以通过多区域接入点全局端点请求或写入数据。当针对距离最近的可用区域中已复制的数据集发出请求时，Amazon S3 会自动为这些请求提供服务。在 Amazon Web Services Management Console中，还可以查看与多区域接入点请求相关的底层复制拓扑和复制指标。这样，您就可以更轻松地构建、管理和监控多区域应用程序的存储。或者，可以使用 Amazon CloudFront 自动创建和配置 S3 多区域接入点。

下图是处于活动-活动配置中的 Amazon S3 多区域接入点的图形表示。该图显示了 Amazon S3 请求如何自动路由到距离最近的活动 Amazon Web Services 区域中的桶。




下图是处于活动-被动配置中的 Amazon S3 多区域接入点的图形表示。该图显示如何控制 Amazon S3 数据访问流量以在主动和被动 Amazon Web Services 区域之间进行失效转移。




要了解有关如何使用多区域接入点的更多信息，请参阅教程：Amazon S3 多区域接入点入门。

主题

- 创建多区域接入点
- 配置多区域接入点以便与 Amazon PrivateLink 共同使用
- 通过多区域接入点发出请求

## 创建多区域接入点

要在 Amazon S3 中创建多区域接入点，请执行以下操作：

- 指定多区域接入点的名称。
- 在每个 Amazon Web Services 区域中选择一个桶，以便为针对多区域接入点的请求提供服务。
- 为多区域接入点配置 Amazon S3 屏蔽公共访问权限设置。

您可以在创建请求中提供所有这些信息，Amazon S3 将异步处理该请求。Amazon S3 为您提供了一个令牌，您可以使用该令牌监控异步创建请求状态。

确保保存策略之前解决来自 Amazon Identity and Access Management Access Analyzer 的安全警告、错误、一般警告和建议。IAM Access Analyzer 将根据 IAM 策略语法和最佳实践运行策略检查，以验证您的策略。这些检查项生成结果并提供可操作的建议，可帮助您编写可操作且符合安全最佳实践的策略。要了解有关使用 IAM Access Analyzer 验证策略的更多信息，请参阅 IAM 用户指南中的 IAM Access Analyzer 策略验证。要查看 IAM Access Analyzer 返回的警告、错误和建议的列表，请参阅 IAM Access Analyzer 策略检查引用。

使用 API 时，创建多区域接入点的请求是异步的。当提交创建多区域接入点的请求时，Amazon S3 会同步授权该请求。然后，它会立即返回一个您可以用来跟踪创建请求进度的令牌。有关跟踪异步请求以创建和管理多区域接入点的详细信息，请参阅 将多区域接入点与支持的 API 操作结合使用。

创建多区域接入点后，可以为其创建访问控制策略。每个多区域接入点都可以有一个关联的策略。多区域接入点策略是一个基于资源的策略，您可以使用它来按资源、用户或其他条件限制多区域接入点的使用。

> **Note**
>
> 要使应用程序或用户能够通过多区域接入点访问对象，以下两个策略都必须允许此请求：
>
> - 多区域接入点的访问策略
> - 包含对象的底层桶的访问策略
>
> 这两个策略不同时，限制性较强的策略优先。
> 要简化多区域接入点的权限管理，您可以将桶中的访问控制委托给多区域接入点。有关更多信息，请参阅 the section called “多区域接入点策略示例”。

通过现有桶名称或 Amazon 资源名称（ARN）访问桶时，将桶与多区域接入点结合使用不会更改桶的行为。针对桶的所有现有操作将继续像以前一样运行。您在多区域接入点策略中包括的限制仅适用于通过多区域接入点发出的请求。

您可以在创建多区域接入点后更新策略，但无法删除该策略。但是，您可以更新多区域接入点策略以拒绝所有权限。

主题


- 命名 Amazon S3 多区域接入点的规则
- 为 Amazon S3 多区域接入点选择桶的规则
- 创建 Amazon S3 多区域接入点
- 用 Amazon S3 多区域接入点阻止公有访问
- 查看 Amazon S3 多区域接入点配置详细信息
- 删除多区域接入点


## 命名 Amazon S3 多区域接入点的规则

创建多区域接入点时，您可以为其指定一个名称，该名称是您选择的字符串。创建多区域接入点后，无法更改该接入点的名称。名称在您的 Amazon Web Services 账户 中必须唯一，必须符合 多区域接入点限制和限制 中列出的命名要求。要帮助您识别多区域接入点，请使用对您、您的组织有意义或能够反映场景的名称。

在调用多区域接入点管理操作，如 `GetMultiRegionAccessPoint` 和 `PutMultiRegionAccessPointPolicy`，您使用此名称。该名称不用于向多区域接入点发送请求，也不需要向使用多区域接入点发出请求的客户端公开。

Amazon S3 创建多区域接入点时，会自动为其分配一个别名。此别名是唯一结尾为 `.mrap` 的字母数字字符串。别名用于构建多区域接入点的主机名和 Amazon Resource Name（ARN）。完全限定名称还基于多区域接入点的别名。

您无法根据其别名确定多区域接入点的名称，因此您可以泄露别名，而不会暴露多区域接入点的名称、用途或所有者。Amazon S3 会为每个新的多区域接入点选择别名，不能更改别名。有关多区域接入点寻址的更多信息，请参阅 通过多区域接入点发出请求。

多区域接入点的别名始终是唯一的，不基于多区域接入点的名称或配置。如果创建一个多区域接入点，然后将其删除并创建另一个具有相同名称和配置的接入点，第二个多区域接入点将具有与第一个不同的别名。新的多区域接入点不得具有与之前的多区域接入点相同的别名。

## 为 Amazon S3 多区域接入点选择桶的规则

每个多区域接入点都与您要满足请求的区域相关联。多区域接入点必须与每个区域中的一个桶相关联。您可以在请求中指定每个桶的名称来创建多区域接入点。支持多区域接入点的桶可以位于拥有多区域接入点的同一个 Amazon Web Services 账户中，也可以位于其他 Amazon Web Services 账户中。

多个多区域接入点可以使用同一个桶。

**Important**

- 您只能在创建多区域接入点时指定与多区域接入点关联的桶。创建该桶后，您无法从多区域接入点配置中添加、修改或删除桶。要更改桶，您必须删除整个多区域接入点，然后创建新的接入点。
- 您无法删除属于多区域接入点的桶。如果要删除附加到多区域接入点的桶，请先删除多区域接入点。
- 如果您将其他账户拥有的桶添加到多区域接入点，桶拥有者还必须更新其桶策略，以授予对多区域接入点的访问权限。否则，多区域接入点将无法从该桶检索数据。有关显示如何授予此类访问权限的示例策略，请参阅多区域接入点策略示例。
- 并非所有区域都支持多区域接入点。要查看支持的区域列表，请参阅 多区域接入点限制和限制。

您可以创建复制规则在桶之间同步数据。这些规则让您能够自动将数据从源桶复制到目标桶。将桶连接到多区域接入点不会影响复制的工作方式。后面的部分将介绍如何使用多区域接入点配置复制。

**Important**

当向多区域接入点发出请求时，多区域接入点不了解多区域接入点中桶的数据内容。因此，收到请求的桶可能不包含所请求的数据。要在 Amazon S3 桶中创建与多区域接入点相关联的一致数据集，我们建议您配置 S3 跨区域复制（CRR）。有关更多信息，请参阅 配置用于多区域接入点的复制。

## 创建 Amazon S3 多区域接入点

以下示例演示了如何使用 Amazon S3 控制台创建多区域接入点。

使用 S3 控制台

创建多区域接入点

1. 登录到Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Multi-Region Access Points（多区域接入点）。
3. 选择创建多区域接入点，以开始创建多区域接入点。
4. 在多区域接入点页面上，在多区域接入点名称字段中为多区域接入点提供名称。
5. 选择将与此多区域接入点关联的桶。您可以选择您账户中的桶，也可以从其他账户中选择桶。

> **Note**
>
> 您必须从您的账户或其他账户中添加至少一个桶。另请注意，多区域接入点对于每个 Amazon Web Services 区域仅支持一个桶。因此，您无法添加来自同一个区域的两个桶。不支持原定设置情况下禁用的 Amazon Web Services 区域。

- 要添加位于您的账户中的桶，请选择添加桶。将显示您的账户中所有桶的列表。您可以按名称搜索桶，也可以按字母顺序对桶名称进行排序。
- 要从其他账户添加桶，请选择从其他账户添加桶。请确保您知道确切的桶名称和 Amazon Web Services 账户 ID，因为您无法搜索或浏览其他账户中的桶。

> **Note**
>
> 您必须输入有效的 Amazon Web Services 账户 ID 和桶名称。桶还必须位于支持的区域中，否则在尝试创建多区域接入点时会遇到错误。有关支持多区域接入点的区域列表，请参阅多区域接入点限制和局限性。

6. （可选）如果您需要移除已添加的桶，请选择移除。

> **Note**
>
> 创建完此多区域接入点后，您无法在该多区域接入点中添加或移除桶。

7. 在阻止接入点的公有访问设置下，选择要应用于多区域接入点的阻止公有访问设置。默认情况下为新的多区域接入点启用所有阻止公有访问设置。除非您有特定的需求要禁用任何一个设置，我们建议您保持启用所有设置。

> **Note**
>
> 创建多区域接入点后，您无法更改多区域接入点的屏蔽公共访问权限设置。因此，如果您要阻止公有访问，请在创建多区域接入点之前，确保您的应用程序在没有公有访问的情况下正常运行。

8. 选择创建多区域接入点。

> **Important**
>
> 当您将其他账户拥有的桶添加到多区域接入点时，桶拥有者还必须更新其桶策略，以授予对多区域接入点的访问权限。否则，多区域接入点将无法从该桶检索数据。有关显示如何授予此类访问权限的示例策略，请参阅多区域接入点策略示例。

使用 Amazon CLI

您可以使用 Amazon CLI 创建多区域接入点。当您创建多区域接入点时，您必须提供它将支持的所有桶。创建多区域接入点后，无法将桶添加到该多区域接入点。

以下示例使用 Amazon CLI 创建一个具有两个桶的多区域接入点。要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control create-multi-region-access-point --account-id 111122223333 --details '{
        "Name": "simple-multiregionaccesspoint-with-two-regions",
        "PublicAccessBlock": {
            "BlockPublicAcls": true,
            "IgnorePublicAcls": true,
            "BlockPublicPolicy": true,
            "RestrictPublicBuckets": true
        },
        "Regions": [
            { "Bucket": "amzn-s3-demo-bucket1" },
            { "Bucket": "amzn-s3-demo-bucket2" }
        ]
```

```
    }' --region us-west-2
```

## 用 Amazon S3 多区域接入点阻止公有访问

每个多区域接入点都有不同的 Amazon S3 阻止公有访问设置。这些设置与拥有多区域接入点和底层桶的 Amazon Web Services 账户的屏蔽公共访问权限设置一起运行。

当 Amazon S3 授权请求时，会应用这些设置的最严格组合。如果任何这些资源（多区域接入点拥有者账户、底层桶或桶拥有者账户）的屏蔽公共访问权限设置屏蔽对所请求的操作或资源的访问，Amazon S3 将拒绝该请求。

除非您特别需要禁用其中任何设置，我们建议您启用所有阻止公共访问设置。默认情况下，为多区域接入点启用所有阻止公有访问设置。如果启用了屏蔽公共访问权限，则多区域接入点将无法接受基于互联网的请求。

> **Important**
>
> 在创建多区域接入点之后，您无法更改其屏蔽公共访问权限设置。

有关 Amazon S3 阻止公有访问的更多信息，请参阅 阻止对您的 Amazon S3 存储的公有访问。

## 查看 Amazon S3 多区域接入点配置详细信息

以下示例演示如何使用 Amazon S3 控制台查看多区域接入点的配置详细信息。

使用 S3 控制台

创建多区域接入点

1. 登录到Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Multi-Region Access Points（多区域接入点）。
3. 选择要查看其配置详细信息的多区域接入点的名称。
   - 属性选项卡列出了与您的多区域接入点关联的所有桶、创建日期、Amazon 资源名称（ARN）和别名。Amazon Web Services 账户 ID 列还列出了与多区域接入点关联的外部账户拥有的所有桶。

- 权限选项卡列出了应用于与该多区域接入点相关联的桶的屏蔽公共访问权限设置。您还可以查看多区域接入点的多区域接入点策略（如果已创建）。权限页面上的信息提醒还列出了此多区域接入点的已启用屏蔽公共访问权限设置的所有桶（无论该桶是在您的账户中还是在其他账户中）。
- 复制和失效转移选项卡提供与您的多区域接入点关联的桶以及桶所在区域的地图视图。如果有来自另一个账户的桶，但您无权从中提取数据，则该区域将在复制摘要地图上标记为红色，表明它是一个在获取复制状态时出错的 Amazon Web Services 区域。

> **Note**
>
> 要从外部账户中的桶检索复制状态信息，桶拥有者必须在其桶策略中向您授予 `s3:GetBucketReplication` 权限。

此选项卡还提供与多区域接入点结合使用的区域的复制指标、复制规则和失效转移状态。

使用 Amazon CLI

您可以使用 Amazon CLI 查看多区域接入点的配置详细信息。

以下 Amazon CLI 示例获取当前的多区域接入点配置。要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control get-multi-region-access-point --account-id 111122223333 --name amzn-s3-demo-bucket
```

## 删除多区域接入点

以下步骤介绍如何使用 Amazon S3 控制台删除多区域接入点。

删除多区域接入点并不会删除与多区域接入点相关联的桶，只会删除多区域接入点本身。

使用 S3 控制台

删除多区域接入点

1. 登录到Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Multi-Region Access Points（多区域接入点）。

3. 选择多区域接入点名称旁边的选项按钮。
4. 选择删除。
5. 在删除多区域接入点对话框中，输入要删除的 Amazon 桶的名称。

> **Note**
>
> 确保输入有效的桶名称。否则，删除按钮将被禁用。

6. 选择删除以确认删除多区域接入点。

使用 Amazon CLI

您可以使用 Amazon CLI 删除多区域接入点。此操作不会删除与多区域接入点相关联的桶，只会删除多区域接入点本身。要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control delete-multi-region-access-point --account-id 123456789012 --details
 Name=example-multi-region-access-point-name
```

## 配置多区域接入点以便与 Amazon PrivateLink 共同使用

您可以使用多区域接入点在 Amazon Web Services 区域之间路由 Amazon S3 请求流量。每个多区域接入点全局端点可路由来自多个来源的 Amazon S3 数据请求流量，而无需使用单独的端点构建复杂的网络配置。这些数据请求流量来源包括：

- 源自虚拟私有云（VPC）的流量
- 通过 Amazon PrivateLink 传输的来自本地数据中心的流量
- 来自公共互联网的流量

如果您与 S3 多区域接入点建立 Amazon PrivateLink 连接，则可以使用简单的网络架构和配置，通过私有连接将 S3 请求路由到 Amazon 或跨多个 Amazon Web Services 区域路由请求。使用 Amazon PrivateLink 时，无需配置 VPC 对等连接。

主题


- 配置多区域接入点以便与 Amazon PrivateLink 共同使用
- 从 VPC 端点删除对多区域接入点的访问

## 配置多区域接入点以便与 Amazon PrivateLink 共同使用

使用虚拟私有云（VPC）中的私有 IP 地址，Amazon PrivateLink 为您提供与 Amazon S3 的私有连接。您可以在 VPC 内预置一个或多个接口端点，连接到 Amazon S3 多区域接入点。

通过 Amazon Web Services Management Console、Amazon CLI 或 Amazon 开发工具包，您可以创建多区域接入点的 com.amazonaws.s3-global.accesspoint 端点。要了解有关如何为多区域接入点配置接口端点的更多信息，请参阅 VPC 用户指南中的接口 VPC 端点。

要通过接口端点向多区域接入点发出请求，请按照以下步骤配置 VPC 和多区域接入点。

配置多区域接入点与 Amazon PrivateLink 一起使用

1. 创建或拥有可连接到多区域接入点的适当 VPC 端点。有关创建 VPC 端点的更多信息，请参阅 VPC 用户指南中的接口 VPC 端点。

   > **Important**
   >
   > 请确保创建 com.amazonaws.s3-global.accesspoint 端点。其他端点类型无法访问多区域接入点。

   创建此 VPC 端点后，如果为端点启用了私有 DNS，则 VPC 中的所有多区域接入点请求都会通过此端点路由。默认为启用状态。
2. 如果多区域接入点策略不支持来自 VPC 端点的连接，需要对其进行更新。
3. 验证各个桶策略是否允许访问多区域接入点的用户。

请记住，多区域接入点的工作方式是将请求路由到桶，而不是自行完成请求。重要的是要牢记，因为请求的发起人必须具有对多区域接入点的权限，并允许访问多区域接入点中的各个桶。否则，请求可能会被路由到发起方没有执行请求的权限的桶。多区域接入点和关联的桶必须由相同或另一个 Amazon 账户拥有。但是，如果权限配置正确，来自不同帐户的 VPC 可以使用多区域接入点。

因此，VPC 端点策略必须允许访问多区域接入点和您希望能够满足请求的每个底层桶。例如，假设您有一个别名为 `mfzwi23gnjvgw.mrap` 的多区域接入点。它由桶 `amzn-s3-demo-bucket1` 和 `amzn-s3-demo-bucket2` 提供支持，所有这些都归 AWS 账户 `123456789012` 所有。在这种情况下，以下 VPC 端点策略将允许来自 VPC 的对 `mfzwi23gnjvgw.mrap` 发出的 `GetObject` 请求由任一备份桶来完成。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
    {
        "Sid": "Read-buckets-and-MRAP-VPCE-policy",
        "Principal": "*",
        "Action": [
            "s3:GetObject"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "arn:aws:s3:::amzn-s3-demo-bucket2/*",
            "arn:aws:s3::123456789012:accesspoint/mfzwi23gnjvgw.mrap/object/*"
        ]
    }]
}
```

如前所述，您还必须确保将多区域接入点策略配置为支持通过 VPC 端点进行访问。您无需指定正在请求访问的 VPC 端点。以下示例策略将向任何试图使用多区域接入点进行 GetObject 请求的请求者授予访问权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Sid": "Open-read-MRAP-policy",
        "Effect": "Allow",
        "Principal": "*",
        "Action": [
            "s3:GetObject"
          ],
        "Resource": "arn:aws:s3::123456789012:accesspoint/mfzwi23gnjvgw.mrap/object/*"
    }]
}
```

当然，每个桶都需要一个策略来支持通过 VPC 端点提交请求的访问。以下示例策略向任何匿名用户授予读取权限，其中包括通过 VPC 端点发出的请求。

```
{
    "Version":"2012-10-17",
   "Statement": [
   {
```

```
        "Sid": "Public-read",
        "Effect":"Allow",
        "Principal": "*",
        "Action": "s3:GetObject",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket1",
            "arn:aws:s3:::amzn-s3-demo-bucket2/*"]
    }]
}
```

有关编辑 VPC 端点策略的更多信息，请参阅《VPC 用户指南》中的使用 VPC 端点控制对服务的访问。

### 从 VPC 端点删除对多区域接入点的访问

如果您拥有多区域接入点，并希望从接口端点删除对该接入点的访问权限，则必须为多区域接入点提供新的访问策略，以防止访问通过 VPC 端点的请求。但是，如果您的多区域接入点中的桶支持通过 VPC 端点的请求，它们将继续支持这些请求。如果想阻止该支持，还必须更新桶的策略。向多区域接入点提供新的访问策略只会阻止访问多区域接入点，而不会阻止访问底层桶。

> **Note**
>
> 您无法删除多区域接入点的访问策略。要删除对多区域接入点的访问权限，必须提供一个新的访问策略，其中包含所需的修改访问权限。

您可以更新桶策略来阻止通过 VPC 端点的请求，而不是更新多区域接入点的访问策略。在这种情况下，用户仍然可以通过 VPC 端点访问多区域接入点。但是，如果多区域接入点请求路由到某个桶，而该桶中的桶策略阻止访问，则该请求将生成错误消息。

## 通过多区域接入点发出请求

像其他资源一样，Amazon S3 多区域接入点具有 Amazon 资源名称（ARN）。您可以使用这些 ARN，通过 Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 Amazon S3 API 将请求定向到多区域接入点。您还可以使用这些 ARN 在访问控制策略中识别多区域接入点。多区域接入点 ARN 不包括或披露多区域接入点的名称。有关 ARN 的更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon 资源名称（ARN）。

> **Note**
>
> 多区域接入点别名和 ARN 不能互换使用。

多区域接入点 ARN 使用以下格式：

`arn:aws:s3::account-id:accesspoint/MultiRegionAccessPoint_alias`

以下是多区域接入点 ARN 的几个示例：

- `arn:aws:s3::123456789012:accesspoint/mfzwi23gnjvgw.mrap` 表示别名为 `mfzwi23gnjvgw.mrap` 的多区域接入点，它由 Amazon Web Services 账户 `123456789012` 拥有。
- `arn:aws:s3::123456789012:accesspoint/*` 表示账户 `123456789012` 下的所有多区域接入点。此 ARN 匹配账户 `123456789012` 的所有多区域接入点，但不匹配任何区域 Amazon S3 接入点，因为 ARN 不包括 Amazon Web Services 区域。相比之下，ARN `arn:aws:s3:us-west-2:123456789012:accesspoint/*` 匹配账户 `123456789012` 下区域 `us-west-2` 中的所有区域 Amazon S3 接入点，但不匹配任何多区域接入点。

通过多区域接入点访问的对象的 ARN 采用以下格式：

`arn:aws:s3::account_id:accesspoint/MultiRegionAccessPoint_alias//key`

与多区域接入点 ARN 一样，通过多区域接入点访问的对象的 ARN 不包括 Amazon Web Services 区域。下面是一些示例。

- `arn:aws:s3::123456789012:accesspoint/mfzwi23gnjvgw.mrap//-01` 表示 `-01`，可通过别名为 `mfzwi23gnjvgw.mrap` 的多区域接入点访问，由账户 `123456789012` 拥有。
- `arn:aws:s3::123456789012:accesspoint/mfzwi23gnjvgw.mrap//*` 表示账户 `123456789012` 中可以通过别名为 `mfzwi23gnjvgw.mrap` 的多区域接入点访问的所有对象。
- `arn:aws:s3::123456789012:accesspoint/mfzwi23gnjvgw.mrap//-01/finance/*` 表示账户 `123456789012` 中可以在别名为 `mfzwi23gnjvgw.mrap` 的多区域接入点的 `-01/finance/` 下访问的所有对象。

## 多区域接入点主机名

您可以通过多区域接入点使用多区域接入点的主机名访问 Amazon S3 中的数据。可以将请求从公共互联网定向到该主机名。如果已为多区域接入点配置了一个或多个互联网网关，则请求也可以从虚拟私有云（VPC）定向到此主机名。有关创建与多区域接入点使用 VPC 接口端点的更多信息，请参阅 配置多区域接入点以便与 Amazon PrivateLink 共同使用。

要使用 VPC 端点通过多区域接入点从 VPC 发出请求，可以使用 Amazon PrivateLink。当您使用 Amazon PrivateLink 对多区域接入点发出请求时，不能直接使用以 *region*.vpce.amazonaws.com 结尾的端点特定的区域域名系统（DNS）。此主机名将没有与其关联的证书，因此无法直接使用。您仍可以将 VPC 端点的公有域名系统（DNS）名称用作 CNAME 或 ALIAS 目标。或者，您可以在端点上启用私有域名系统（DNS），并使用标准的多区域接入点 *MultiRegionAccessPoint_alias*.accesspoint.s3-global.amazonaws.com 域名系统（DNS）名称，如本节所述。

通过多区域接入点向 API 请求 Amazon S3 数据操作时（例如 GetObject），请求的主机名如下所示：

*MultiRegionAccessPoint_alias*.accesspoint.s3-global.amazonaws.com

例如，要通过别名为 mfzwi23gnjvgw.mrap 的多区域接入点发出 GetObject 请求，请向主机名 mfzwi23gnjvgw.mrap.accesspoint.s3-global.amazonaws.com 发出请求。此主机名的 s3-global 部分表明此主机名不适用于特定区域。

通过多区域接入点发出请求类似于通过单区域接入点发出请求。但是，务必注意以下差异：

- 多区域接入点 ARN 不包括 Amazon Web Services 区域。他们遵循的格式 arn:aws:s3::*account-id*:accesspoint/*MultiRegionAccessPoint_alias*。
- 对于通过 API 操作发出的请求（这些请求不要求使用 ARN），多区域接入点使用不同的端点方案。模式是 *MultiRegionAccessPoint_alias*.accesspoint.s3-global.amazonaws.com — 例如，mfzwi23gnjvgw.mrap.accesspoint.s3-global.amazonaws.com。请注意与单区域接入点相比的差异：
  - 多区域接入点主机名使用其别名，而不是多区域接入点名称。
  - 多区域接入点主机名不包括拥有者的 Amazon Web Services 账户 ID。
  - 多区域接入点主机名不包括 Amazon Web Services 区域。
  - 多区域接入点主机名包括 s3-global.amazonaws.com 而不是 s3.amazonaws.com。
- 必须使用签名版本 4A（SigV4A）签署多区域接入点请求。使用 Amazon SDK 时，SDK 会自动将 SigV4 转换为 SigV4A。因此，请确保您的 Amazon SDK 支持将 SigV4A 作为用于签署全局 Amazon

Web Services 区域请求的签名实现。有关 SigV4A 的更多信息，请参阅《Amazon Web Services 一般参考》中的签署 Amazon API 请求。

## 多区域接入点和 Amazon S3 Transfer Acceleration

Amazon S3 Transfer Acceleration 是一项启用数据快速转换到桶的功能。Transfer Acceleration 是在单个桶级别上配置的。有关 Transfer Acceleration 的更多信息，请参阅使用 Amazon S3 Transfer Acceleration 配置快速、安全的文件传输。

多区域接入点使用类似于 Transfer Acceleration 的加速传输机制，通过 Amazon 网络发送大对象。因此，在通过多区域接入点发送请求时，您无需使用 Transfer Acceleration。这种提高的传输性能会自动融入到多区域接入点中。

主题

- 权限
- 多区域接入点限制和限制
- 多区域接入点请求路由
- Amazon S3 多区域接入点失效转移控制
- 配置用于多区域接入点的复制
- 将多区域接入点与支持的 API 操作结合使用
- 监视和记录通过多区域接入点发出的对底层资源的请求

## 权限

Amazon S3 多区域接入点可以简化多个 Amazon Web Services 区域中 Amazon S3 桶的数据访问。多区域接入点称为全局端点，您可以使用这些接入点执行 Amazon S3 数据接入点操作，如 `GetObject` 和 `PutObject`。对于通过全局端点发出的任何请求，每个多区域接入点都可以具有不同的权限和网络控制。

每个多区域接入点也可以强制实施自定义访问策略，该策略与附加到底层桶的桶策略结合使用。要使跨账户请求获得成功，以下所有策略都必须允许该操作：

- 多区域接入点策略
- 底层 Amazon Identity and Access Management（IAM）策略
- 底层桶策略（请求路由到哪里）

> **Note**
>
> 对于同账户请求，只需要授予相应访问权限的基础 IAM 策略。

您可以将任何多区域接入点策略配置为仅接受来自特定 IAM 用户或组的请求。有关如何执行此操作的示例，请参阅the section called “多区域接入点策略示例”中的示例 2。为了限制 Amazon S3 数据访问私有网络，您可以将任何多区域接入点策略配置为仅接受来自虚拟私有云（VPC）的请求。

例如，假设您通过多区域接入点使用您的 Amazon 账户中名为 `AppDataReader` 的用户发出一个 `GetObject` 请求。为了帮助确保请求不会被拒绝，`AppDataReader` 用户必须被多区域接入点和多区域接入点底层的每个桶授予 `s3:GetObject` 权限。`AppDataReader` 将无法从任何未授予此权限的任何桶中检索数据。

> **Important**
>
> 通过桶名称或 Amazon 资源名称（ARN）直接访问桶时，将桶的访问控制委派给多区域接入点策略不会改变桶的行为。直接对桶进行的所有操作将继续像以前一样运行。您在多区域接入点策略中包括的限制仅适用于通过该多区域接入点发出的请求。

管理多区域接入点的公共访问

多区域接入点支持每个多区域接入点的独立阻止公有访问设置。创建多区域接入点时，您可以指定应用于该多区域接入点的阻止公有访问设置。

> **Note**
>
> 即使多区域接入点的独立屏蔽公共访问权限设置被禁用，在此账户的屏蔽公共访问权限设置（在您自己的账户中）或外部桶的屏蔽公共访问权限设置下启用的任何屏蔽公共访问权限设置也仍然适用。

对于通过多区域接入点发出的任何请求，Amazon S3 会评估以下各项的阻止公有访问设置：

- 多区域接入点
- 底层桶（包括外部桶）
- 拥有多区域接入点的账户

- 拥有底层桶的账户（包括外部账户）

如果这些设置中的任何一个指示应阻止请求，则 Amazon S3 会拒绝请求。有关 Amazon S3 阻止公有访问功能的更多信息，请参阅 阻止对您的 Amazon S3 存储的公有访问。

> **Important**
>
> 原定设置情况下，为多区域接入点启用所有阻止公有访问设置。您必须明确禁用不希望应用于多区域接入点的任何设置。
> 在创建多区域接入点之后，您无法更改其屏蔽公共访问权限设置。

查看多区域接入点的阻止公有访问设置

查看多区域接入点的阻止公有访问设置

1. 登录到Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Multi-Region Access Points（多区域接入点）。
3. 请选择要查看的多区域接入点的名称。
4. 选择 Permissions（权限）选项卡。
5. 在 Block Public Access settings for this Multi-Region Access Point（多区域接入点的阻止公有访问设置）下，查看多区域接入点的阻止公有访问设置。

> **Note**
>
> 创建多区域接入点后，无法编辑阻止公有访问设置。因此，如果您要阻止公有访问，请在创建多区域接入点之前，确保您的应用程序在没有公有访问的情况下正常运行。

使用多区域接入点策略

以下示例多区域接入点策略授予 IAM 用户从多区域接入点列出和下载文件的访问权限。要使用此示例策略，请将 *user input placeholders* 替换为您自己的信息。

```
{
  "Version":"2012-10-17",
```

```
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "AWS":"arn:aws:iam::123456789012:user/JohnDoe"
         },
         "Action":[
            "s3:ListBucket",
            "s3:GetObject"
         ],
         "Resource":[
            "arn:aws:s3::111122223333:accesspoint/MultiRegionAccessPoint_alias",
            "arn:aws:s3::111122223333:accesspoint/MultiRegionAccessPoint_alias/object/
*"
         ]
      }
   ]
}
```

要使用 Amazon Command Line Interface（Amazon CLI）将多区域接入点策略与指定的多区域接入点关联，请使用以下 `put-multi-region-access-point-policy` 命令。要使用此示例命令，请将 *`user input placeholders`* 替换为您自己的信息。每个多区域接入点只能有一个策略，因此，对 `put-multi-region-access-point-policy` 操作发出的请求将替换与指定多区域接入点关联的任何现有策略。

Amazon CLI

```
aws s3control put-multi-region-access-point-policy
--account-id 111122223333
--details { "Name": "amzn-s3-demo-bucket-MultiRegionAccessPoint",
 "Policy": "{ \"Version\": \"2012-10-17\", \"Statement\": { \"Effect\":
 \"Allow\", \"Principal\": { \"AWS\": \"arn:aws:iam::111122223333:root
\" }, \"Action\": [\"s3:ListBucket\", \"s3:GetObject\"], \"Resource\":
 [ \"arn:aws:s3::111122223333:accesspoint/MultiRegionAccessPoint_alias",
 \"arn:aws:s3::111122223333:accesspoint/MultiRegionAccessPoint_alias/object/*
\" ] } }" }
```

要查询上次操作的结果，请使用以下命令：

Amazon CLI

```
aws s3control describe-multi-region-access-point-operation
--account-id 111122223333
--request-token-arn requestArn
```

要检索多区域接入点策略，请使用以下命令：

Amazon CLI

```
aws s3control get-multi-region-access-point-policy
--account-id 111122223333
--name=amzn-s3-demo-bucket-MultiRegionAccessPoint
```

### 编辑多区域接入点策略

多区域接入点策略（以 JSON 编写）提供对与多区域接入点结合使用的 Amazon S3 桶的存储访问。您可以允许或拒绝特定主体对您的多区域接入点执行各种操作。当一个请求通过多区域接入点路由到一个桶时，多区域接入点和桶的访问策略都适用。限制性更强的访问策略始终优先。

> **Note**
>
> 如果桶包含由其他账户拥有的对象，则多区域接入点策略不适用于由其他 Amazon Web Services 账户拥有的对象。

应用多区域接入点策略后，无法删除该策略。您可以编辑策略，也可以创建覆盖现有策略的新策略。

编辑多区域接入点策略

1. 登录到Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Multi-Region Access Points（多区域接入点）。
3. 选择要为其编辑策略的多区域接入点的名称。
4. 选择 Permissions（权限）选项卡。
5. 向下滚动到 Multi-Region Access Point policy（多区域接入点策略）部分。选择 Edit（编辑）以更新策略（采用 JSON 格式）。

6. 将显示 Edit Multi-Region Access Point policy（编辑多区域接入点策略）页面。您可以直接在文本字段中输入策略，也可以选择 Add statement（添加语句）以从下拉列表中选择策略元素。

> **Note**
>
> 控制台会自动显示您可以在策略中使用的多区域接入点 Amazon 资源名称（ARN）。有关多区域接入点策略示例，请参阅 the section called “多区域接入点策略示例”。

多区域接入点策略示例

Amazon S3 多区域接入点支持 Amazon Identity and Access Management（IAM）资源策略。您可以使用这些策略，按资源、用户或其他条件控制多区域接入点的使用。为了使应用程序或用户能够通过多区域接入点访问对象，多区域接入点和底层桶都必须允许相同的访问权限。

要允许对多区域接入点和底层桶进行相同访问，请执行以下操作之一：

- （推荐）要简化使用 Amazon S3 多区域接入点时的访问控制，请将 Amazon S3 桶的访问控制权委托给多区域接入点。有关如何执行此操作的示例，请参阅本节中的示例 1。
- 将多区域接入点策略中包含的相同权限添加到底层桶策略中。

> **Important**
>
> 通过桶名称或 Amazon 资源名称（ARN）直接访问桶时，将桶的访问控制委派给多区域接入点策略不会改变桶的行为。直接对桶进行的所有操作将继续像以前一样运行。您在多区域接入点策略中包括的限制仅适用于通过该多区域接入点发出的请求。

Example 1 – 将访问权限委托给桶策略中的特定多区域接入点（针对同一账户或跨账户）

以下示例桶策略授予对特定多区域接入点的完全桶访问权限。这意味着，对此桶的所有访问都由附加到多区域接入点的策略控制。我们建议您以这种方式为所有不需要直接访问存储桶的使用案例配置存储桶。您可以将此桶策略结构用于同一账户或其他账户中的多区域接入点。

```
{
    "Version": "2012-10-17",
    "Statement" : [
    {
```

```
        "Effect": "Allow",
        "Principal" : { "AWS": "*" },
        "Action" : "*",
        "Resource" : [ "Bucket ARN", "Bucket ARN/*"],
        "Condition": {
            "StringEquals" : { "s3:DataAccessPointArn" : "MultiRegionAccessPoint_ARN" }
        }
    }]
}
```

> **Note**
>
> 如果您正在授予对多个多区域接入点的访问权限，请确保列出每个多区域接入点。

Example 2 – 在您的多区域接入点策略中授予账户对多区域接入点的访问权限

以下多区域接入点策略向账户 *123456789012* 授予列出和读取由 *MultiRegionAccessPoint_ARN* 定义的多区域接入点中包含的对象的权限。

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
       "Effect": "Allow",
       "Principal": {
          "AWS":"arn:aws:iam::123456789012:user/JohnDoe"
       },
       "Action":[
          "s3:ListBucket",
          "s3:GetObject"
       ],
       "Resource":[
          "MultiRegionAccessPoint_ARN",
          "MultiRegionAccessPoint_ARN/object/*"
       ]
     }
  ]
}
```

Example 3 – 允许列出桶内容的多区域接入点策略

以下多区域接入点策略向账户 *123456789012* 授予列出由 *MultiRegionAccessPoint_ARN* 定义的多区域接入点中包含的对象的权限。

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
       "Effect": "Allow",
       "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/JohnDoe"
        },
        "Action": "s3:ListBucket",
        "Resource": "MultiRegionAccessPoint_ARN"
       }
    ]
}
```

## 多区域接入点限制和限制

Amazon S3 多区域接入点具有以下限制和局限性：

- 多区域接入点名称：
  - 在单个 Amazon 账户内必须是唯一的
  - 必须以数字或小写字母开头
  - 长度必须介于 3-50 个字符之间
  - 不能以连字符（-）开头或结尾
  - 不能包含下划线（_）、大写字母或句点（.）
  - 创建后无法对其进行编辑
- 多区域接入点别名由 Amazon S3 生成，无法编辑或重复使用。
- 您无法使用网关端点通过多区域接入点访问数据。但是，您可以使用接口端点通过多区域接入点访问数据。要使用 Amazon PrivateLink，您必须创建 VPC 端点。有关更多信息，请参阅 配置多区域接入点以便与 Amazon PrivateLink 共同使用。
- 要在 Amazon CloudFront 中使用多区域接入点，必须将多区域接入点配置为 `Custom Origin` 分配类型。有关各种源类型的更多信息，请参阅在 CloudFront 分配中使用各种源。有关在 Amazon CloudFront 中使用多区域接入点的更多信息，请参阅 Amazon 存储博客上的跨多个区域构建主动-主动、基于距离远近的应用程序。

- 多区域接入点最低要求：
  - 传输层安全性 (TLS) v1.2
  - 签名版本 4 (SigV4A)

    多区域接入点支持签名版本 4A。此版本的 SigV4 允许对多个 Amazon Web Services 区域签署请求。此特征对于可能导致从多个区域之一访问数据的 API 操作非常有用。使用 Amazon SDK，您可以提供凭证，并且对多区域接入点的请求将使用签名版本 4A，而无需进行其他配置。请务必检查您的 Amazon SDK 与 SigV4A 算法的兼容性。有关 SigV4A 的更多信息，请参阅《Amazon Web Services 一般参考》中的签署 Amazon API 请求。

    > **Note**
    >
    > 要将 SigV4A 与临时安全凭证一起使用 [例如，在使用 Amazon Identity and Access Management（IAM）角色时]，您可以从区域 Amazon Security Token Service（Amazon STS）端点请求临时凭证。如果您从全局 Amazon STS 端点（`sts.amazonaws.com`）请求临时凭证，则必须先将全局端点会话令牌的区域兼容性设置为在所有 Amazon Web Services 区域中都有效。有关更多信息，请参阅《IAM 用户指南》中的在 Amazon Web Services 区域中管理 Amazon STS。

- 多区域接入点不支持匿名请求。
- 多区域接入点限制：
  - 不支持 IPv6。
  - 不支持 Outposts 桶上面的 Amazon S3。
  - 当使用多区域接入点 ARN 时，多区域接入点仅支持使用多区域接入点的复制操作作为目标。
  - 不支持 S3 批量操作特征。
- 不支持某些 Amazon SDK。要确认多区域接入点支持哪些 Amazon SDK，请参阅与 Amazon SDK 的兼容性。
- 多区域接入点的服务限额如下所示：
  - 每个账户最多有 100 个多区域接入点。
  - 单个多区域接入点的限制为 17 个区域。
- 创建多区域接入点后，您无法从多区域接入点配置中添加、修改或删除桶。要更改桶，您必须删除整个多区域接入点，然后创建新的接入点。如果删除了多区域接入点中的跨账户桶，则重新连接此桶的唯一方法是使用该账户中的相同名称和区域重新创建该桶。
- 只有在删除多区域接入点后，才能删除多区域接入点中使用的底层桶（在同一账户中）。

- 所有创建或维护多区域接入点的控制面板请求都必须路由到 US West (Oregon) 区域。对于多区域接入点数据面板请求，无需指定区域。
- 对于多区域接入点失效转移控制面板，必须将请求路由到以下五个支持的区域之一：
  - US East (N. Virginia)
  - US West (Oregon)
  - Asia Pacific (Sydney)
  - Asia Pacific (Tokyo)
  - Europe (Ireland)
- 多区域接入点仅支持以下 Amazon Web Services 区域中的桶：
  - US East (N. Virginia)
  - US East (Ohio)
  - US West (N. California)
  - US West (Oregon)
  - Asia Pacific (Mumbai)
  - Asia Pacific (Osaka)
  - Asia Pacific (Seoul)
  - Asia Pacific (Singapore)
  - Asia Pacific (Sydney)
  - Asia Pacific (Tokyo)
  - Canada (Central)
  - Europe (Frankfurt)
  - Europe (Ireland)
  - Europe (London)
  - Europe (Paris)
  - Europe (Stockholm)
  - South America (São Paulo)

## 多区域接入点请求路由

通过多区域接入点发出请求时，Amazon S3 会确定与多区域接入点相关联的桶中的哪一个桶距离您最近。然后，Amazon S3 将请求定向到该桶，而不考虑 Amazon 它所在的区域。

在多区域接入点将请求路由到距离最近的桶之后，Amazon S3 会像您直接向该桶发出请求一样处理请求。多区域接入点不了解 Amazon S3 桶的数据内容。因此，收到请求的桶可能不包含所请求的数据。要在 Amazon S3 桶中创建与多区域接入点相关联的一致数据集，您可以配置 S3 跨区域复制（CRR）。然后任何桶都可以成功满足 请求。

Amazon S3 根据以下规则导向多区域接入点请求：

- Amazon S3 根据距离远近优化要完成的请求。它查看多区域接入点支持的桶，并将请求中继到距离最近的桶。
- 如果请求指定了现有资源（例如，`GetObject`），Amazon S3 在满足请求时不会考虑对象的名称。这意味着，即使多区域接入点中的一个桶中存在某个对象，您的请求也可能路由到不包含该对象的桶。这种情况会导致向客户端返回 404 错误消息。

  为了避免 404 错误，我们建议您为桶配置 S3 跨区域复制（CRR）。当您需要的对象位于多区域接入点中的桶中，但不在您的请求路由到的特定桶中时，复制有助于解决潜在问题。有关复制配置的信息，请参阅 配置用于多区域接入点的复制。

  为了确保使用所需的特定对象满足您的请求，我们还建议您启用桶版本控制并在请求中包含版本 ID。这种方法有助于确保您具有您正在查找的对象的正确版本。启用了版本控制的桶还可以帮助您恢复意外覆盖的对象。有关更多信息，请参阅在 S3 桶中使用 S3 版本控制。
- 如果请求是创建一个资源（例如，`PutObject` 或 `CreateMultipartUpload`），则 Amazon S3 将使用距离最近的桶完成请求。例如，假设一家视频公司希望支持从世界任何地方上传视频。当用户将 PUT 请求发送到多区域接入点时，该对象将放入距离最近的桶中。然后，要以最低的延迟将上传的视频提供给世界各地的其他人下载，您可以将 CRR 与双向复制结合使用。将 CRR 与双向复制结合使用，可使与多区域接入点关联的所有桶的内容保持同步。有关将复制与多区域接入点结合使用的更多信息，请参阅配置用于多区域接入点的复制。

## Amazon S3 多区域接入点失效转移控制

借助 Amazon S3 多区域接入点失效转移控制，您可以在区域流量中断期间保持业务连续性，同时还可以为您的应用程序提供多区域架构以满足合规性和冗余需求。如果您的区域流量中断，您可以使用多区域接入点失效转移控制来选择 Amazon S3 多区域接入点后面的哪个 Amazon Web Services 区域将处理数据访问和存储请求。

要支持失效转移，您可以将多区域接入点设置为主动-被动配置，在正常情况下流量流向主动区域，而被动区域处于备用状态以用于失效转移。

例如，要执行到您选择的某个 Amazon Web Services 区域的失效转移，您需要将流量从主要（主动）区域转移到辅助（被动）区域。在这样的主动-被动配置中，一个桶处于主动状态并接受流量，而另一个桶是被动的，不接受流量。被动桶用于灾难恢复。当您启动失效转移时，所有流量（例如 GET 或 PUT 请求）都将定向到处于主动状态的桶（位于一个区域中），并远离处于被动状态的桶（位于另一个区域中）。

如果您通过双向复制规则启用 S3 跨区域复制（CRR)，则可以在失效转移期间保持桶同步。此外，如果您在主动-主动配置中启用了 CRR，Amazon S3 多区域接入点还可以从距离最近的桶位置提取数据，从而提高应用程序性能。

Amazon Web Services 区域 支持

借助 Amazon S3 多区域接入点失效转移控制，您的 S3 桶可以位于支持多区域接入点的 17 个区域中的任何一个区域。您可以一次跨任意两个区域启动失效转移。

> **Note**
>
> 尽管一次只能在两个区域之间启动失效转移，但您可以在多区域接入点中同时单独更新多个区域的路由状态。

以下主题演示如何使用和管理 Amazon S3 多区域接入点失效转移控制。

主题

- Amazon S3 多区域接入点路由状态
- 使用 Amazon S3 多区域接入点失效转移控制
- Amazon S3 多区域接入点失效转移控制错误

Amazon S3 多区域接入点路由状态

您的 Amazon S3 多区域接入点失效转移配置决定了与多区域接入点结合使用的 Amazon Web Services 区域的路由状态。您可以将 Amazon S3 多区域接入点配置为主动-主动状态或主动-被动状态。

- 主动-主动 – 在主动-主动配置中，所有请求都会自动发送到多区域接入点中距离最近的 Amazon Web Services 区域。将多区域接入点配置为活动-活动状态后，所有区域都可以接收流量。如果在主动-主动配置中发生流量中断，网络流量将自动重定向到其中一个活动的区域。

- 主动-被动 – 在主动-被动配置中，多区域接入点中的主动区域接收流量，而被动区域不接收流量。如果您打算在灾难情况下使用 S3 失效转移控制启动失效转移，请在测试和执行灾难恢复计划时以主动-被动配置设置您的多区域接入点。

## 使用 Amazon S3 多区域接入点失效转移控制

本部分介绍如何通过 Amazon Web Services Management Console来管理和使用 Amazon S3 多区域接入点失效转移控制。

在 Amazon Web Services Management Console中的多区域接入点详细信息页面上的 Failover configuration（失效转移配置）部分中有两个失效转移控制：Edit routing status（编辑路由状态）和 Failover（失效转移）。您可以使用这些控件执行以下操作：

- Edit routing status（编辑路由状态）- 通过选择 Edit routing status（编辑路由状态），您可以在多区域接入点的单个请求中手动编辑最多 17 个 Amazon Web Services 区域的路由状态。您可以将 Edit routing status（编辑路由状态）用于以下目的：
  - 设置或编辑多区域接入点中一个或多个区域的路由状态
  - 通过将两个区域配置为主动-被动状态来为您的多区域接入点创建失效转移配置
  - 手动失效转移您的区域
  - 在区域之间手动切换流量
- Failover（失效转移）– 当您选择 Failover（失效转移）以启动失效转移时，您只更新已配置为主动-被动状态的两个区域的路由状态。在通过选择 Failover（失效转移）启动的失效转移期间，两个区域之间的路由状态将自动切换。

### 编辑多区域接入点中区域的路由状态

通过在多区域接入点详细信息页面的 Failover configuration（失效转移配置）部分中选择 Edit routing status（编辑路由状态），您可以在多区域接入点的单个请求中手动更新最多 17 个 Amazon Web Services 区域的路由状态。但是，当您通过选择 Failover（失效转移）启动失效转移时，您只更新已配置为主动-被动状态的两个区域的路由状态。在通过选择 Failover（失效转移）启动的失效转移期间，两个区域之间的路由状态将自动切换。

您可以将 Edit routing status（编辑路由状态）（如以下步骤所述）用于以下目的：

- 设置或编辑多区域接入点中一个或多个区域的路由状态
- 通过将两个区域配置为主动-被动状态来为您的多区域接入点创建失效转移配置
- 手动失效转移您的区域

- 在区域之间手动切换流量

使用 S3 控制台

更新多区域接入点中区域的路由状态

1. 登录 Amazon 管理控制台。
2. 通过以下网址打开 Simple Storage Service（Amazon S3）控制台：https://console.aws.amazon.com/s3/。
3. 在左侧导航窗格中，选择 Multi-Region Access Points（多区域接入点）。
4. 请选择要更新的多区域接入点。
5. 选择 Replication and failover（复制和失效转移）选项卡。
6. 请选择要编辑其路由状态的一个或多个区域。

   > **Note**
   >
   > 要启动失效转移，必须在多区域接入点中将至少一个 Amazon Web Services 区域指定为 Active（主动），并将一个区域指定为 Passive（被动）。

7. 选择 Edit routing status（编辑路由状态）。
8. 在出现的对话框中，为每个区域的 Routing status（路由状态）选择 Active（主动）或 Passive（被动）。

   活动状态允许将流量路由到该区域。被动状态会阻止任何流量定向到该区域。

   如果您正在为多区域接入点创建失效转移配置或启动失效转移，必须在多区域接入点中将至少一个 Amazon Web Services 区域指定为 Active（主动），并将一个区域指定为 Passive（被动）。
9. 选择 Save routing status（保存路由状态）。重定向流量大约需要 2 分钟。

在对于多区域接入点提交 Amazon Web Services 区域的路由状态后，您可以验证路由状态的变化。要验证这些变化，请访问 Amazon CloudWatch（网址为 https://console.aws.amazon.com/cloudwatch/）以监控您的 Amazon S3 数据请求流量（例如 GET 和 PUT 请求）在主动和被动区域之间的转移。在失效转移期间不会终止任何现有连接。现有连接将一直持续到它们达到成功或失败状态。

使用 Amazon CLI

> **Note**
>
> 您可以对以下五个区域中的任何一个运行多区域接入点 Amazon CLI 路由命令：
>
> - ap-southeast-2
> - ap-northeast-1
> - us-east-1
> - us-west-2
> - eu-west-1

以下示例命令更新您当前的多区域接入点路由配置。要更新桶的主动或被动状态，请对于主动将 TrafficDialPercentage 值设置为 100，对于被动则设置为 0。在此示例中，*amzn-s3-demo-bucket1* 设置为主动，*amzn-s3-demo-bucket2* 设置为被动。要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control submit-multi-region-access-point-routes
--region ap-southeast-2
--account-id 123456789012
--mrap MultiRegionAccessPoint_ARN
--route-updates Bucket=amzn-s3-demo-bucket1,TrafficDialPercentage=100
                Bucket=amzn-s3-demo-bucket2
,TrafficDialPercentage=0
```

以下示例命令获取更新的多区域接入点路由配置。要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control get-multi-region-access-point-routes
--region eu-west-1
--account-id 123456789012
--mrap MultiRegionAccessPoint_ARN
```

启动失效转移

当您通过在多区域接入点详细信息页面上的 Failover configuration（失效转移配置）部分中选择 Failover（失效转移）来启动失效转移时，Amazon S3 请求流量会自动转移到备用 Amazon Web Services 区域。失效转移过程在 2 分钟内完成。

您可以一次跨任意两个 Amazon Web Services 区域（属于支持多区域接入点的 17 个区域）启动失效转移。然后，在 Amazon CloudTrail 中记录失效转移事件。失效转移完成后，您可以在 Amazon CloudWatch 中监控 Amazon S3 流量和对于新活动区域的任何流量路由更新。

> **Important**
>
> 要在数据复制期间使所有元数据和对象在桶之间保持同步，我们建议您在配置失效转移控制之前创建双向复制规则并启用副本修改同步。
> 双向复制规则有助于确保在将数据写入流量失效转移到的 Amazon S3 桶时，该数据随后被复制回源桶。副本修改同步有助于确保在双向复制期间，对象元数据也在桶之间同步。
> 有关配置复制以支持失效转移的更多信息，请参阅the section called “桶复制”。

在复制的桶之间启动失效转移

1. 登录 Amazon 管理控制台。
2. 通过以下网址打开 Simple Storage Service（Amazon S3）控制台：https://console.aws.amazon.com/s3/。
3. 在左侧导航窗格中，选择 Multi-Region Access Points（多区域接入点）。
4. 请选择要用于启动失效转移的多区域接入点。
5. 选择 Replication and failover（复制和失效转移）选项卡。
6. 向下滚动到 Failover configuration（失效转移配置）部分，然后选择两个 Amazon Web Services 区域。

   > **Note**
   >
   > 要启动失效转移，必须在多区域接入点中将至少一个 Amazon Web Services 区域指定为 Active（主动），并将一个区域指定为 Passive（被动）。活动状态允许将流量定向到区域。被动状态会阻止任何流量定向到该区域。

7. 选择 Failover（故障转移）。
8. 在此对话框中，再次选择 Failover（失效转移）以启动失效转移过程。在此过程中，两个区域的路由状态会自动切换。所有新流量都定向到变为活动状态的区域，而流量将停止定向到变为被动状态的区域。重定向流量大约需要 2 分钟。

   启动失效转移过程后，您可以验证流量变化。要验证这些变化，请访问 Amazon CloudWatch（网址为 https://console.aws.amazon.com/cloudwatch/）以监控您的 Amazon S3 数据请求流量（例

如 GET 和 PUT 请求）在主动和被动区域之间的转移。在失效转移期间不会终止任何现有连接。现有连接将一直持续到它们达到成功或失败状态。

### 查看您的 Amazon S3 多区域接入点路由控制

#### 使用 S3 控制台

查看您的 Amazon S3 多区域接入点的路由控制

1. 登录 Amazon 管理控制台。
2. 通过以下网址打开 Simple Storage Service（Amazon S3）控制台：https://console.aws.amazon.com/s3/。
3. 在左侧导航窗格中，选择 Multi-Region Access Points（多区域接入点）。
4. 请选择要查看的多区域接入点。
5. 选择 Replication and failover（复制和失效转移）选项卡。此页面显示您的多区域接入点的路由配置详细信息和摘要、关联的复制规则和复制指标。您可以在 Failover configuration（失效转移配置）部分查看区域的路由状态。

#### 使用 Amazon CLI

以下示例 Amazon CLI 命令获取指定区域的当前多区域接入点路由配置。要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control get-multi-region-access-point-routes
--region eu-west-1
--account-id 123456789012
--mrap MultiRegionAccessPoint_ARN
```

> **Note**
>
> 此命令只能对以下五个区域执行：
>
> - ap-southeast-2
> - ap-northeast-1
> - us-east-1
> - us-west-2

- eu-west-1

Amazon S3 多区域接入点失效转移控制错误

更新多区域接入点的失效转移配置时，可能会遇到以下错误之一：

- HTTP 400 错误请求：如果您在更新失效转移配置时输入了无效的多区域接入点 ARN，就会发生此错误。您可以通过查看多区域接入点策略来确认多区域接入点 ARN。要查看或更新多区域接入点策略，请参阅编辑多区域接入点策略。如果您在更新 Amazon S3 多区域接入点失效转移控制时使用空字符串或随机字符串，也会发生此错误。确保使用多区域接入点 ARN 格式：

  `arn:aws:s3::account-id:accesspoint/MultiRegionAccessPoint_alias`
- HTTP 503 Slow Down（HTTP 503 减慢速度）：如果您在短时间内发送的请求过多，就会出现此错误。被拒绝的请求将导致错误。
- HTTP 409 Conflict（HTTP 409 冲突）：当两个或多个并发的路由配置更新请求以单个多区域接入点为目标时，就会出现此错误。第一个请求成功，但任何其他请求都失败而出现错误。
- HTTP 405 Method Not Allowed（HTTP 405 不允许方法）：当您在启动失效转移时选择了只有一个 Amazon Web Services 区域的多区域接入点时，就会出现此错误。在启动失效转移之前，必须选择两个区域。否则，将返回错误。

## 配置用于多区域接入点的复制

向多区域接入点端点发出请求时，Amazon S3 会自动将请求路由到离您最近的桶。Amazon S3 在做出这一决定时不考虑请求的内容。如果发出请求以 GET 对象，您的请求可能会被路由到没有此对象副本的桶。如果发生这种情况，您将收到 HTTP 状态代码 404（找不到）错误。有关多区域接入点请求路由的更多信息，请参阅the section called “请求路由”。

如果您希望多区域接入点能够检索对象，而无论哪个桶接收请求，则必须配置 Amazon S3 跨区域复制（CRR）。

例如，考虑具有三个桶的多区域接入点：

- 区域 US West (Oregon) 中包含对象 my-image.jpg 的名为 *amzn-s3-demo-bucket1* 的桶
- 区域 Asia Pacific (Mumbai) 中包含对象 my-image.jpg 的名为 *amzn-s3-demo-bucket2* 的桶
- 区域 Europe (Frankfurt) 中不包含对象 my-image.jpg 且名为 *amzn-s3-demo-bucket* 的桶

在这种情况下，如果您向 GetObject 对象发出请求 my-image.jpg，则该请求的成功取决于接收您请求的桶。由于 Amazon S3 不考虑请求的内容，因此它可能会将 GetObject 请求添加到 *amzn-s3-demo-bucket* 桶（如果该桶响应距离最近的请求）。即使您的对象位于多区域接入点中的桶中，因为收到您请求的单个桶没有该对象，您仍会收到 HTTP 404 Not Found（HTTP 404 找不到）错误。

启用跨区域复制（CRR）有助于避免这种结果。使用适当的复制规则，将 my-image.jpg 对象复制到 *amzn-s3-demo-bucket* 桶。因此，如果 Amazon S3 将您的请求路由到该桶，您现在可以检索该对象。

对于分配给多区域接入点的桶，复制工作正常。Amazon S3 不会对位于多区域接入点中的桶执行任何特殊复制。有关在桶中配置复制的更多信息，请参阅 设置实时复制概述。

对多区域接入点使用复制的建议

为了在使用多区域接入点时获得最佳的复制性能，我们建议采取以下措施：

- 配置 S3 Replication Time Control（S3 RTC）。要在可预测的时间范围内跨不同区域复制您的数据，您可以使用 S3 RTC。S3 RTC 在 15 分钟内复制 Amazon S3 中存储的 99.99% 的新对象（由服务等级协议提供支持）。有关更多信息，请参阅 the section called “使用 S3 Replication Time Control”。使用 S3 RTC 无需额外付费。有关信息，请参阅 Amazon S3 定价。
- 使用双向复制，以支持在通过多区域接入点更新桶时保持桶同步。有关更多信息，请参阅 the section called “为多区域接入点创建双向复制规则”。
- 创建跨账户多区域接入点，以将数据分别复制到单独 Amazon Web Services 账户中的桶。这种方法提供了账户级分离，这样，就可以从与源桶不同的区域中的不同账户访问数据以及跨不同账户复制数据。设置跨账户多区域接入点无需额外费用。如果您是桶拥有者但不拥有多区域接入点，则只需支付数据传输和请求费用。多区域接入点拥有者支付数据路由和互联网加速费用。有关更多信息，请参阅 Amazon S3 定价。
- 为每个复制规则启用副本修改同步，以使对于对象的元数据更改也保持同步。有关更多信息，请参阅启用副本修改同步。
- 启用 Amazon CloudWatch 指标来监控复制事件。将收取 CloudWatch 指标费用。有关更多信息，请参阅 Amazon CloudWatch 定价。

主题

- 为多区域接入点创建单向复制规则
- 为多区域接入点创建双向复制规则
- 查看多区域接入点的复制规则

为多区域接入点创建单向复制规则

复制规则允许跨桶自动和异步复制对象。单向复制规则有助于确保将数据从一个 Amazon Web Services 区域中的源桶完全复制到另一个区域的目标桶。当设置单向复制时，将创建从源存储桶（*amzn-s3-demo-bucket*）到目标存储桶（*amzn-s3-demo-bucket*）的复制规则。与所有复制规则一样，您可以将单向复制规则应用于整个 Amazon S3 桶，也可以应用于按前缀或对象标签筛选的对象子集。

> **Important**
>
> 如果您的用户只使用目标桶中的对象，我们建议使用单向复制。如果您的用户要上传或修改目标桶中的对象，请使用双向复制来保持所有桶同步。如果您计划使用多区域接入点进行失效转移，我们也建议使用双向复制。要设置双向复制，请参阅the section called “为多区域接入点创建双向复制规则”。

为多区域接入点创建单向复制规则

1. 登录到Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Multi-Region Access Points（多区域接入点）。
3. 请选择多区域接入点的名称。
4. 选择 Replication and failover（复制和失效转移）选项卡。
5. 向下滚动到 Replication rules（复制规则）部分，然后选择 Create replication rules（创建复制规则）。确保您有足够的权限来创建复制规则，否则将禁用版本控制。

   > **Note**
   >
   > 您只能为自己账户中的桶创建复制规则。要为外部桶创建复制规则，桶拥有者必须为这些桶创建复制规则。

6. 在创建复制规则页面上，选择将对象从一个或多个源桶复制到一个或多个目标桶模板。

   > **Important**
   >
   > 当您使用此模板创建复制规则时，它们会替换已经分配给桶的任何现有复制规则。要添加或修改任何现有的复制规则而不是替换它们，请转到控制台中每个桶的 Management（管理）选项卡，然后在 Replication rules（复制规则）部分编辑规则。还

可以使用 Amazon CLI、SDK 或 REST API 添加或修改现有复制规则。有关更多信息，请参阅 复制配置文件元素。

7. 在源和目标部分中的源桶下，选择要从中复制对象的一个或多个桶。选择进行复制的所有桶（源和目标）都必须启用 S3 版本控制，并且每个桶必须位于不同的 Amazon Web Services 区域中。有关 S3 版本控制的更多信息，请参阅在 Amazon S3 桶中使用版本控制。

   在目标桶下，选择要将对象复制到其中的一个或多个桶。

8. 在 Replication rule configuration（复制规则配置）部分中，选择在创建复制规则时将其设置为 Enabled（启用）还是 Disabled（禁用）。

   > **Note**
   >
   > 您无法在 Replication rule name（复制规则名称）框中输入名称。复制规则名称是根据您创建复制规则时的配置生成的。

9. 在 Scope（范围）部分中，为复制选择适当的范围。

   - 要复制整个桶，请选择 Apply to all objects in the bucket（应用到桶中的所有对象）。
   - 为了复制桶中对象的子集，请选择 Limit the scope of this rule using one or more filters（使用一个或多个筛选条件限制此规则的范围)。

     可按前缀、对象标签或二者的组合筛选对象。

     - 要将复制限制为名称以相同字符串（例如 `pictures`）开头的所有对象，请在 Prefix（前缀）框中输入前缀。

       如果输入的前缀是文件夹的名称，则必须使用分隔符 [如 /（正斜杠）] 来指示其层次级别（例如 `pictures/`）。有关前缀的更多信息，请参阅使用前缀整理对象。

     - 要复制具有一个或多个对象标签的所有对象，请选择 Add tag（添加标签），然后在框中输入键值对。要添加另一个标签，请重复该过程。有关对象标签的更多信息，请参阅 使用标签对存储进行分类。

10. 向下滚动到 Additional replication options（其他复制选项）部分，然后选择要应用的复制选项。

    > **Note**
    >
    > 我们建议您应用以下选项：

- Replication time control（RTC）[复制时间控制（RTC）] – 要在可预测的时间范围内跨不同区域复制您的数据，您可以使用 S3 Replication Time Control（S3 RTC）。S3 RTC 在 15 分钟内复制 Amazon S3 中存储的 99.99% 的新对象（由服务等级协议提供支持）。有关更多信息，请参阅 the section called “使用 S3 Replication Time Control”。
- Replication metrics and notifications（复制指标和通知）– 启用 Amazon CloudWatch 指标以监控复制事件。
- 删除标记复制 - 将复制由 S3 删除操作创建的删除标记。不会复制由生命周期规则创建的删除标记。有关更多信息，请参阅在桶之间复制删除标记。

S3 RTC 和 CloudWatch 复制指标和通知需要额外收费。有关更多信息，请参阅 Amazon S3 定价和 Amazon CloudWatch 定价。

11. 如果您正在编写取代现有复制规则的新复制规则，请选择 I acknowledge that by choosing Create replication rules, these existing replication rules will be overwritten（我确认通过选择“创建复制规则”，这些现有的复制规则将被覆盖）。
12. 选择创建复制规则以创建和保存新的单向复制规则。

为多区域接入点创建双向复制规则

复制规则允许跨桶自动和异步复制对象。双向复制规则可确保数据在不同 Amazon Web Services 区域中的两个或更多桶之间完全同步。设置双向复制时，将创建从源桶（DOC-EXAMPLE-BUCKET-1）到包含副本的桶（DOC-EXAMPLE-BUCKET-2）的复制规则。然后，创建从包含副本的桶（DOC-EXAMPLE-BUCKET-2）到源桶（DOC-EXAMPLE-BUCKET-1）的第二个复制规则。

与所有复制规则一样，您可以将双向复制规则应用于整个 Amazon S3 桶，也可以应用于按前缀或对象标签筛选的对象子集。您还可以通过为每个复制规则启用副本修改同步来保持对于对象的元数据更改同步。您可以通过 Amazon S3 控制台、Amazon CLI、Amazon SDK、Amazon S3 REST API 或 Amazon CloudFormation 启用副本修改同步。

要监控 Amazon CloudWatch 中对象和对象元数据的复制进度，请启用 S3 复制指标和通知。有关更多信息，请参阅使用复制指标和 Amazon S3 事件通知监控进度。

为多区域接入点创建双向复制规则

1. 登录到Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Multi-Region Access Points（多区域接入点）。
3. 请选择要更新的多区域接入点的名称。
4. 选择 Replication and failover（复制和失效转移）选项卡。
5. 向下滚动到 Replication rules（复制规则）部分，然后选择 Create replication rules（创建复制规则）。
6. 在 Create replication rules（创建复制规则）页面上，选择 Replicate objects among all specified buckets（在所有指定桶间复制对象）模板。Replicate objects among all specified buckets（在所有指定桶间复制对象）模板可为您的桶设置双向复制（具有失效转移功能）。

   > **Important**
   >
   > 当您使用此模板创建复制规则时，它们会替换已经分配给桶的任何现有复制规则。要添加或修改任何现有的复制规则而不是替换它们，请转到控制台中每个桶的 Management（管理）选项卡，然后在 Replication rules（复制规则）部分编辑规则。还可以使用 Amazon CLI、Amazon SDK 或 Amazon S3 REST API 添加或修改现有复制规则。有关更多信息，请参阅 复制配置文件元素。

7. 在 Buckets（桶）部分中，选择至少两个要从中复制对象的桶。选择进行复制的所有桶都必须启用 S3 版本控制，并且每个桶必须位于不同的 Amazon Web Services 区域中。有关 S3 版本控制的更多信息，请参阅在 Amazon S3 桶中使用版本控制。

   > **Note**
   >
   > 确保您具有建立复制所需的读取和复制权限，否则会遇到错误。有关更多信息，请参阅创建 IAM 角色。

8. 在 Replication rule configuration（复制规则配置）部分中，选择在创建复制规则时将其设置为 Enabled（启用）还是 Disabled（禁用）。

   > **Note**
   >
   > 您无法在 Replication rule name（复制规则名称）框中输入名称。复制规则名称是根据您创建复制规则时的配置生成的。

9. 在 Scope（范围）部分中，为复制选择适当的范围。

- 要复制整个桶，请选择 Apply to all objects in the bucket（应用到桶中的所有对象）。
- 为了复制桶中对象的子集，请选择 Limit the scope of this rule using one or more filters（使用一个或多个筛选条件限制此规则的范围)。

  可按前缀、对象标签或二者的组合筛选对象。

  - 要将复制限制为名称以相同字符串（例如 `pictures`）开头的所有对象，请在 Prefix（前缀）框中输入前缀。

    如果您输入属于文件夹名称的前缀，则必须使用 `/`（正斜杠）作为最后一个字符（例如，`pictures/`）。
  - 要复制具有一个或多个对象标签的所有对象，请选择 Add tag（添加标签），然后在框中输入键值对。要添加另一个标签，请重复该过程。有关对象标签的更多信息，请参阅 使用标签对存储进行分类。

10. 向下滚动到 Additional replication options（其他复制选项）部分，然后选择要应用的复制选项。

> **Note**
>
> 我们建议您应用以下选项，尤其是在您打算将多区域接入点配置为支持失效转移时：
>
> - Replication time control（RTC）[复制时间控制（RTC）] – 要在可预测的时间范围内跨不同区域复制您的数据，您可以使用 S3 Replication Time Control（S3 RTC）。S3 RTC 在 15 分钟内复制 Amazon S3 中存储的 99.99% 的新对象（由服务等级协议提供支持）。有关更多信息，请参阅 the section called “使用 S3 Replication Time Control”。
> - Replication metrics and notifications（复制指标和通知）– 启用 Amazon CloudWatch 指标以监控复制事件。
> - 删除标记复制 - 将复制由 S3 删除操作创建的删除标记。不会复制由生命周期规则创建的删除标记。有关更多信息，请参阅在桶之间复制删除标记。
> - Replica modification sync（副本修改同步）– 为每个复制规则启用副本修改同步，以使对于对象的元数据更改保持同步。有关更多信息，请参阅启用副本修改同步。
>
> S3 RTC 和 CloudWatch 复制指标和通知需要额外收费。有关更多信息，请参阅 Amazon S3 定价和 Amazon CloudWatch 定价。

11. 如果您正在编写取代现有复制规则的新复制规则，请选择 I acknowledge that by choosing Create replication rules, these existing replication rules will be overwritten（我确认通过选择“创建复制规则”，这些现有的复制规则将被覆盖）。
12. 选择 Create replication rules（创建复制规则）以创建和保存新的双向复制规则。

查看多区域接入点的复制规则

使用多区域接入点，您可以设置单向复制规则或双向复制规则。有关如何管理复制规则的信息，请参阅使用 Amazon S3 控制台管理复制规则。

查看多区域接入点的复制规则

1. 登录到Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Multi-Region Access Points（多区域接入点）。
3. 请选择多区域接入点的名称。
4. 选择 Replication and failover（复制和失效转移）选项卡。
5. 向下滚动到复制规则部分。本节将列出已为多区域接入点创建的所有复制规则。

> **Note**
>
> 如果您已将来自其他账户的桶添加到此多区域接入点，则必须从桶拥有者获得 `s3:GetBucketReplication` 权限才能查看该桶的复制规则。

## 将多区域接入点与支持的 API 操作结合使用

Amazon S3 提供了一组操作用来管理多区域访问点。Amazon S3 同步处理其中一些操作，异步处理另一些操作。当您调用异步操作时，Amazon S3 首先同步授权请求的操作。如果授权成功，Amazon S3 将返回一个令牌，您可以使用该令牌来跟踪所请求操作的进度和结果。

> **Note**
>
> 通过 Amazon S3 控制台发出的请求始终是同步的。控制台等待，直到请求完成，然后再允许您提交另一个请求。

您可以使用控制台查看异步操作的当前状态和结果，也可以使用 Amazon CLI、Amazon SDK 或 REST API 中的 DescribeMultiRegionAccessPointOperation。Amazon S3 在响应异步操作时提供跟踪令牌。您将该跟踪令牌作为 DescribeMultiRegionAccessPointOperation。当您包括跟踪令牌时，Amazon S3 会返回指定操作的当前状态和结果，包括任何错误或相关资源信息。Amazon S3 执行 DescribeMultiRegionAccessPointOperation 同步操作。

所有创建或维护多区域接入点的控制面板请求都必须路由到 US West (Oregon) 区域。对于多区域接入点数据面板请求，无需指定区域。对于多区域接入点失效转移控制面板，请求必须路由到五个支持的区域之一。有关支持多区域接入点的区域的更多信息，请参阅多区域接入点限制和限制。

此外，您必须将 s3:ListAllMyBuckets 权限授予请求管理多区域接入点的用户、角色或其他 Amazon Identity and Access Management（IAM）实体。

以下示例演示如何在 Amazon S3 中将多区域接入点与兼容操作结合使用。

主题


- 多区域接入点与 Amazon Web Services 服务和 Amazon SDK 的兼容性
- 多区域接入点与 S3 操作的兼容性
- 查看您的多区域接入点路由配置
- 更新您的底层 Amazon S3 存储桶策略
- 更新多区域接入点路由配置
- 将对象添加到多区域接入点的桶中
- 从多区域接入点检索对象
- 列出存储在多区域接入点底层桶中的对象
- 将预签名 URL 与多区域接入点结合使用
- 将配置了申请方付款的桶与多区域接入点结合使用


### 多区域接入点与 Amazon Web Services 服务和 Amazon SDK 的兼容性

要在需要 Amazon S3 存储桶名称的应用程序中使用多区域接入点，请在使用 Amazon SDK 发出请求时使用多区域接入点的 Amazon 资源名称（ARN）。要检查哪些 Amazon SDK 与多区域接入点兼容，请参阅与 Amazon SDK 的兼容性。

### 多区域接入点与 S3 操作的兼容性

您可以使用以下 Amazon S3 数据面板 API 操作，对桶中与您的多区域接入点关联的对象执行操作。以下 S3 操作可以接受多区域接入点 ARN：

- AbortMultipartUpload
- CompleteMultipartUpload
- CreateMultipartUpload
- DeleteObject
- DeleteObjectTagging
- GetObject
- GetObjectAcl
- GetObjectLegalHold
- GetObjectRetention
- GetObjectTagging
- HeadObject
- ListMultipartUploads
- ListObjectsV2
- ListParts
- PutObject
- PutObjectAcl
- PutObjectLegalHold
- PutObjectRetention
- PutObjectTagging
- RestoreObject
- UploadPart

> **Note**
>
> 当使用多区域接入点 ARN 时，多区域接入点仅支持使用多区域接入点的复制操作作为目标。

您可以使用以下 Amazon S3 控制面板操作来创建和管理多区域接入点：

- CreateMultiRegionAccessPoint
- DescribeMultiRegionAccessPointOperation

- GetMultiRegionAccessPoint
- GetMultiRegionAccessPointPolicy
- GetMultiRegionAccessPointPolicyStatus
- GetMultiRegionAccessPointRoutes
- ListMultiRegionAccessPoints
- PutMultiRegionAccessPointPolicy
- SubmitMultiRegionAccessPointRoutes

### 查看您的多区域接入点路由配置

#### Amazon CLI

以下示例命令检索您的多区域接入点路由配置，以便您可以查看桶的当前路由状态。要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control get-multi-region-access-point-routes
--region eu-west-1
--account-id 111122223333
--mrap arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap
```

#### SDK for Java

以下 SDK for Java 代码检索您的多区域接入点路由配置，以便您可以查看桶的当前路由状态。要使用此示例语法，请将 *user input placeholders* 替换为您自己的信息。

```
S3ControlClient s3ControlClient = S3ControlClient.builder()
    .region(Region.US_EAST_1)
    .credentialsProvider(credentialsProvider)
    .build();

GetMultiRegionAccessPointRoutesRequest request =
 GetMultiRegionAccessPointRoutesRequest.builder()
    .accountId("111122223333")
    .mrap("arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap")
    .build();

GetMultiRegionAccessPointRoutesResponse response =
 s3ControlClient.getMultiRegionAccessPointRoutes(request);
```

SDK for JavaScript

以下 SDK for JavaScript 代码检索您的多区域接入点路由配置，以便您可以查看桶的当前路由状态。要使用此示例语法，请将 *user input placeholders* 替换为您自己的信息。

```
const REGION = 'us-east-1'

const s3ControlClient = new S3ControlClient({
  region: REGION
})

export const run = async () => {
  try {
    const data = await s3ControlClient.send(
      new GetMultiRegionAccessPointRoutesCommand({
        AccountId: '111122223333',
        Mrap: 'arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap',
      })
    )
    console.log('Success', data)
    return data
  } catch (err) {
    console.log('Error', err)
  }
}

run()
```

SDK for Python

以下 SDK for Python 代码检索您的多区域接入点路由配置，以便您可以查看桶的当前路由状态。要使用此示例语法，请将 *user input placeholders* 替换为您自己的信息。

```
s3.get_multi_region_access_point_routes(
        AccountId=111122223333,
        Mrap=arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap)['Routes']
```

### 更新您的底层 Amazon S3 存储桶策略

要授予适当的访问权限，您还必须更新底层 Amazon S3 存储桶策略。以下示例将访问控制委托给多区域接入点策略。在将访问控制委托给多区域接入点策略后，当通过多区域接入点发出请求时，桶策略不再用于访问控制。

以下是将访问控制委托给多区域接入点策略的示例桶策略。要使用这一示例桶策略，请将 *user input placeholders* 替换为您自己的信息。要通过 Amazon CLI put-bucket-policy 命令应用此策略，如下一个示例所示，请将策略保存在文件中，例如 policy.json。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Principal": { "AWS": "*" },
    "Effect": "Allow",
    "Action": ["s3:*"],
    "Resource": ["arn:aws:s3:::111122223333/*", "arn:aws:s3:::amzn-s3-demo-bucket"],
    "Condition": {
      "StringEquals": {
        "s3:DataAccessPointAccount": "444455556666"
      }
    }
  }
}
```

以下 put-bucket-policy 示例命令将更新后的 S3 存储桶策略与您的 S3 存储桶关联起来：

```
aws s3api put-bucket-policy
  --bucket amzn-s3-demo-bucket
  --policy file:///tmp/policy.json
```

更新多区域接入点路由配置

以下示例命令更新多区域接入点路由配置。可以对以下五个区域运行多区域接入点路由命令：

- ap-southeast-2
- ap-northeast-1
- us-east-1
- us-west-2
- eu-west-1

在多区域接入点路由配置中，您可以将桶设置为主动或被动路由状态。主动桶接收流量，而被动桶不接收流量。您可以通过将桶的 TrafficDialPercentage 值设置为 100（表示主动）或 0（表示被动）来设置桶的路由状态。

### Amazon CLI

以下示例命令将更新您的多区域接入点路由配置。在此示例中，*amzn-s3-demo-bucket1* 设置为主动状态，*amzn-s3-demo-bucket2* 设置为被动状态。要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control submit-multi-region-access-point-routes
--region ap-southeast-2
--account-id 111122223333
--mrap arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap
--route-updates Bucket=amzn-s3-demo-bucket1,TrafficDialPercentage=100
                Bucket=amzn-s3-demo-bucket2,TrafficDialPercentage=0
```

### SDK for Java

以下 SDK for Java 代码将更新您的多区域接入点路由配置。要使用此示例语法，请将 *user input placeholders* 替换为您自己的信息。

```
S3ControlClient s3ControlClient = S3ControlClient.builder()
    .region(Region.ap-southeast-2)
    .credentialsProvider(credentialsProvider)
    .build();

SubmitMultiRegionAccessPointRoutesRequest request =
 SubmitMultiRegionAccessPointRoutesRequest.builder()
    .accountId("111122223333")
    .mrap("arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap")
    .routeUpdates(
        MultiRegionAccessPointRoute.builder()
            .region("eu-west-1")
            .trafficDialPercentage(100)
            .build(),
        MultiRegionAccessPointRoute.builder()
            .region("ca-central-1")
            .bucket("111122223333")
            .trafficDialPercentage(0)
            .build()
    )
    .build();

SubmitMultiRegionAccessPointRoutesResponse response =
 s3ControlClient.submitMultiRegionAccessPointRoutes(request);
```

SDK for JavaScript

以下 SDK for JavaScript 代码将更新您的多区域接入点路由配置。要使用此示例语法，请将 *user input placeholders* 替换为您自己的信息。

```
const REGION = 'ap-southeast-2'

const s3ControlClient = new S3ControlClient({
  region: REGION
})

export const run = async () => {
  try {
    const data = await s3ControlClient.send(
      new SubmitMultiRegionAccessPointRoutesCommand({
        AccountId: '111122223333',
        Mrap: 'arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap',
        RouteUpdates: [
          {
            Region: 'eu-west-1',
            TrafficDialPercentage: 100,
          },
          {
            Region: 'ca-central-1',
            Bucket: 'amzn-s3-demo-bucket1',
            TrafficDialPercentage: 0,
          },
        ],
      })
    )
    console.log('Success', data)
    return data
  } catch (err) {
    console.log('Error', err)
  }
}

run()
```

SDK for Python

以下 SDK for Python 代码将更新您的多区域接入点路由配置。要使用此示例语法，请将 *user input placeholders* 替换为您自己的信息。

```
s3.submit_multi_region_access_point_routes(
        AccountId=111122223333,
        Mrap=arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap,
        RouteUpdates= [{
            'Bucket': amzn-s3-demo-bucket,
            'Region': ap-southeast-2,
            'TrafficDialPercentage': 10
        }])
```

### 将对象添加到多区域接入点的桶中

要将对象添加到与多区域接入点关联的桶中，您可以使用 PutObject 操作。要使多区域接入点中的所有桶保持同步，请启用跨区域复制。

> **Note**
>
> 要使用此操作，您必须对多区域接入点拥有 s3:PutObject 权限。有关多区域接入点权限要求的更多信息，请参阅权限。

#### Amazon CLI

以下示例数据面板请求将 *example.txt* 上传到指定的多区域接入点。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3api put-object --bucket
 arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap --key example.txt --
body example.txt
```

#### SDK for Java

```
S3Client s3Client = S3Client.builder()
        .build();

PutObjectRequest objectRequest = PutObjectRequest.builder()
        .bucket("arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap")
        .key("example.txt")
        .build();
```

```
s3Client.putObject(objectRequest, RequestBody.fromString("Hello S3!"));
```

SDK for JavaScript

```
const client = new S3Client({});

async function putObjectExample() {
    const command = new PutObjectCommand({
        Bucket: "arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap",
        Key: "example.txt",
        Body: "Hello S3!",
    });

    try {
        const response = await client.send(command);
        console.log(response);
    } catch (err) {
        console.error(err);
    }
}
```

SDK for Python

```
import boto3

client = boto3.client('s3')
client.put_object(
    Bucket='arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap',
    Key='example.txt',
    Body='Hello S3!'
)
```

### 从多区域接入点检索对象

要从多区域接入点检索对象，可以使用 GetObject 操作。

> **Note**
>
> 要使用此 API 操作，您必须对多区域接入点拥有 `s3:GetObject` 权限。有关多区域接入点权限要求的更多信息，请参阅权限。

### Amazon CLI

以下示例数据面板请求从指定的多区域接入点检索 *example.txt* 并将其下载为 *downloaded_example.txt*。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3api get-object --bucket
 arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap --
key example.txt downloaded_example.txt
```

### SDK for Java

```
S3Client s3 = S3Client
   .builder()
   .build();

GetObjectRequest getObjectRequest = GetObjectRequest.builder()
    .bucket("arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap")
    .key("example.txt")
    .build();

s3Client.getObject(getObjectRequest);
```

### SDK for JavaScript

```
const client = new S3Client({})

async function getObjectExample() {
    const command = new GetObjectCommand({
        Bucket: "arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap",
        Key: "example.txt"
    });

    try {
        const response = await client.send(command);
        console.log(response);
    } catch (err) {
        console.error(err);
    }
}
```

SDK for Python

```
import boto3

client = boto3.client('s3')
client.get_object(
    Bucket='arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap',
    Key='example.txt'
)
```

列出存储在多区域接入点底层桶中的对象

要返回存储在多区域接入点底层桶中的对象的列表，请使用 ListObjectsV2 操作。在以下示例命令中，使用多区域接入点的 ARN 列出了指定多区域接入点的所有对象。在这种情况下，多区域接入点 ARN 为：

`arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap`

> **Note**
>
> 要使用此 API 操作，您必须对于多区域接入点和底层桶拥有 `s3:ListBucket` 权限。有关多区域接入点权限要求的更多信息，请参阅权限。

Amazon CLI

以下示例数据面板请求列出了桶中的对象，该桶位于 ARN 指定的多区域接入点的底层。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3api list-objects-v2 --bucket
 arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap
```

SDK for Java

```
S3Client s3Client = S3Client.builder()
        .build();

String bucketName = "arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap";
```

```
ListObjectsV2Request listObjectsRequest = ListObjectsV2Request
    .builder()
    .bucket(bucketName)
    .build();

 s3Client.listObjectsV2(listObjectsRequest);
```

SDK for JavaScript

```
const client = new S3Client({});

async function listObjectsExample() {
    const command = new ListObjectsV2Command({
        Bucket: "arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap",
    });

    try {
        const response = await client.send(command);
        console.log(response);
    } catch (err) {
        console.error(err);
    }
}
```

SDK for Python

```
import boto3

client = boto3.client('s3')
client.list_objects_v2(
    Bucket='arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap'
)
```

### 将预签名 URL 与多区域接入点结合使用

您可以使用预签名 URL 生成一个 URL，该 URL 允许其他人通过 Amazon S3 多区域接入点访问 Amazon S3 存储桶。创建预签名 URL 时，请将它与特定的对象操作相关联，例如 S3 上传（PutObject）或 S3 下载（GetObject）。您可以共享预签名 URL，任何有权访问该 URL 的人都可以像原始签名用户一样执行嵌入在 URL 中的操作。

预签名 URL 具有到期日期。到达到期时间后，URL 将不再起作用。

在将 S3 多区域接入点与预签名 URL 结合使用之前，请检查 Amazon SDK 与 SigV4A 算法的兼容性。验证您的 SDK 版本是否支持将 SigV4A 作为用于签署全局 Amazon Web Services 区域请求的签名实现。有关在 Amazon S3 中使用预签名 URL 的更多信息，请参阅使用预签名 URL 共享对象。

以下示例说明如何将多区域接入点与预签名 URL 结合使用。要使用这些示例，请将 *user input placeholders* 替换为您自己的信息。

Amazon CLI

```
aws s3 presign
 arn:aws:s3::123456789012:accesspoint/MultiRegionAccessPoint_alias/example-file.txt
```

SDK for Python

```
import logging
import boto3
from botocore.exceptions import ClientError

s3_client = boto3.client('s3',aws_access_key_id='xxx',aws_secret_access_key='xxx')
s3_client.generate_presigned_url(HttpMethod='PUT',ClientMethod="put_object",
 Params={'Bucket':'arn:aws:s3::123456789012:accesspoint/
abcdef0123456.mrap','Key':'example-file'})
```

SDK for Java

```
S3Presigner s3Presigner = S3Presigner.builder()
    .credentialsProvider(StsAssumeRoleCredentialsProvider.builder()
        .refreshRequest(assumeRole)
        .stsClient(stsClient)
        .build())
    .build();

GetObjectRequest getObjectRequest = GetObjectRequest.builder()
    .bucket("arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap")
    .key("example-file")
    .build();

GetObjectPresignRequest preSignedReq = GetObjectPresignRequest.builder()
    .getObjectRequest(getObjectRequest)
    .signatureDuration(Duration.ofMinutes(10))
    .build();
```

```
PresignedGetObjectRequest presignedGetObjectRequest =
 s3Presigner.presignGetObject(preSignedReq);
```

> **Note**
>
> 要将 SigV4A 与临时安全凭证结合使用 [例如，在使用 IAM 角色时]，请确保从 Amazon Security Token Service（Amazon STS）中的区域端点而非全局端点请求临时凭证。如果您对 Amazon STS（`sts.amazonaws.com`）使用全局端点，则 Amazon STS 将从全局端点生成临时证书，而 Sig4A 不支持全局端点。因此，您将得到错误。要解决此问题，请使用列出的任何适用于 Amazon STS 的区域性端点。

### 将配置了申请方付款的桶与多区域接入点结合使用

如果与您的多区域接入点关联的 S3 存储桶配置为使用申请方付款，则申请方将支付桶请求费用、下载费用以及任何与多区域接入点相关的费用。有关更多信息，请参阅 Amazon S3 定价。

以下是向连接到申请方付款桶的多区域接入点发出数据面板请求的示例。

#### Amazon CLI

要从连接到申请方付款桶的多区域接入点下载对象，您必须指定 `--request-payer requester` 作为 get-object 请求的一部分。您还必须指定桶中文件的名称以及应存储所下载文件的位置。

```
aws s3api get-object --bucket MultiRegionAccessPoint_ARN --request-payer requester
 --key example-file-in-bucket.txt example-location-of-downloaded-file.txt
```

#### SDK for Java

要从连接到申请方付款桶的多区域接入点下载对象，您必须指定 `RequestPayer.REQUESTER` 作为 `GetObject` 请求的一部分。您还必须指定桶中文件的名称及其存储位置。

```
GetObjectResponse getObjectResponse = s3Client.getObject(GetObjectRequest.builder()
    .key("example-file.txt")
    .bucket("arn:aws:s3::
123456789012:accesspoint/abcdef0123456.mrap")
    .requestPayer(RequestPayer.REQUESTER)
    .build()
).response();
```

## 监视和记录通过多区域接入点发出的对底层资源的请求

Amazon S3 记录通过多区域接入点发出的请求以及对管理这些接入点的 API 操作（如 CreateMultiRegionAccessPoint 和 GetMultiRegionAccessPointPolicy）发出的请求。通过接入点向 Amazon S3 发出的请求将显示在 S3 服务器访问日志和具有多区域接入点主机名的 Amazon CloudTrail 日志中。接入点的主机名采用此形式：*MRAP_alias*.accesspoint.s3-global.amazonaws.com。例如，假设您具有以下桶和接入点配置：

- 区域 us-west-2 中包含对象 my-image.jpg 且名为 my-bucket-usw2 的桶。
- 区域 ap-south-1 中包含对象 my-image.jpg 且名为 my-bucket-aps1 的桶。
- 区域 eu-central-1 中不包含名为 my-image.jpg 的对象且名为 my-bucket-euc1 的桶。
- 名为 my-mrap 别名 mfzwi23gnjvgw.mrap 的多区域接入点配置为满足来自所有三个桶的请求。
- 您的 Amazon 账户 ID 是 123456789012。

为了直接通过日志中显示的主机名为 *bucket_name*.s3.*Region*.amazonaws.com 的桶检索 my-image.jpg 而发出的请求。

如果您改为通过多区域接入点发出请求，Amazon S3 首先确定不同区域中的哪个桶距离最近。Amazon S3 确定用于满足请求的桶后，它会将请求发送到该桶并使用多区域接入点主机名记录操作。在此示例中，如果 Amazon S3 将请求中继到 my-bucket-aps1，则您的日志将反映对 my-bucket-aps1 中 my-image.jpg 的成功 GET 请求，使用的主机名为 mfzwi23gnjvgw.mrap.accesspoint.s3-global.amazonaws.com。

> **Important**
>
> 多区域接入点不了解底层桶的数据内容。因此，收到请求的桶可能不包含所请求的数据。例如，如果 Amazon S3 确定 my-bucket-euc1 桶距离最近，则您的日志将反映对于 my-bucket-euc1 中 my-image.jpg 的失败 GET 请求，使用的主机名为 mfzwi23gnjvgw.mrap.accesspoint.s3-global.amazonaws.com。如果请求已改而路由到 my-bucket-usw2，您的日志将表明成功的 GET 请求。

有关 Amazon S3 服务器访问日志的更多信息，请参阅 使用服务器访问日志记录来记录请求。有关 Amazon CloudTrail 的更多信息，请参阅《Amazon CloudTrail 用户指南》中的什么是 Amazon CloudTrail？。

### 监控和记录对多区域接入点管理 API 操作发出的请求

Amazon S3 提供了多个 API 操作来管理多区域接入点，例如 `CreateMultiRegionAccessPoint` 和 `GetMultiRegionAccessPointPolicy`。当您使用 Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 Amazon S3 REST API 请求这些 API 操作时，Amazon S3 将异步处理这些请求。只要您对请求具有相应的权限，Amazon S3 将返回这些请求的令牌。您可以将此令牌与 `DescribeAsyncOperation` 用来帮助您查看正在进行的异步操作的状态。Amazon S3 同步处理 `DescribeAsyncOperation` 请求。要查看异步请求的状态，可以使用 Amazon S3 控制台、Amazon CLI、SDK 或 REST API。

> **Note**
>
> 控制台仅显示前 14 天内发出的异步请求的状态。要查看旧请求的状态，请使用 Amazon CLI、开发工具包或 REST API。

异步管理操作可以处于以下几种状态之一：

NEW

Amazon S3 已收到请求，并准备执行该操作。

IN_PROGRESS

Amazon S3 当前正在执行该操作。

SUCCESS

操作已成功。响应包括相关信息，例如 `CreateMultiRegionAccessPoint` 请求。

FAILED

该操作失败。响应包含一条错误消息，指示请求失败的原因。

### 将 Amazon CloudTrail 与多区域接入点结合使用

您可以使用 Amazon CloudTrail 来查看、搜索、下载、归档、分析和响应您的 Amazon 基础设施中的账户活动。通过多区域接入点和 CloudTrail 日志记录，您可以确定以下各项：

- 谁或什么执行了哪个操作
- 对哪些资源执行了操作
- 事件发生的时间

- 有关事件的其他详细信息

您可以使用此日志记录信息来帮助您分析和响应通过多区域接入点发生的活动。

如何设置 Amazon CloudTrail 多区域接入点

要针对与创建或维护多区域接入点相关的任何操作启用 CloudTrail 日志记录，您必须配置 CloudTrail 日志记录来记录美国西部（俄勒冈州）区域中的事件。您必须以这种方式设置日志记录配置，而无论您在发出请求时所在的区域，也无论多区域接入点支持哪些区域。创建或维护多区域接入点的所有请求都通过美国西部（俄勒冈州）区域路由。我们建议您将此区域添加到现有跟踪中，或者创建包含此区域以及与多区域接入点关联的所有区域的新跟踪。

Amazon S3 记录通过多区域接入点发出的所有请求以及对管理接入点的 API 操作（如 `CreateMultiRegionAccessPoint` 和 `GetMultiRegionAccessPointPolicy`）发出的请求。当您通过多区域接入点记录这些请求时，它们将显示在 Amazon CloudTrail 日志中包含多区域接入点的主机名。例如，如果您通过带有别名 `mfzwi23gnjvgw.mrap` 的多区域接入点向桶发出请求，则 CloudTrail 日志中的条目的主机名将为 `mfzwi23gnjvgw.mrap.accesspoint.s3-global.amazonaws.com`。

多区域接入点将请求路由到最近的桶。由于这种行为，当您查看多区域接入点的 CloudTrail 日志时，您将看到对底层桶发出的请求。其中一些请求可能是对桶的直接请求，这些请求不是通过多区域接入点路由的。在查看流量时，请记住这一事实。当桶位于多区域接入点中时，仍可直接向该桶发出请求，而无需通过多区域接入点。

创建和管理多区域接入点涉及异步事件。异步请求在 CloudTrail 日志中没有完成事件。有关异步请求的更多信息，请参阅 监控和记录对多区域接入点管理 API 操作发出的请求。

有关 Amazon CloudTrail 的更多信息，请参阅《Amazon CloudTrail 用户指南》中的什么是 Amazon CloudTrail？。

# 使用 S3 版本控制保留对象的多个版本

Amazon S3 中的版本控制是在相同的存储桶中保留对象的多个变量的方法。对于存储桶中存储的每个对象，您可以使用 S3 版本控制功能来保留、检索和还原它们的各个版本。使用版本控制能够更加轻松地从用户意外操作和应用程序故障中恢复数据。为存储桶启用版本控制后，如果 Amazon S3 同时收到针对同一对象的多个写入请求，它会存储所有对象。

启用了版本控制的存储桶可以协助您恢复因意外删除或覆盖操作而失去的对象。例如，如果您删除对象，Amazon S3 会插入删除标记，而不是永久删除该对象。删除标记将成为当前对象版本。如果覆盖

对象，则会导致存储桶中出现新的对象版本。您始终可以恢复以前的版本。有关更多信息，请参阅 从启用了版本控制的存储桶中删除对象版本。

默认情况下，S3 版本控制在存储桶上处于禁用状态，您必须明确启用它。有关更多信息，请参阅 在存储桶上启用版本控制。

> **Note**
>
> - SOAP API 不支持 S3 版本控制。HTTP 上的 SOAP 支持已弃用，但是仍可在 HTTPS 上使用。SOAP 不支持新增的 Amazon S3 功能。
> - 对于存储和传输的每个对象版本，都适用正常 Amazon S3 费率。对象的每个版本都是完整的对象；它并非只是与上一版本有所不同。因此，如果您存储了三个版本的对象，则会收取您三个对象的费用。

## 不受版本控制、启用了版本控制和已暂停版本控制的存储桶

存储桶可能处于以下三种状态之一：

- 不受版本控制（默认）
- 已启用版本控制
- 已暂停版本控制

您可以在存储桶级别启用和暂停版本控制。一旦您对存储桶启用了版本控制，它将无法返回到不受版本控制状态。但是，您可以在该存储桶上暂停版本控制。

版本控制状态将应用到该存储桶中的所有（不是某些）对象。当您在存储桶中启用版本控制功能时，所有新对象都将受版本控制，并为其指定唯一的版本 ID。此后，在启用版本控制功能时，存储桶中已存在的对象将始终受版本控制，并在以后的请求修改时为其提供唯一的版本 ID。请注意以下几点：

- 在您设置版本控制状态之前存储在存储桶中的对象的版本 ID 为 `null`。启用版本控制时，存储桶中的现有对象不会更改。更改的是 Amazon S3 在以后的请求中处理这些对象的方式。有关更多信息，请参阅 使用启用版本控制的存储桶中的对象。
- 存储桶拥有者（或任何具有适当权限的用户）可以暂停版本控制以停止累积对象版本。暂停版本控制时，存储桶中的现有对象不会更改。更改的是 Amazon S3 在以后的请求中处理对象的方式。有关更多信息，请参阅 使用已暂停版本控制的存储桶中的对象。

# 将 S3 版本控制与 S3 生命周期结合使用

要自定义您的数据保留方法和控制存储成本，请将对象版本控制与 S3 生命周期结合使用。有关更多信息，请参阅 管理对象的生命周期。有关使用 Amazon Web Services Management Console、Amazon CLI、Amazon SDK 或 REST API 创建 S3 生命周期配置的信息，请参阅在存储桶上设置 S3 生命周期配置。

> **Important**
>
> 如果您在不受版本控制的存储桶中具有对象到期生命周期配置，并且希望在启用版本控制时保持相同的永久删除行为，则必须添加非当前版本到期策略。非当前版本到期生命周期配置将管理在启用版本控制的存储桶中删除非当前对象版本的行为。（启用版本控制的存储桶会维护一个当前对象版本，以及零个或更多非当前对象版本。）有关更多信息，请参阅 在存储桶上设置 S3 生命周期配置。

有关使用 S3 版本控制的信息，请参阅以下主题。

主题

- S3 版本控制的工作原理
- 在存储桶上启用版本控制
- 配置 MFA 删除
- 使用启用版本控制的存储桶中的对象
- 使用已暂停版本控制的存储桶中的对象
- 版本控制故障排除

## S3 版本控制的工作原理

您可以使用 S3 版本控制将对象的多个版本保存在一个存储桶中，以便您能够还原意外删除或覆盖的对象。例如，如果您将 S3 版本控制应用于存储桶，则会发生以下变化：

- 如果删除对象（而不是永久移除此对象），则 Amazon S3 会插入删除标记，它将成为当前对象版本。然后，您可以恢复以前的版本。有关更多信息，请参阅 从启用了版本控制的存储桶中删除对象版本。
- 如果覆盖对象，则 Amazon S3 会在存储桶中添加新的对象版本。之前的版本保留在存储桶中，成为非当前版本。您可以还原以前的版本。

> **Note**
>
> 对于存储和传输的每个对象版本，都适用正常 Amazon S3 费率。对象的每个版本都是完整的对象；它与以前的版本没有什么区别。因此，如果您存储了三个版本的对象，则会收取您三个对象的费用。

您创建的每个 S3 存储桶都具有关联的 versioning 子资源。（有关更多信息，请参阅 通用存储桶配置选项。）默认情况下，您的存储桶不受版本控制，且对子资源进行版本控制会存储空的版本控制配置，如下所示。

```
<VersioningConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
</VersioningConfiguration>
```

要启用版本控制，您可以向 Amazon S3 发送请求，在请求中指定包含 Enabled 状态的版本控制配置。

```
<VersioningConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Status>Enabled</Status>
</VersioningConfiguration>
```

要暂停版本控制，请将状态值设置为 Suspended。

> **Note**
>
> 当您首次对存储桶启用版本控制时，可能只需很短的时间即可完全传播更改。当此更改传播时，在对启用版本控制后创建或更新的对象发出请求时，您可能会遇到间歇性 HTTP 404 NoSuchKey 错误。我们建议您在启用版本控制后等待 15 分钟，然后再对存储桶中的对象发出写入操作（PUT 或 DELETE）。

存储桶拥有者和所有获得授权的 Amazon Identity and Access Management（IAM）用户都可以启用版本控制。创建存储桶的存储桶拥有者为 Amazon Web Services 账户。有关权限的更多信息，请参阅 Amazon S3 的身份和访问管理。

有关使用 Amazon Web Services Management Console、Amazon Command Line Interface（Amazon CLI）或 REST API 启用和禁用 S3 版本控制的更多信息，请参阅the section called “在存储桶上启用版本控制”。

主题


- 版本 ID
- 版本控制工作流程


## 版本 ID

如果您为存储桶启用版本控制，Amazon S3 会自动为要存储的对象生成唯一版本 ID。例如，在一个存储桶中，您可以拥有两个具有相同键（对象名称）的对象，但版本 ID 不同，例如 photo.gif（版本 111111）和 photo.gif（版本 121212）。
图中描述了一个启用了版本控制的存储桶，该存储桶有两个具有相同键但版本 ID 不同的对象。

无论 S3 版本控制是否启用，每个对象都有一个版本 ID。如果未启用 S3 版本控制，Amazon S3 将版本 ID 的值设置为 null。如果您启用 S3 版本控制，Amazon S3 会为对象分配版本 ID 值。此值将该对象与同一个键的其他版本区分开来。

在现有存储桶上启用 S3 版本控制时，已存储在存储桶中的对象将保持不变。版本 ID（null）、内容和权限保持不变。启用 S3 版本控制后，添加到存储桶的每个对象都会获得一个版本 ID，该 ID 将此版本与同一个键的其他版本区分开来。

Amazon S3 仅生成版本 ID，不能编辑它们。版本 ID 是 Unicode、UTF-8 编码、URL 就绪、不透明的字符串，长度不超过 1,024 字节。以下是示例：

```
3sL4kqtJlcpXroDTDmJ+rmSpXd3dIbrHY+MTRCxf3vjVBH40Nr8X8gdRQBpUMLUo
```

> **Note**
>
> 为简单起见，本主题中的其他示例使用更短的 ID。

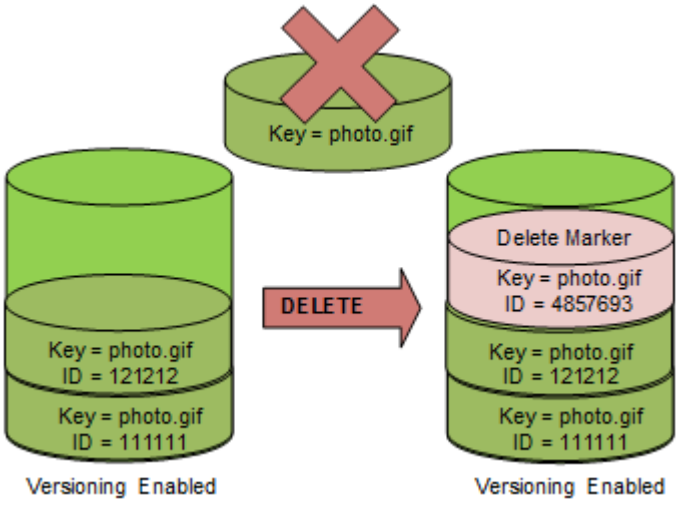
## 版本控制工作流程

当您在启用版本控制的存储桶中通过 PUT 放入对象时，不会覆盖非当前版本。如下图所示，当将 photo.gif 的新版本 PUT 到一个已经包含同名对象的存储桶中时，会发生以下行为：

- 原始对象（ID = 111111）保留在存储桶中。
- Amazon S3 生成一个新的版本 ID（121212），并将这个较新版本的对象添加到存储桶中。

使用此功能，如果对象被意外覆盖或删除，则可以检索对象的先前版本。

当 DELETE 对象时，所有版本都将保留在存储桶中，而 Amazon S3 将插入删除标记，如下图所示。




删除标记将成为对象的当前版本。默认情况下，GET 请求将检索最新存储的版本。在当前版本为删除标记时，执行 GET Object 请求将返回 404 Not Found 错误，如下图所示。

但是，您可以通过指定对象版本 ID，通过 GET 获取非当前版本的对象。在下图中，GET 特定对象版本 111111。即使该对象版本不是当前版本，Amazon S3 也会返回它。

有关更多信息，请参阅 从启用了版本控制的存储桶中检索对象版本。

您可以通过指定要删除的版本来永久删除对象。只有 Amazon S3 存储桶的拥有者或者授权的 IAM 用户才能永久删除某个版本。如果您的 DELETE 操作指定了 versionId，则会永久删除该对象版本，Amazon S3 不会插入删除标记。

您可以通过配置存储桶来启用多重身份验证（MFA）删除，从而提升安全性。对存储桶启用 MFA 删除时，存储桶拥有者必须在任何请求中包含两种形式的身份验证，以删除版本或更改存储桶的版本控制状态。有关更多信息，请参阅 配置 MFA 删除。

何时为对象创建新版本？

仅当您 PUT 新对象时，才会创建对象的新版本。请注意，某些操作（如 CopyObject）通过实现 PUT 操作来发挥作用。

某些修改当前对象的操作不会创建新版本，因为它们没有 PUT 新对象。这包括更改对象上的标签等操作。

> **Important**
>
> 如果您注意到，在对存储桶启用 S3 版本控制后，Amazon S3 对该存储桶的 PUT 或 DELETE 对象请求收到的 HTTP 503（服务不可用）响应数量显著增加，那么该存储桶中可能有一个或多个对象有数以百万计的版本。有关更多信息，请参阅版本控制故障排除的“S3 版本控制”一节。

## 在存储桶上启用版本控制

您可以使用 S3 版本控制在一个存储桶中保留对象的多个版本。本部分提供了如何使用控制台、REST API、Amazon SDK 和 Amazon Command Line Interface（Amazon CLI）在存储桶上启用版本控制的示例。

> **Note**
>
> 首次在存储桶上启用版本控制后，更改可能需要长达 15 分钟才能在 S3 系统中完全传播。在此期间，对启用版本控制后创建或更新的对象的 GET 请求可能会导致 HTTP 404 NoSuchKey 错误。我们建议在启用版本控制后等待 15 分钟，然后再对存储桶中的对象执行任何写入操作（PUT 或 DELETE）。此等待期有助于避免在对象可见性和版本跟踪方面可能出现的问题。

有关 S3 版本控制的更多信息，请参阅使用 S3 版本控制保留对象的多个版本。有关使用已启用版本控制的存储桶中的对象的信息，请参阅 使用启用版本控制的存储桶中的对象。

要了解有关如何使用 S3 版本控制保护数据的更多信息，请参阅教程：使用 S3 版本控制、S3 对象锁定和 S3 复制保护 Amazon S3 上的数据免遭意外删除或应用程序错误。

您创建的每个 S3 存储桶都具有关联的 versioning 子资源。（有关更多信息，请参阅 通用存储桶配置选项。）默认情况下，您的存储桶不受版本控制，且对子资源进行版本控制会存储空的版本控制配置，如下所示。

```
<VersioningConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
</VersioningConfiguration>
```

要启用版本控制，您可以向 Amazon S3 发送一个请求，在请求中指定包含状态的版本控制配置。

```
<VersioningConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Status>Enabled</Status>
```

```
</VersioningConfiguration>
```

要暂停版本控制，请将状态值设置为 `Suspended`。

存储桶拥有者和所有授权用户都可以启用版本控制。存储桶拥有者是创建存储存储桶的 Amazon Web Services 账户（根账户）。有关许可的更多信息，请参阅Amazon S3 的身份和访问管理。

以下部分提供了有关使用控制台、Amazon CLI 和 Amazon SDK 启用 S3 版本控制的更多详细信息。

使用 S3 控制台

请按照以下步骤使用 Amazon Web Services Management Console 在 S3 存储桶上启用版本控制。

在 S3 通用存储桶上启用或禁用版本控制

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在存储桶列表中，选择要为其启用版本控制的存储桶的名称。
4. 请选择属性。
5. 在存储桶版本控制下，请选择编辑。
6. 请选择 Suspend (暂停) 或 Enable (启用)，然后选择 Save changes (保存更改)。

> **Note**
>
> 您可以将 Amazon Multi-Factor Authentication (MFA) 与版本控制结合使用。将 MFA 与版本控制结合使用时，您必须提供 Amazon Web Services 账户的访问密钥和账户 MFA 设备中的有效代码，才能永久删除对象版本或暂停或重新激活版本控制。
> 要将 MFA 与版本控制结合使用，请启用 `MFA Delete`。但是，您无法使用 Amazon Web Services Management Console 启用 `MFA Delete`。您必须使用 Amazon Command Line Interface (Amazon CLI) 或 API。有关更多信息，请参阅 配置 MFA 删除。

使用 Amazon CLI

以下示例在 S3 通用存储桶上启用版本控制。

```
aws s3api put-bucket-versioning --bucket amzn-s3-demo-bucket1 --versioning-
configuration Status=Enabled
```

以下示例在存储桶上启用 S3 版本控制和多重身份验证（MFA）删除。

```
aws s3api put-bucket-versioning --bucket amzn-s3-demo-bucket1 --versioning-
configuration Status=Enabled,MFADelete=Enabled --mfa "SERIAL 123456"
```

> **Note**
>
> 使用 MFA 删除需要获得批准的物理或虚拟身份验证设备。有关在 Amazon S3 中使用 MFA 删除的更多信息，请参阅配置 MFA 删除。

有关使用 Amazon CLI 启用版本控制的更多信息，请参阅《Amazon CLI 命令参考》中的 put-bucket-versioning。

使用 Amazon SDK

以下示例在存储桶上启用版本控制，然后使用 适用于 Java 的 Amazon SDK 和 适用于 .NET 的 Amazon SDK 检索版本控制状态。有关使用其他 Amazon SDK 的信息，请参阅 Amazon 开发人员中心。

.NET

有关设置和运行代码示例的信息，请参阅《适用于 .NET 的 Amazon SDK 开发人员指南》中的适用于 .NET 的 Amazon SDK 入门。

```
using System;
using Amazon.S3;
using Amazon.S3.Model;

namespace s3.amazon.com.docsamples
{
    class BucketVersioningConfiguration
    {
        static string bucketName = "*** bucket name ***";

        public static void Main(string[] args)
```

```
        {
            using (var client = new AmazonS3Client(Amazon.RegionEndpoint.USEast1))
            {
                try
                {
                    EnableVersioningOnBucket(client);
                    string bucketVersioningStatus =
RetrieveBucketVersioningConfiguration(client);
                }
                catch (AmazonS3Exception amazonS3Exception)
                {
                    if (amazonS3Exception.ErrorCode != null &&
                        (amazonS3Exception.ErrorCode.Equals("InvalidAccessKeyId")
                        ||
                        amazonS3Exception.ErrorCode.Equals("InvalidSecurity")))
                    {
                        Console.WriteLine("Check the provided AWS Credentials.");
                        Console.WriteLine(
                        "To sign up for service, go to http://aws.amazon.com/s3");
                    }
                    else
                    {
                        Console.WriteLine(
                         "Error occurred. Message:'{0}' when listing objects",
                         amazonS3Exception.Message);
                    }
                }
            }

            Console.WriteLine("Press any key to continue...");
            Console.ReadKey();
        }

        static void EnableVersioningOnBucket(IAmazonS3 client)
        {

                PutBucketVersioningRequest request = new PutBucketVersioningRequest
                {
                    BucketName = bucketName,
                    VersioningConfig = new S3BucketVersioningConfig
                    {
                        Status = VersionStatus.Enabled
                    }
                };
```

```
                PutBucketVersioningResponse response =
 client.PutBucketVersioning(request);
        }


        static string RetrieveBucketVersioningConfiguration(IAmazonS3 client)
        {
                GetBucketVersioningRequest request = new GetBucketVersioningRequest
                {
                    BucketName = bucketName
                };

                GetBucketVersioningResponse response =
 client.GetBucketVersioning(request);
                return response.VersioningConfig.Status;
            }
    }
}
```

Java

有关如何创建和测试有效示例的说明，请参阅《适用于 Java 的 Amazon SDK 开发人员指南》中的入门。

```
import java.io.IOException;

import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Region;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3Client;
import com.amazonaws.services.s3.model.AmazonS3Exception;
import com.amazonaws.services.s3.model.BucketVersioningConfiguration;
import com.amazonaws.services.s3.model.SetBucketVersioningConfigurationRequest;

public class BucketVersioningConfigurationExample {
    public static String bucketName = "*** bucket name ***";
    public static AmazonS3Client s3Client;

    public static void main(String[] args) throws IOException {
        s3Client = new AmazonS3Client(new ProfileCredentialsProvider());
        s3Client.setRegion(Region.getRegion(Regions.US_EAST_1));
        try {
```

```
            // 1. Enable versioning on the bucket.
          BucketVersioningConfiguration configuration =
            new BucketVersioningConfiguration().withStatus("Enabled");

    SetBucketVersioningConfigurationRequest setBucketVersioningConfigurationRequest
 =
      new SetBucketVersioningConfigurationRequest(bucketName,configuration);


 s3Client.setBucketVersioningConfiguration(setBucketVersioningConfigurationRequest);

    // 2. Get bucket versioning configuration information.
    BucketVersioningConfiguration conf =
 s3Client.getBucketVersioningConfiguration(bucketName);
     System.out.println("bucket versioning configuration status:    " +
 conf.getStatus());

        } catch (AmazonS3Exception amazonS3Exception) {
            System.out.format("An Amazon S3 error occurred. Exception: %s",
 amazonS3Exception.toString());
        } catch (Exception ex) {
            System.out.format("Exception: %s", ex.toString());
        }
    }
}
```

## 配置 MFA 删除

在 Amazon S3 存储桶中使用 S3 版本控制时，您可以选择通过将存储桶配置为启用 MFA（多重身份验证）删除来添加另一层安全保护。执行此操作时，存储桶拥有者必须在任何请求中包含两种形式的身份验证，以删除版本或更改存储桶的版本控制状态。

MFA 删除要求对以下任一操作进行额外身份验证：

- 更改存储桶的版本控制状态
- 永久删除对象版本

MFA 删除需要结合使用两种形式的身份验证：

- 您的安全凭证

- 在已批准的身份验证设备上显示的有效序列号、空格和 6 位代码的组合

MFA 删除因此可在某些情况下（例如在安全凭证被泄露时）提供更高的安全性。MFA 删除要求启动删除操作的用户证明其实际拥有具有 MFA 代码的 MFA 设备，并为删除操作增加额外的摩擦和安全性，从而帮助防止存储桶被意外删除。

要识别已启用了 MFA 删除的存储桶，您可以使用 Amazon S3 Storage Lens 存储统计管理工具指标。S3 Storage Lens 存储统计管理工具是一项云存储分析功能，您可以使用它在整个组织范围内了解对象存储的使用情况和活动。有关更多信息，请参阅使用 S3 Storage Lens 存储统计管理工具访问存储活动和使用情况。有关指标的完整列表，请参阅 S3 Storage Lens 存储统计管理工具指标词汇表。

存储桶拥有者、创建存储存储桶的 Amazon Web Services 账户（根账户）以及所有授权用户都可以启用版本控制。但是，只有存储桶拥有者（根账户）才能启用 MFA 删除。有关更多信息，请参阅 Amazon 安全博客中的使用 MFA 保护对 Amazon 的访问。

> **Note**
>
> 要将 MFA 删除与版本控制结合使用，请启用 `MFA Delete`。但是，您无法使用 Amazon Web Services Management Console 启用 `MFA Delete`。您必须使用 Amazon Command Line Interface (Amazon CLI) 或 API。
>
> 有关将 MFA 删除与版本控制结合使用的示例，请参阅主题 在存储桶上启用版本控制 中的示例部分。
>
> 不能将 MFA 删除与生命周期配置一起使用。有关生命周期配置以及如何与其他配置交互的详细信息，请参阅 S3 生命周期如何与其它存储桶配置进行交互。

要启用或禁用 MFA 删除，请使用对存储桶配置版本控制时所用的相同 API。Amazon S3 将 MFA 删除配置存储在用于存储桶版本控制状态的相同 versioning 子资源中。

```
<VersioningConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Status>VersioningState</Status>
  <MfaDelete>MfaDeleteState</MfaDelete>
</VersioningConfiguration>
```

要使用 MFA 删除，您可以使用硬件或虚拟 MFA 设备来生成身份验证代码。以下示例显示了在硬件设备上显示的生成的身份验证代码。




MFA 删除和受 MFA 保护的 API 访问的功能旨在提供对不同方案的保护。您可以在存储存储桶上配置 MFA 删除，以协助确保存储桶中的数据不会被意外删除。受 MFA 保护的 API 访问用于在访问敏感的 Amazon S3 资源时，强制执行其他身份验证因素（MFA 代码）。您可以要求使用 MFA 创建的临时证书来完成针对这些 Amazon S3 资源的任何操作。有关示例，请参阅需要 MFA。

有关如何购买和激活身份验证设备的更多信息，请参阅多重身份验证。

### 启用 S3 版本控制并配置 MFA 删除

使用 Amazon CLI

序列号是唯一标识 MFA 设备的数字。对于物理 MFA 设备，这是设备随附的唯一序列号。对于虚拟 MFA 设备，序列号是设备 ARN。

以下示例在存储桶上启用 S3 版本控制和多重身份验证（MFA）删除。

```
aws s3api put-bucket-versioning --bucket amzn-s3-demo-bucket1 --versioning-
configuration Status=Enabled,MFADelete=Enabled --mfa "SERIAL 123456"
```

使用 REST API

有关使用 Amazon S3 REST API 指定 MFA 删除的更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 PutBucketVersioning。

## 使用启用版本控制的存储桶中的对象

在您设置版本控制状态之前存储在 Amazon S3 存储桶中的对象的版本 ID 为 null。启用版本控制时，存储桶中的现有对象不会更改。更改的是 Amazon S3 在以后的请求中处理这些对象的方式。

转换对象版本

可为具有明确定义的生命周期的对象定义生命周期配置规则，以便在对象生命周期的特定时间将对象版本转换为 S3 Glacier Flexible Retrieval 存储类。有关更多信息，请参阅 管理对象的生命周期。

此部分中的主题说明在启用了版本控制的存储桶中进行的各种对象操作。有关版本控制的更多信息，请参阅使用 S3 版本控制保留对象的多个版本。

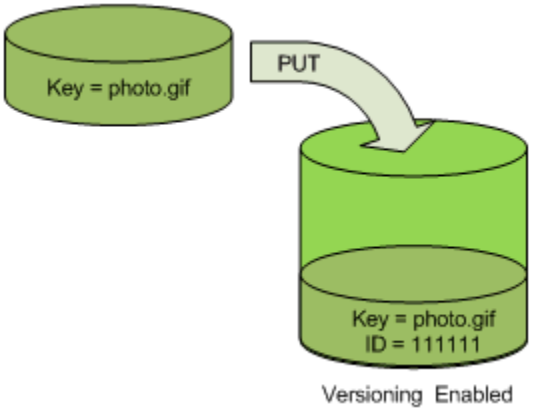
主题

- 将对象添加到已启用版本控制的存储桶
- 列出启用版本控制的存储桶中的对象
- 从启用了版本控制的存储桶中检索对象版本
- 从启用了版本控制的存储桶中删除对象版本
- 配置受版本控制的对象权限

## 将对象添加到已启用版本控制的存储桶

您在存储桶上启用了版本控制后，Amazon S3 会自动将唯一的版本 ID 添加到存储在该存储桶中的每个对象（使用 PUT、POST 或 CopyObject）。

下图显示当将对象添加到已启用版本控制的存储桶时，Amazon S3 会向其添加唯一的版本 ID。




> **Note**
>
> Amazon S3 分配的版本 ID 值是 URL 安全的（可以包含在 URI 中）。

有关版本控制的更多信息，请参阅使用 S3 版本控制保留对象的多个版本。您可以使用控制台、Amazon SDK 和 REST API 将对象版本添加到启用版本控制的存储桶中。

使用 控制台

有关说明，请参阅上传对象。

使用 Amazon SDK

有关使用适用于 Java、.NET 和 PHP 的 Amazon SDK 上传对象的示例，请参阅 上传对象。在无版本控制和启用版本控制的存储桶中上传对象的示例是相同的，只是对于启用版本控制的存储桶，Amazon S3 会分配版本号。否则，版本号为空。

有关使用其他 Amazon SDK 的信息，请参阅 Amazon 开发人员中心。

使用 REST API

要将对象添加到已启用版本控制的存储桶

1. 使用 `PutBucketVersioning` 请求在存储桶上启用版本控制。

   有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 PutBucketVersioning。
2. 发送 `PUT`、`POST` 或 `CopyObject` 请求，以在存储桶中存储对象。

当您将对象添加到已启用版本控制的存储桶时，Amazon S3 将在 `x-amz-version-id` 响应标头中返回该对象的版本 ID，如下面的示例所示。

```
x-amz-version-id: 3/L4kqtJlcpXroDTDmJ+rmSpXd3dIbrHY
```

## 列出启用版本控制的存储桶中的对象

此部分提供从启用版本控制的存储桶列出对象版本的示例。Amazon S3 将对象版本信息存储在与存储桶关联的 versions 子资源中。有关更多信息，请参阅 通用存储桶配置选项。要列出已启用版本控制的存储桶中的对象，您需要 `ListBucketVersions` 权限。

使用 S3 控制台

请按照以下步骤使用 Amazon S3 控制台查看对象的不同版本。

查看对象的多个版本

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在存储桶列表中，请选择包含对象的存储桶的名称。
3. 要查看存储桶中对象的版本列表，请选择显示版本开关。

控制台会显示每个对象版本的唯一版本 ID、对象版本的创建日期和时间以及其他属性。（在您设置版本控制状态之前存储在存储桶中的对象具有版本 ID null。）

要列出没有版本的对象，请选择 List versions (列出版本) 开关。

您也可以在控制台中的对象概述面板中查看、下载和删除对象版本。有关更多信息，请参阅 在 Amazon S3 控制台中查看对象属性。

> **Note**
>
> 要访问早于 300 个版本的对象版本，必须使用 Amazon CLI 或对象的 URL。

> **Important**
>
> 仅当对象已作为最新（当前）版本删除时，您才能取消删除它。您无法取消删除已删除对象的早期版本。有关更多信息，请参阅 使用 S3 版本控制保留对象的多个版本。

使用 Amazon SDK

此部分中的示例说明了如何从启用了版本控制的存储桶中检索对象列表。每个请求最多返回 1000 个版本，除非您指定一个较小的数字。如果存储桶包含的版本数超过此限制，请发送一系列请求来检索所有版本的列表。以“页面”形式返回结果的过程称为分页。

为了说明分页的工作原理，该示例将每个响应限制为两个对象版本。在检索第一页结果后，每个示例将检查以确定版本列表是否已被截断。如果是，示例将继续检索页面，直至检索到所有版本。

> **Note**
>
> 以下示例还使用未启用版本控制的存储桶或用于没有单独版本的对象。在这些情况下，Amazon S3 将返回版本 ID 为 `null` 的对象列表。

有关使用其他 Amazon SDK 的信息，请参阅 Amazon 开发人员中心。

Java

有关创建和测试有效示例的说明，请参阅《适用于 Java 的 Amazon SDK 开发人员指南》中的入门。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.ListVersionsRequest;
import com.amazonaws.services.s3.model.S3VersionSummary;
import com.amazonaws.services.s3.model.VersionListing;

public class ListKeysVersioningEnabledBucket {

    public static void main(String[] args) {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Retrieve the list of versions. If the bucket contains more versions
            // than the specified maximum number of results, Amazon S3 returns
            // one page of results per request.
            ListVersionsRequest request = new ListVersionsRequest()
                    .withBucketName(bucketName)
                    .withMaxResults(2);
            VersionListing versionListing = s3Client.listVersions(request);
            int numVersions = 0, numPages = 0;
            while (true) {
                numPages++;
                for (S3VersionSummary objectSummary :
 versionListing.getVersionSummaries()) {
                    System.out.printf("Retrieved object %s, version %s\n",
                            objectSummary.getKey(),
                            objectSummary.getVersionId());
                    numVersions++;
```

```
                }
                // Check whether there are more pages of versions to retrieve. If
                // there are, retrieve them. Otherwise, exit the loop.
                if (versionListing.isTruncated()) {
                    versionListing =
 s3Client.listNextBatchOfVersions(versionListing);
                } else {
                    break;
                }
            }
            System.out.println(numVersions + " object versions retrieved in " +
 numPages + " pages");
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

有关设置和运行代码示例的信息，请参阅《适用于 .NET 的 Amazon SDK 开发人员指南》中的适用于 .NET 的 Amazon SDK 入门。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class ListObjectsVersioningEnabledBucketTest
    {
        static string bucketName = "*** bucket name ***";
        // Specify your bucket region (an example region is shown).
```

```
        private static readonly RegionEndpoint bucketRegion =
RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main(string[] args)
        {
            s3Client = new AmazonS3Client(bucketRegion);
            GetObjectListWithAllVersionsAsync().Wait();
        }

        static async Task GetObjectListWithAllVersionsAsync()
        {
            try
            {
                ListVersionsRequest request = new ListVersionsRequest()
                {
                    BucketName = bucketName,
                    // You can optionally specify key name prefix in the request
                    // if you want list of object versions of a specific object.

                    // For this example we limit response to return list of 2
versions.
                    MaxKeys = 2
                };
                do
                {
                    ListVersionsResponse response = await
s3Client.ListVersionsAsync(request);
                    // Process response.
                    foreach (S3ObjectVersion entry in response.Versions)
                    {
                        Console.WriteLine("key = {0} size = {1}",
                            entry.Key, entry.Size);
                    }

                    // If response is truncated, set the marker to get the next
                    // set of keys.
                    if (response.IsTruncated)
                    {
                        request.KeyMarker = response.NextKeyMarker;
                        request.VersionIdMarker = response.NextVersionIdMarker;
                    }
                    else
                    {
```

```
                        request = null;
                    }
                } while (request != null);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
        }
    }
}
```

使用 REST API

Example — 列出存储桶中的所有对象版本

要列出存储桶中所有对象的所有版本，请在 versions 请求中使用 GET Bucket 子资源。Amazon S3 最多能检索 1000 个对象，且每个对象版本都将计为一个完整的对象。因此，如果存储桶包含两个键（例如 photo.gif 和 picture.jpg），并且第一个键有 990 个版本，第二个键有 400 个版本，则单个请求将检索 photo.gif 的所有 990 个版本，另加 picture.jpg 的最近 10 个版本。

Amazon S3 将按照存储的顺序返回对象版本，最先返回最近存储的版本。

在 GET Bucket 请求中，包含 versions 子资源。

```
GET /?versions HTTP/1.1
Host: bucketName.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 +0000
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

Example — 检索键的所有版本

要检索对象版本的子集，请为 GET Bucket 使用请求参数。有关更多信息，请参阅 GET Bucket。

1. 将 prefix 参数设置为您要检索的对象的键。

2. 使用 GET Bucket 子资源和 versions 发送 prefix 请求。

```
GET /?versions&prefix=objectName HTTP/1.1
```

Example — 使用前缀检索对象

以下示例将检索其键是 myObject 或由它开头的对象。

```
GET /?versions&prefix=myObject HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

您可以使用其他请求参数来检索对象的所有版本的子集。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 GET Bucket。

Example — 在响应截断时检索其他对象的列表

如果可以在 GET 请求中返回的对象数量超过 max-keys 的值，则响应将包含 <isTruncated>true</isTruncated>，并包含满足该请求但不会返回的第一个键 (在 NextKeyMarker 中) 和第一个版本 ID (在 NextVersionIdMarker 中)。您可以在后续请求中将这些返回的值用作开始位置，以检索满足 GET 请求的其他对象。

使用以下过程从存储桶中检索满足原始 GET Bucket versions 请求的其他对象。有关 key-marker、version-id-marker、NextKeyMarker 和 NextVersionIdMarker 的更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 GET Bucket。

以下是满足原始 GET 请求的其他响应：

- 将 key-marker 的值设置为在上一个响应中的 NextKeyMarker 中返回的键。
- 将 version-id-marker 的值设置为在上一个响应中的 NextVersionIdMarker 中返回的版本 ID。
- 使用 GET Bucket versions 和 key-marker 发送 version-id-marker 请求。

Example — 检索以指定的键和版本 ID 开始的对象

```
GET /?versions&key-marker=myObject&version-id-marker=298459348571 HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
```

```
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

使用 Amazon CLI

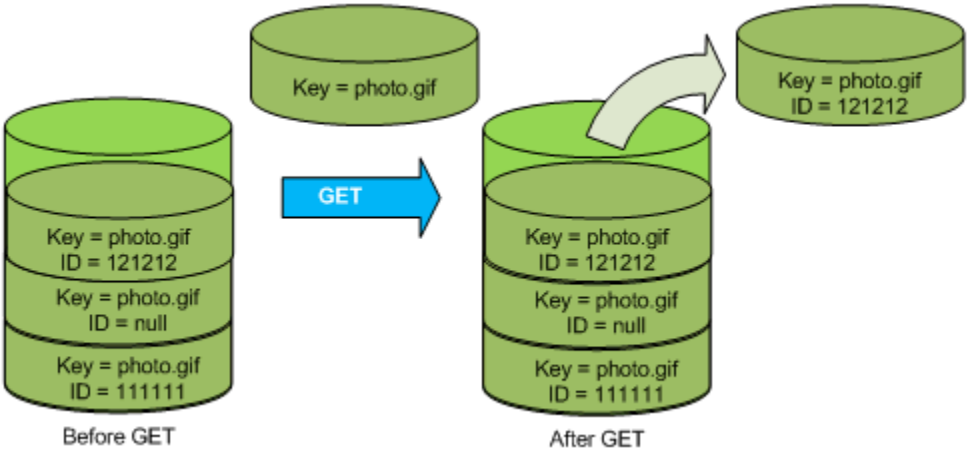
以下命令返回有关存储桶中的对象的所有版本的元数据。

```
aws s3api list-object-versions --bucket amzn-s3-demo-bucket1
```

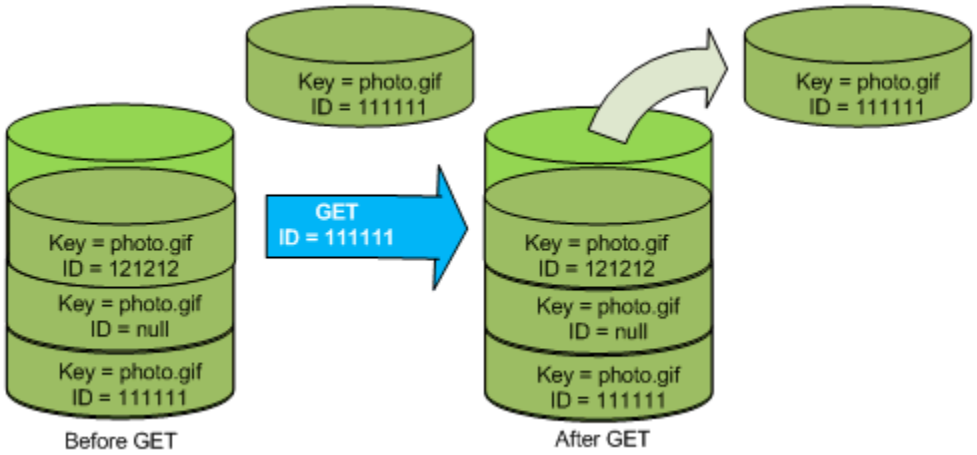
有关 `list-object-versions` 的更多信息，请参阅《Amazon CLI 命令参考》中的 list-object-versions。

## 从启用了版本控制的存储桶中检索对象版本

Amazon S3 中的版本控制是在相同的存储桶中保留对象的多个变量的方法。简单 GET 请求将检索对象的当前版本。下图显示 GET 如何返回 `photo.gif` 对象的当前版本。




要检索特定版本，您需要指定其版本 ID。下图显示 `GET versionId` 请求检索对象的指定版本 (不一定是当前版本)。



您可以使用控制台、Amazon SDK 或 REST API 在 Amazon S3 中检索对象版本。

> **Note**
>
> 要访问早于 300 个版本的对象版本，必须使用 Amazon CLI 或对象的 URL。

使用 S3 控制台

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在存储桶列表中，请选择包含对象的存储桶的名称。
3. 在 Objects（对象）列表中，请选择对象的名称。
4. 请选择 Versions（版本）。

   Amazon S3 显示了对象的所有版本。
5. 选中要检索的版本的 Version ID（版本 ID）旁的复选框。
6. 依次选择 Actions（操作）、Download（下载），然后保存对象。

您也可以在对象概述面板中查看、下载和删除对象版本。有关更多信息，请参阅 在 Amazon S3 控制台中查看对象属性。

> **Important**
>
> 仅当对象已作为最新 (当前) 版本删除时，您才能取消删除它。您无法取消删除已删除对象的早期版本。有关更多信息，请参阅 使用 S3 版本控制保留对象的多个版本。

使用 Amazon SDK

在不受版本控制和启用了版本控制的存储桶中上传对象的示例是相同的。但是，对于启用了版本控制的存储桶，Amazon S3 会分配版本号。否则，版本号为空。

有关使用适用于 Java、.NET 和 PHP 的 Amazon SDK 下载对象的示例，请参阅下载对象。

有关使用适用于 .NET 和 Rust 的 Amazon SDK 列出对象版本的示例，请参阅列出 Amazon S3 存储桶中对象的版本。

使用 REST API

检索特定对象版本的步骤

1. 将 `versionId` 设置为您要检索的对象的版本 ID。
2. 发送 `GET Object versionId` 请求。

Example — 检索受版本控制的对象

以下请求将检索 `L4kqtJlcpXroDTDmpUMLUo` 的版本 `my-image.jpg`。

```
GET /my-image.jpg?versionId=L4kqtJlcpXroDTDmpUMLUo HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

您可以仅检索对象的元数据（而不是内容）。有关信息，请参阅 the section called “检索版本元数据”。

有关还原早期对象版本的信息，请参阅 the section called “还原早期版本”。

检索对象版本的元数据

如果您仅想检索对象的元数据 (而不是其内容)，您可以使用 HEAD 操作。默认情况下，您将获得最新版本的元数据。要检索特定对象版本的元数据，需要指定其版本 ID。

检索对象版本的元数据的步骤

1. 将 `versionId` 设置为您要检索其元数据的对象的版本 ID。
2. 发送 `HEAD Object versionId` 请求。

Example — 检索受版本控制的对象的元数据

以下请求将检索 `my-image.jpg` 的版本 `3HL4kqCxf3vjVBH40Nrjfkd` 的元数据。

```
HEAD /my-image.jpg?versionId=3HL4kqCxf3vjVBH40Nrjfkd HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

以下显示了示例响应。

```
HTTP/1.1 200 OK
x-amz-id-2: ef8yU9AS1ed4OpIszj7UDNEHGran
x-amz-request-id: 318BC8BC143432E5
x-amz-version-id: 3HL4kqtJlcpXroDTDmjVBH40Nrjfkd
Date: Wed, 28 Oct 2009 22:32:00 GMT
Last-Modified: Sun, 1 Jan 2006 12:00:00 GMT
ETag: "fba9dede5f27731c9771645a39863328"
Content-Length: 434234
Content-Type: text/plain
Connection: close
Server: AmazonS3
```

### 还原早期版本

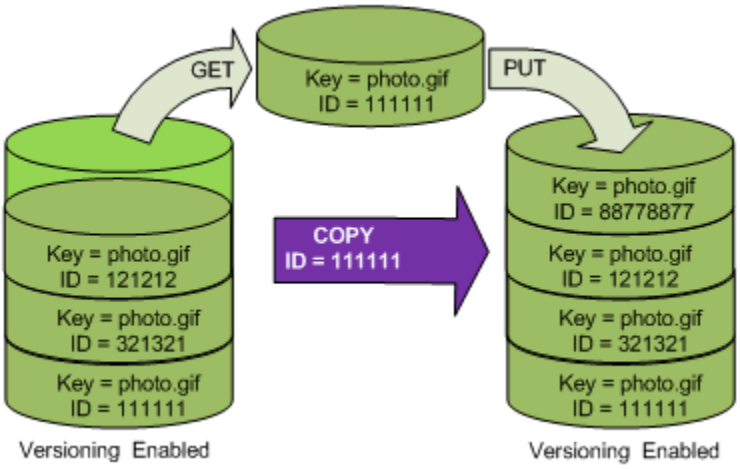
您可以使用版本控制来检索对象的早期版本。有两种方法可执行该操作：

- 将对象的早期版本复制到同一存储桶中。

  复制的对象将成为该对象的当前版本，且所有对象版本都保留。
- 永久删除对象的当前版本。

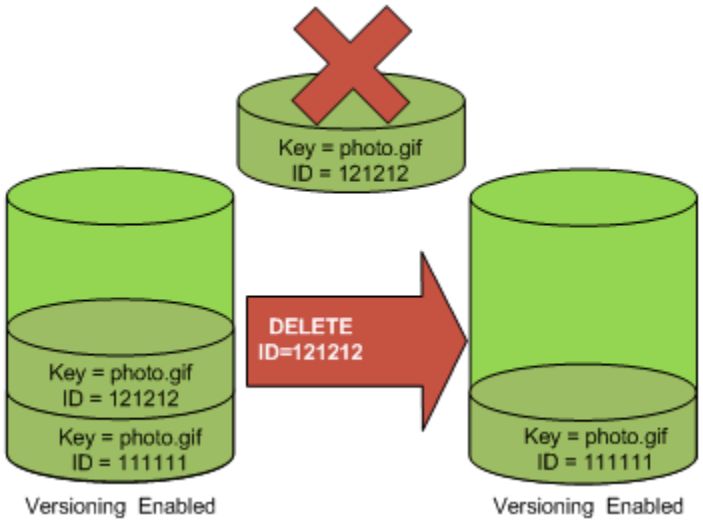
  当您删除当前对象版本时，实际上会将先前版本转换为该对象的当前版本。

由于所有对象版本都保留，所以您可以通过将对象的特定版本复制到同一存储桶，使任何较早版本成为当前版本。在下图中，源对象（ID = 111111）已复制到同一存储桶中。Amazon S3 将提供一个新 ID (88778877)，且它将成为该对象的当前版本。因此，该存储桶同时具有原始对象版本（111111）及其副本（88778877）。有关获取先前版本，然后将其上传以使其成为当前版本的更多信息，请参阅从启用了版本控制的存储桶中检索对象版本和上传对象。



随后，GET 将检索版本 88778877。

下图显示了如何删除对象的当前版本 (121212)，该操作保留早期版本 (111111) 作为当前版本。有关删除对象的更多信息，请参阅删除单个对象。




随后，GET 将检索版本 111111。

> **Note**
>
> 要批量还原对象版本，可以使用 CopyObject 操作。CopyObject 操作会复制清单中指定的每个对象。但请注意，不必以对象在清单中出现的相同顺序复制这些对象。对于受版本控制的存储桶，如果保留当前/非当前版本顺序很重要，您应首先复制所有非当前版本。然后，在第一个任务完成后，在后续任务中复制当前版本。

还原以前的对象版本

使用 S3 控制台

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在存储桶列表中，请选择包含对象的存储桶的名称。
3. 在 Objects（对象）列表中，请选择对象的名称。
4. 请选择 Versions（版本）。

   Amazon S3 显示了对象的所有版本。
5. 选中要检索的版本的 Version ID（版本 ID）旁的复选框。

6. 依次选择 Actions（操作）、Download（下载），然后保存对象。

您也可以在对象概述面板中查看、下载和删除对象版本。有关更多信息，请参阅 在 Amazon S3 控制台中查看对象属性。

> **Important**
>
> 仅当对象已作为最新 (当前) 版本删除时，您才能取消删除它。您无法取消删除已删除对象的早期版本。有关更多信息，请参阅 使用 S3 版本控制保留对象的多个版本。

使用 Amazon SDK

有关使用其他 Amazon SDK 的信息，请参阅 Amazon 开发人员中心。

Python

以下 Python 代码示例通过删除指定回滚版本之后的所有版本，来还原版本控制对象的以前版本。

```
def rollback_object(bucket, object_key, version_id):
    """
    Rolls back an object to an earlier version by deleting all versions that
    occurred after the specified rollback version.

    Usage is shown in the usage_demo_single_object function at the end of this
 module.

    :param bucket: The bucket that holds the object to roll back.
    :param object_key: The object to roll back.
    :param version_id: The version ID to roll back to.
    """
    # Versions must be sorted by last_modified date because delete markers are
    # at the end of the list even when they are interspersed in time.
    versions = sorted(
        bucket.object_versions.filter(Prefix=object_key),
        key=attrgetter("last_modified"),
        reverse=True,
    )

    logger.debug(
        "Got versions:\n%s",
        "\n".join(
```

```
            [
                f"\t{version.version_id}, last modified {version.last_modified}"
                for version in versions
            ]
        ),
    )

    if version_id in [ver.version_id for ver in versions]:
        print(f"Rolling back to version {version_id}")
        for version in versions:
            if version.version_id != version_id:
                version.delete()
                print(f"Deleted version {version.version_id}")
            else:
                break

        print(f"Active version is now {bucket.Object(object_key).version_id}")
    else:
        raise KeyError(
            f"{version_id} was not found in the list of versions for "
f"{object_key}."
        )
```

## 从启用了版本控制的存储桶中删除对象版本

您在需要时随时可以从 Amazon S3 存储桶中删除对象版本。您还可为具有明确定义的生命周期的对象定义生命周期配置规则，请求 Amazon S3 使当前对象版本过期，或者永久删除非当前对象版本。当存储桶已启用版本控制或者版本控制已暂停时，生命周期配置操作的工作方式如下：

- `Expiration` 操作适用于当前对象版本。Amazon S3 通过添加删除标记将当前版本作为非当前版本保留（而不是删除当前对象版本），然后删除标记将成为当前版本。
- `NoncurrentVersionExpiration` 操作适用于非当前对象版本，Amazon S3 会永久删除这些对象版本。无法恢复永久删除的对象。

有关 S3 生命周期的更多信息，请参阅管理对象的生命周期和S3 生命周期配置的示例。

要查看您的存储桶有多少个当前和非当前对象版本，您可以使用 Amazon S3 Storage Lens 存储统计管理工具指标。S3 Storage Lens 存储统计管理工具是一项云存储分析功能，您可以使用它在整个组织范

围内了解对象存储的使用情况和活动。有关更多信息，请参阅使用 S3 Storage Lens 存储统计管理工具优化存储成本。有关指标的完整列表，请参阅 S3 Storage Lens 存储统计管理工具指标词汇表。

> **Note**
>
> 正常的 Amazon S3 费率适用于存储和传输的每个对象版本，包括非当前对象版本。有关更多信息，请参阅 Amazon S3 定价。

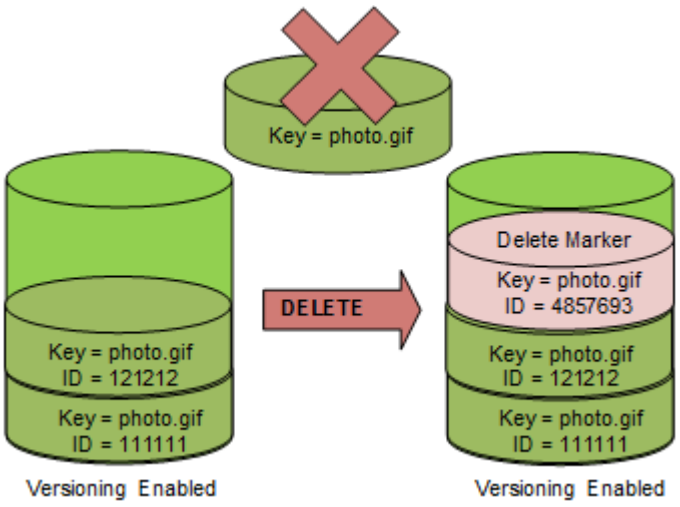
删除请求使用案例

DELETE 请求具有以下使用案例：

- 启用版本控制后，简单 DELETE 无法永久删除对象。（简单 DELETE 请求是指未指定版本 ID 的请求。）Amazon S3 将在存储桶中插入删除标记，该删除标记将成为对象的当前版本并具有新的 ID。

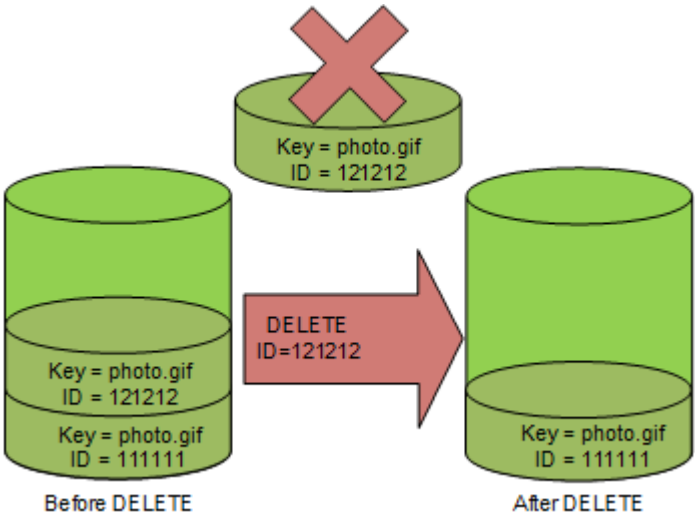
  当您尝试对当前版本为删除标记的对象执行 GET 操作时，Amazon S3 将该对象作为已删除对象对待（即使它尚未被擦除），并返回 404 错误。有关更多信息，请参阅 使用删除标记。

  下图显示简单 DELETE 实际上不会删除指定的对象。但是，Amazon S3 将插入一个删除标记。




- 要永久删除受版本控制的对象，您必须使用 DELETE Object versionId。

  下图显示删除指定的对象版本将永久删除该对象。




要删除对象版本

您可以使用控制台、Amazon SDK 或 REST API 或 Amazon Command Line Interface 删除 Amazon S3 中的对象版本。

使用 S3 控制台

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在存储桶列表中，请选择包含对象的存储桶的名称。
3. 在 Objects（对象）列表中，请选择对象的名称。
4. 请选择 Versions（版本）。

   Amazon S3 显示了对象的所有版本。
5. 选中要检索的版本的版本 ID 旁的复选框。
6. 请选择 Delete（删除）。
7. 在 Permanently delete objects?（永久删除对象？）中，输入 **`permanently delete`**。

   > **Warning**
   >
   > 永久删除对象版本时，该操作将无法撤消。

8. 请选择 Delete objects（删除对象）。

   Amazon S3 将删除对象版本。

使用 Amazon SDK

有关使用适用于 Java、.NET 和 PHP 的 Amazon SDK 删除对象的示例，请参阅 删除 Amazon S3 对象。在不受版本控制和启用了版本控制的存储桶中删除对象的示例是相同的。但是，对于启用了版本控制的存储桶，Amazon S3 会分配版本号。否则，版本号为空。

有关使用其他 Amazon SDK 的信息，请参阅 Amazon 开发人员中心。

Python

以下 Python 代码示例通过删除版本控制对象的所有版本永久删除了该对象。

```
def permanently_delete_object(bucket, object_key):
    """
    Permanently deletes a versioned object by deleting all of its versions.

    Usage is shown in the usage_demo_single_object function at the end of this
 module.

    :param bucket: The bucket that contains the object.
    :param object_key: The object to delete.
    """
    try:
        bucket.object_versions.filter(Prefix=object_key).delete()
        logger.info("Permanently deleted all versions of object %s.", object_key)
    except ClientError:
        logger.exception("Couldn't delete all versions of %s.", object_key)
        raise
```

使用 REST API

删除对象的特定版本

- 在 DELETE 中，指定版本 ID。

Example — 删除特定版本

以下示例删除了 photo.gif 的版本 UIORUnfnd89493jJFJ。

```
DELETE /photo.gif?versionId=UIORUnfnd89493jJFJ HTTP/1.1
```

```
Host: bucket.s3.amazonaws.com
Date: Wed, 12 Oct 2009 17:50:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:xQE0diMbLRepdf3YB+FIEXAMPLE=
Content-Type: text/plain
Content-Length: 0
```

使用 Amazon CLI

以下命令从名为 *amzn-s3-demo-bucket1* 的存储桶中删除名为 test.txt 的对象。要删除特定版本的对象，您必须是存储桶拥有者，并且您必须使用版本 Id 子资源。

```
aws s3api delete-object --bucket amzn-s3-demo-bucket1 --key test.txt --version-
id versionID
```

有关 `delete-object` 的更多信息，请参阅《Amazon CLI 命令参考》中的 delete-object。

有关删除对象版本的更多信息，请参阅以下主题：

- 使用删除标记
- 删除删除标记以使旧版本变为当前版本
- 从启用了 MFA 删除的存储桶中删除对象

使用删除标记

Amazon S3 中的删除标记是用于在简单 DELETE 请求中指定的、启用了版本控制的对象的占位符（或标记）。简单 DELETE 请求是指未指定版本 ID 的请求。因为对象位于已启用版本控制的存储桶中，所以不能删除该对象。但是，删除标记可以使 Amazon S3 的行为类似于对象已被删除。在删除标记上可以使用 Amazon S3 API DELETE 调用。为此，您必须使用具有适当权限的 Amazon Identity and Access Management (IAM) 用户或角色来发出 DELETE 请求。

与任何其他对象一样，删除标记同样有键名（或键）和版本 ID。但是，删除标记在以下方面与其他对象不同：

- 删除标记没有与之关联的数据。
- 删除标记不与访问控制列表 (ACL) 值关联。
- 如果您针对删除标记发出 GET 请求，则 GET 请求不会检索任何内容，因为删除标记没有数据。具体而言，如果您的 GET 请求未指定 `versionId`，则会收到 404（未找到）错误。

删除标记会对 Amazon S3 中的存储产生极少的费用。删除标记的存储大小等于删除标记键名的大小。键名是 Unicode 字符序列。对于名称中的每个字符，键名的 UTF-8 编码将 1 到 4 字节的存储添加到存储桶中。删除标记存储在 S3 Standard 存储类中。

如果您想知道自己有多少个删除标记以及它们存储在哪个存储类中，可以使用 Amazon S3 Storage Lens 存储统计管理工具。有关更多信息，请参阅使用 Amazon S3 Storage Lens 存储统计管理工具评估您的存储活动和使用情况和Amazon S3 Storage Lens 存储统计管理工具指标词汇表。

有关键名称的更多信息，请参阅 为 Amazon S3 对象命名。有关将删除标记删除的信息，请参阅 管理删除标记。

仅 Amazon S3 可以创建删除标记，且当您在已启用版本控制或已暂停版本控制的存储桶的对象上发送 `DeleteObject` 请求时执行此操作。在 `DELETE` 请求中指定的对象不会实际删除。而是使删除标记成为对象的当前版本。该对象的键名（键）将成为删除标记的键。

如果您获取对象而未在请求中指定 `versionId`，如果其当前版本是一个删除标记，则 Amazon S3 的响应如下：

- 404（未找到）错误
- 响应标头，`x-amz-delete-marker: true`

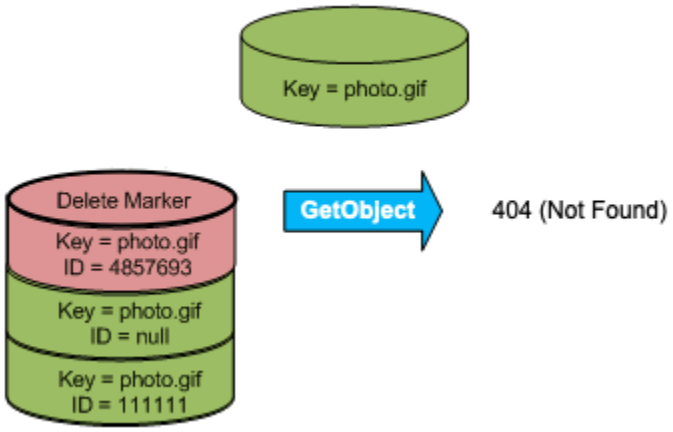
当您通过在请求中指定 `versionId` 来获取对象时，如果其当前版本是一个删除标记，则 Amazon S3 的响应如下：

- 405（不允许此方法）错误
- 响应标头，`x-amz-delete-marker: true`
- 响应标头，`Last-Modified: timestamp`（仅在使用 HeadObject 或 GetObject API 操作时）

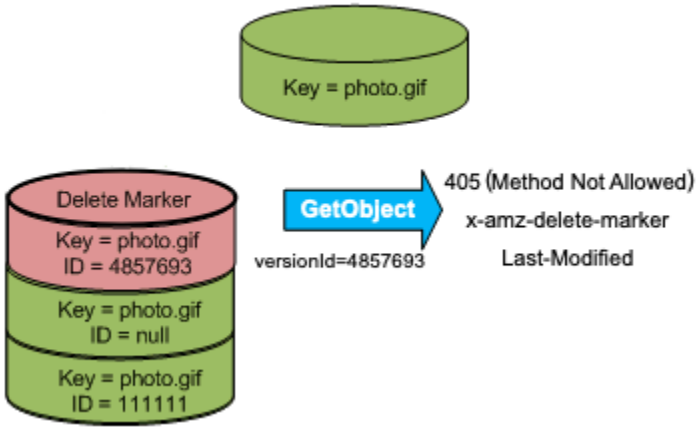
`x-amz-delete-marker: true` 响应标头告知您所访问的对象是删除标记。此响应标头永远不会返回 `false`，因为当值为时 `false`，对象的当前版本或指定版本不是删除标记。

`Last-Modified` 响应标头提供删除标记的创建时间。

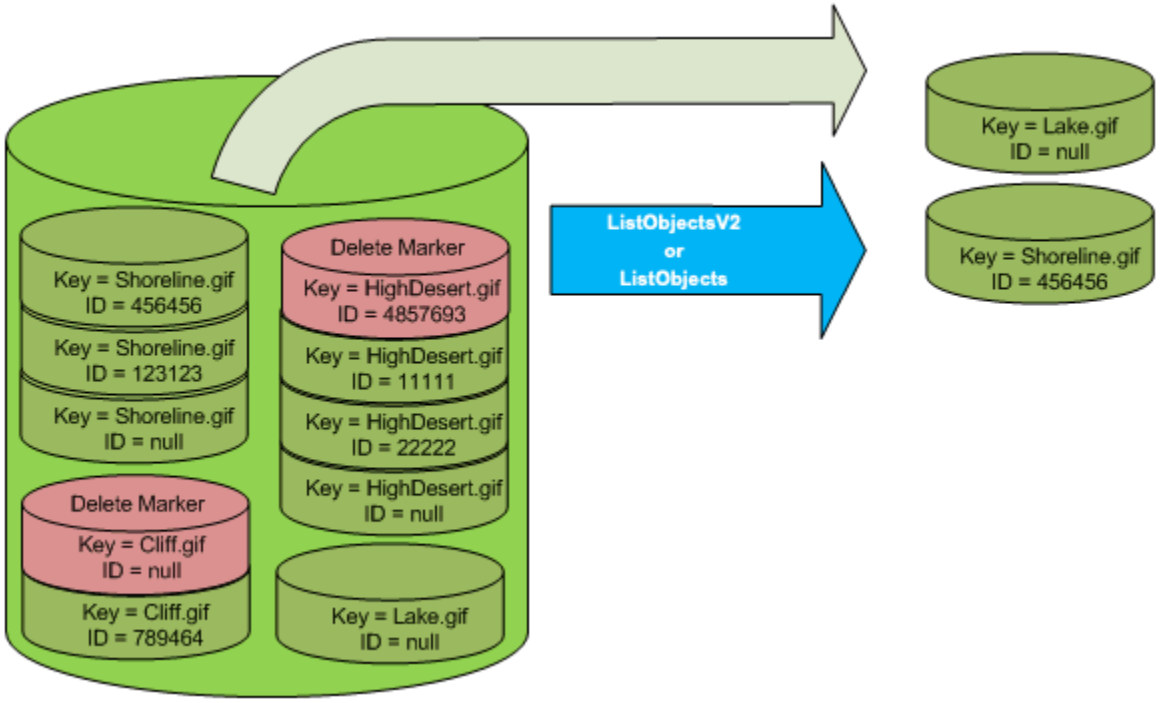
下图显示了对当前版本为删除标记的对象进行 `GetObject` API 调用时，该调用如何使用 404（未找到）错误进行响应且响应标头中包括 `x-amz-delete-marker: true`。




如果您通过在请求中指定 `versionId` 来对对象进行 `GetObject` 调用，并且指定的版本是删除标记，则 Amazon S3 会以 405（不允许方法）错误进行响应，且响应标头包括 `x-amz-delete-marker: true` 和 `Last-Modified: timestamp`。




列出删除标记（和对象的其他版本）的唯一方法在 `versions` 请求中使用 ListObjectVersions 子资源。下图显示 ListObjectsV2 或 ListObjects 请求不会返回其当前版本为删除标记的对象。




管理删除标记

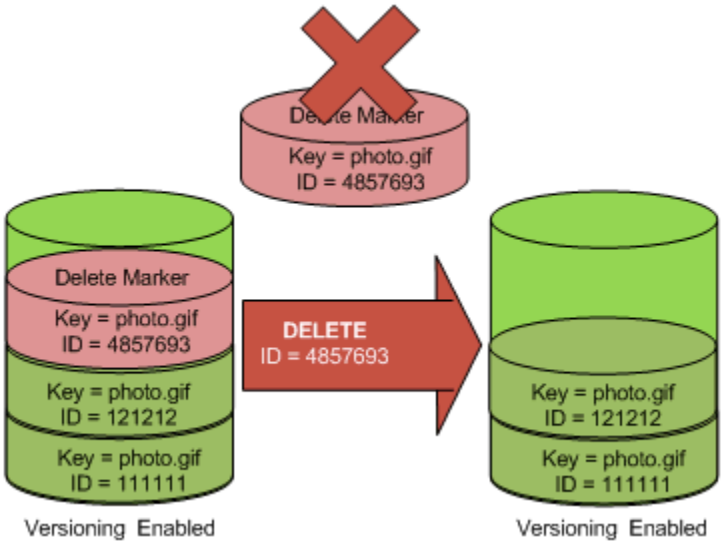
配置生命周期以自动清理过期的删除标记

过期的对象删除标记是指，删除所有对象版本而只保留一个删除标记。如果生命周期配置设置为删除当前版本，或显式设置了 `ExpiredObjectDeleteMarker` 操作，则 Amazon S3 会删除过期对象的删除标记。有关示例，请参阅在启用了版本控制的存储桶中移除到期对象删除标记。

删除删除标记以使旧版本变为当前版本

当您删除启用了版本控制的存储桶中的某个对象时，所有版本都将保留在存储桶中并且 Amazon S3 将为该对象创建一个删除标记。要取消删除该对象，您必须删除此删除标记。有关版本控制和删除标记的更多信息，请参阅使用 S3 版本控制保留对象的多个版本。

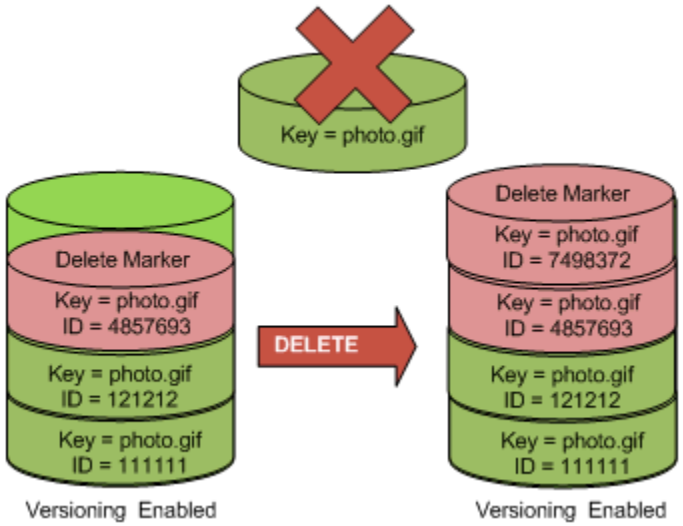
要永久删除“删除标记”，必须在 `DeleteObject versionId` 请求中包含其版本 ID。下图显示了 `DeleteObject versionId` 请求如何永久删除“删除标记”。




去除删除标记的效果是：简单的 GET 请求现在将检索对象的当前版本 ID（121212）。

> **Note**
>
> 如果在当前版本是一个删除标记（未指定删除标记的版本 ID）的情况下使用 DeleteObject 请求，Amazon S3 将不会删除该删除标记，而是对另一个删除标记执行 PUTs 请求。

要删除具有 NULL 版本 ID 的删除标记，必须在 DeleteObject 请求中将 NULL 作为版本 ID 传递。下图显示了在没有版本 ID（当前版本是一个删除标记）的情况下如何发出简单的 DeleteObject 请求，未删除任何内容，而是再添加一个具有唯一版本 ID (7498372) 的删除标记。



使用 S3 控制台

按照以下步骤，从 S3 存储桶中恢复文件夹之外的已删除对象，包括这些文件夹中的对象。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在存储桶列表中，请选择您想要的存储桶的名称。
3. 要查看存储桶中对象的版本列表，请选择列出版本开关。您将能够看到已删除对象的删除标记。
4. 要取消删除对象，您必须删除掉删除标记。选中要恢复的对象的删除标记旁边的复选框，然后选择 Delete (删除)。
5. 在 Delete objects (删除对象) 页面上确认删除。
   a. 对于 Permanently delete objects? ( 永久删除对象？ ) ，输入 **`permanently delete`**。
   b. 请选择 Delete objects ( 删除对象 ) 。

> **Note**
>
> 您无法使用 Amazon S3 控制台取消删除文件夹。您必须使用 Amazon CLI 或 SDK。例如，请参阅 Amazon 知识中心中的如何检索启用版本控制的存储桶中已被删除的 Amazon S3 对象？。

使用 REST API

永久删除“删除标记”的步骤

1. 将 `versionId` 设置为要删除的删除标记的版本 ID。
2. 发送 `DELETE Object versionId` 请求。

Example — 删除“删除标记”

以下示例删除用于 `photo.gif` 版本 4857693 的删除标记。

```
DELETE /photo.gif?versionId=4857693 HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
```

```
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

删除“删除标记”时，Amazon S3 将在响应中包含以下内容：

```
204 NoContent
x-amz-version-id: versionID
x-amz-delete-marker: true
```

使用 Amazon SDK

有关使用其他 Amazon SDK 的信息，请参阅 Amazon 开发人员中心。

Python

以下 Python 代码示例演示了如何从对象中删除“删除标记”，从而使最新的非当前版本成为对象的当前版本。

```
def revive_object(bucket, object_key):
    """
    Revives a versioned object that was deleted by removing the object's active
    delete marker.
    A versioned object presents as deleted when its latest version is a delete
 marker.
    By removing the delete marker, we make the previous version the latest version
    and the object then presents as *not* deleted.

    Usage is shown in the usage_demo_single_object function at the end of this
 module.

    :param bucket: The bucket that contains the object.
    :param object_key: The object to revive.
    """
    # Get the latest version for the object.
    response = s3.meta.client.list_object_versions(
        Bucket=bucket.name, Prefix=object_key, MaxKeys=1
    )

    if "DeleteMarkers" in response:
        latest_version = response["DeleteMarkers"][0]
        if latest_version["IsLatest"]:
            logger.info(
                "Object %s was indeed deleted on %s. Let's revive it.",
                object_key,
```

```
                latest_version["LastModified"],
            )
            obj = bucket.Object(object_key)
            obj.Version(latest_version["VersionId"]).delete()
            logger.info(
                "Revived %s, active version is now %s  with body '%s'",
                object_key,
                obj.version_id,
                obj.get()["Body"].read(),
            )
        else:
            logger.warning(
                "Delete marker is not the latest version for %s!", object_key
            )
    elif "Versions" in response:
        logger.warning("Got an active version for %s, nothing to do.", object_key)
    else:
        logger.error("Couldn't get any version info for %s.", object_key)
```

从启用了 MFA 删除的存储桶中删除对象

如果存储桶的版本控制配置已启用 MFA 删除，则存储桶拥有者必须在请求中包含 `x-amz-mfa` 请求标头，才能永久删除对象版本或更改该存储存储桶的版本控制状态。包含 `x-amz-mfa` 的请求必须使用 HTTPS。

标头的值由身份验证设备的序列号、空格，以及在该设备上显示的身份验证代码组成。如果您没有包含此请求标头，则请求失败。

有关身份验证设备的更多信息，请参阅多重身份验证。

Example — 从启用了 MFA 删除的存储桶中删除对象

以下示例删除了在存储桶中配置为启用 MFA 删除的 `my-image.jpg`（具有指定版本）。

请注意 *`[SerialNumber]`* 和 *`[AuthenticationCode]`* 之间的空格。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 DeleteObject。

```
DELETE /my-image.jpg?versionId=3HL4kqCxf3vjVBH40Nrjfkd HTTPS/1.1
Host: bucketName.s3.amazonaws.com
x-amz-mfa: 20899872 301749
```

```
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

有关启用 MFA 删除的更多信息，请参阅 配置 MFA 删除。

## 配置受版本控制的对象权限

Amazon S3 中的对象的权限在版本级别设置。每个版本都有自己的对象拥有者。创建对象版本的 Amazon Web Services 账户 是拥有者。因此，您可以为同一对象的不同版本设置不同的权限。要这样做，您必须指定要在 PUT Object versionId acl 请求中设置其权限的对象的版本 ID。有关详细描述和关于使用 ACL 的说明，请参阅 Amazon S3 的身份和访问管理。

Example — 为对象版本设置权限

以下请求将被授权者（BucketOwner@amazon.com）对键（my-image.jpg）和版本 ID（3HL4kqtJvjVBH40Nrjfkd）的权限设置为 FULL_CONTROL。

```
PUT /my-image.jpg?acl&versionId=3HL4kqtJvjVBH40Nrjfkd HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
Content-Length: 124

<AccessControlPolicy>
  <Owner>
    <ID>75cc57f09aa0c8caeab4f8c24e99d10f8e7faeebf76c078efc7c6caea54ba06a</ID>
    <DisplayName>mtd@amazon.com</DisplayName>
  </Owner>
  <AccessControlList>
    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:type="CanonicalUser">
        <ID>a9a7b886d6fd24a52fe8ca5bef65f89a64e0193f23000e241bf9b1c61be666e9</ID>
        <DisplayName>BucketOwner@amazon.com</DisplayName>
      </Grantee>
      <Permission>FULL_CONTROL</Permission>
    </Grant>
  </AccessControlList>
  </AccessControlPolicy>
```

同样地，要获取特定对象版本的权限，必须在 GET Object versionId acl 请求中指定它的版本 ID。您需要包含版本 ID，因为在默认情况下，GET Object acl 将返回对象的当前版本的权限。

Example — 检索用于指定对象版本的权限

在以下示例中，Amazon S3 将返回对于键（my-image.jpg）和版本 ID（DVBH40Nr8X8gUMLUo）的权限。

```
GET /my-image.jpg?versionId=DVBH40Nr8X8gUMLUo&acl HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU
```

有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 GetObjectAcl。

## 使用已暂停版本控制的存储桶中的对象

在 Amazon S3 中，您可以暂停版本控制，以停止在存储桶中累积同一对象的新版本。您可能这样做是因为您只想在存储桶中使用单个版本的对象。或者，您可能不想为多个版本累积费用。

暂停版本控制时，存储桶中的现有对象不会更改。更改的是 Amazon S3 在以后的请求中处理对象的方式。本部分中的主题介绍了暂停版本控制的存储桶中的各种对象操作，包括添加、检索和删除对象。

有关 S3 版本控制的更多信息，请参阅使用 S3 版本控制保留对象的多个版本。有关检索对象版本的更多信息，请参阅 从启用了版本控制的存储桶中检索对象版本。

主题

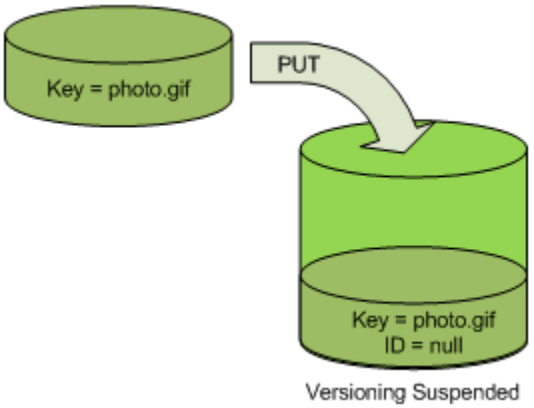
- 将对象添加到已暂停版本控制的存储桶
- 从已暂停版本控制的存储桶检索对象
- 从已暂停版本控制的存储桶中删除对象

### 将对象添加到已暂停版本控制的存储桶

您可以将对象添加到 Amazon S3 中已暂停版本控制的存储桶中，以便创建具有空版本 ID 的对象，或者覆盖具有匹配版本 ID 的任何对象版本。

您在存储桶上暂停了版本控制后，Amazon S3 会自动将 null 版本 ID 添加到之后存储在该存储段中的每个后续对象（使用 PUT、POST 或 CopyObject）。

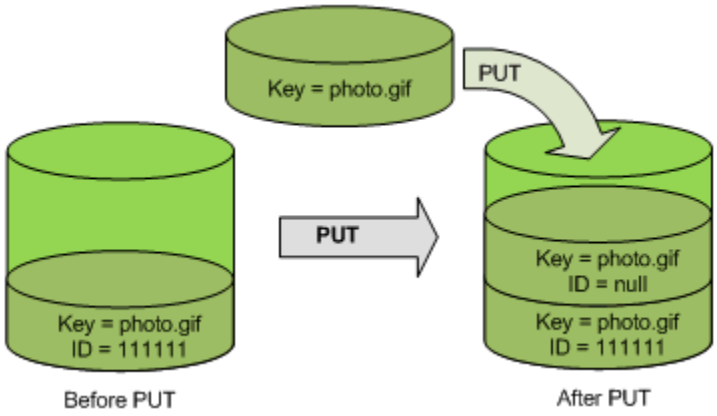
下图显示了当将对象添加到暂停版本控制的存储桶时，Amazon S3 将如何向该对象添加 null 的版本 ID。



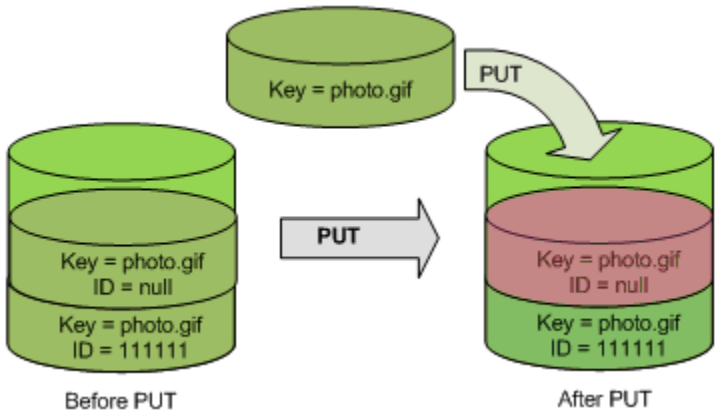

如果存储桶中已存在空版本，且您使用同一键添加了其他对象，则添加的对象将覆盖原始的空版本。

如果存储桶中存在受版本控制的对象，则使用 PUT 存储的版本将成为该对象的当前版本。下图显示了如何将对象添加到包含受版本控制的对象（不会覆盖已存在于该存储桶中的对象）的存储桶。

在这种情况下，版本 111111 已存在于该存储桶中。Amazon S3 会将空的版本 ID 附加到所添加的对象，并将其存储在存储桶中。版本 111111 不会被覆盖。



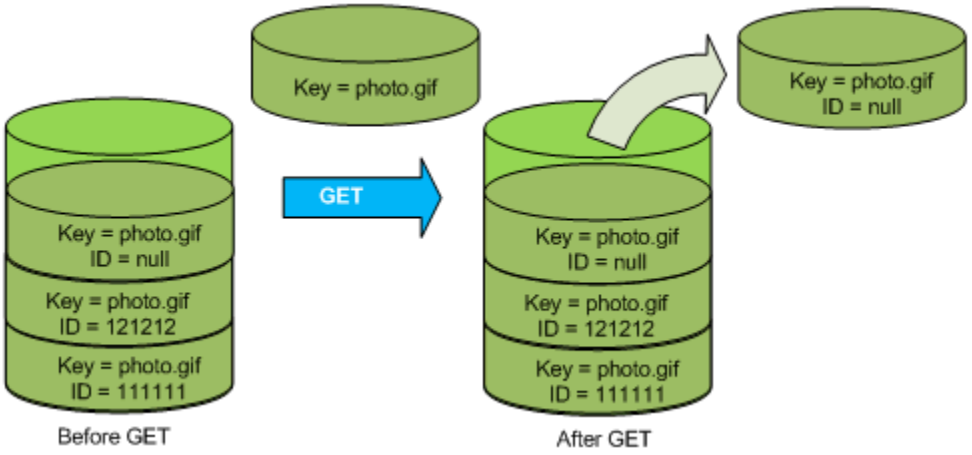

如果存储桶中已存在空版本，则该空版本将被覆盖，如下图所示。



虽然空版本的键和版本 ID（null）在 PUT 之前和之后都相同，但是原来存储在存储桶中的空版本的内容将替换为该存储桶中对象 PUT 的内容。

## 从已暂停版本控制的存储桶检索对象

无论是否在存储桶上启用版本控制，GET Object 请求都将返回对象的当前版本。下图显示了简单 GET 将如何返回对象的当前版本。



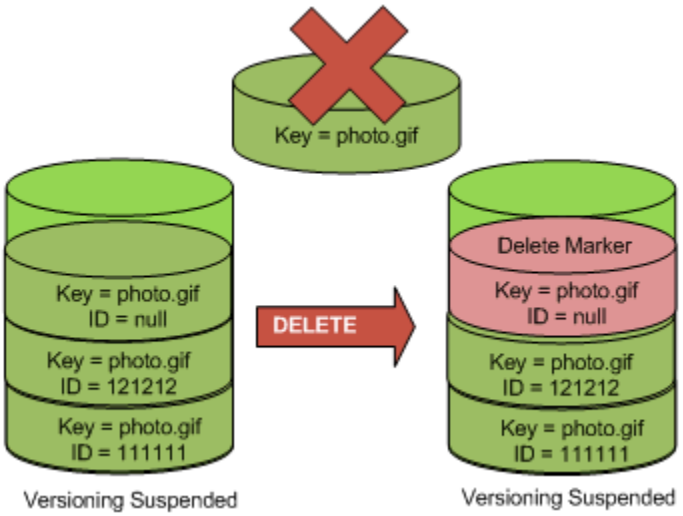

## 从已暂停版本控制的存储桶中删除对象

您可以将对象从暂停版本控制的存储桶中删除，以便删除具有空版本 ID 的对象。

如果某个存储桶的版本控制已暂停，DELETE 请求：

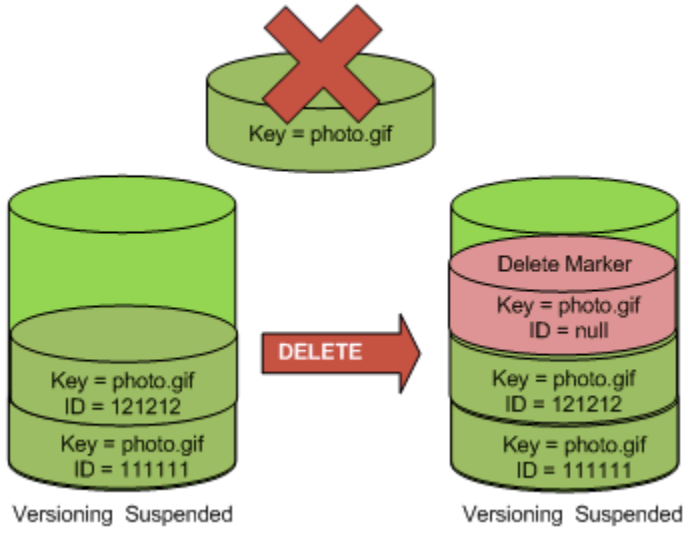
- 可以仅删除其版本 ID 为 null 的对象。
- 如果存储桶中没有对象的空版本，则不删除任何内容。
- 将删除标记插入到存储桶。

如果暂停存储桶版本控制，该操作会移除具有空 versionId 的对象。如果版本 ID 存在，Amazon S3 会插入删除标记，该删除标记将成为对象的当前版本。下图显示了简单的 DELETE 移除空版本和 Amazon S3 改而使用 null 版本 ID 在其位置中插入删除标记的方式。

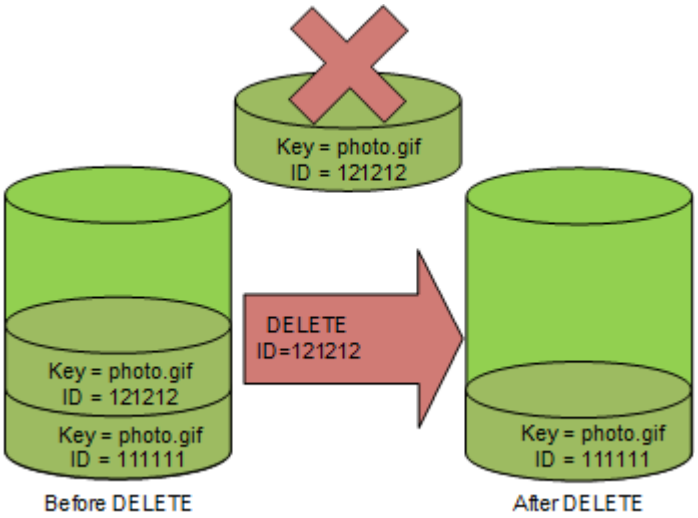



要永久删除具有 `versionId` 的对象，必须在请求中包含对象的 `versionId`。由于删除标记不包含任何内容，因此，您将在删除标记替换 `null` 版本时丢失该版本的内容。

下图显示不具有空版本的存储桶。在这种情况下，DELETE 不会移除任何内容。而是 Amazon S3 仅仅插入一个删除标记。




即使是在已暂停版本控制的存储桶中，存储桶拥有者也可以通过在 DELETE 请求中包括版本 ID 来永久删除指定版本。下图显示删除指定的对象版本将永久删除该版本的对象。只有存储桶拥有者可以删除指定的对象版本。




# 版本控制故障排除

以下主题可以帮助您排查一些常见的 Amazon S3 版本控制问题。

主题

- 我想恢复在启用版本控制的存储桶中意外删除的对象
- 我想永久删除受版本控制的对象
- 启用存储桶版本控制后，我遇到了性能下降问题

## 我想恢复在启用版本控制的存储桶中意外删除的对象

通常，当从 S3 存储桶中删除对象版本时，Amazon S3 无法恢复它们。但是，如果您在 S3 存储桶上启用了 S3 版本控制，则未指定版本 ID 的 DELETE 请求无法永久删除对象。而是添加删除标记作为占位符。此删除标记将成为对象的当前版本。

要验证已删除的对象是永久删除还是临时删除（在其所在位置有删除标记），请执行以下操作：

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 在存储桶列表中，请选择包含对象的存储桶的名称。
4. 在对象列表中，开启搜索栏右侧的显示版本开关，然后在搜索栏中搜索已删除的对象。仅当之前在存储桶上启用了版本控制时，此开关才可用。

   您也可以使用 S3 清单来搜索已删除的对象。

5. 如果在切换显示版本或创建清单报告后找不到对象，也找不到该对象的删除标记，则删除是永久性的，无法恢复该对象。

您还可以使用 Amazon Command Line Interface（Amazon CLI）中的 HeadObject API 操作来验证已删除对象的状态。要执行此操作，请使用以下 head-object 命令并将 *user input placeholders* 替换为您自己的信息：

```
aws s3api head-object --bucket amzn-s3-demo-bucket --key index.html
```

如果您对受版本控制的对象运行 head-object 命令，而此对象的当前版本为删除标记，则会收到 404 找不到错误。例如：

调用 HeadObject 操作时发生错误（404）：找不到

如果您对受版本控制的对象运行 head-object 命令并提供该对象的版本 ID，Amazon S3 将检索该对象的元数据，确认该对象仍然存在而未被永久删除。

```
aws s3api head-object --bucket amzn-s3-demo-bucket --key index.html --
version-id versionID
```

```
{
"AcceptRanges": "bytes",
"ContentType": "text/html",
"LastModified": "Thu, 16 Apr 2015 18:19:14 GMT",
"ContentLength": 77,
"VersionId": "Zg5HyL7m.eZU9iM7AVlJkrqAiE.0UG4q",
"ETag": "\"30a6ec7e1a9ad79c203d05a589c8b400\"",
"Metadata": {}
}
```

如果找到该对象并且最新版本是删除标记，则该对象的先前版本仍然存在。由于删除标记是对象的当前版本，因此您可以通过删除该删除标记来恢复对象。

永久移除删除标记后，该对象的第二个最新版本将成为该对象的当前版本，从而使您的对象再次可用。有关如何恢复对象的直观描述，请参阅移除删除标记。

要删除对象的特定版本，您必须是存储桶拥有者。要永久删除“删除标记”，必须在 DeleteObject 请求中包含其版本 ID。要删除该删除标记，请使用以下命令，然后将 *user input placeholders* 替换为您自己的信息：

```
aws s3api delete-object --bucket amzn-s3-demo-bucket --key index.html --
version-id versionID
```

有关 delete-object 命令的更多信息，请参阅《Amazon CLI 命令参考》中的 delete-object。有关永久删除相应删除标记的更多信息，请参阅管理删除标记。

### 我想永久删除受版本控制的对象

在已启用版本控制的存储桶中，没有版本 ID 的 DELETE 请求无法永久删除对象。相反，此类请求会插入一个删除标记。

要永久删除受版本控制的对象，可从以下方法中进行选择：

- 创建 S3 生命周期规则以永久删除非当前版本。要永久删除非当前版本，请选择永久删除对象的非当前版本，然后在对象变为非当前对象后的天数下输入一个数字。您可以选择在 Number of newer versions to retain（要保留的较新版本的数量）下输入一个值，从而指定要保留的较新版本数量。有关创建此规则的更多信息，请参阅设置 S3 生命周期配置。
- 通过在 DELETE 请求中包含版本 ID 来删除指定的版本。有关更多信息，请参阅如何永久删除受版本控制的对象。
- 创建生命周期规则以使当前版本过期。要使对象的当前版本过期，请选择将对象的当前版本设为过期，然后在创建对象后的天数下输入一个数字。有关创建此生命周期规则的更多信息，请参阅设置 S3 生命周期配置。
- 要永久删除所有受版本控制的对象以及删除标记，请创建两个生命周期规则：一个用于使当前版本过期并永久删除对象的非当前版本，另一个用于删除过期的对象删除标记。

在启用版本控制的存储桶中，未指定版本 ID 的 DELETE 请求只能删除具有 NULL 版本 ID 的对象。如果对象是在启用版本控制后上传的，则未指定版本 ID 的 DELETE 请求会创建该对象的删除标记。

> **Note**
>
> 对于启用了 S3 对象锁定的存储桶，具有受保护对象版本 ID 的 DELETE 对象请求会导致 403 拒绝访问错误。没有版本 ID 的 DELETE 对象请求会添加删除标记作为该对象的最新版本，响应为 200 OK。受对象锁定保护的对象只有在解除其保留期和法定保留之后才可永久删除。有关更多信息，请参阅 the section called “S3 对象锁定的工作原理”。

## 启用存储桶版本控制后，我遇到了性能下降问题

如果删除标记或受版本控制的对象过多，以及如果未遵循最佳实践，则启用版本控制的存储桶可能会出现性能降低问题。

删除标记过多

对存储桶启用版本控制后，针对对象发出的没有版本 ID 的 DELETE 请求将创建具有唯一版本 ID 的删除标记。具有将对象的当前版本设为过期规则的生命周期配置会向每个对象添加一个带有唯一版本 ID 的删除标记。过多的删除标记会降低存储桶的性能。

在对存储桶暂停版本控制时，Amazon S3 会对于新创建的对象将版本 ID 标记为 NULL。版本控制已暂停的存储桶中的过期操作会导致 Amazon S3 创建一个以 NULL 作为版本 ID 的删除标记。在版本控制已暂停的存储桶中，将为任何删除请求创建 NULL 删除标记。当删除所有对象版本而只保留单个删除标记时，这些 NULL 删除标记也称为过期对象删除标记。如果累积的 NULL 删除标记过多，则存储桶的性能会降低。

受版本控制的对象过多

如果启用了版本控制的存储桶包含具有数百万个版本的对象，则可能会出现 503 服务不可用错误。如果您注意到针对启用版本控制的存储存储桶的 PUT 或 DELETE 对象请求接收的 HTTP 503 服务不可用响应的数量显著增加，则存储桶中可能有一个或多个对象具有数百万个版本。如果您的对象有数以百万计的版本，Amazon S3 会自动限制对该存储桶的请求。限制请求数可以保护您的存储桶免受过多请求流量的影响，但也可能会妨碍对该存储桶发出的其他请求。

要确定哪些对象具有数以百万计的版本，请使用 S3 清单。S3 清单生成一份报告，用于提供存储桶中对象的平面文件列表。有关更多信息，请参阅 使用 S3 清单对数据进行编目和分析。

要验证存储桶中是否存在大量受版本控制的对象，请使用 S3 Storage Lens 存储统计管理工具指标来查看当前版本对象计数、非当前版本对象计数和删除标记对象计数。有关 Storage Lens 存储统计管理工具指标的更多信息，请参阅Amazon S3 Storage Lens 存储统计管理工具指标词汇表。

Amazon S3 团队鼓励客户调查重复覆盖同一对象的应用程序（可能会为该对象创建数百万个版本），以确定应用程序是否正常工作。例如，如果某个应用程序每分钟都要覆盖同一个对象，那么在一周时间内创建的版本数量会超过一万个。我们建议，为每个对象存储的版本数不超过十万个。如果您的应用场景需要一个或多个对象的数百万个版本，请联系 Amazon Web Services 支持 团队以获得帮助，从而确定更好的解决方案。

最佳实践

为防止与版本控制相关的性能降级问题，建议您采用以下最佳实践：

- 启用生命周期规则以使对象的先前版本过期。例如，您可以创建生命周期规则，以使非当前版本在对象变为非当前状态的 30 天后过期。如果您不想全部删除非当前版本，也可以保留多个非当前版本。有关更多信息，请参阅设置 S3 生命周期配置。
- 启用生命周期规则，以删除存储桶中没有关联数据对象的过期对象删除标记。有关更多信息，请参阅删除过期对象删除标记。

有关其他 Amazon S3 性能优化最佳实践，请参阅最佳实践设计模式。

# 使用对象锁定以锁定对象

S3 对象锁定可以协助在固定的时间长度内或无限期地阻止删除或覆盖 Amazon S3 对象。对象锁定使用一次写入多次读取（WORM）模式存储对象。您可以使用对象锁定来协助满足需要 WORM 存储的法规要求，或用于添加额外的保护层来防止对象被更改和删除。

> **Note**
>
> S3 对象锁定已由 Cohasset Associates 评估，可在受 SEC 17a-4、CFTC 和 FINRA 法规约束的环境中使用。有关对象锁定与这些法规关系的更多信息，请参阅 Cohasset Associates 合规性评估。

对象锁定提供了以下两种方式来管理对象保留：保留期限和依法保留。对象版本可以同时具有保留期限和/或依法保留。

- 保留期：保留期指定对象版本可以保持锁定状态的固定时间长度。您可以为各个对象设置唯一的保留期。此外，您可以在 S3 存储桶上设置默认保留期。您还可以在桶策略中使用 `s3:object-lock-remaining-retention-days` 条件键限制允许的最小和最大保留期。这有助于您确定保留期的范围，并限制可能短于或长于该范围的保留期。
- 依法保留 – 依法保留提供的保护与保留期限相同，但没有到期日期。依法保留将一直有效，直至您明确将其删除。法定保留与保留期无关，且应该对单独的对象目标应用。

对象锁定仅在启用 S3 版本控制的存储桶中生效。当您锁定某一对象版本时，Amazon S3 会将锁定信息存储在该对象版本的元数据中。在对象上实施保留期限或依法保留仅保护在请求中指定的版本。保留期和法定保留不会阻止创建对象的新版本，也不会阻止在对象顶部添加删除标记。有关 S3 版本控制的信息，请参阅使用 S3 版本控制保留对象的多个版本。

如果您将一个对象放入存储桶中，而存储桶中包含的现有受保护对象与其具有相同的对象键名，Amazon S3 将创建对象的新版本。现有受保护版本的对象将根据其保留配置保持锁定状态。

# S3 对象锁定的工作原理

主题


- 保留期限
- 保留模式
- 法定保留
- 使用 S3 对象锁定的最佳实践
- 所需的权限


## 保留期限

保留期限可在固定时间内保护对象版本。当您对对象版本施加保留期限时，Amazon S3 会在该对象版本的元数据中存储时间戳，以指示保留期限的到期时间。在保留期限到期后，便可覆盖或删除对象版本。

您可以对单独对象版本或在存储桶属性上明确设置保留期限，以便它自动应用于存储桶中的所有对象。将保留期显式应用于对象版本时，即为对象版本指定保留到期日期。Amazon S3 将此日期存储在对象版本的元数据中。

您还可以在存储桶的属性中设置保留期限。在存储存储桶上设置保留期限时，您可以指定放入存储桶中的每个对象版本受保护的持续时间，以天或年为单位。当您将对象放入存储桶时，Amazon S3 将该对象版本的创建时间戳加上指定的持续时间，以此来计算保留到期日。然后，在您对该对象版本明确应用的单独锁定保留期限内，对象版本将受到保护。

> **Note**
>
> 当您在存储桶中 PUT 具有明确的单独保留模式和期限的对象版本时，该对象版本的单独对象锁定设置会覆盖所有存储桶属性保留设置。

与所有其他对象锁定设置一样，保留期限适用于各个对象版本。单个对象的不同版本可以具有不同的保留模式和周期。

例如，如果您将 15 天的对象放入 30 天保留期限，并将一个保留期限为 60 天的同名对象 PUT 到 Amazon S3 中。在这种情况下，您的 PUT 请求将成功，Amazon S3 将创建一个保留期限为 60 天的新对象版本。较旧版本将保持其原来的保留期限，并且可在 15 天内删除。

在某个对象版本上应用了保留设置后，您可以延长保留期限。要执行此操作，您需对该对象版本提交新对象锁定请求，其保留到期日晚于当前为该对象版本配置的保留到期日期。Amazon S3 将用更长的新期限替换现有的保留期限。任何用户只要具有实施对象保留期限的权限，即可对象版本的保留期限。要设置保留期限，您必须具有 `s3:PutObjectRetention` 权限。

在对象或 S3 存储桶上设置保留权期限时，您必须选择两种保留模式之一：合规性或监管。

## 保留模式

S3 对象锁定提供了两种保留模式，可为对象应用不同级别的保护：

- 合规性模式
- 监管模式

在合规性模式中，任何用户都不能覆盖或删除受保护的对象版本，包括 Amazon Web Services 账户中的根用户。在合规性模式下锁定对象后，其保留模式便无法更改，其保留期限也不能缩短。合规性模式可帮助确保在保留期限内无法覆盖或删除对象版本。

> **Note**
>
> 在合规模式下，要想在保留日期到期前删除对象，唯一的方法就是删除相关的 Amazon Web Services 账户。

在监管 模式中，除非用户具有特殊权限，否则用户不能覆盖或删除对象版本，或更改其锁定设置。使用监管模式，您可以保护对象以免被大多数用户删除，但您仍可向部分用户授予权限，以在必要时更改保留设置或删除对象。您还可以在创建合规性模式保留期限之前使用监管模式测试保留期限设置。

要覆盖或删除监管模式保留设置，您必须具有 `s3:BypassGovernanceRetention` 权限，并且在需要覆盖监管模式的任何请求中，必须明确包含 `x-amz-bypass-governance-retention:true` 作为请求标头。

> **Note**
>
> 默认情况下，Amazon S3 控制台包括 `x-amz-bypass-governance-retention:true` 标头。如果您尝试删除受监管模式保护的对象并且拥有 `s3:BypassGovernanceRetention` 权限，则操作将会成功。

## 法定保留

使用对象锁定，您还可以在对象版本上实施依法保留。与保留期限相似，依法保留可防止对象版本被覆盖或删除。但是，依法保留没有关联的固定时间长度，会一直有效，直至删除。拥有 `s3:PutObjectLegalHold` 权限的任何用户均可自由实施和删除依法保留。

依法保留与保留期限无关。对对象版本实施依法保留不会影响该对象版本的保留模式或保留期限。

例如，假设您对某一对象版本实施依法保留，同时该对象版本也受保留期限保护。如果保留期限过期，该对象不会失去其 WORM 保护。那么依法保留将继续保护该对象，直至授权用户明确删除依法保留对象。与之相似，如果您在对象版本的保留期限生效时删除依法保留，该对象版本将一直受保护，直至保留期限过期。

## 使用 S3 对象锁定的最佳实践

如果您想保护对象在预定义的保留期内不被大多数用户删除，但同时又希望一些具有特殊权限的用户能够灵活地更改保留设置或删除对象，请考虑使用监管模式。

如果您从不希望任何用户（包括您的 Amazon Web Services 账户中的根用户）能够在预定义的保留期内删除对象，请考虑使用合规模式。如果您需要存储合规数据，则可以使用此模式。

当您不确定要让对象保持不可变的时长时，可以使用依法保留。这可能是因为您即将对数据进行外部审计，并希望在审计完成之前保持对象不可变。或者，您可能有一个正在进行的项目，而您希望在项目完成之前，让该项目使用的数据集保持不变。

## 所需的权限

对象锁定操作需要特定的权限。根据您正在尝试的确切操作，您可能需要以下任意权限：

- `s3:BypassGovernanceRetention`
- `s3:GetBucketObjectLockConfiguration`
- `s3:GetObjectLegalHold`
- `s3:GetObjectRetention`

- `s3:PutBucketObjectLockConfiguration`
- `s3:PutObjectLegalHold`
- `s3:PutObjectRetention`

有关 Amazon S3 权限的完整列表及其描述，请参阅《Service Authorization Reference》中的 Actions, resources, and condition keys for Amazon S3。

有关按 S3 资源类型对 S3 API 操作的权限的更多信息，请参阅 Amazon S3 API 操作所需的权限。

有关将条件与权限结合使用的信息，请参阅 使用条件键的存储桶策略示例。

## 对象锁定注意事项

Amazon S3 对象锁定可以协助在固定的时间长度内或无限期地阻止删除或覆盖对象。

您可以使用 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 Amazon S3 REST API 来查看或设置对象锁定信息。有关 S3 对象锁定功能的一般信息，请参阅使用对象锁定以锁定对象。

> **Important**
>
> - 在某个存储桶上启用对象锁定后，您将无法为该存储桶禁用对象锁定或暂停版本控制。
> - 具有对象锁定的 S3 存储桶不能用作服务器访问日志的目标存储桶。有关更多信息，请参阅 the section called “记录服务器访问”。

主题


- 查看锁定信息的权限
- 绕过监管模式
- 将对象锁定与 S3 复制结合使用
- 将对象锁定与加密结合使用
- 将对象锁定与 Amazon S3 清单结合使用
- 使用对象锁定管理 S3 生命周期策略
- 使用对象锁定管理删除标记
- 将 S3 Storage Lens 存储分析功能与对象锁定结合
- 将对象上传到启用了对象锁定的桶

- 配置事件和通知
- 使用存储桶策略为保留期限设置限制

## 查看锁定信息的权限

您可以使用 HeadObject 或 GetObject 操作，以编程方式查看 Amazon S3 对象版本的对象锁定状态。这两个操作都会返回指定对象版本的保留模式、保留到期日和依法保留状态。此外，您可以使用 S3 清单来查看 S3 存储桶中多个对象的对象锁定状态。

要查看对象版本的保留模式和保留期限，您必须拥有 `s3:GetObjectRetention` 权限。要查看对象版本的依法保留状态，您必须拥有 `s3:GetObjectLegalHold` 权限。要查看存储桶的默认保留配置，您必须具有 `s3:GetBucketObjectLockConfiguration` 权限。如果您对未启用 S3 对象锁定的存储桶请求对象锁定配置，则 Amazon S3 将返回错误。

## 绕过监管模式

如果您具有 `s3:BypassGovernanceRetention` 权限，则在对象未受保护时，您可对在监管模式下锁定的对象版本执行操作。这些操作包括删除对象版本、缩短保留期限，或者通过实施参数为空的新 `PutObjectRetention` 请求来删除对象锁定保留期限。

要绕过监管模式，您必须在请求中明确指明您要绕过此模式。为此，在 `PutObjectRetention` API 操作请求中包含 `x-amz-bypass-governance-retention:true` 标头，或将等效参数用于通过 Amazon CLI 或 Amazon SDK 发出的请求。如果您具有 `s3:BypassGovernanceRetention` 权限，则 S3 控制台会自动将此标头应用于通过 S3 控制台发出的请求。

> **Note**
>
> 绕过监管模式不会影响对象版本的依法保留状态。如果某个对象版本已启用依法保留，则依法保留将保持有效，并可阻止覆盖或删除该对象版本的请求。

## 将对象锁定与 S3 复制结合使用

您可以将对象锁定与 S3 复制结合使用，以便跨 S3 存储桶，对锁定对象及其保留元数据启用自动异步复制。这意味着，对于复制的对象，Amazon S3 采用源存储桶的对象锁定配置。换句话说，如果源存储桶已启用对象锁定，则目标存储桶也必须启用对象锁定。如果将对象直接上传到目标存储桶（在 S3 复制之外），它将使用目标存储桶上设置的对象锁定。如果您使用复制功能，则源存储桶中的对象会被复制到目标存储桶。

要在启用了对象锁定的存储桶上设置复制功能，您可以使用 S3 控制台、Amazon CLI、Amazon S3 REST API 或 Amazon SDK。

> **Note**
>
> 要将对象锁定与复制功能结合使用，您必须在用于设置复制的 Amazon Identity and Access Management（IAM）角色中，授予对源 S3 存储桶的两项额外的权限。这两项额外的权限是 `s3:GetObjectRetention` 和 `s3:GetObjectLegalHold`。如果角色已有 `s3:Get*` 权限声明，则该声明已满足要求。有关更多信息，请参阅 为实时复制设置权限。
> 有关 S3 复制的一般信息，请参阅在区域内和跨区域复制对象。
> 有关设置 S3 复制的示例，请参阅配置实时复制的示例。

## 将对象锁定与加密结合使用

默认情况下，Amazon S3 会对所有新对象进行加密。您可以对加密的对象使用对象锁定。有关更多信息，请参阅 利用加密来保护数据。

虽然对象锁定有助于防止删除或覆盖 Amazon S3 对象，但并不能防止加密密钥的访问权限丢失，也不能防止加密密钥遭删除。例如，如果您使用 Amazon KMS 服务器端加密为对象加密，而 Amazon KMS 密钥被删除，则对象可能会变得无法读取。

## 将对象锁定与 Amazon S3 清单结合使用

您可以配置 Amazon S3 清单，以便按预定的计划创建 S3 存储桶中对象的列表。对于您的对象，您可以将 Amazon S3 清单配置为包含以下对象锁定元数据：

- 保留截止日
- 保留模式
- 依法保留状态

有关更多信息，请参阅 使用 S3 清单对数据进行编目和分析。

## 使用对象锁定管理 S3 生命周期策略

对象生命周期管理配置将继续正常应用于受保护的对象，包括实施删除标记。但是，S3 生命周期过期策略无法删除对象的锁定版本。无论对象位于哪个存储类，以及在存储类之间的整个 S3 生命周期转换过程中，都将保持对象锁定。

有关管理对象生命周期的更多信息，请参阅管理对象的生命周期。

### 使用对象锁定管理删除标记

尽管您无法删除受保护的对象版本，但您仍可为该对象创建删除标记。对对象实施删除标记不会删除对象或它的对象版本。但会使 Amazon S3 的行为方式在最大程度上与对象被删除时相似。有关更多信息，请参阅 使用删除标记。

> **Note**
>
> 无论基础对象中实施任何保留期限或依法保留，删除标记均不受 WORM 保护。

## 将 S3 Storage Lens 存储分析功能与对象锁定结合

要查看启用对象锁定的存储字节数和对象计数的指标，您可以使用 Amazon S3 Storage Lens 存储统计管理工具。S3 Storage Lens 存储统计管理工具是一项云存储分析功能，您可以使用它在整个组织范围内了解对象存储的使用情况和活动。

有关更多信息，请参阅 使用 S3 Storage Lens 存储统计管理工具保护您的数据。

要获得指标的完整列表，请参阅 Amazon S3 Storage Lens 存储统计管理工具指标词汇表。

### 将对象上传到启用了对象锁定的桶

如果使用对象锁定为某个对象配置了保留期，则任何上传该对象的请求都需要 `Content-MD5` 或 `x-amz-sdk-checksum-algorithm` 标头。这些标头是在上传过程中验证对象完整性的一种方式。

使用 Amazon S3 控制台上传对象时，S3 会自动添加 `Content-MD5` 标头。可以选择通过控制台指定额外的校验和函数和校验和值作为 `x-amz-sdk-checksum-algorithm` 标头。如果您使用 PutObject API，则必须指定 `Content-MD5` 标头、`x-amz-sdk-checksum-algorithm` 标头或两者来配置对象锁定保留期。

有关更多信息，请参阅 在 Amazon S3 中检查对象完整性。

## 配置事件和通知

您可以使用 Amazon S3 事件通知，通过 Amazon CloudTrail 跟踪在对象锁定配置及数据上进行的访问和更改。有关 CloudTrail 的信息，请参阅《Amazon CloudTrail 用户指南》中的什么是 Amazon CloudTrail？

您还可以使用 Amazon CloudWatch 根据此数据生成警报。有关 CloudWatch 的信息，请参阅《Amazon CloudWatch 用户指南》中的什么是 Amazon CloudWatch？

## 使用存储桶策略为保留期限设置限制

您可以使用存储桶策略为存储桶设置允许的最小和最大保留期限。最长保留周期为 100 年。

以下示例显示一个存储桶策略，它使用 `s3:object-lock-remaining-retention-days` 条件键将最长保留期限设置为 10 天。

```
{
    "Version": "2012-10-17",
    "Id": "SetRetentionLimits",
    "Statement": [
        {
            "Sid": "SetRetentionPeriod",
            "Effect": "Deny",
            "Principal": "*",
            "Action": [
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition": {
                "NumericGreaterThan": {
                    "s3:object-lock-remaining-retention-days": "10"
                }
            }
        }
    ]
}
```

> **Note**
>
> 如果您的存储桶是复制配置的目标存储桶，则对于通过使用复制功能创建的对象副本，您可以设置允许的最小和最大保留期限。为此，您必须在存储桶策略中允许 `s3:ReplicateObject` 操作。有关复制权限的更多信息，请参阅the section called “设置权限”。

有关存储桶的更多信息，请参阅以下主题：

- 《Service Authorization Reference》中的 Actions, resources, and condition keys for Amazon S3。

有关按 S3 资源类型对 S3 API 操作的权限的更多信息，请参阅 Amazon S3 API 操作所需的权限。

- 对象操作
- 使用条件键的存储桶策略示例

# 配置 S3 对象锁定

借助 Amazon S3 对象锁定，您可以使用一次写入多次读取（WORM）模式在 Amazon S3 通用存储桶中存储对象。您可以使用 S3 对象锁定在固定的时间段内或无限期地阻止删除或覆盖对象。有关对象锁定功能的一般信息，请参阅使用对象锁定以锁定对象。

在锁定任何对象之前，必须在通用存储桶上启用 S3 版本控制和对象锁定。之后，您可以设置保留期和/或依法保留。

要使用对象锁定功能，您必须拥有一定的权限。有关与各种对象锁定操作相关的权限列表，请参阅the section called “所需的权限”。

> **Important**
>
> - 在某个存储桶上启用对象锁定后，您将无法为该存储桶禁用对象锁定或暂停版本控制。
> - 具有对象锁定的 S3 存储桶不能用作服务器访问日志的目标存储桶。有关更多信息，请参阅 the section called “记录服务器访问”。

主题

- 创建新的 S3 通用存储桶时启用对象锁定
- 在现有 S3 存储桶上启用对象锁定
- 设置或修改 S3 对象的依法保留
- 设置或修改 S3 对象的保留期
- 设置或修改 S3 存储桶的默认保留期

## 创建新的 S3 通用存储桶时启用对象锁定

可以在使用 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 Amazon S3 REST API 创建新的 S3 通用存储桶时启用对象锁定。

使用 S3 控制台

1. 登录到Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 选择创建存储桶。

   此时将打开创建存储桶页面。
4. 对于存储桶名称，输入存储桶的名称。

   > **Note**
   >
   > 创建存储桶后，便无法更改其名称。有关给存储桶命名的更多信息，请参阅通用存储桶命名规则。

5. 对于区域，选择要放置存储桶的 Amazon Web Services 区域。
6. 在对象所有权下，选择禁用或启用访问控制列表（ACL），并控制上传到存储桶中的对象的所有权。
7. 在此存储桶的屏蔽公共访问权限设置下，选择要应用于存储桶的屏蔽公共访问权限设置。
8. 在存储桶版本控制下，选择已启用。

   对象锁定仅适用于受版本控制的存储桶。
9. （可选）在标签下，您可以选择向存储桶添加标签。标签是用于对存储进行分类和分配成本的键/值对。
10. 在高级设置下，找到对象锁定，然后选择启用。

    您必须确认，启用对象锁定将永久允许锁定此存储桶中的对象。
11. 选择创建存储桶。

使用 Amazon CLI

以下 `create-bucket` 示例创建了一个名为 *`amzn-s3-demo-bucket1`* 的新 S3 存储桶，该存储桶启用了对象锁定：

```
aws s3api create-bucket --bucket amzn-s3-demo-bucket1 --object-lock-enabled-for-bucket
```

有关更多信息和示例，请参阅《Amazon CLI 命令参考》中的 create-bucket。

> **Note**
>
> 您可以从控制台中使用 Amazon CloudShell 运行 Amazon CLI 命令。Amazon CloudShell 是一个基于浏览器、经过预验证的 Shell，您可以直接从Amazon Web Services Management Console中启动它。有关更多信息，请参阅《Amazon CloudShell 用户指南》中的什么是 CloudShell？

使用 REST API

您可以使用 REST API 创建一个启用了对象锁定的新 S3 存储桶。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 CreateBucket。

使用 Amazon SDK

有关在使用 Amazon SDK 创建新的 S3 存储桶时如何启用对象锁定的示例，请参阅《Amazon S3 API 参考》中的 Code examples。

有关如何使用 Amazon SDK 获取当前对象锁定配置的示例，请参阅《Amazon S3 API 参考》中的 Code examples。

有关使用 Amazon SDK 演示不同对象锁定功能的交互式场景，请参阅《Amazon S3 API 参考》中的 Code examples。

有关使用不同 Amazon SDK 的一般信息，请参阅《Amazon S3 API 参考》中的 Developing with Amazon S3 using the Amazon SDKs。

## 在现有 S3 存储桶上启用对象锁定

您可以使用 Amazon S3 控制台、Amazon CLI、Amazon SDK 或 Amazon S3 REST API 为现有 S3 存储桶启用对象锁定。

使用 S3 控制台

> **Note**
>
> 对象锁定仅适用于受版本控制的存储桶。

1. 登录到Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。

2. 在左侧导航窗格中，选择存储桶。
3. 在存储桶列表中，选择要为其启用对象锁定的存储桶的名称。
4. 选择属性选项卡。
5. 在属性下，向下滚动到对象锁定部分，然后选择编辑。
6. 在对象锁定下，选择启用。

   您必须确认，启用对象锁定将永久允许锁定此存储桶中的对象。
7. 选择 Save changes（保存更改）。

使用 Amazon CLI

以下 `put-object-lock-configuration` 示例命令在名为 *amzn-s3-demo-bucket1* 的存储桶上设置 50 天的对象锁定保留期：

```
aws s3api put-object-lock-configuration --bucket amzn-s3-demo-bucket1 --object-
lock-configuration='{ "ObjectLockEnabled": "Enabled", "Rule": { "DefaultRetention":
 { "Mode": "COMPLIANCE", "Days": 50 }}}'
```

有关更多信息和示例，请参阅《Amazon CLI 命令参考》中的 put-object-lock-configuration。

> **Note**
>
> 您可以从控制台中使用 Amazon CloudShell 运行 Amazon CLI 命令。Amazon CloudShell 是一个基于浏览器、经过预验证的 Shell，您可以直接从Amazon Web Services Management Console中启动它。有关更多信息，请参阅《Amazon CloudShell 用户指南》中的什么是 CloudShell？

使用 REST API

您可以使用 Amazon S3 REST API 在现有 S3 存储桶上启用对象锁定。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 PutObjectLockConfiguration。

使用 Amazon SDK

有关如何使用 Amazon SDK 为现有 S3 存储桶启用对象锁定的示例，请参阅《Amazon S3 API 参考》中的 Code examples。

有关如何使用 Amazon SDK 获取当前对象锁定配置的示例，请参阅《Amazon S3 API 参考》中的 Code examples。

有关使用 Amazon SDK 演示不同对象锁定功能的交互式场景，请参阅《Amazon S3 API 参考》中的 Code examples。

有关使用不同 Amazon SDK 的一般信息，请参阅《Amazon S3 API 参考》中的 Developing with Amazon S3 using the Amazon SDKs。

## 设置或修改 S3 对象的依法保留

您可以使用 Amazon S3 控制台、Amazon CLI、Amazon SDK 或 Amazon S3 REST API 设置或移除 S3 对象的依法保留。

> **Important**
>
> - 如果要对一个对象设置依法保留，则该对象的存储桶必须已启用对象锁定。
> - 当您在存储桶中 PUT 具有明确的单独保留模式和期限的对象版本时，该对象版本的单独对象锁定设置会覆盖所有存储桶属性保留设置。

有关更多信息，请参阅 the section called “法定保留”。

使用 S3 控制台

1. 登录到Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 在存储桶列表中，选择包含要设置或修改其依法保留的对象的存储桶名称。
4. 在对象列表中，选择要设置或修改其依法保留的对象。
5. 在对象属性页面上，找到对象锁定依法保留部分，然后选择编辑。
6. 选择启用以设置依法保留，或选择禁用以移除依法保留。
7. 选择 Save changes（保存更改）。

使用 Amazon CLI

以下 `put-object-legal-hold` 示例为名为 *`amzn-s3-demo-bucket1`* 的存储桶中的对象 *`my-image.fs`* 设置了依法保留：

```
aws s3api put-object-legal-hold --bucket amzn-s3-demo-bucket1 --key my-image.fs --
legal-hold="Status=ON"
```

以下 put-object-legal-hold 示例为名为 *amzn-s3-demo-bucket1* 的存储桶中的对象 *my-image.fs* 移除了依法保留：

```
aws s3api put-object-legal-hold --bucket amzn-s3-demo-bucket1 --key my-image.fs --
legal-hold="Status=OFF"
```

有关更多信息和示例，请参阅《Amazon CLI 命令参考》中的 put-object-legal-hold。

> **Note**
>
> 您可以从控制台中使用 Amazon CloudShell 运行 Amazon CLI 命令。Amazon CloudShell 是一个基于浏览器、经过预验证的 Shell，您可以直接从Amazon Web Services Management Console中启动它。有关更多信息，请参阅《Amazon CloudShell 用户指南》中的什么是 CloudShell？

使用 REST API

您可以使用 REST API 设置或修改对象的依法保留。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 PutObjectLegalHold。

使用 Amazon SDK

有关如何使用 Amazon SDK 为对象设置法定保留的示例，请参阅《Amazon S3 API 参考》中的 Code examples。

有关如何使用 Amazon SDK 获取当前法定保留状态的示例，请参阅《Amazon S3 API 参考》中的 Code examples。

有关使用 Amazon SDK 演示不同对象锁定功能的交互式场景，请参阅《Amazon S3 API 参考》中的 Code examples。

有关使用不同 Amazon SDK 的一般信息，请参阅《Amazon S3 API 参考》中的 Developing with Amazon S3 using the Amazon SDKs。

## 设置或修改 S3 对象的保留期

您可以使用 Amazon S3 控制台、Amazon CLI、Amazon SDK 或 Amazon S3 REST API 设置或修改 S3 对象的保留期。

> **Important**
>
> - 如果要对一个对象设置保留期，则该对象的存储桶必须已启用对象锁定。
> - 当您在存储桶中 PUT 具有明确的单独保留模式和期限的对象版本时，该对象版本的单独对象锁定设置会覆盖所有存储桶属性保留设置。
> - 在合规模式下，要想在保留日期到期前删除对象，唯一的方法就是删除相关的 Amazon Web Services 账户。

有关更多信息，请参阅 保留期限。

使用 S3 控制台

1. 登录到Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 在存储桶列表中，选择包含要设置或修改其保留期的对象的存储桶名称。
4. 在对象列表中，选择要设置或修改其保留期的对象。
5. 在对象属性页面上，找到对象锁定保留部分，然后选择编辑。
6. 在保留下，选择启用以设置保留期，或者选择禁用以删除保留期。
7. 如果选择启用，请在保留模式下选择治理模式或合规模式。有关更多信息，请参阅 保留模式。
8. 在保留截止日期下，选择您希望保留期结束的日期。在该时间段内，您的对象将受 WORM 保护，不能被覆盖或删除。有关更多信息，请参阅 保留期限。
9. 选择 Save changes（保存更改）。

使用 Amazon CLI

以下 `put-object-retention` 示例将名为 *`amzn-s3-demo-bucket1`* 的存储桶中对象 *`my-image.fs`* 的保留期限设置为 2025 年 1 月 1 日：

```
aws s3api put-object-retention --bucket amzn-s3-demo-bucket1 --key my-image.fs --
retention='{ "Mode": "GOVERNANCE", "RetainUntilDate": "2025-01-01T00:00:00" }'
```

有关更多信息和示例，请参阅《Amazon CLI 命令参考》中的 put-object-retention。

> **Note**
>
> 您可以从控制台中使用 Amazon CloudShell 运行 Amazon CLI 命令。Amazon CloudShell 是一个基于浏览器、经过预验证的 Shell，您可以直接从Amazon Web Services Management Console中启动它。有关更多信息，请参阅《Amazon CloudShell 用户指南》中的什么是 CloudShell？

使用 REST API

您可以使用 REST API 设置对象的保留期。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 PutObjectRetention。

使用 Amazon SDK

有关如何使用 Amazon SDK 为对象设置保留期的示例，请参阅《Amazon S3 API 参考》中的 Code examples。

有关如何使用 Amazon SDK 获取对象保留期的示例，请参阅《Amazon S3 API 参考》中的 Code examples。

有关使用 Amazon SDK 演示不同对象锁定功能的交互式场景，请参阅《Amazon S3 API 参考》中的 Code examples。

有关使用不同 Amazon SDK 的一般信息，请参阅《Amazon S3 API 参考》中的 Developing with Amazon S3 using the Amazon SDKs。

## 设置或修改 S3 存储桶的默认保留期

您可以使用 Amazon S3 控制台、Amazon CLI、Amazon SDK 或 Amazon S3 REST API 设置或修改 S3 存储桶的默认保留期。您可以指定放入存储桶中的每个对象版本受保护的持续时间，以天或年为单位。

> **Important**
>
> - 如果要为某个存储桶设置默认保留期，则该存储桶必须已启用对象锁定。

- 当您在存储桶中 PUT 具有明确的单独保留模式和期限的对象版本时，该对象版本的单独对象锁定设置会覆盖所有存储桶属性保留设置。
- 在合规模式下，要想在保留日期到期前删除对象，唯一的方法就是删除相关的 Amazon Web Services 账户。

有关更多信息，请参阅 保留期限。

使用 S3 控制台

1. 登录到Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 在存储桶列表中，选择要设置或修改其默认保留期的存储桶的名称。
4. 选择属性选项卡。
5. 在属性下，向下滚动到对象锁定部分，然后选择编辑。
6. 在默认保留期下，选择启用以设置默认保留期，或者选择禁用以删除默认保留期。
7. 如果选择启用，请在保留模式下选择治理模式或合规模式。有关更多信息，请参阅 保留模式。
8. 在默认保留期下，选择您希望保留期持续的天数或年数。放置在此存储桶中的对象将在此天数或年数内被锁定。有关更多信息，请参阅 保留期限。
9. 选择 Save changes（保存更改）。

使用 Amazon CLI

以下 `put-object-lock-configuration` 示例命令使用合规模式在名为 *amzn-s3-demo-bucket1* 的存储桶上设置 50 天的对象锁定保留期：

```
aws s3api put-object-lock-configuration --bucket amzn-s3-demo-bucket1 --object-
lock-configuration='{ "ObjectLockEnabled": "Enabled", "Rule": { "DefaultRetention":
 { "Mode": "COMPLIANCE", "Days": 50 }}}'
```

以下 `put-object-lock-configuration` 示例删除了存储桶上的默认保留配置：

```
aws s3api put-object-lock-configuration --bucket amzn-s3-demo-bucket1 --object-lock-
configuration='{ "ObjectLockEnabled": "Enabled"}'
```

有关更多信息和示例，请参阅《Amazon CLI 命令参考》中的 put-object-lock-configuration。

> **Note**
>
> 您可以从控制台中使用 Amazon CloudShell 运行 Amazon CLI 命令。Amazon CloudShell 是一个基于浏览器、经过预验证的 Shell，您可以直接从Amazon Web Services Management Console中启动它。有关更多信息，请参阅《Amazon CloudShell 用户指南》中的什么是 CloudShell？

使用 REST API

您可以使用 REST API 在现有的 S3 存储桶上设置默认保留期。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 PutObjectLockConfiguration。

使用 Amazon SDK

有关如何使用 Amazon SDK 在现有 S3 存储桶上设置默认保留期的示例，请参阅《Amazon S3 API 参考》中的 Code examples。

有关使用 Amazon SDK 演示不同对象锁定功能的交互式场景，请参阅《Amazon S3 API 参考》中的 Code examples。

有关使用不同 Amazon SDK 的一般信息，请参阅《Amazon S3 API 参考》中的 Developing with Amazon S3 using the Amazon SDKs。

# 备份 Amazon S3 数据

Amazon S3 与 Amazon Backup 本机集成，后者是一项完全托管式、基于策略的服务，您可以使用它来集中定义备份策略，以保护 Amazon S3 中的数据。在定义备份策略并将 Amazon S3 资源分配给策略之后，Amazon Backup 自动创建 Amazon S3 备份，并将备份安全存储在备份计划中指定的加密备份文件库中。

当将 Amazon Backup 用于 Amazon S3 时，您可以执行以下操作：

- 创建连续备份和定期备份。连续备份对于时间点还原很有用，定期备份对于满足您的长期数据保留需求很有用。
- 通过集中配置备份策略，自动化备份计划和保留。
- 将 Amazon S3 数据备份还原到您指定的时间点。

您可以连同 Amazon Backup 使用 S3 版本控制和 S3 复制来帮助从意外删除中恢复并执行自己的自我恢复操作。

先决条件

您必须先在桶上激活 S3 版本控制，Amazon Backup 才可以对它进行备份。

> **Note**
>
> 我们建议您为正在备份的启用版本控制的桶设置生命周期过期规则。如果您没有设置生命周期过期的时段，则 Amazon S3 存储成本可能会增加，原因是 Amazon Backup 将保留 Amazon S3 数据的所有版本。

开始使用

要开始对 Amazon S3 使用 Amazon Backup，请参阅《Amazon Backup 开发人员指南》中的创建 Amazon S3 备份。

限制和局限性

要了解相关限制，请参阅《Amazon Backup 开发人员指南》中的创建 Amazon S3 备份。

# 成本优化

Amazon S3 提供了一系列功能和存储类，有助于您在整个数据生命周期中优化成本。存储类通过以相应的成本提供不同的数据访问级别，而无需预付费用或承诺存储多少内容，从而灵活地管理成本。与其它 Amazon 服务一样，您按实际使用量付费，只需为所用的资源付费。

Amazon S3 存储类是专门为不同的访问规律提供成本极低的存储而设计的。其中包括：

- S3 Standard 适用于频繁访问数据的通用存储。
- Amazon S3 Express One Zone 存储类适用于单可用区中高性能频繁访问的数据。
- S3 Intelligent-Tiering 可自动优化其访问规律为未知或不断变化的数据的成本。
- S3 Standard-IA 和 S3 One Zone-IA 适用于长期存在但访问频率较低的数据。
- S3 Glacier Instant Retrieval 适用于需要立即访问的归档数据。
- S3 Glacier 适用于不要求立即访问但需要灵活地免费检索大量数据的归档数据。
- S3 Glacier Deep Archive 适用于在云中以极低的存储成本进行长期归档和数字保留。

可以随时将对象移到更经济实惠的存储类。此外，Amazon S3 提供了管理数据生命周期的功能。例如，可以使用 S3 生命周期配置，来自动将对象转换到更具成本效益的存储类，或者根据您定义的规则自动删除到期的对象。

诸如 S3 存储类分析、成本分配标记以及账单和使用情况报告等功能有助于您分析成本和使用规律。

主题


- Amazon S3 的账单和使用情况报告
- 了解和管理 Amazon S3 存储类
- 管理对象的生命周期


# Amazon S3 的账单和使用情况报告

当使用 Amazon S3 时，您不必支付任何前期费用或承诺您将存储多少内容。与其它 Amazon Web Services 服务一样，您按实际使用量付费，只需为所用的资源付费。

Amazon 提供 Amazon S3 的以下报告：

- 账单报告 – 包含多份报告，旨在提供您正在使用的 Amazon Web Services 服务（包括 Amazon S3）的所有活动的详细信息。Amazon 始终向 S3 存储桶拥有者收取 Amazon S3 费用，除非该桶是

作为申请方付款桶创建的。有关请求者付费的更多信息，请参阅 使用申请方付款通用存储桶进行存储传输和使用。有关账单报告的更多信息，请参阅 Amazon S3 的 Amazon Billing报告。

- 使用情况报告 – 概括了特定服务按小时、天或月聚合的活动情况。可以选择要包括的使用类型和操作。您还可以选择数据聚合的方式。有关更多信息，请参阅 Amazon S3 的 Amazon 使用情况报告。

以下主题提供有关 Amazon S3 账单和使用情况报告的信息。

主题

- 使用成本分配 S3 存储桶标签
- Amazon S3 的 Amazon Billing报告
- Amazon S3 的 Amazon 使用情况报告
- 了解 Amazon S3 的 Amazon 账单和使用情况报告
- Amazon S3 错误响应的账单计费

## 使用成本分配 S3 存储桶标签

要跟踪单个项目或项目组的存储成本或其他标准，请使用成本分配标签标记您的 Amazon S3 存储桶。成本分配标签是与 S3 存储桶相关联的键-值对。在激活成本分配标签后，Amazon 将使用这些标签在成本分配报告上整理您的资源成本。成本分配标签只能用于标记存储桶。有关用于标记对象的标签的信息，请参阅使用标签对存储进行分类。

成本分配报告会按产品分类和关联的账户用户列出您账户的 Amazon 使用量。该报告包含与详细账单报告相同的行项目 (请参阅了解 Amazon S3 的 Amazon 账单和使用情况报告) 和用于您的标签键的附加列。

Amazon 提供了两种类型的成本分配标签，即 Amazon 生成的标签和用户定义的标签。Amazon 在 Amazon S3 CreateBucket 事件之后为您定义、创建和应用 Amazon 生成的 `createdBy` 标签。您定义、创建用户定义的 标签并将其应用到 S3 存储桶。

必须在账单和成本管理控制台中分别激活这两种类型的标签，然后它们才能出现在账单报告中。有关 Amazon 生成的标签的更多信息，请参阅 Amazon 生成的成本分配标签。

- 要在控制台中创建标签，请参阅查看 S3 通用存储桶的属性。
- 要使用 Amazon S3 API 创建标签，请参阅《Amazon Simple Storage Service API 参考》中的 PUT 存储桶标记。
- 要使用 Amazon CLI 创建标签，请参阅《Amazon CLI 命令参考》中的 put-bucket-tagging。

- 有关激活标签的更多信息，请参阅《Amazon Billing 用户指南》中的使用成本分配标签。

用户定义的成本分配标签

用户定义的成本分配标签有以下组成部分：

- 标签键。标签键是标签的名称。例如，在标签 project/Trinity 中，project 是键。标记键是一个区分大小写的字符串，它可以包含 1 到 128 个 Unicode 字符。

- 标签值。标签值是必需的字符串。例如，在标签 project/Trinity 中，Trinity 是值。标记值是一个区分大小写的字符串，它可以包含 0 到 256 个 Unicode 字符。

有关用户定义的标签的允许字符以及其他限制的详细信息，请参阅《Amazon Billing 用户指南》中的用户定义的标签限制。有关用户定义的标签的更多信息，请参阅《Amazon Billing 用户指南》中的用户定义的成本分配标签。

S3 存储桶标签

每个 S3 存储桶都有一个标签集。标签集包含了分配到该存储桶的所有标签。一个标签集可以包含多达 50 个标签，也可以为空。键在标签集中必须是唯一的，但标签集中的值不必是唯一的。例如，您可以在名为 project/Trinity 和 cost-center/Trinity 的标签集中使用相同的值。

在存储桶内，如果您要添加的标签与现有标签的键相同，则新值会覆盖旧值。

Amazon不会对您的标签应用任何语义意义。我们严格按字符串解释标签。

要添加、列出、编辑或删除标签，您可以使用 Amazon S3 控制台、Amazon Command Line Interface (Amazon CLI) 或 Amazon S3 API。

## 更多信息

- 《Amazon Billing 用户指南》中的使用成本分配标签
- 了解 Amazon S3 的 Amazon 账单和使用情况报告
- Amazon S3 的 Amazon Billing报告

# Amazon S3 的 Amazon Billing报告

Amazon 为您提供的月度账单按 Amazon Web Services 服务和功能分隔您的使用情况信息和成本。有多种 Amazon Billing报告可用：月度报告、成本分配报告和详细账单报告。有关如何查看您的账单报告的信息，请参阅《Amazon Billing 用户指南》中的查看您的账单。

要跟踪您的 Amazon 使用情况并提供与您的账户关联的估算费用，您可以设置 Amazon Cost and Usage Reports。有关更多信息，请参阅《Amazon Data Exports Guide》中的 What are AmazonCost and Usage Reports?

还可以下载使用情况报告，它会比账单报告给出更多有关 Amazon S3 存储使用量的详细信息。有关更多信息，请参阅 Amazon S3 的 Amazon 使用情况报告。

下表列出了与 Amazon S3 使用率相关联的费用。

| 费用 | 注释 |
| --- | --- |
| 存储 | 您要为在您的 S3 存储桶中存储对象付费。您付费的费率取决于对象的大小、当月存储对象的时长以及存储类。Amazon S3 提供以下存储类：S3 Standard、S3 Express One Zone、S3 Intelligent-Tiering、S3 Standard-IA（IA 表示不频繁访问）、S3 One Zone-IA、S3 Glacier Instant Retrieval、S3 Glacier Flexible Retrieval、S3 Glacier Deep Archive 或低冗余存储（RRS）。有关存储类的更多信息，请参阅 了解和管理 Amazon S3 存储类。<br><br>请注意，如果启用了 S3 版本控制，则您需要为保留的对象的每个版本付费。有关版本控制的更多信息，请参阅S3 版本控制的工作原理。 |
| 通用存储桶 | 您无需为账户中创建的前 2000 个通用存储桶付费。但是，对于超出前 2000 个的存储桶，您创建的每个存储桶都将按存储桶数量计费。此费率按存储桶/月来计费。有关通用存储桶定价的信息，请参阅 Amazon S3 定价。 |

| 费用 | 注释 |
| --- | --- |
| 监控和自动化 | 您需要按月为 S3 Intelligent-Tiering 存储类中存储的每个对象支付监控和自动化费用，以便监控访问模式和在 S3 Intelligent-Tiering 中的访问层之间移动对象。 |
| 请求 | 您要为请求付费，例如，针对您的 S3 存储桶和对象进行的 GET 请求。这包括生命周期请求。请求的费率取决于您发出的请求类型。有关请求定价的信息，请参阅 Amazon S3 定价。 |
| 检索 | 您要为检索存储在 S3 Standard-IA、S3 One Zone-IA、S3 Glacier Instant Retrieval、S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 存储中的对象付费。 |
| 提前删除 | 如果在最小存储承诺过去之前删除存储在、S3 Standard-IA、S3 One Zone-IA、S3 Glacier Instant Retrieval、S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储中的对象，您需要为该对象支付提前删除费用。 |
| 存储管理 | 您需要为在您账户的桶上启用的存储管理特征（Amazon S3 清单、分析和对象标记）支付费用。 |

| 费用 | 注释 |
| --- | --- |
| 带宽 | 您需要为所有进出 Amazon S3 的带宽支付费用，以下各项除外：<br>• 从 Internet 传入的数据<br>• 传出到 Amazon Elastic Compute Cloud（Amazon EC2）实例的数据，当实例与 S3 存储桶位于同一 Amazon Web Services 区域 时<br>• 传出到 Amazon CloudFront (CloudFront) 的数据<br><br>您还需要为使用 Amazon S3 Transfer Acceleration 传输的任何数据支付费用。 |

有关存储、数据传输和服务的 Amazon S3 使用收费的详细信息，请参阅 Amazon S3 定价和 Amazon S3 常见问题。

有关了解在 Amazon S3 的账单和使用情况报告中使用的代码和缩写的信息，请参阅了解 Amazon S3 的 Amazon 账单和使用情况报告。

### 更多信息

- Amazon S3 的 Amazon 使用情况报告
- 使用成本分配 S3 存储桶标签
- Amazon Billing与成本管理
- Amazon S3 定价

## Amazon S3 的 Amazon 使用情况报告

在下载使用率报告时，您可以选择按小时、天或月聚合使用量数据。Amazon S3 使用情况报告将按使用类型和 Amazon Web Services 区域 列示操作。有关您的 Amazon S3 存储使用量的更多详细报告，请下载动态生成的 Amazon 使用情况报告。可以选择要包括的使用类型、操作和时间段。您还可以选

择数据聚合的方式。有关使用情况报告的更多信息，请参阅《Amazon Data Exports User Guide》中的 Amazon Usage Report。

Amazon S3 使用情况报告包含以下信息：

- Service – Amazon S3
- Operation – 对您的存储桶或对象执行的操作。有关 Amazon S3 操作的详细说明，请参阅 跟踪使用率报告中的操作。
- UsageType – 以下值之一：
  - 标识存储类型的代码
  - 标识请求类型的代码
  - 标识检索类型的代码
  - 标识数据传输类型的代码
  - 标识从 S3 Intelligent-Tiering、S3 Standard-IA、S3 One Zone-Infrequent Access (S3 One Zone-IA)、S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储中进行的提前删除的代码
  - `StorageObjectCount` – 在给定存储桶中存储的对象计数

  有关 Amazon S3 使用类型的详细说明，请参阅 了解 Amazon S3 的 Amazon 账单和使用情况报告。
- Resource – 与列出的使用率相关联的存储桶的名称。
- StartTime – 以协调世界时 (UTC) 表示的使用开始时间。
- EndTime – 以协调世界时 (UTC) 表示的使用结束时间。
- UsageValue – 以下容量值之一：数据的典型度量单位是千兆字节 (GB)。但是，根据服务和报告的不同，可能会显示万亿字节 (TB)。
  - 指定时间段内的请求数
  - 传输的数据量
  - 给定小时内存储的数据量
  - 与从 S3 Standard-IA、S3 One Zone-IA、S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储中进行的还原相关联的数据量

> **Tip**
>
> 有关 Amazon S3 收到的针对您对象的每个请求的详细信息，请打开您的存储桶的服务器访问日志记录。有关更多信息，请参阅 使用服务器访问日志记录来记录请求。

有关更多信息，请参阅 了解 Amazon S3 的 Amazon 账单和使用情况报告。

### 下载 Amazon 使用率报告

您可以下载 XML 或 CSV 文件格式的使用情况报告。

下载使用率报告

1. 登录到Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在标题栏中，选择您的用户名或账户 ID，然后选择账单与成本管理。
3. 在导航窗格中，选择旧版页面，然后选择成本和使用情况报告。
4. 在“Amazon 使用情况报告”下，选择创建使用情况报告。
5. 在下载使用情况报告页面上，选择以下设置:
   - 服务 – 选择 Amazon Simple Storage Service。
   - Usage Types (使用类型) – 有关 Amazon S3 使用类型的详细说明，请参阅 了解 Amazon S3 的 Amazon 账单和使用情况报告。
   - Operation (操作) – 有关 Amazon S3 操作的详细说明，请参阅 跟踪使用率报告中的操作。
   - Time Period (时间段) – 您希望报告涵盖的时间段。
   - Report Granularity (报告粒度) – 您是否要让报告包含按小时、天或月计算的小计。
6. 选择下载，选择下载格式（XML 报告或 CSV 报告），然后按照提示打开或保存报告。

### 更多信息

- 了解 Amazon S3 的 Amazon 账单和使用情况报告
- Amazon S3 的 Amazon Billing报告

## 了解 Amazon S3 的 Amazon 账单和使用情况报告

Amazon S3 账单和使用情况报告使用代码和缩写。对于下表中的使用类型，请使用此列表中的缩写替换 *region*、*region1* 和 *region2*：

- APE1：亚太地区（香港）
- APN1：亚太地区（东京）
- APN2：亚太地区（首尔）

- APN3：亚太地区（大阪）
- APS1：亚太地区（新加坡）
- APS2：亚太地区（悉尼）
- APS3：亚太地区（孟买）
- APS4：亚太地区（雅加达）
- APS5：亚太地区（海得拉巴）
- APS6：亚太地区（墨尔本）
- APS7：亚太地区（马来西亚）
- APS9：亚太地区（泰国）
- CAN1：加拿大（中部）
- CAN2：加拿大西部（卡尔加里）
- CNN1：中国（北京）
- CNW1：中国（宁夏）
- AFS1：非洲（开普敦）
- EUC2：欧洲（苏黎世）
- EUN1：欧洲（斯德哥尔摩）
- EUS2：欧洲（西班牙）
- EUC1：欧洲（法兰克福）
- EU：欧洲（爱尔兰）
- EUS1：欧洲（米兰）
- EUW2：欧洲（伦敦）
- EUW3：欧洲（巴黎）
- ILC1：以色列（特拉维夫）
- MEC1：中东（阿联酋）
- MES1：中东（巴林）
- MXC1：墨西哥（中部）
- SAE1：南美洲（圣保罗）
- UGW1： Amazon GovCloud（美国西部）
- UGE1： Amazon GovCloud（美国东部）
- USE1（或无前缀）：美国东部（弗吉尼亚北部）

- USE2：美国东部（俄亥俄）
- USW1：美国西部（加利福尼亚北部）
- USW2：美国西部（俄勒冈）

对于下表中的 S3 多区域接入点使用类型，请使用此列表中的缩写替换 *regiongroup1* 和 *regiongroup2*：

- AP：亚太地区
- AU：澳大利亚
- EU：欧洲
- IN：印度
- NA：北美洲
- SA：南美洲

区域组是由多个 Amazon Web Services 区域组成的地理分组。有关更多信息，请参阅区域和可用区。有关各 Amazon Web Services 区域 的定价信息，请参阅 Amazon S3 定价。

下表中的第一列列出了您的账单和使用率报告中显示的使用类型。数据的典型度量单位是千兆字节 (GB)。但是，根据服务和报告的不同，可能会显示万亿字节 (TB)。

| Usage Type | 单位 | 粒度 | 描述 |
| --- | --- | --- | --- |
| *region1*-*region2*-AWS-In-A Bytes | GB | 每小时 | 从 *region2* 传输到 *region1* 的加速数据量 |
| *region1*-*region2*-AWS-In-A Bytes-T1 | GB | 每小时 | 从 *region2* 传输到 *region1* 的 T1 加速数据量，其中 T1 是向美国、欧洲和日本的节点（POPs）发出的 CloudFront 请求 |
| *region1*-*region2*-AWS-In-A Bytes-T2 | GB | 每小时 | 从 *region2* 传输到 *region1* 的 T2 加速数据量，其中 T2 是向所有其它 Amazon 边缘站点的 |

| Usage Type | 单位 | 粒度 | 描述 |
| --- | --- | --- | --- |
| | | | POPs 发出的 CloudFront 请求 |
| *region1*-*region2*-AWS-In-Bytes | GB | 每小时 | 从 *region2* 传输到 *region1* 的数据量 |
| *region1*-*region2*-AWS-Out-ABytes | GB | 每小时 | 从 *region1* 传输到 *region2* 的加速数据量 |
| *region1*-*region2*-AWS-Out-ABytes-T1 | GB | 每小时 | 从 *region1* 传输到 *region2* 的 T1 加速数据量，其中 T1 是向美国、欧洲和日本的 POP 发出的 CloudFront 请求 |
| *region1*-*region2*-AWS-Out-ABytes-T2 | GB | 每小时 | 从 *region1* 传输到 *region2* 的 T2 加速数据量，其中 T2 是向所有其它 Amazon 边缘站点的 POP 发出的 CloudFront 请求 |
| *region1*-*region2*-AWS-Out-Bytes | GB | 每小时 | 从 *region1* 传输到 *region2* 的数据量 |
| *region*-BatchOperations-Jobs | 计数 | 每小时 | 执行的 S3 批量操作作业数 |
| *region*-BatchOperations-Objects | 计数 | 每小时 | 由 S3 批量操作执行的对象操作数 |
| *region*-Bulk-Retrieval-Bytes | GB | 每小时 | 使用批量 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 请求检索的数据量 |

| Usage Type | 单位 | 粒度 | 描述 |
| --- | --- | --- | --- |
| *region*-BytesDeleted-GDA | GB | 每月 | DeleteObject 操作从 S3 Glacier Deep Archive 存储中删除的数据量 |
| *region*-BytesDeleted-GIR | GB | 每月 | DeleteObject 操作从 S3 Glacier Instant Retrieval 存储中删除的数据量。 |
| *region*-BytesDeleted-GLACIER | GB | 每月 | DeleteObject 操作从 S3 Glacier Flexible Retrieval 存储中删除的数据量 |
| *region*-BytesDeleted-INT | GB | 每月 | DeleteObject 操作从 S3 Intelligent-Tiering 存储中删除的数据量 |
| *region*-BytesDeleted-RRS | GB | 每月 | DeleteObject 操作从低冗余存储（RRS）存储中删除的数据量 |
| *region*-BytesDeleted-SIA | GB | 每月 | DeleteObject 操作从 S3 Standard-IA 存储中删除的数据量 |
| *region*-BytesDeleted-STANDARD | GB | 每月 | DeleteObject 操作从 S3 Standard 存储中删除的数据量 |
| *region*-BytesDeleted-ZIA | GB | 每月 | DeleteObject 操作从 S3 One Zone-IA 存储中删除的数据量 |

| Usage Type | 单位 | 粒度 | 描述 |
| --- | --- | --- | --- |
| *region*-C3DataTransfer-In-Bytes | GB | 每小时 | 在同一 Amazon Web Services 区域 内从 Amazon EC2 传输到 Amazon S3 的数据量 |
| *region*-C3DataTransfer-Out-Bytes | GB | 每小时 | 在同一 Amazon Web Services 区域 内从 Amazon S3 传输到 Amazon EC2 的数据量 |
| *region*-CloudFront-In-Bytes | GB | 每小时 | 从 CloudFront 分配传输到 Amazon Web Services 区域 的数据量 |
| *region*-CloudFront-Out-Bytes | GB | 每小时 | 从 Amazon Web Services 区域 传输到 CloudFront 分配的数据量 |
| *region*-DataTransfer-In-Bytes | GB | 每小时 | 从 Internet 传输到 Amazon S3 的数据量 |
| *region*-DataTransfer-Out-Bytes | GB | 每小时 | 从 Amazon S3 传输到 Internet 的数据量[1] |
| *region*-DataTransfer-Regional-Bytes | GB | 每小时 | 在同一 Amazon Web Services 区域 内从 Amazon S3 传输到 Amazon 资源的数据量 |
| *region*-EarlyDelete-ByteHrs | GB-小时数 | 每小时 | 在 90 天最低承诺结束之前，从 S3 Glacier Flexible Retrieval 存储中删除的对象的按比例存储使用量[2] |

| Usage Type | 单位 | 粒度 | 描述 |
| --- | --- | --- | --- |
| *region*-EarlyDelete-GDA | GB-小时数 | 每小时 | 在 180 天最低承诺结束之前，从 S3 Glacier Deep Archive 存储中删除的对象的按比例存储使用量2 |
| *region*-EarlyDelete-GIR | GB-小时数 | 每小时 | 在 90 天最低承诺结束之前，从 S3 Glacier Instant Retrieval 中删除的对象的比例存储使用。 |
| *region*-EarlyDelete-GIR-SmObjects | GB-小时数 | 每小时 | 在 90 天最低承诺结束之前，从 S3 Glacier Instant Retrieval 中删除的小对象 (小于 128KB) 的按比例存储使用量3 |
| *region*-EarlyDelete-SIA | GB-小时数 | 每小时 | 在 30 天最低承诺结束之前，从 S3 Standard-IA 中删除的对象的按比例存储使用量[3] |
| *region*-EarlyDelete-SIA-SmObjects | GB-小时数 | 每小时 | 在 30 天最低承诺结束之前，从 S3 Standard-IA 中删除的小对象 (小于 128KB) 的按比例存储使用量[3] |
| *region*-EarlyDelete-ZIA | GB-小时数 | 每小时 | 在 30 天最低承诺结束之前，从 S3 One Zone-IA 中删除的对象的按比例存储使用量[3] |

| Usage Type | 单位 | 粒度 | 描述 |
| --- | --- | --- | --- |
| *region*-EarlyDelete-ZIA-SmObjects | GB-小时数 | 每小时 | 在 30 天最低承诺结束之前，从 S3 One Zone-IA 中删除的小对象 (小于 128KB) 的按比例存储使用量[3] |
| *region*-Expedited-Retrieval-Bytes | GB | 每小时 | 使用 Expedited S3 Glacier Flexible Retrieval 的数据量 |
| Global-Bucket-Hrs-FreeTier | 存储桶 | 每月 | 您账户中属于 2000 个存储桶账户级免费套餐内的通用存储桶数量 |
| Global-Bucket-Hrs | 存储桶 | 每月 | 您账户中超出 2000 个存储桶账户级免费套餐的通用存储桶数量 |
| *region*-Inventory-Objects Listed | 对象 | 每小时 | 为采用清单列表的对象组（对象按存储桶或前缀分组）列出的对象数 |
| *region*-Metadata-Updates | 更新 | 每小时 | 由 S3 元数据处理的更新的每次更新费用 |
| *region*-Monitoring-Automation-INT | 对象 | 每小时 | S3 Intelligent-Tiering 存储类中被监控和自动分层的唯一对象的数量 |
| *region*-MRAP-Out-Bytes | GB | 每小时 | 通过 S3 多区域接入点端点，从区域中的桶中传出的数据量（MRAP 数据路由定价）。 |

| Usage Type | 单位 | 粒度 | 描述 |
| --- | --- | --- | --- |
| *region*-MRAP-In-Bytes | GB | 每小时 | 通过 S3 多区域接入点端点，从区域中的桶中传出的数据量（MRAP 数据路由定价）。 |
| *regiongroup1-regiongroup2-* -MRAP-Out-Bytes | GB | 每小时 | 通过 S3 多区域接入点端点，从 *regiongroup1* 中的桶传输到位于 Amazon 网络外部的 *regiongroup2* 中客户端的数据量。 |
| *regiongroup1-regiongroup2-* -MRAP-In-Bytes | GB | 每小时 | 通过 S3 多区域接入点端点，从位于 Amazon 网络外部的 *regiongroup2* 中的客户端传输到 *regiongroup1* 中桶的数据量。 |
| *region*-OverwriteBytes-Copy-GDA | GB | 每月 | CopyObject 操作从 S3 Glacier Deep Archive 存储中覆盖的数据量 |
| *region*-OverwriteBytes-Copy-GIR | GB | 每月 | CopyObject 操作从 S3 Glacier Instant Retrieval 存储中覆盖的数据量。 |
| *region*-OverwriteBytes-Copy-GLACIER | GB | 每月 | CopyObject 操作从 S3 Glacier Flexible Retrieval 存储中覆盖的数据量 |
| *region*-OverwriteBytes-Copy-INT | GB | 每月 | CopyObject 操作从 S3 Intelligent-Tiering 存储中覆盖的数据量 |

| Usage Type | 单位 | 粒度 | 描述 |
| --- | --- | --- | --- |
| *region*-OverwriteBytes-Copy-RRS | GB | 每月 | CopyObject 操作从低冗余存储（RRS）存储中覆盖的数据量 |
| *region*-OverwriteBytes-Copy-SIA | GB | 每月 | CopyObject 操作从 S3 Standard-IA 存储中覆盖的数据量 |
| *region*-OverwriteBytes-Copy-STANDARD | GB | 每月 | CopyObject 操作从 S3 Standard 存储中覆盖的数据量 |
| *region*-OverwriteBytes-Copy-ZIA | GB | 每月 | CopyObject 操作从 S3 One Zone-IA 存储中覆盖的数据量 |
| *region*-OverwriteBytes-Put-GDA | GB | 每月 | PutObject 操作从 S3 Glacier Deep Archive 存储中覆盖的数据量 |
| *region*-OverwriteBytes-Put-GIR | GB | 每月 | PutObject 操作从 S3 Glacier Instant Retrieval 存储中覆盖的数据量。 |
| *region*-OverwriteBytes-Put-GLACIER | GB | 每月 | PutObject 操作从 S3 Glacier Flexible Retrieval 存储中覆盖的数据量 |
| *region*-OverwriteBytes-Put-INT | GB | 每月 | PutObject 操作从 S3 Intelligent-Tiering 存储中覆盖的数据量 |
| *region*-OverwriteBytes-Put-RRS | GB | 每月 | PutObject 操作从低冗余存储（RRS）存储中覆盖的数据量 |

| Usage Type | 单位 | 粒度 | 描述 |
| --- | --- | --- | --- |
| *region*-OverwriteBytes-Put-SIA | GB | 每月 | PutObject 操作从 S3 Standard-IA 存储中覆盖的数据量 |
| *region*-OverwriteBytes-Put-STANDARD | GB | 每月 | PutObject 操作从 S3 Standard 存储中覆盖的数据量 |
| *region*-OverwriteBytes-Put-ZIA | GB | 每月 | PutObject 操作从 S3 One Zone-IA 存储中覆盖的数据量 |
| *region1*-*region2*-S3RTC-In-Bytes | GB | 每月 | 由 PutObject ReplTime 、GetObject ReplTime 、InitiateMultipartUploadReplTime 、UploadPartReplTime 、CompleteMultipartUploadReplTime 和 WriteACLReplTime 操作针对 S3 Replication Time Control（S3 RTC）从 *region2* 传输到 *region1* 的数据量 |

| Usage Type | 单位 | 粒度 | 描述 |
| --- | --- | --- | --- |
| *region1*-*region2*-S3RTC-Out-Bytes | GB | 每月 | 由 PutObject ReplTime 、GetObject ReplTime 、InitiateMultipartUploadReplTime 、UploadPartTReplTime 、CompleteMultipartUploadReplTime 和 WriteACLReplTime 操作针对 S3 Replication Time Control ( S3 RTC ) 从 *region1* 传输到 *region2* 的数据量 |
| *region*-Requests-GDA-Tier1 | 计数 | 每小时 | 对 S3 Glacier Deep Archive 对象的 PUT、COPY、POST、CreateMultipartUpload 、UploadPart 或 CompleteMultipartUpload 请求的数量 [6] |
| *region*-Requests-GDA-Tier2 | 计数 | 每小时 | 对 S3 Glacier Deep Archive 对象的 GET 和 HEAD 请求的数量 |
| *region*-Requests-GDA-Tier3 | 计数 | 每小时 | S3 Glacier Deep Archive 标准还原请求的数量 |
| *region*-Requests-GDA-Tier5 | 计数 | 每小时 | 批量 S3 Glacier Deep Archive 还原请求的数量 |

| Usage Type | 单位 | 粒度 | 描述 |
| --- | --- | --- | --- |
| *region*-Requests-GIR-Tier1 | 计数 | 每小时 | 对 S3 Glacier Instant Retrieval 对象的 PUT、COPY 或 POST 请求的数量。 |
| *region*-Requests-GIR-Tier2 | 计数 | 每小时 | 对 S3 Glacier Instant Retrieval 对象的 GET 和所有其它非 S3 Glacier Instant Retrieval-Tier1 请求的数量。 |
| *region*-Requests-GLACIER-Tier1 | 计数 | 每小时 | 对 S3 Glacier Flexible Retrieval 对象的 PUT、COPY、POST、CreateMultipartUpload 、UploadPart 或 CompleteMultipartUpload 请求的数量 [6] |
| *region*-Requests-GLACIER-Tier2 | 计数 | 每小时 | 对 S3 Glacier Flexible Retrieval 对象的 GET 和所有其它未列出的请求的数量 |
| *region*-Requests-INT-Tier1 | 计数 | 每小时 | 对 S3 Intelligent-Tiering 对象的 PUT、COPY 或 POST 请求的数量 |
| *region*-Requests-INT-Tier2 | 计数 | 每小时 | 对 S3 Intelligent-Tiering 对象的 GET 和所有其它非 Tier1 请求的数量 |
| *region*-Requests-SIA-Tier1 | 计数 | 每小时 | 对 S3 Standard-IA 对象的 PUT、COPY 或 POST 请求的数量 |

| Usage Type | 单位 | 粒度 | 描述 |
| --- | --- | --- | --- |
| *region*-Requests-SIA-Tier2 | 计数 | 每小时 | 对 S3 Standard-IA 对象的 GET 和所有其它非 S3 Glacier Instant Retrieval-Tier1 请求的数量。 |
| *region*-Requests-Tier1 | 计数 | 每小时 | 对 S3 Standard、RRS 和标签的 PUT、COPY 或 POST 请求以及对所有桶和对象的 LIST 请求的数量 |
| *region*-Requests-Tier2 | 计数 | 每小时 | GET 和其它非 Tier1 请求的数量 |
| *region*-Requests-Tier3 | 计数 | 每小时 | S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 的生命周期请求和标准 S3 Glacier Flexible Retrieval 还原请求的数量 |
| *region*-Requests-Tier4 | 计数 | 每小时 | 转换到 S3 Glacier Instant Retrieval、S3 Intelligent-Tiering、S3 Standard-IA 或 S3 One Zone-IA storage 存储的生命周期转换数 |
| *region*-Requests-Tier5 | 计数 | 每小时 | 批量 S3 Glacier Flexible Retrieval 还原请求的数量 |
| *region*-Requests-Tier6 | 计数 | 每小时 | 批量 Expedited S3 Glacier Flexible Retrieval 还原请求的数量 |
| *region*-Requests-Tier8 | 计数 | 每小时 | S3 访问授权请求的数量 |

| Usage Type | 单位 | 粒度 | 描述 |
| --- | --- | --- | --- |
| *region*-Requests-XZ-Tier1 | 计数 | 每小时 | 对 S3 Express One Zone 对象的 PUT 或 COPY 请求的数量 |
| *region*-Requests-XZ-Tier2 | 计数 | 每小时 | 对 S3 Express One Zone 对象的 GET 和其它所有非 S3 Express One Zone-Tier1 请求的数量 |
| *region*-Requests-ZIA-Tier1 | 计数 | 每小时 | 对 S3 One Zone-IA 对象的 PUT、COPY 或 POST 请求的数量 |
| *region*-Requests-ZIA-Tier2 | 计数 | 每小时 | 对 S3 One Zone-IA 对象的 GET 和所有其它非 S3 One Zone-IA-Tier1 请求的数量 |
| *region*-Retrieval-GIR | GB | 每小时 | 从 S3 Glacier Instant Retrieval 存储检索的数据量。 |
| *region*-Retrieval-SIA | GB | 每小时 | 从 S3 Standard-IA 存储检索的数据量 |
| *region*-Retrieval-XZ | GB | 每小时 | 使用 S3 Express One Zone 存储的给定检索请求（PUT 或 COPY）中超过 512KB 的数据部分 |
| *region*-Retrieval-ZIA | GB | 每小时 | 从 S3 One Zone-IA 存储检索的数据量 |
| *region*-S3DSSE-In-Bytes | GB | 每月 | Amazon S3 双重加密的数据量 |

| Usage Type | 单位 | 粒度 | 描述 |
| --- | --- | --- | --- |
| *region*-S3DSSE-Out-Bytes | GB | 每月 | Amazon S3 解密的双重加密数据量 |
| *region*-S3G-DataTransfer-In-Bytes | GB | 每小时 | 为了从 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储中还原对象而传入 Amazon S3 的数据量 |
| *region*-S3G-DataTransfer-Out-Bytes | GB | 每小时 | 为了将对象转移到 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储而从 Amazon S3 传输的数据量 |
| *region*-Select-Returned-Bytes | GB | 每小时 | 使用 Select 请求从 S3 Standard存储返回的数据量 |
| *region*-Select-Returned-GIR-Bytes | GB | 每小时 | 通过 S3 Glacier Instant Retrieval 存储的选择请求返回的数据量。 |
| *region*-Select-Returned-INT-Bytes | GB | 每小时 | 使用 Select 请求从 S3 Intelligent-Tiering存储返回的数据量 |
| *region*-Select-Returned-SIA-Bytes | GB | 每小时 | 使用 Select 请求从 S3 Standard-IA 存储返回的数据量 |
| *region*-Select-Returned-ZIA-Bytes | GB | 每小时 | 使用 Select 请求从 S3 One Zone-IA 存储返回的数据量 |

| Usage Type | 单位 | 粒度 | 描述 |
| --- | --- | --- | --- |
| *region*-Select-Scanned-Bytes | GB | 每小时 | 使用 Select 请求从 S3 Standard存储扫描的数据量 |
| *region*-Select-Scanned-GIR-Bytes | GB | 每小时 | 通过 S3 Glacier Instant Retrieval 存储的选择请求扫描的数据量。 |
| *region*-Select-Scanned-INT-Bytes | GB | 每小时 | 使用 Select 请求从 S3 Intelligent-Tiering存储扫描的数据量 |
| *region*-Select-Scanned-SIA-Bytes | GB | 每小时 | 使用 Select 请求从 S3 Standard-IA 存储扫描的数据量 |
| *region*-Select-Scanned-ZIA-Bytes | GB | 每小时 | 使用 Select 请求从 S3 One Zone-IA 存储扫描的数据量 |
| *region*-Standard-Retrieval-Bytes | GB | 每小时 | 使用标准 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 请求检索的数据量 |
| *region*-StorageAnalytics-ObjCount | 对象 | 每小时 | 在每个存储类分析配置中监视的唯一对象的数量。 |
| *region*-StorageLens-ObjCount | 对象 | 每天 | 每个 S3 Storage Lens 存储统计管理工具控制面板中由 S3 Storage Lens 存储统计管理工具高级指标和建议跟踪的唯一对象的数量。 |

| Usage Type | 单位 | 粒度 | 描述 |
| --- | --- | --- | --- |
| *region*-StorageLensFreeTier-ObjCount | 对象 | 每天 | 每个 S3 Storage Lens 存储统计管理工具控制面板中由 S3 Storage Lens 存储统计管理工具使用量指标跟踪的唯一对象的数量。 |
| StorageObjectCount | 计数 | 每天 | 在给定存储桶中存储的对象数 |
| *region*-Tables-CompactedObjects | 对象 | 每小时 | 在 Amazon S3 表存储桶中压缩的对象数量 |
| *region*-Tables-MonitoredObjects | 对象 | 每小时 | Amazon S3 表存储桶中的对象数量 |
| *region*-Tables-ProcessedBytes | GB | 每小时 | Amazon S3 表存储桶中为压缩而处理的数据量 |
| *region*-Tables-Requests-Tier1 | 计数 | 每小时 | Amazon S3 表存储桶上的 PUT 请求数量 |
| *region*-Tables-Requests-Tier2 | 计数 | 每小时 | Amazon S3 表存储桶上 GET 和所有其它非 Tier1 请求的数量 |
| *region*-Tables-TimedStorage-ByteHrs | GB-月 | 每天 | 数据存储在 Amazon S3 表存储桶中的 GB-月数 |
| *region*-TagStorage-TagHrs | 标签小时数 | 每天 | 按小时报告的存储桶中所有对象上的标签总数 |
| *region*-TimedStorage-ByteHrs | GB-月 | 每天 | 数据存储在 S3 Standard 存储中的 GB-月数 |

| Usage Type | 单位 | 粒度 | 描述 |
| --- | --- | --- | --- |
| *region*-TimedStorage-GDA-ByteHrs | GB-月 | 每天 | 数据存储在 S3 Glacier Deep Archive 存储中的 GB-月数 |
| *region*-TimedStorage-GDA-Staging | GB-月 | 每天 | 数据存储在 S3 Glacier Deep Archive 暂存存储中的 GB-月数 |
| *region*-TimedStorage-GIR-ByteHrs | GB-月 | 每天 | 数据存储在 S3 Glacier Instant Retrieval 存储中的 GB-月数。 |
| *region*-TimedStorage-GIR-SmObjects | GB-月 | 每天 | 小对象（小于 128 KB）存储在 S3 Glacier Instant Retrieval 存储中的 GB-月数。 |
| *region*-TimedStorage-GlacierByteHrs | GB-月 | 每天 | 数据存储在 S3 Glacier Flexible Retrieval 存储中的 GB-月数 |
| *region*-TimedStorage-GlacierStaging | GB-月 | 每天 | 数据存储在 S3 Glacier Flexible Retrieval 暂存存储中的 GB-月数 |
| *region*-TimedStorage-INT-FA-ByteHrs | GB-月 | 每天 | 数据存储在 S3 Intelligent-Tiering 存储的频繁访问层中的 GB-月数 [5] |
| *region*-TimedStorage-INT-IA-ByteHrs | GB-月 | 每天 | 数据存储在 S3 Intelligent-Tiering 存储的不频繁访问层中的 GB-月数 |
| *region*-TimedStorage-INT-AA-ByteHrs | GB-月 | 每天 | 数据存储在 S3 Intelligent-Tiering 存储的归档访问层中的 GB-月数 |

| Usage Type | 单位 | 粒度 | 描述 |
| --- | --- | --- | --- |
| *region*-TimedStorage-INT-AIA-ByteHrs | GB-月 | 每天 | 数据存储在 S3 Intelligent-Tiering 存储的归档即时访问层中的 GB-月数 |
| *region*-TimedStorage-INT-DAA-ByteHrs | GB-月 | 每天 | 数据存储在 S3 Intelligent-Tiering 存储的深层归档访问层中的 GB-月数 |
| *region*-TimedStorage-RRS-ByteHrs | GB-月 | 每天 | 数据存储在低冗余存储（RRS）存储中的 GB-月数 |
| *region*-TimedStorage-SIA-ByteHrs | GB-月 | 每天 | 数据存储在 S3 Standard-IA 存储中的 GB-月数 |
| *region*-TimedStorage-SIA-SmObjects | GB-月 | 每天 | 小对象（小于 128 KB）存储在 S3 Standard-IA 存储中的 GB-月数 [4] |
| *region*-TimedStorage-XZ-ByteHrs | GB-月 | 每天 | 数据存储在 S3 Express One Zone 存储中的 GB-月数 |
| *region*-TimedStorage-ZIA-ByteHrs | GB-月 | 每天 | 数据存储在 S3 One Zone-IA 存储中的 GB-月数 |
| *region*-TimedStorage-ZIA-SmObjects | GB-月 | 每天 | 小对象（小于 128 KB）存储在 S3 One Zone-IA 存储中的 GB-月数 |
| *region*-Upload-XZ | GB | 每小时 | 使用 S3 Express One Zone 的给定上传请求（PUT 或 COPY）中超过 512KB 的数据量 |

备注

1. `Global-Bucket-Hrs` 和 `Global-Bucket-Hrs-FreeTier` 使用类型适用于商用 Amazon Web Services 区域 和 Amazon GovCloud (US) 中的通用存储桶。
2. `Global-Bucket-Hrs` 和 `Global-Bucket-Hrs-FreeTier` 使用类型仅适用于商用 Amazon Web Services 区域 和 Amazon GovCloud (US) 中的通用存储桶。中国的通用存储桶采用 `CNW1-Bucket-Hrs`、`CNN1-Bucket-Hrs`、`CNN1-Bucket-Hrs-FreeTier` 和 `CNW1-Bucket-Hrs-FreeTier` 使用类型。
3. 如果您在传输完成之前终止传输，传输的数据量可能会超过您的应用程序接收的数据量。由于无法立即执行传输终止请求，并且有些数据量可能在传输中，正在等待终止请求的执行，因此会出现此差异。传输中数据以传“出”数据计费。
4. 当归档到 S3 Glacier Instant Retrieval、S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储类的对象在最小存储承诺（对于 S3 Glacier Instant Retrieval 和 S3 Glacier Flexible Retrieval 为 90 天，或对于 S3 Glacier Deep Archive 为 180 天）过去之前被删除、覆盖或转换为不同的存储类时，对剩余的天数会以 GB 为单位按比例收费。
5. 对于位于 S3 Standard-IA 或 S3 One Zone-IA 存储中的对象，当它们在 30 天之前被删除、覆盖或转换为其它存储类时，对剩余的天数会以 GB 为单位按比例收费。
6. 对于位于 S3 Standard-IA 或 S3 One Zone-IA 存储中的小对象（小于 128KB），当它们在 30 天之前被删除、覆盖或转换为其它存储类时，对剩余的天数会以 GB 为单位按比例收费。
7. S3 Intelligent-Tiering 存储类中的对象没有最小可计费对象大小。小于 128 KB 的对象不受监控，也不符合自动分层条件。较小的对象始终存储在 S3 Intelligent-Tiering 频繁访问层中。
8. 当您向 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储类发起 `CreateMultipartUpload`、`UploadPart` 或 `UploadPartCopy` 请求时，请求将按 S3 Standard 请求费率计费，直到您完成分段上传。完成上传后，单个 `CompleteMultipartUpload` 请求将按目标 S3 Glacier 存储的 PUT 费率计费。在上传完成之前，针对 S3 Glacier Flexible Retrieval 存储类的 PUT 的正在上传的分段采用 S3 Standard 存储费率，按 S3 Glacier Flexible Retrieval 暂存存储计费。同样，在上传完成之前，针对 S3 Glacier Deep Archive 存储类的 PUT 的正在上传的分段采用 S3 Standard 存储费率，按 S3 Glacier Deep Archive 暂存存储计费。
9. 对于大小不超过 512KB 的请求，S3 Express One Zone 按请求收取统一费用。对于请求中超过 512KB 的部分，PUT 请求和 GET 请求将按每 GB 额外收费。
10. 有关 S3 Express One Zone 存储类支持的功能的信息，请参阅 目录存储桶不支持的 Amazon S3 功能。
11. 单位以 GB 计费的使用量类型在使用量报告中以字节为单位进行计算。
12. GB-月的计算方法是：取 GB 小时总数，将一个月内的这些数量汇总，然后除以该月的小时数。要了解更多信息，请参阅常见问题：使用 Amazon S3 是如何收费和计费的？

> **Note**
>
> 通常，S3 存储桶拥有者需要为获得 HTTP 200 OK 成功响应和 HTTP 4XX 客户端错误响应的请求付费。存储桶拥有者无需为 HTTP 5XX 服务器错误响应（例如 HTTP 503 Slow Down 错误）付费。有关不予计费的 HTTP 3XX 和 4XX 状态码下的 S3 错误代码的更多信息，请参阅 Amazon S3 错误响应的账单计费。有关在存储桶配置为申请方付款存储桶时的账单费用的更多信息，请参阅申请方付款的费用支付方式。

### 跟踪使用率报告中的操作

操作描述指定的使用类型对您的 Amazon 对象或存储桶所采取的操作。操作由不言自明的代码表示，如 PutObject 或 ListBucket。要查看存储桶上的哪些操作生成了特定类型的用途，请使用这些代码。当您创建使用率报告时，可以选择包括 All Operations 或特定操作 (例如 GetObject) 以进行报告。

### 更多信息

- Amazon S3 的 Amazon 使用情况报告
- Amazon S3 的 Amazon Billing报告
- Amazon S3 定价
- Amazon S3 常见问题

## Amazon S3 错误响应的账单计费

通常，S3 存储桶拥有者需要为获得 HTTP 200 OK 成功响应和 HTTP 4XX 客户端错误响应的请求付费。存储桶拥有者无需为 HTTP 5XX 服务器错误响应（例如 HTTP 503 Slow Down 错误）付费。有关在存储桶配置为申请方付款存储桶时的账单费用的更多信息，请参阅申请方付款的费用支付方式。

下表列出了不予计费的 HTTP 3XX 和 4XX 状态码下的特定错误代码。对于配置了网站托管的存储桶，当 S3 返回自定义错误文档或进行自定义重定向时，仍将收取适用的请求和其它费用。

> **Note**
>
> 对于 AccessDenied（HTTP 403 Forbidden），如果请求是在存储桶拥有者的个人 Amazon 账户或 Amazon 组织外部发起，则 S3 不会向存储桶拥有者收费。

| HTTP 状态代码 | 错误代码 | 错误代码说明 | |
|---|---|---|---|
| 301 永久移动 | PermanentRedirect | 必须使用指定的端点来寻址您正在尝试访问的存储桶。请将未来的所有请求发送到此端点。 | |
| | PermanentRedirectControlError | 必须使用指定的端点来寻址您正在尝试访问的 API 操作。请将未来的所有请求发送到此端点。 | |
| 307 临时重新导向 | TemporaryRedirect | 域名系统（DNS）服务器更新时您会被重定向至存储桶。 | |
| 400 错误请求 | AuthorizationHeaderMalformed | 您提供的授权标头无效。 | |
| | AuthorizationQueryParametersError | 您提供的授权查询参数无效。 | |
| | ConnectionClosedByRequester | 如果在读取 WriteGetObjectResponse 正文时遇到错误，则返回给原始调用方。 | |
| | DeviceNotActiveError | 设备当前处于不活动状态。 | |
| | EndpointNotFound | 将请求定向到正确的端点。 | |
| | ExpiredToken | 提供的令牌过期。 | |
| | IllegalLocationConstraintException | 您正在尝试从存储桶所在区域以外的区域访问存储桶。要避免此错误， | |

| HTTP 状态代码 | 错误代码 | 错误代码说明 | |
|---|---|---|---|
| | | 请使用 `--region` 选项。例如：`aws s3 cp awsexample.txt s3://amzn-s3-demo-bucket/ --region ap-east-1` 。 | |
| | InvalidArgument | 出现此错误可能的原因如下：<br>• 指定的参数无效。<br>• 请求缺少必需的标头。<br>• 指定的参数不完整或格式有误。<br>• 指定的参数长度必须大于或等于 3。 | |
| | InvalidBucketOwnerAWSAccountID | 预期的存储桶拥有者参数的值必须为 Amazon Web Services 账户 ID。 | |
| | InvalidDigest | 指定的 Content-MD5 或校验和值无效。 | |
| | InvalidEncryptionAlgorithmError | 指定的加密请求无效。有效值为 AES256。 | |
| | InvalidHostHeader | 请求中提供的主机标头使用了不正确的样式寻址。 | |
| | InvalidHttpMethod | 请求是使用意外的 HTTP 方法发出的。 | |

| HTTP 状态代码 | 错误代码 | 错误代码说明 | |
|---|---|---|---|
| | InvalidRequest | 出现此错误可能的原因如下：<br>• 请求使用了错误的签名版本。请使用 AWS4-HMAC-SHA256 （签名版本 4）。<br>• 只能为现有存储桶创建接入点。<br>• 接入点未处于可以删除的状态。<br>• 只能列出现有存储桶的接入点。<br>• 下一个令牌无效。<br>• 生命周期规则中必须至少指定一个操作。<br>• 必须至少指定一个生命周期规则。<br>• 生命周期规则的数量不得超过所允许的 1000 条规则的限制。<br>• MaxResults 参数的范围无效。<br>• SOAP 请求必须通过 HTTPS 连接发出。 | |

| HTTP 状态代码 | 错误代码 | 错误代码说明 | |
|---|---|---|---|
| | | • 名称不符合 DNS 的存储桶不支持 Amazon S3 Transfer Acceleration。<br>• 名称中包含点（.）的存储桶不支持 Amazon S3 Transfer Acceleration。<br>• Amazon S3 Transfer Acceleration 端点仅支持虚拟样式的请求。<br>• 此存储桶上未配置 Amazon S3 Transfer Acceleration。<br>• 此存储桶上已禁用 Amazon S3 Transfer Acceleration。<br>• 该存储桶上不支持 Amazon S3 Transfer Acceleration。如需帮助，请联系 Amazon Web Services 支持。<br>• 此存储桶上不能启用 Amazon S3 Transfer Acceleration。如需帮助，请联系 Amazon Web Services 支持。<br>• HTTP 标头和查询参数中提供的值相互冲突。 | |

| HTTP 状态代码 | 错误代码 | 错误代码说明 | |
|---|---|---|---|
| | | • HTTP 标头和 POST 表单字段中提供的值相互冲突。<br>• 在大于 5GB 的对象上发出 CopyObject 请求。 | |
| | InvalidSessionException | 如果会话因超时或过期而不再存在，则返回。 | |
| | InvalidSignature | 服务器计算出的请求签名与您提供的签名不匹配。请检查您的 Amazon 秘密访问密钥和签名方法。有关更多信息，请参阅签署和对 REST 请求进行身份验证。 | |
| | InvalidSOAPRequest | SOAP 请求正文无效。 | |
| | InvalidStorageClass | 指定的存储类无效。 | |
| | InvalidTag | 您的请求包含无效的标签输入。例如，您的请求可能包含重复的键、过长的键或值，或包含系统标签。 | |
| | InvalidToken | 提供的令牌格式不正确或者无效。 | |
| | InvalidURI | 无法解析指定的 URI。 | |
| | KeyTooLongError | 键过长。 | |

| HTTP 状态代码 | 错误代码 | 错误代码说明 | |
|---|---|---|---|
| | KMS.DisabledException | 由于指定的 KMS 密钥未启用，请求被拒绝。 | |
| | KMS.InvalidKeyUsageException | 由于以下原因之一，请求被拒绝：<br>• KMS 密钥的 KeyUsage 值与 API 操作不兼容。<br>• 为操作指定的加密算法或签名算法与 KMS 密钥（KeySpec）中的密钥材料类型不兼容。<br><br>要加密、解密、重新加密和生成数据密钥，KeyUsage 必须为 ENCRYPT_DECRYPT。要对消息进行签名和验证，KeyUsage 必须为 SIGN_VERIFY。要生成和验证消息身份验证代码（MAC），KeyUsage 必须为 GENERATE_VERIFY_MAC。要获取密钥协议密钥，KeyUsage 必须为 KEY_AGREEMENT。要查找 KMS 密钥的 KeyUsage，请使用 DescribeKey 操作。要查找特定 KMS 密钥支持的加密或签名算法，请使用 DescribeKey 操作。 | |

| HTTP 状态代码 | 错误代码 | 错误代码说明 | |
|---|---|---|---|
| | KMS.KMSInvalidStateException | 由于指定资源的状态对此请求无效，请求被拒绝。此异常意味着以下情况之一：<br>• KMS 密钥的密钥状态与操作不兼容。<br>要查找密钥状态，请使用 DescribeKey 操作。有关哪些密钥状态与每个 KMS 操作兼容的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的 Key states of Amazon KMS keys。<br>• 对于自定义密钥存储中 KMS 密钥的加密操作，此异常表示存在一般性故障，原因可能有很多。要确定原因，请参阅随异常显示的错误消息。 | |
| | KMS.NotFoundException | 由于找不到指定的实体或资源，请求被拒绝。 | |

| HTTP 状态代码 | 错误代码 | 错误代码说明 | |
|---|---|---|---|
| | LambdaInvalidResponse | 当 WriteGetObjectResponse 向 Amazon Lambda 响应 ValidationError 时，返回给原始调用方。有关更多详细信息，请参阅 ValidationError 消息。并非所有 ValidationError 情况都会导致 LambdaInvalidResponse 错误。 | |
| | LambdaInvocationFailed | Lambda 函数调用失败。当 S3 对象 Lambda 无法成功调用已配置的 Lambda 函数时，调用方可能会收到以下错误。错误消息可能包含有关在调用函数时 Amazon Lambda 服务返回的最终错误的详细信息（例如，状态代码、错误代码、错误消息和请求 ID）。 | |
| | MalformedACLError | 您提供的 ACL 格式有误，或者没有根据我们发布的架构进行验证。 | |
| | MalformedPOSTRequest | 您的 POST 请求正文的分段/表单数据格式不正确。 | |
| | MalformedXML | 您提供的 XML 格式不正确，或者没有根据我们发布的架构进行验证。 | |
| | MaxPostPreDataLengthExceededError | 上传文件前的 POST 请求字段太大。 | |

| HTTP 状态代码 | 错误代码 | 错误代码说明 | |
|---|---|---|---|
| | MetadataTooLarge | 您的元数据标头超过了允许的最大元数据大小。 | |
| | MissingAttachment | 预计会有 SOAP 附件，但未找到任何附件。 | |
| | MissingRequestBodyError | 您发送了一个空的 XML 文档作为请求。 | |
| | MissingSecurityHeader | 请求缺少必需的标头。 | |
| | NoLoggingStatusForKey | 不存在针对某个键的日志记录状态子资源之类的内容。 | |
| | NotDeviceOwnerError | 生成令牌的设备不归经过身份验证的用户拥有。 | |
| | ResponseInterrupted | 如果在读取 WriteGetObjectResponse 正文时遇到错误，则返回给原始调用方。 | |
| | RequestHeaderSectionTooLarge | 用于发出请求的请求标头和查询参数超出允许的最大大小 | |
| | TokenCodeInvalidError | 您提供的序列号和/或令牌代码无效。 | |
| | UnexpectedContent | 此请求包含不支持的内容。 | |
| | UnsupportedArgument | 该请求包含不支持的参数。 | |

| HTTP 状态代码 | 错误代码 | 错误代码说明 | |
|---|---|---|---|
| | UnsupportedSignature | 所提供的请求使用不受支持的 STS 令牌版本进行签名，或者签名版本不受支持。 | |
| | UserKeyMustBeSpecified | 存储桶 POST 请求必须包含指定的字段名称。如果已指定，请检查字段的顺序。 | |
| | IncorrectEndpoint | 指定的存储桶存在于其它区域中。将请求定向到正确的端点。 | |
| | ValidationError | 验证错误可能从 WriteGetObjectResponse API 操作中返回，并且可能由于多种原因而发生。有关更多详细信息，请参阅错误消息。 | |
| 403 禁止访问 | RequestTimeTooSkewed | 请求时间和服务器时间之间的差异太大。 | |
| | SignatureDoesNotMatch | 服务器计算出的请求签名与您提供的签名不匹配。请检查您的 Amazon 秘密访问密钥和签名方法。有关更多信息，请参阅 REST 身份验证和 SOAP 身份验证。 | |

| HTTP 状态代码 | 错误代码 | 错误代码说明 | |
|---|---|---|---|
| | NotSignedUp | 您的账户未注册 Amazon S3 服务。您必须先注册，然后才能使用 Amazon S3。您可以通过以下 URL 注册：https://aws.amazon.com/s3 | |
| | InvalidSecurity | 提供的安全凭证无效。 | |
| | InvalidPayer | 已禁用针对此对象的所有访问权限。如需更多帮助，请参阅联系我们。 | |
| | InvalidAccessKeyId | 您提供的 Amazon 访问密钥 ID 在记录中不存在。 | |
| | AccountProblem | 您的 Amazon Web Services 账户存在问题，导致无法成功完成操作。如需更多帮助，请参阅联系我们。 | |
| | UnauthorizedAccessError | 仅适用于中国区域。在向没有 ICP 许可证的存储桶发出请求时返回。有关更多信息，请参阅 ICP Recordal。 | |
| | UnexpectedIPError | 仅适用于中国区域。由于 IP 不符合预期，请求被拒绝。 | |
| | MissingAuthenticationToken | 未对请求进行签名。 | |

| HTTP 状态代码 | 错误代码 | 错误代码说明 | |
|---|---|---|---|
| | LambdaPermissionError | 调用方未获授权，无法调用 Lambda 函数。调用方必须具有调用 Lambda 函数的权限。检查附加到调用方的策略，并确保这些策略已获准将 `lambda:Invoke` 用于所配置的函数。错误消息可能包含有关在调用函数时 Lambda 服务返回的最终错误的详细信息（例如，状态代码、错误代码、错误消息和请求 ID）。 | |
| 404 未找到 | LambdaNotFound | 找不到 Amazon Lambda 函数。尝试调用配置的 Lambda 函数、版本或别名时找不到它。确保 S3 对象 Lambda 接入点配置指向正确的 Lambda 函数 ARN。错误消息可能包含有关在调用函数时 Amazon Lambda 服务返回的最终错误的详细信息（例如，状态代码、错误代码、错误消息和请求 ID）。 | |
| | NoSuchAsyncRequest | 找不到指定的请求。 | |
| | NoSuchObjectLockConfiguration | 指定的对象没有 ObjectLock 配置。 | |

| HTTP 状态代码 | 错误代码 | 错误代码说明 | |
|---|---|---|---|
| | NoSuchUpload | 指定的分段上传不存在。上传 ID 可能无效，或者分段上传可能已中止或已完成。 | |
| | NoSuchWebsiteConfiguration | 指定的存储桶没有网站配置。 | |
| | NoTransformationDefined | 找不到此对象 Lambda 接入点的转换。 | |
| | ObjectLockConfigurationNotFoundError | 此存储桶不存在对象锁定配置。 | |
| 405 不允许的方法 | MethodNotAllowed | 不允许对此资源使用指定的方法。 | |
| 409 冲突 | BucketAlreadyExists | 请求的存储桶名称不可用。存储桶命名空间由系统的所有用户共享。请指定其它名称，然后重试。 | |
| | InvalidBucketState | 请求对于存储桶的当前状态无效。 | |
| | OperationAborted | 当前正在对此资源执行冲突的条件操作。请重试。 | |
| 411 需要长度 | MissingContentLength | 您必须提供 Content-Length HTTP 标头。 | |
| 412 前提条件失败 | RequestIsNotMultiPartContent | 存储桶 POST 请求必须是附件类型的分段/表单数据。 | |

| HTTP 状态代码 | 错误代码 | 错误代码说明 | |
|---|---|---|---|
| 416 请求的范围无法满足 | InvalidRange | 请求的范围对请求无效。尝试其它范围。 | |

# 了解和管理 Amazon S3 存储类

Amazon S3 中的每个对象都有与之关联的存储类。默认情况下，S3 中的对象存储在 S3 Standard 存储类中，但 Amazon S3 为您存储的对象提供了一系列其它存储类。请根据您的使用案例场景和性能访问要求选择一个类。选择专为您的使用案例设计的存储类，可以优化对象的存储成本、性能和可用性。所有这些存储类都提供高持久性存储。

以下各节提供了关于各种存储类以及如何为对象设置存储类的详细信息。

主题


- 经常访问对象的存储类
- 用于自动优化访问模式不断变化或未知的数据的存储类
- 不经常访问对象的存储类
- 极少访问的对象的存储类
- Amazon S3 on Outposts 的存储类
- 比较 Amazon S3 存储类
- 设置对象的存储类
- Amazon S3 分析 – 存储类分析
- 使用 Amazon S3 Intelligent-Tiering 管理存储成本
- 了解用于长期数据存储的 S3 Glacier 存储类
- 使用归档的对象


## 经常访问对象的存储类

对于性能敏感的使用案例（需要毫秒级访问时间的用例）和经常访问的数据，Amazon S3 提供以下存储类：

- S3 Standard (STANDARD)：默认存储类。如果在上传对象时未指定存储类，Amazon S3 会分配 S3 Standard 存储类。要协助您优化 S3 Standard 与 S3 Standard-IA 之间的成本，可以使用 Amazon S3 分析 – 存储类分析。
- S3 Express One Zone (EXPRESS_ONEZONE)：Amazon S3 Express One Zone 存储类是高性能的单区 Amazon S3 存储类，专门用于为延迟要求极高的应用程序提供稳定的个位数毫秒级数据访问。S3 Express One Zone 是目前具有极低延迟的云对象存储类，相比 S3 Standard，其数据访问速度要快 10 倍，且请求成本低 50%。使用 S3 Express One Zone，您的数据将冗余地存储在单个可用区中的多个设备上。有关更多信息，请参阅 S3 Express One Zone。
- 低冗余存储 (REDUCED_REDUNDANCY)：低冗余存储（RRS）类设计用于可使用低于 S3 Standard 存储类的冗余级别存储的非关键性、可复现数据。

  > **Important**
  >
  > 我们建议不要使用此存储类。S3 Standard 存储类更经济高效。

  为了实现持久性，RRS 对象的预期平均每年对象损失率为 0.01%。如果 RRS 对象丢失，则在对该对象发出请求时，Amazon S3 会返回 405 错误。

## 用于自动优化访问模式不断变化或未知的数据的存储类

S3 Intelligent-Tiering (INTELLIGENT_TIERING) 是一种 Amazon S3 存储类，旨在通过自动将数据移动到最具成本效益的访问层来优化存储成本，而不会影响性能或产生运营开销。S3 Intelligent-Tiering 是可实现以下目标的唯一一种云存储类：它通过在访问模式更改时在访问层之间的细粒度对象级别上移动数据，实现自动成本节约。如果您希望针对具有未知或不断变化的访问模式的数据优化存储成本，S3 Intelligent-Tiering 存储类非常适合。S3 Intelligent-Tiering 没有检索费用。

每月只需支付少量的对象监控和自动化费用，S3 Intelligent-Tiering 即可监控访问模式并自动将尚未访问的对象移动到成本较低的访问层。S3 Intelligent-Tiering 可利用三个低延迟和高吞吐量访问层自动节省存储成本。对于可以异步访问的数据，您可以选择激活 S3 Intelligent-Tiering 存储类中的自动存档功能。S3 Intelligent-Tiering 专为 99.9% 的可用性和 99.999999999% 的耐用性而设计。

S3 Intelligent-Tiering 会自动将对象存储在三个访问层：

- 频繁访问 – 上传或转换到 S3 Intelligent-Tiering 的对象将自动存储在频繁访问层中。
- 不频繁访问 – S3 Intelligent-Tiering 将连续 30 天未访问的对象移动到不频繁访问层。

- 归档即时访问 – 使用 S3 Intelligent-Tiering，连续 90 天未访问的任何现有对象都会自动移动到归档即时访问层。

除了这三个层之外，S3 Intelligent-Tiering 还提供两个可选的归档访问层：

- 归档访问 – S3 Intelligent-Tiering 为您提供了一个选项，可让您对可以异步访问的数据激活归档访问层。激活后，归档访问层会自动存档至少连续 90 天未访问的对象。
- 深度归档访问 – S3 Intelligent-Tiering 为您提供了一个选项，可让您对可以异步访问的数据激活深度归档访问层。激活后，深度归档访问层会自动存档至少连续 180 天未访问的对象。

> **Note**
>
> - 如果您想绕过归档即时访问层，则只激活 90 天的归档访问层。归档访问层提供了略低的存储成本，只需几分钟到一小时的检索时间。归档即时访问层提供毫秒级的访问和高吞吐量性能。
> - 仅当您的应用程序可以异步访问对象时，才激活归档访问和深层归档访问层。如果您正在检索的对象存储在归档访问层或深度归档访问层中，请首先使用 `RestoreObject` 还原对象。

您可以将新创建的数据移动到 S3 Intelligent-Tiering，并将其设置为默认存储类。您还可以使用 `PutBucketIntelligentTieringConfiguration` API 操作、Amazon CLI 或 Amazon S3 控制台，选择激活其中一个或这两个归档访问层。有关使用 S3 Intelligent-Tiering 和激活归档访问层的更多信息，请参阅 使用 S3 Intelligent-Tiering。

要访问归档访问层或深度归档访问层中的对象，您首先需要将其还原。有关更多信息，请参阅 从 S3 Intelligent-Tiering 归档访问和深度归档访问层恢复对象。

> **Note**
>
> 如果对象大小小于 128 KB，未被监控，不符合自动分层条件。较小的对象始终存储在频繁访问层中。有关 S3 Intelligent-Tiering 的更多信息，请参阅S3 Intelligent-Tiering 访问层。。

## 不经常访问对象的存储类

S3 Standard-IA 和 S3 One Zone-IA 存储类用于长时间运行且不经常访问的数据。（IA 表示不经常访问。）S3 Standard-IA 和 S3 One Zone-IA 对象可用于毫秒级访问（类似于 S3 Standard存储

类）。Amazon S3 会收取这些对象的检索费，因此，它们最适合不经常访问的数据。有关定价信息，请参阅 Amazon S3 定价。

例如，您可以选择 S3 Standard-IA 和 S3 One Zone-IA 存储类执行以下操作：

- 用于存储备份。
- 用于不经常访问但仍需要毫秒级访问的旧数据。例如，上传数据时，您可能会选择 S3 Standard存储类，然后使用生命周期配置指示 Amazon S3 将对象转换为 S3 Standard-IA 或 S3 One Zone-IA 类。

  有关生命周期管理的更多信息，请参阅 管理对象的生命周期。

> **Note**
>
> S3 Standard-IA 和 S3 One Zone-IA 存储类适用于您计划存储至少 30 天并且大小超过 128 KB 的对象。如果对象小于 128 KB，Amazon S3 会收取 128 KB 的费用。如果您在 30 天的最短存储期结束前删除对象，则需支付 30 天的费用。在 30 天之前删除、覆盖或转换为其他存储类的对象将产生正常存储使用费，外加最低 30 天剩余时间的按比例收费。有关定价信息，请参阅 Amazon S3 定价。

这些存储类在以下方面有所不同：

- S3 Standard-IA (`STANDARD_IA`)：Amazon S3 跨多个地理位置独立的可用区以冗余方式存储对象数据（类似于 S3 Standard 存储类）。S3 Standard-IA 对象可在出现可用区丢失时复原。此存储类可提供比 S3 One Zone-IA 类更好的可用性和弹性。要协助您优化 S3 Standard 与 S3 Standard-IA 之间的成本，可以使用 Amazon S3 分析 – 存储类分析
- S3 One Zone-IA (`ONEZONE_IA`)：Amazon S3 只在一个可用区存储对象数据，因此比 S3 Standard-IA 更便宜。但是，数据无法灵活地应对由于地震和洪水灾害而造成可用区物理丢失的情况。S3 One Zone-IA 存储类和 S3 Standard-IA 一样具有持久性，但是可用性和弹性较差。有关存储类的持久性和可用性比较，请参阅此部分结尾的 比较 Amazon S3 存储类。有关定价信息，请参阅 Amazon S3 定价。对于数据驻留和隔离应用场景，您可以在 Amazon Local Zones 中创建目录存储桶，并使用 S3 Express One Zone (`EXPRESS_ONEZONE`) 和 S3 One Zone-IA (`ONEZONE_IA`) 存储类。有关 Local Zones 中的目录存储桶的更多信息，请参阅数据驻留工作负载。

我们建议执行下列操作：

- S3 Standard-IA (`STANDARD_IA`)：用于无法重新创建的主数据或唯一数据副本。

- S3 One Zone-IA (ONEZONE_IA)：如果在可用区出现故障时可重新创建数据，可在配置 S3 跨区域复制（CRR）时用于对象副本。此外，对于数据驻留和隔离，您可以在 Amazon Local Zones 中创建目录存储桶，并使用 S3 One Zone-IA 存储类。

## 极少访问的对象的存储类

S3 Glacier Instant Retrieval (GLACIER_IR)、S3 Glacier Flexible Retrieval (GLACIER) 和 S3 Glacier Deep Archive (DEEP_ARCHIVE) 存储类专为低成本、长期数据存储和数据归档而设计。这些存储类要求最低存储持续时间和检索费用，因此它们对极少访问的数据最有效。有关 S3 Glacier 存储类的更多信息，请参阅了解用于长期数据存储的 S3 Glacier 存储类。

Amazon S3 提供以下 S3 Glacier 存储类：

- S3 Glacier Instant Retrieval (GLACIER_IR)：用于极少访问且需要毫秒级检索的长期数据。此存储类中的数据可用于实时访问。
- S3 Glacier Flexible Retrieval (GLACIER)：用于可能需要在几分钟内检索其部分数据的归档。此存储类中的数据已归档，不可用于实时访问。
- S3 Glacier Deep Archive (DEEP_ARCHIVE)：用于归档极少需要访问的数据。此存储类中的数据已归档，不可用于实时访问。

### 检索存档的对象

您可以按照与其它存储类相同的方式（如设置对象的存储类一节所述），将对象的存储类设置为 S3 Glacier Flexible Retrieval (GLACIER) 或 S3 Glacier Deep Archive (DEEP_ARCHIVE)。但是，S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 对象已归档，不可用于实时访问。有关更多信息，请参阅 了解 S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 中的归档存储。

> **Note**
>
> 如果使用 S3 Glacier 存储类，您的对象将保留在 Amazon S3 中。您无法直接通过单独的 Amazon S3 Glacier 服务访问它们。有关 Amazon S3 Glacier 的更多信息，请参阅 Amazon S3 Glacier 开发人员指南。

## Amazon S3 on Outposts 的存储类

通过使用 Amazon S3 on Outposts，您可以在 Amazon Outposts 资源上创建 S3 存储桶，并在本地为需要本地数据访问、本地数据处理和数据驻留的应用程序存储和检索对象。您可以像在 Amazon S3 中一样在 Amazon Outposts 上使用相同的 API 操作和特征，包括访问策略、加密和标记。您可以通过 Amazon Web Services Management Console、Amazon CLI、Amazon SDK 或 REST API 使用 S3 on Outposts。

S3 on Outposts 提供了一个新的存储类 S3 Outposts (OUTPOSTS)。S3 Outposts 存储类仅可用于存储在 Outposts 上的存储桶中的对象。如果您尝试将此存储类与 Amazon Web Services 区域中的 S3 存储桶一起使用，则会出现 `InvalidStorageClass` 错误。此外，如果您尝试将其他 S3 存储类与存储在 S3 on Outposts 存储桶中的对象一起使用，则会出现相同的错误。

存储在 S3 Outposts (OUTPOSTS) 存储类中的对象始终使用具有 Amazon S3 托管式加密密钥的服务器端加密 (SSE-S3) 进行加密。有关更多信息，请参阅 使用具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）。

您还可以明确选择使用具有客户提供的加密密钥的服务器端加密 (SSE-C) 来加密存储在 S3 Outposts 存储类中的对象。有关更多信息，请参阅 使用具有客户提供的密钥的服务器端加密（SSE-C）。

> **Note**
>
> S3 on Outposts 不支持带 Amazon Key Management Service (Amazon KMS) 密钥的服务器端加密 (SSE-KMS)。

有关 S3 on Outposts 的更多信息，请参阅《Amazon S3 on Outposts 用户指南》中的 What is S3 on Outposts。

## 比较 Amazon S3 存储类

下表比较了存储类，包括其可用性、持久性、最短存储持续时间和其他注意事项。

| Storage Class | Designed for | Durability (designed for) | Availability (designed for) | Availability Zones | Min storage duration | Min billable object size | Other Considerations |
|---|---|---|---|---|---|---|---|
| STANDARD | Frequently accessed data | 99.999999999% | 99.99% | >= 3 | None | None | None |
| STANDARD_IA | Long-lived, infrequently accessed data | 99.999999999% | 99.9% | >= 3 | 30 days | 128 KB | Per GB retrieval fees apply. |
| INTELLIGENT_TIERING | Long-lived data with changing or unknown access patterns | 99.999999999% | 99.9% | >= 3 | 30 days | None | Monitoring and automation fees per object apply. No retrieval fees. |
| ONEZONE_IA | Long-lived, infrequently accessed, non-critical data | 99.999999999% | 99.5% | 1 | 30 days | 128 KB | Per GB retrieval fees apply. Not resilient to the loss of the Availability Zone. |
| GLACIER | Long-term data archiving with retrieval times ranging from minutes to hours | 99.999999999% | 99.99% (after you restore objects) | >= 3 | 90 days | None | Per GB retrieval fees apply. You must first restore archived objects before you can access them. For more information, see Restoring Archived Objects. |
| DEEP_ARCHIVE | Archiving rarely accessed data with a default retrieval time of 12 hours | 99.999999999% | 99.99% (after you restore objects) | >= 3 | 180 days | None | Per GB retrieval fees apply. You must first restore archived objects before you can access them. For more information, see Restoring Archived Objects. |
| RRS (Not recommended) | Frequently accessed, non-critical data | 99.99% | 99.99% | >= 3 | None | None | None |

* S3 Glacier Flexible Retrieval 要求为每个归档对象提供 40KB 的额外元数据。这包括以 S3 Glacier Flexible Retrieval 费率计费的 32KB 元数据（识别和检索您的数据所需），以及按 S3 Standard 费率计费的额外 8KB 数据。需要使用 S3 Standard 速率来维护归档到 S3 Glacier Flexible Retrieval 的对象的用户定义名称和元数据。有关存储类的更多信息，请参阅 Amazon S3 存储类。

** S3 Glacier Deep Archive 要求为每个归档对象提供 40KB 的额外元数据。这包括以 S3 Glacier Deep Archive 费率计费的 32KB 元数据（识别和检索您的数据所需），以及按 S3 Standard 费率计费的额外 8KB 数据。需要使用 S3 Standard 速率来维护归档到 Amazon S3 Glacier Deep Archive 的对象的用户定义名称和元数据。有关存储类的更多信息，请参阅 Amazon S3 存储类。

请注意，除了 S3 One Zone-IA (`ONEZONE_IA`) 和 S3 Express One Zone (`EXPRESS_ONEZONE`) 之外，所有的存储类都设计为能够应对由灾难导致的可用区的物理损失。除了应用场景的性能要求之外，还考虑了成本。有关存储类定价，请参阅 Amazon S3 定价。

## 设置对象的存储类

可以在上传对象时为其指定存储类。如果未指定，则 Amazon S3 对通用存储桶中的对象使用默认 Amazon S3 Standard 存储类。还可以通过使用 Amazon S3 控制台、Amazon SDK 或 Amazon Command Line Interface（Amazon CLI），将已存储在 Amazon S3 通用存储桶中的对象的存储类更改为任何其它存储类。所有这些方法都使用 Amazon S3 API 操作将请求发送到 Amazon S3。

> **Note**
>
> 您无法更改存储在目录存储桶中的对象的存储类。

可以通过向存储桶添加 S3 生命周期配置来指示 Amazon S3 自动更改对象的存储类。有关更多信息，请参阅 管理对象的生命周期。

在设置 S3 复制配置时，可以将已复制对象的存储类设置为其它任何存储类。但是，您无法复制存储在 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储类中的对象。有关更多信息，请参阅 复制配置文件元素。

以编程方式设置存储类时，需要提供存储类的值。以下是存储类的控制台名称及其相应 API 值的列表：

- 低冗余存储：`REDUCED_REDUNDANCY`
- S3 Express One Zone – `EXPRESS_ONEZONE`
- S3 Glacier Deep Archive – `DEEP_ARCHIVE`
- S3 Glacier Flexible Retrieval – `GLACIER`
- S3 Glacier Instant Retrieval – `GLACIER_IR`
- S3 Intelligent-Tiering – `INTELLIGENT_TIERING`
- S3 One Zone-IA – `ONEZONE_IA`
- S3 Standard – `STANDARD`
- S3 Standard-IA – `STANDARD_IA`

## 设置新对象的存储类

要在上传对象时设置存储类，可以使用以下方法。

使用 S3 控制台

要在控制台中上传新对象时设置存储类，请执行以下操作：

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在存储桶列表中，选择要将文件夹和文件上传到的存储桶的名称。

4. 请选择 Upload（上传）。
5. 在上传窗口中，选择属性。
6. 在“存储类”下，为正在上传的文件选择存储类。
7. （可选）为您正在上传的文件配置任何其它属性。有关更多信息，请参阅上传对象
8. 在上传窗口中，执行下列操作之一：
   - 将文件和文件夹拖到“上传”窗口。
   - 选择添加文件或添加文件夹，选择要上传的文件或文件夹，然后选择打开。
9. 在页面底部，选择上传。

### 使用 REST API

使用 PutObject、POST Object 和 CreateMultipartUpload API 操作创建对象时，可以在对象上指定存储类，并添加 x-amz-storage-class 标头。如果您未添加此标头，Amazon S3 将使用默认的 S3 Standard (STANDARD) 存储类。

此示例请求使用 PutObject 命令将新对象的存储类设置为 S3 Intelligent-Tiering：

```
PUT /my-image.jpg HTTP/1.1
Host: amzn-s3-demo-bucket1.s3.Region.amazonaws.com
Date: Wed, 12 Oct 2009 17:50:00 GMT
Authorization: authorization string
Content-Type: image/jpeg
Content-Length: 11434
Expect: 100-continue
x-amz-storage-class: INTELLIGENT_TIERING
```

### 使用 Amazon CLI

此示例使用 put-object 命令将 *my_images.tar.bz2* 上传到 *GLACIER* 存储类中的 *amzn-s3-demo-bucket1*：

```
aws s3api put-object --bucket amzn-s3-demo-bucket1 --key dir-1/my_images.tar.bz2 --
storage-class GLACIER --body my_images.tar.bz2
```

如果对象大小超过 5 GB，请使用以下命令来设置存储类：

```
aws s3 cp large_test_file s3://amzn-s3-demo-bucket1 --storage-class GLACIER
```

## 更改现有对象的存储类

要在上传对象时设置存储类，可以使用以下方法。

使用 S3 控制台

如果对象大小小于 5 GB，则可以使用 Amazon S3 控制台来更改对象的存储类。如果更大，我们建议添加 S3 生命周期配置来更改对象的存储类。

要在控制台中更改对象的存储类，请执行以下操作：

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在存储桶列表中，选择包含您想要更改的对象的存储桶的名称。
4. 选中待更改对象的名称左侧的复选框。
5. 在操作菜单上，从显示的选项列表中选择编辑存储类。
6. 从可用于对象的存储类中进行选择。
7. 在其它复制设置下，选择是要复制源设置、请勿指定设置还是指定设置。复制源设置是默认选项。如果您只想复制不带源设置属性的对象，请选择请勿指定设置。选择指定设置，来指定存储类、ACL、对象标签、元数据、服务器端加密和其它校验和的设置。
8. 选择右下角的保存更改。Amazon S3 将保存更改。

使用 REST API

要更改现有对象的存储类，请使用以下方法。

此示例请求使用 PutObject 命令将现有对象的存储类设置为 S3 Intelligent-Tiering：

```
PUT /my-image.jpg HTTP/1.1
Host: amzn-s3-demo-bucket1.s3.Region.amazonaws.com
```

```
Date: Wed, 12 Oct 2009 17:50:00 GMT
Authorization: authorization string
Content-Type: image/jpeg
Content-Length: 11434
Expect: 100-continue
x-amz-storage-class: INTELLIGENT_TIERING
```

使用 Amazon CLI

此示例使用 cp 命令将现有对象的存储类从其当前存储类更改为 *DEEP_ARCHIVE* 存储类：

```
aws s3 cp object_S3_URI object_S3_URI --storage-class DEEP_ARCHIVE
```

### 将访问策略权限限制到特定存储类

在授予 Amazon S3 操作的访问策略权限时，您可以使用 `s3:x-amz-storage-class` 条件键限制存储上传的对象时使用的存储类。例如，授予 `s3:PutObject` 权限时，您可以将对象上传限制到特定的存储类。有关策略示例，请参阅 示例：将对象上传限制为具有特定存储类的对象。

有关在策略中使用条件的更多信息和 Amazon S3 条件键的完整列表，请参阅以下主题：

- 《Service Authorization Reference》中的 Actions, resources, and condition keys for Amazon S3。

  有关按 S3 资源类型对 S3 API 操作的权限的更多信息，请参阅 Amazon S3 API 操作所需的权限。
- 使用条件键的存储桶策略示例

## Amazon S3 分析 – 存储类分析

通过使用 Amazon S3 分析存储类分析，您可以分析存储访问模式以帮助您决定何时将正确的数据转换为正确的存储类。这个新的 Amazon S3 分析功能可观察数据访问模式以帮助您确定何时将不常访问的 STANDARD 存储转换为 STANDARD_IA（IA，适用于不频繁访问）存储类。有关存储类的更多信息，请参阅 了解和管理 Amazon S3 存储类。

在存储类分析在一段时间内观察到一组筛选出的数据的不常访问模式后，您可以使用分析结果来帮助改进您的生命周期配置。您可以将存储类分析配置为分析存储桶中的所有对象。或者，也可以配置筛选条件以按通用前缀 (即，名称以通用字符串开头的对象)、对象标签或前缀和标签的组合对对象进行分组以便进行分析。您很有可能会发现，按对象组进行筛选是从存储类分析获益的最佳方式。

> **Important**
>
> 存储类分析仅针对标准类到标准 IA 类提供建议。

每个存储桶可具有多个存储类分析筛选条件 (最多 1,000 个)，并且将收到针对每个筛选条件的单独分析。利用多个筛选配置，您可以分析特定对象组，以改进将对象转换为 STANDARD_IA 的生命周期配置。

存储类分析提供了 Amazon S3 控制台中的存储使用率可视化项，这些可视化项每天将进行更新。您也可以将此类日常使用数据导出到 S3 存储桶，并在电子表格应用程序中或使用商业智能工具（如 QuickSight）查看它们。

存储类分析会产生相关的成本。有关定价信息，请参阅管理和复制 Amazon S3 定价。

主题


- 如何设置存储类分析？
- 如何使用存储类分析？
- 如何导出存储类分析数据？
- 配置存储类分析


## 如何设置存储类分析？

通过配置要分析的对象数据来设置存储类分析。您可将存储类分析配置为执行以下操作：

- 分析存储桶的全部内容。

  您将收到针对存储桶中所有对象的分析。

- 分析按前缀和标签分组的对象。

  您可以配置按前缀、对象标签或前缀和标签的组合对对象进行分组以进行分析的筛选条件。您将收到针对配置的每个筛选条件的单独分析。每个存储桶可具有多个筛选配置（最多 1000 个）。

- 导出分析数据。

  当您为存储桶或筛选条件配置存储类分析时，可以选择每天将分析数据导出到一个文件。当天的分析将添加到该文件以形成针对配置的筛选条件的历史分析日志。该文件会在所选目标上每天进行更新。选择要导出的数据时，指定写入文件的目标存储桶和可选目标前缀。

您可以使用 Amazon S3 控制台、REST API、Amazon CLI 或 Amazon SDK 配置存储类分析。

- 有关如何在 Amazon S3 控制台中配置存储类分析的信息，请参阅 配置存储类分析。
- 要使用 Amazon S3 API，可使用 PutBucketAnalyticsConfiguration REST API 或者 Amazon CLI 或 Amazon SDK 中的等效项。

## 如何使用存储类分析？

您使用存储类分析观察数据访问模式一段时间来收集信息，以帮助您改进 STANDARD_IA 存储的生命周期管理。配置一个筛选条件后，您首先会在 Amazon S3 控制台中看到 24 到 48 小时内基于该筛选条件的数据分析。但是，存储类分析会观察筛选的数据集的访问模式 30 天或更长时间，以便在提供结果前收集用于分析的信息。分析会在初始结果后继续运行，并在访问模式发生更改时更新结果。

首次配置筛选条件时，Amazon S3 控制台可能需要一些时间来分析您的数据。

存储类分析观察筛选的对象数据集的访问模式 30 天或更长时间，以便收集足量信息来进行分析。在存储类分析收集足量信息后，您将在 Amazon S3 控制台中看到一条表示分析已完成的消息。

对不常访问的对象执行分析时，存储类分析基于期限查看已分组的筛选的对象集，因为这些对象已上传到 Amazon S3。存储类分析通过查看筛选的数据集的以下因素来确定是否不常访问期限组：

- STANDARD 存储类中大于 128 KB 的对象。
- 每个期限组内的平均总存储量。
- 每个期限组传出的平均字节数 (非频率)。
- 分析导出数据仅包含与存储类分析有关的数据请求。这可能导致相对于存储指标所示或您自己内部系统的跟踪结果，请求数量以及上传和请求总字节数存在差异。
- 失败的 GET 和 PUT 请求不计入分析。但是，您会在存储指标中看到失败的请求。

### 我检索了多少我的存储空间？

Amazon S3 控制台用图表表示观察期间检索到的筛选的数据集中的存储空间量。

### 我检索了多少百分比的我的存储空间？

Amazon S3 控制台也用图表表示观察期间检索到的筛选的数据集中的存储空间百分比。

如本主题中先前所述，当您对不常访问的对象执行分析时，存储类分析会基于期限查看已分组的筛选的对象集，因为这些对象已上传到 Amazon S3。存储类分析使用以下预定义的对象期限组：

- 不超过 15 天的 Amazon S3 对象
- 15-29 天的 Amazon S3 对象
- 30-44 天的 Amazon S3 对象
- 45-59 天的 Amazon S3 对象
- 60-74 天的 Amazon S3 对象
- 75-89 天的 Amazon S3 对象
- 90-119 天的 Amazon S3 对象
- 120-149 天的 Amazon S3 对象
- 150-179 天的 Amazon S3 对象
- 180-364 天的 Amazon S3 对象
- 365-729 天的 Amazon S3 对象
- 730 天及更长时间的 Amazon S3 对象

通常大约需要 30 天来观察访问模式以收集足够信息来获得分析结果。根据您的数据的独特访问模式，这可能需要 30 天以上的时间。但在配置一个筛选条件后，您首先会在 Amazon S3 控制台中看到 24 到 48 小时内基于该筛选条件的数据分析。您可以查看 Amazon S3 控制台中每天按对象期限组划分的对象访问的分析。

我的多少存储空间是不常访问的？

Amazon S3 控制台显示按预定义的对象期限组分组的访问模式。显示的 Frequently accessed (经常访问) 或 Infrequently accessed (不经常访问) 文本旨在以直观的方式帮助您完成生命周期创建过程。

## 如何导出存储类分析数据？

您可以选择使存储类分析将分析报告导出到逗号分隔值 (CSV) 平面文件。报告每天都会更新且基于您配置的对象期限组筛选条件。使用 Amazon S3 控制台时，您可以在创建筛选条件时选择导出报告选项。选择要导出的数据时，指定写入文件的目标存储桶和可选目标前缀。您可以将数据导出到不同账户中的目标存储桶。目标存储桶必须位于与您配置为进行分析的存储桶相同的区域中。

您必须在目标存储桶上创建存储桶策略以向 Amazon S3 授予验证哪些 Amazon Web Services 账户 拥有存储桶以及将对象写入定义位置的存储桶中的权限。有关策略示例，请参阅 向 S3 清单和 S3 分析功能授予权限。

在配置存储类分析报告后，您将在 24 小时后开始获得每日导出报告。之后，Amazon S3 会继续监控并提供每日导出。

您可以在电子表格应用程序中打开此 CSV 文件，或将此文件导入其他应用程序中，如 Amazon QuickSight。有关将 Amazon S3 文件用于 Amazon QuickSight 的信息，请参阅《Amazon QuickSight 用户指南》中的使用 Amazon S3 文件创建数据集。

导出的文件中的数据在对象期限组内按日期进行排序，如以下示例所示。如果存储类为 STANDARD，则行还包含 ObjectAgeForSIATransition 和 RecommendedObjectAgeForSIATransition 列的数据。

| Date | ConfigId | Filter | StorageClass | ObjectAge | ObjectCount | DataUploaded_MB | Storage_MB | DataRetrieved_MB | GetRequestCount | CumulativeAccessRatio | ObjectAgeForSIATransition | RecommendedObjectAgeForSIATransition |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 8/17/2021 | SalesMaterial | SalesMaterial | STANDARD | 000-014 | | | 0.4313 | | | 0 | | |
| 9/2/2021 | SalesMaterial | SalesMaterial | STANDARD | 000-014 | | | | | | 0.04096734 | | |
| 8/22/2021 | SalesMaterial | SalesMaterial | STANDARD | 000-014 | | | 0.4313 | | | 0 | | |
| 8/25/2021 | SalesMaterial | SalesMaterial | STANDARD | 000-014 | | | 0.4313 | | | 0 | | |
| 9/6/2021 | SalesMaterial | SalesMaterial | STANDARD | 000-014 | | | | | | 0.04096734 | | |
| 8/30/2021 | SalesMaterial | SalesMaterial | STANDARD | 000-014 | | | | | | 0.04096734 | | |
| 8/28/2021 | SalesMaterial | SalesMaterial | STANDARD | 000-014 | | | | | | 0.04096734 | | |
| 8/21/2021 | SalesMaterial | SalesMaterial | STANDARD | 000-014 | | | 0.4313 | | | 0 | | |
| 9/5/2021 | SalesMaterial | SalesMaterial | STANDARD | 000-014 | | | | | | 0.04096734 | | |

报告结束时，给出的对象期限组为 ALL。ALL 行包含当天所有使用期限组的累计总数，包括小于 128 KB 的对象。

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 8/24/2021 | SalesMaterial | SalesMaterial | STANDARD | ALL | 3 | | 0.4599 | | | 0 | 000-014 |
| 9/3/2021 | SalesMaterial | SalesMaterial | STANDARD | ALL | 3 | | 0.4599 | | | 0.02426125 | 015-029 |
| 8/28/2021 | SalesMaterial | SalesMaterial | STANDARD | ALL | 3 | | 0.4599 | | | 0.03545875 | 015-029 |
| 8/17/2021 | SalesMaterial | SalesMaterial | STANDARD | ALL | 3 | | 0.4599 | | | 0 | 000-014 |
| 8/25/2021 | SalesMaterial | SalesMaterial | STANDARD | ALL | 3 | | 0.4599 | | | 0 | 000-014 |
| 9/6/2021 | SalesMaterial | SalesMaterial | STANDARD | ALL | 3 | | 0.4599 | | | 0.0209529 | 015-029 |
| 9/4/2021 | SalesMaterial | SalesMaterial | STANDARD | ALL | 3 | | 0.4599 | | | 0.02304819 | 015-029 |
| 8/22/2021 | SalesMaterial | SalesMaterial | STANDARD | ALL | 3 | | 0.4599 | | | 0 | 000-014 |
| 8/21/2021 | SalesMaterial | SalesMaterial | STANDARD | ALL | 3 | | 0.4599 | | | 0 | 000-014 |
| 8/30/2021 | SalesMaterial | SalesMaterial | STANDARD | ALL | 3 | | 0.4599 | | | 0.03073092 | 015-029 |
| 8/20/2021 | SalesMaterial | SalesMaterial | STANDARD | ALL | 3 | | 0.4599 | | | 0 | 000-014 |

下一部分介绍报告中使用的列。

导出的文件布局

下表描述了 Amazon S3 存储类分析导出文件布局。

## 配置存储类分析

通过使用 Amazon S3 分析存储类分析工具，您可以分析存储访问模式以帮助您决定何时将正确的数据转换为正确的存储类。存储类分析发现数据访问模式以帮助您确定何时将不常访问的 STANDARD 存储转换为 STANDARD_IA (IA，适用于不常访问) 存储类。有关 STANDARD_IA 的更多信息，请参阅 Amazon S3 常见问题和 了解和管理 Amazon S3 存储类。

通过配置要分析的对象数据来设置存储类分析。您可将存储类分析配置为执行以下操作：

- 分析存储桶的全部内容。

  您将收到针对存储桶中所有对象的分析。
- 分析按前缀和标签分组的对象。

您可以配置按前缀、对象标签或前缀和标签的组合对对象进行分组以进行分析的筛选条件。您将收到针对配置的每个筛选条件的单独分析。每个存储桶可具有多个筛选配置（最多 1000 个）。

- 导出分析数据。

  当您为存储桶或筛选条件配置存储类分析时，可以选择每天将分析数据导出到一个文件。当天的分析将添加到该文件以形成针对配置的筛选条件的历史分析日志。该文件会在所选目标上每天进行更新。选择要导出的数据时，指定写入文件的目标存储桶和可选目标前缀。

您可以使用 Amazon S3 控制台、REST API、Amazon CLI 或 Amazon SDK 配置存储类分析。

> **Important**
>
> 存储类分析不提供转换到 ONEZONE_IA 或 S3 Glacier Flexible Retrieval 存储类的建议。
> 如果要配置存储类分析以将结果导出为 .csv 文件，并且目标存储桶使用带有 Amazon KMS key 的原定设置存储桶加密，则必须更新 Amazon KMS 密钥策略以授予 Amazon S3 加密 .csv 文件的权限。有关说明，请参阅 向 Amazon S3 授予权限以使用客户自主管理型密钥进行加密。

有关分析的更多信息，请参阅 Amazon S3 分析 – 存储类分析。

使用 S3 控制台

配置存储类分析

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶或目录存储桶。
3. 在存储桶列表中，选择要为其配置存储类分析的存储桶的名称。
4. 请选择 Metrics (指标) 选项卡。
5. 在 Storage Class Analysis（存储类分析）下，请选择 Create analytics configuration（创建分析配置）。
6. 为筛选器键入名称。如果要分析整个存储桶，请将 Prefix（前缀）字段保留为空。
7. 在 Prefix（前缀）字段中，键入要分析的对象的前缀文本。
8. 要添加标签，请选择添加标签。输入标签的键和值。您可以输入一个前缀和多个标签。

9. （可选）您可以选择导出 CSV 下的启用，以将分析报告导出到逗号分隔值（.csv）平面文件。请选择可将文件存储到的目标存储桶。您可以键入目标存储桶的前缀。目标存储桶必须位于与您为其设置分析的存储桶相同的 Amazon Web Services 区域 中。目标存储桶可处于不同的 Amazon Web Services 账户 中。

   如果 .csv 文件的目标存储桶使用 KMS 密钥的原定设置存储桶加密，则必须更新 Amazon KMS 密钥策略以授予 Amazon S3 加密 .csv 文件的权限。有关说明，请参阅向 Amazon S3 授予权限以使用客户自主管理型密钥进行加密。

10. 请选择 Create Configuration (创建配置)。

Amazon S3 在授予 Amazon S3 写入权限的目标存储桶上创建存储桶策略。此操作允许它将导出数据写入存储桶。

如果在您尝试创建存储桶策略出现错误，则将为您提供相关修复说明。例如，如果您在其他 Amazon Web Services 账户 中选择了目标存储桶，而没有权限读取和写入存储桶策略，则您会看到以下消息。您必须让目标存储桶的拥有者将显示的存储桶策略添加到目标存储桶中。如果策略未添加到目标存储桶中，则您不会获得导出数据，因为 Amazon S3 无权写入目标存储桶。如果源存储桶属于其他账户而非当前用户，则在策略中必须替换掉源存储桶的正确账户 ID。

有关导出的数据以及筛选器工作原理的信息，请参阅 Amazon S3 分析 – 存储类分析。

使用 REST API

要使用 REST API 配置存储类分析，请使用 PutBucketAnalyticsConfiguration。您还可以将等效操作与 Amazon CLI 或 Amazon SDK 结合使用。

您可以使用以下 REST API 来处理存储类分析：

- DELETE Bucket Analytics configuration
- GET Bucket Analytics configuration
- List Bucket Analytics Configuration

## 使用 Amazon S3 Intelligent-Tiering 管理存储成本

S3 Intelligent-Tiering 存储类的设计是通过在访问模式发生变化时自动将数据移动到最经济有效的访问层来优化存储成本，而不需要操作开销或对性能产生影响。每月只需支付少量的对象监控和自动化费用，S3 Intelligent-Tiering 即可监控访问模式并将未访问的对象移动到成本较低的访问层。

S3 Intelligent-Tiering 可在三个低延迟和高吞吐量访问层中自动节省存储成本。对于可以异步访问的数据，您可以选择激活 S3 Intelligent-Tiering 存储类中的自动存档功能。S3 Intelligent-Tiering 没有检索费用。如果稍后访问非频繁访问层或归档即时访问层中的对象，则自动将其移回频繁访问层。在 S3 Intelligent-Tiering 存储类中的访问层之间移动对象时，不会产生额外的分层费用。

S3 Intelligent-Tiering 是针对具有未知、不断变化或不可预测访问模式的数据推荐的存储类别，与对象大小或保留期无关，例如数据湖、数据分析和新应用程序。

S3 Intelligent-Tiering 存储类支持所有 Amazon S3 功能，包括以下功能：

- S3 清单，用于验证对象的访问层
- S3 复制，用于将数据复制到任何 Amazon Web Services 区域
- 使用 S3 Storage Lens 查看存储使用情况和活动指标
- 服务器端加密，用于保护对象数据
- S3 对象锁定，用于防止意外删除数据
- Amazon PrivateLink，用于通过虚拟私有云（VPC）中的私有端点访问 Amazon S3

有关使用 S3 Intelligent-Tiering 的信息，请参阅以下部分：

主题


- S3 Intelligent-Tiering 工作原理
- 使用 S3 Intelligent-Tiering
- 管理 S3 Intelligent-Tiering


## S3 Intelligent-Tiering 工作原理

Amazon S3 Intelligent-Tiering 存储类会自动将对象存储在三个访问层。一个层针对频繁访问进行了优化，一个成本较低的层针对不频繁访问进行了优化，另一个低成本层针对很少访问的数据进行了优化。对于每月较低的对象监视和自动化收费，S3 Intelligent-Tiering 监控访问模式，并在连续 30 天未访问对象时自动将对象移动到非频繁访问层。在不访问 90 天后，对象将移动到存档即时访问层，而不会影响性能或运营开销。

要对于几分钟到几小时内可以访问的数据获得最低的存储成本，请激活归档功能以添加其他两个访问层。您可以将对象分层到归档访问层和/或深度归档访问层。借助归档访问，S3 Intelligent-Tiering 会将至少连续 90 天未访问的对象移动到归档访问层。借助深度归档访问，S3 Intelligent Tiering 会在至少

连续 180 天无访问后将对象移动到深度归档访问层。对于这两个层，您可以根据需要配置无访问的天数。

以下操作构成了阻止将对象分层到归档访问层或深度归档访问层的访问：

- 通过 Amazon S3 控制台下载或复制对象。
- 使用 S3 批量复制调用 CopyObject、UploadPartCopy 或复制对象。在这些情况下，复制操作的源对象是分层的。
- 调用 GetObject、PutObject、RestoreObject、CompleteMultipartUpload、ListParts 或 SelectObjectContent。

例如，如果在指定的无访问天数（例如 180 天）之前通过 `SelectObjectContent` 访问了您的对象，则该操作会重置计时器。直到最后一个 `SelectObjectContent` 请求达到您指定的天数后，您的对象才会移动到归档访问层或深度归档访问层。

如果稍后访问非频繁访问层或归档即时访问层中的对象，则自动将其移回频繁访问层。

以下操作构成了自动将对象从不频繁访问层或归档即时访问层移回频繁访问层的访问：

- 通过 Amazon S3 控制台下载或复制对象。
- 使用批量复制调用 CopyObject、UploadPartCopy 或复制对象。在这些情况下，复制操作的源对象是分层的。
- 调用 GetObject、PutObject、RestoreObject、CompleteMultipartUpload 或 ListParts。

其他操作不构成自动将对象从不频繁访问层或归档即时访问层移回频繁访问层的访问：以下是此类操作的示例，而不是最终列表：

- 调用 HeadObject、GetObjectTagging、PutObjectTagging、ListObjects、ListObjectsV2 或 ListObjectVersions。
- 调用 SelectObjectContent 并不构成将对象向上分层到频繁访问层的访问。此外，它不能阻止将对象从频繁访问层向下分层到不频繁访问层，然后再分层到归档即时访问层。

通过在调用 `PutObject`、`CopyObject` 或 `CreateMultipartUpload` 操作时在 `x-amz-storage-class` request header 中指定 `INTELLIGENT-TIERING`，可以将 S3 Intelligent-Tiering 用作新创建数据的默认存储类。S3 Intelligent-Tiering 专为 99.9% 的可用性和 99.999999999% 的耐用性而设计。

> **Note**
>
> 如果对象大小小于 128 KB，则不会受监控，且不符合自动分层条件。较小的对象始终存储在频繁访问层中。

S3 Intelligent-Tiering 访问层。

下一节说明了不同的自动和可选访问层。当对象在访问层之间移动时，存储类保持不变（S3 Intelligent-Tiering）。

频繁访问层（自动）

这是任何对象创建或转换为 S3 Intelligent-Tiering 的对象开始其生命周期的默认访问层。只要对象被访问，对象就会保留在此层中。频繁访问层提供低延迟和高吞吐量性能。

不频繁访问层（自动）

如果对象在连续 30 天内仍未被访问，对象会转换到“不频繁访问层”。不频繁访问层提供低延迟和高吞吐量性能。

归档即时访问层（自动）

如果一个对象连续 90 天未被访问，该对象就会被移到“归档即时访问层”。归档即时访问层提供低延迟和高吞吐量性能。

归档访问层（可选）

S3 Intelligent-Tiering 为您提供了激活可以异步访问的数据的归档访问层的选项。激活后，归档访问层会自动存档至少连续 90 天未访问的对象。您可以将上次存档访问时间延长到最多 730 天。归档访问层的性能与 S3 Glacier Flexible Retrieval 存储类别相同。

此访问层的标准检索时间可从 3 到 5 小时不等。如果您使用 S3 批量操作启动还原请求，则还原将在几分钟内开始。有关检索选项和时间的更多信息，请参阅the section called “从 S3 Intelligent-Tiering 归档访问和深度归档访问层恢复对象”。

> **Note**
>
> 如果您想绕过归档即时访问层，则只激活 90 天的归档访问层。归档访问层提供了略低的存储成本，检索时间只需几分钟到一小时。归档即时访问层提供毫秒级的访问和高吞吐量性能。

深层归档访问层（可选）

S3 Intelligent-Tiering 为您提供了激活可以异步访问的数据的深度归档访问层的选项。激活后，深度归档访问层会自动存档至少连续 180 天未访问的对象。您可以将上次存档访问时间延长到最多 730 天。深层归档访问层的性能与 S3 Glacier Deep Archive 存储类别相同。

在 12 小时内对此访问层中的对象进行标准检索。如果您使用 S3 批量操作启动还原请求，则还原将在 9 小时内开始。有关检索选项和时间的更多信息，请参阅the section called “从 S3 Intelligent-Tiering 归档访问和深度归档访问层恢复对象”。

> **Note**
>
> 仅当您的应用程序可以异步访问对象时，才激活归档访问和深层归档访问层。如果您正在检索的对象存储在归档访问层或深度归档访问层中，必须首先使用 `RestoreObject` 操作来还原对象。

## 使用 S3 Intelligent-Tiering

您可以使用 S3 Intelligent-Tiering 存储类来自动优化存储成本。S3 Intelligent-Tiering 通过在访问模式更改时在访问层之间的细粒度对象级别上移动数据，实现自动成本节约。对于可以异步访问的数据，您可以使用Amazon Web Services Management Console、Amazon CLI 或 Amazon S3 API 选择在 S3 Intelligent-Tiering 存储类中启用自动归档。

将数据移动到 S3 Intelligent-Tiering

有两种方法可以将数据移动到 S3 Intelligent-Tiering 中。可以通过控制台将对象直接上传到 S3 Intelligent-Tiering，也可以使用 PUT 操作以编程方式上传对象。有关更多信息，请参阅 设置对象的存储类。还可以配置 S3 生命周期配置，以便将对象从 S3 Standard 或 S3 Standard-Infrequent Access 转换为 S3 Intelligent-Tiering。

使用 Direct PUT 将数据上载到 S3 Intelligent-Tiering

使用 PUT API 操作将对象上传到 S3 Intelligent-Tiering 存储类时，您可以在 `x-amz-storage-class` 请求标头中指定 S3 Intelligent-Tiering。

以下请求在 `myBucket` 桶中存储镜像 `my-image.jpg`。请求使用 `x-amz-storage-class` 标头来请求使用 S3 Intelligent-Tiering 存储类来存储对象。

Example

```
PUT /my-image.jpg HTTP/1.1
Host: myBucket.s3.<Region>.amazonaws.com (http://amazonaws.com/)
Date: Wed, 1 Sep 2021 17:50:00 GMT
Authorization: authorization string
Content-Type: image/jpeg
Content-Length: 11434
Expect: 100-continue
x-amz-storage-class: INTELLIGENT_TIERING
```

使用 S3 生命周期将数据从 S3 Standard 或 S3 Standard-Infrequent Access 转换到 S3 Intelligent-Tiering

您可以在 S3 生命周期配置中添加规则以指示 Amazon S3 将对象转换为一个存储类。有关支持的转换和相关约束的信息，请参阅使用 S3 生命周期转换对象。

您可以在桶或前缀级别指定 S3 生命周期配置。在此 S3 生命周期配置规则中，筛选条件指定了一个键前缀 (documents/)。因此，此规则应用于带键名前缀 documents/ 的对象，例如 documents/doc1.txt 和 documents/doc2.txt。该规则指定了 Transition 指示 Amazon S3 在对象创建 0 天后将其转换到 S3 Intelligent-Tiering 存储类的操作。在这种情况下，对象有资格在创建后的午夜 UTC 转换到 S3 Intelligent-Tiering。

Example

```
<LifecycleConfiguration>
  <Rule>
    <ID>ExampleRule</ID>
    <Filter>
       <Prefix>documents/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>INTELLIGENT_TIERING</StorageClass>
    </Transition>
 </Rule>
</LifecycleConfiguration>
```

启用了版本控制的存储桶会维护一个当前对象版本，以及零个或零个以上非当前对象版本。可以为当前和非当前对象版本定义单独的生命周期规则。

有关更多信息，请参阅 生命周期配置元素。

启用 S3 Intelligent-Tiering 归档访问和深度归档访问带

为了在几分钟到几小时内就可以访问的数据上获得最低的存储开销，可以通过使用 Amazon Web Services Management Console、Amazon CLI 或 Amazon S3 API 创建一个桶、前缀或对象标签级配置性能来激活一个或两个归档访问层。

使用 S3 控制台

要启用 S3 Intelligent-Tiering 自动归档

1. 登录到Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets（桶）列表中，请选择您想要的桶的名称。
3. 选择属性。
4. 导航到 S3 Intelligent-Tiering 归档配置部分并选择创建配置。
5. 在归档配置设置部分中，为 S3 Intelligent-Tiering 归档配置指定描述性配置名称。
6. 在选择配置范围下，选择要使用的配置范围。您也可以使用共享前缀、对象标签或两者结合，将配置范围限制为桶内的指定对象。

   a. 要限制配置的范围，请选择使用一个或多个筛选条件限制此配置的范围。

   b. 要使用单个前缀限制配置的范围，请在前缀下输入前缀。

   c. 要使用对象标签限制配置的范围，请选择添加标签，然后为密钥输入一个值。
7. 在状态下，选择启用。
8. 在归档设置部分中，选择一个或两个要启用的归档访问层。
9. 选择创建。

使用 Amazon CLI

您可以使用以下 Amazon CLI 命令管理 S3 Intelligent-Tiering 生命周期配置：

- delete-bucket-intelligent-tiering-configuration
- get-bucket-intelligent-tiering-configuration
- list-bucket-intelligent-tiering-configurations
- put-bucket-intelligent-tiering-configuration

有关设置 Amazon CLI 的说明，请参阅《Amazon S3 API 参考》中的 Developing with Amazon S3 using the Amazon CLI。

使用 Amazon CLI，您不能将配置指定为 XML 文件。您必须改为指定 JSON。以下是您可在 Amazon CLI 命令中指定的示例 XML S3 Intelligent-Tiering 生命周期配置和等效 JSON。

以下示例将 S3 Intelligent-Tiering 配置为指定桶。

Example **put-bucket-intelligent-tiering-configuration**

JSON

```
{
  "Id": "string",
  "Filter": {
    "Prefix": "string",
    "Tag": {
      "Key": "string",
      "Value": "string"
    },
    "And": {
      "Prefix": "string",
      "Tags": [
        {
          "Key": "string",
          "Value": "string"
        }
        ...
      ]
    }
  },
  "Status": "Enabled"|"Disabled",
  "Tierings": [
    {
      "Days": integer,
      "AccessTier": "ARCHIVE_ACCESS"|"DEEP_ARCHIVE_ACCESS"
    }
    ...
  ]
}
```

XML

```
PUT /?intelligent-tiering&id=Id HTTP/1.1
Host: Bucket.s3.amazonaws.com
<?xml version="1.0" encoding="UTF-8"?>
<IntelligentTieringConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
   <Id>string</Id>
   <Filter>
      <And>
         <Prefix>string</Prefix>
         <Tag>
            <Key>string</Key>
            <Value>string</Value>
         </Tag>
         ...
      </And>
      <Prefix>string</Prefix>
      <Tag>
         <Key>string</Key>
         <Value>string</Value>
      </Tag>
   </Filter>
   <Status>string</Status>
   <Tiering>
      <AccessTier>string</AccessTier>
      <Days>integer</Days>
   </Tiering>
   ...
</IntelligentTieringConfiguration>
```

使用 PUT API 操作

您可以使用 PutBucketIntelligentTieringConfiguration 操作具体桶，每个桶最多 1000 个 S3 Intelligent-Tiering 配置。您可以使用共享前缀或对象标签，定义存储段中哪些对象符合归档访问层的条件。使用共享前缀或对象标签，您可以使各个指标筛选条件满足特定业务应用程序、工作流或内部组织的需求。您还可以灵活地激活归档访问层、深层归档访问层或两者结合。

开始使用 S3 Intelligent-Tiering

要了解有关如何使用 S3 Intelligent-Tiering 的更多信息，请参阅教程：开始使用 S3 Intelligent-Tiering。

## 管理 S3 Intelligent-Tiering

S3 Intelligent-Tiering 存储类可在三个低延迟和高吞吐量访问层中自动节省存储成本。它还提供可选的归档功能，对于可在几分钟到几小时内访问的数据，这些归档功能可帮助您获得云中最低的存储成本。

标识访问层对象存储在哪个 S3 Intelligent-Tiering

要获取对象及其相应元数据的列表，包括 S3 Intelligent-Tiering 访问层，您可以使用 Amazon S3 清单。S3 清单提供旨在列出您的对象及其相应元数据的 CSV、ORC 或 Parquet 输出文件。您可以每天或每周接收 Amazon S3 桶或共享前缀的这些清单报告。（共享前缀是指名称以通用字符串开头的对象。）

查看 S3 Intelligent-Tiering 中对象的归档状态

要在 S3 Intelligent-Tiering 存储类中的对象移到归档访问层或深度归档访问层时接收通知，您可以设置 S3 事件通知。有关更多信息，请参阅 Enabling event notifications（启用事件通知）。

Amazon S3 可以将事件通知发布到 Amazon Simple Notification Service (Amazon SNS) 主题、Amazon Simple Queue Service (Amazon SQS) 队列或 Amazon Lambda 函数。有关更多信息，请参阅 Amazon S3 事件通知。

以下是 Amazon S3 发送以发布 `s3:IntelligentTiering` 事件的消息示例。有关更多信息，请参阅 the section called “事件消息结构”。

```
{
   "Records":[
      {
         "eventVersion":"2.3",
         "eventSource":"aws:s3",
         "awsRegion":"us-west-2",
         "eventTime":"1970-01-01T00:00:00.000Z",
         "eventName":"IntelligentTiering",
         "userIdentity":{
            "principalId":"s3.amazonaws.com"
         },
         "requestParameters":{
            "sourceIPAddress":"s3.amazonaws.com"
         },
         "responseElements":{
            "x-amz-request-id":"C3D13FE58DE4C810",
            "x-amz-id-2":"FMyUVURIY8/IgAtTv8xRjskZQpcIZ9KG4V5Wp6S7S/
JRWeUWerMUE5JgHvANOjpD"
```

```
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"testConfigRule",
            "bucket":{
               "name":"amzn-s3-demo-bucket",
               "ownerIdentity":{
                  "principalId":"A3NL1KOZZKExample"
               },
               "arn":"arn:aws:s3:::amzn-s3-demo-bucket"
            },
            "object":{
               "key":"HappyFace.jpg",
               "size":1024,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
            }
         },
         "intelligentTieringEventData":{
            "destinationAccessTier": "ARCHIVE_ACCESS"
            }
      }
   ]
}
```

您还可以使用 HEAD 对象请求查看对象的归档状态。如果以 S3 Intelligent-Tiering 存储类存储对象并且对象当前位于其中一个归档层中，则 HEAD 对象响应显示当前归档层。要显示归档层，请求将使用 x-amz-archive-status 标头。

以下 HEAD 对象请求返回对象（在此情况下为 *my-image.jpg*）的元数据。

Example

```
HEAD /my-image.jpg HTTP/1.1
Host: bucket.s3.region.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:02236Q3V0RonhpaBX5sCYVf1bNRuU=
```

也可以使用 HEAD 对象请求来监控 `restore-object` 请求的状态。如果正在进行归档还原，HEAD 对象响应将包括 x-amz-restore 标头。

以下是一个 HEAD 对象响应示例，显示了一个使用 S3 Intelligent-Tiering 归档且还原请求正在进行中的对象。

Example

```
HTTP/1.1 200 OK
x-amz-id-2: FSVaTMjrmBp3Izs1NnwBZeu7M19iI8UbxMbi0A8AirHANJBo+hEftBuiESACOMJp
x-amz-request-id: E5CEFCB143EB505A
Date: Fri, 13 Nov 2020 00:28:38 GMT
Last-Modified: Mon, 15 Oct 2012 21:58:07 GMT
ETag: "1accb31fcf202eba0c0f41fa2f09b4d7"
x-amz-storage-class: 'INTELLIGENT_TIERING'
x-amz-archive-status: 'ARCHIVE_ACCESS'
x-amz-restore: 'ongoing-request="true"'
x-amz-restore-request-date: 'Fri, 13 Nov 2020 00:20:00 GMT'
Accept-Ranges: bytes
Content-Type: binary/octet-stream
Content-Length: 300
Server: AmazonS3
```

从 S3 Intelligent-Tiering 归档访问和深度归档访问层恢复对象

要访问 S3 Intelligent-Tiering 存档访问层和深度存档访问层中的对象，您必须启动还原请求，然后等待对象移动到频繁访问层。有关已存档对象的更多信息，请参阅the section called “使用归档的对象”。

从归档访问层或深度归档访问层进行还原时，对象会转换回 频繁访问层中。之后，如果对象在连续 30 天仍未被访问，它会自动进入不频繁访问层。然后，在至少连续 90 天无访问后，对象会移入归档访问层。在至少连续 180 天无访问后，对象会移入深度归档访问层。有关更多信息，请参阅 the section called “S3 Intelligent-Tiering 工作原理”。

您可以使用 Amazon S3 控制台、S3 批量操作、Amazon S3 REST API、Amazon SDK 或 Amazon Command Line Interface（Amazon CLI）还原存档的对象。有关更多信息，请参阅 the section called “使用归档的对象”。

## 了解用于长期数据存储的 S3 Glacier 存储类

可以使用 Amazon S3 Glacier 存储类来提供经济实惠的解决方案，以便存储不经常访问的长期数据。S3 Glacier 存储类为：

- S3 Glacier Instant Retrieval
- S3 Glacier Flexible Retrieval
- S3 Glacier Deep Archive

您可以根据访问数据的频率和需要检索数据的速度来选择其中一个存储类。这些存储类中的每一个都提供与 S3 Standard 存储类相同的持久性和弹性，但存储成本较低。有关 S3 Glacier 存储类的更多信息，请参阅 https://aws.amazon.com/s3/storage-classes/glacier/。

主题


- 比较 S3 Glacier 存储类
- S3 Glacier Instant Retrieval
- S3 Glacier Flexible Retrieval
- S3 Glacier Deep Archive
- 了解 S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 中的归档存储
- 这些存储类与 S3 Glacier 服务有何不同


## 比较 S3 Glacier 存储类

每个 S3 Glacier 存储类对于所有对象都有最短存储持续时间。如果您在最短存储持续时间之前删除、覆盖对象或将其转换为不同的存储类，则您需要为该持续时间的剩余部分付费。

有些 S3 Glacier 存储类用于归档目的，这意味着存储在这些存储类中的对象已归档，不可用于实时访问。有关更多信息，请参阅 了解 S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 中的归档存储。

专为不太频繁访问模式和较长检索时间而设计的存储类可提供较低的存储成本。有关定价信息，请参阅 https://www.amazonaws.cn/s3/pricing/。

下表汇总了选择 S3 Glacier 存储类时要考虑的要点：

## S3 Glacier Instant Retrieval

对于每季度访问一次且需要毫秒级检索时间的长期数据，我们建议使用 S3 Glacier Instant Retrieval。这种存储类非常适合注重性能的使用案例，例如图像托管、文件共享应用程序以及存储医疗记录以供在预约期间访问。

S3 Glacier Instant Retrieval 存储类提供实时访问对象的能力，具有与 S3 Standard-IA 存储类相同的延迟和吞吐量性能。与 S3 Standard-IA 相比，S3 Glacier Instant Retrieval 的存储成本更低，但数据访问成本更高。

存储在 S3 Glacier Instant Retrieval 存储类中的数据对象大小最低为 128 KB。此存储类还具有 90 天的最短存储持续时间。

## S3 Glacier Flexible Retrieval

对于每年访问一到两次且不需要立即访问的归档数据，我们建议使用 S3 Glacier Flexible Retrieval。S3 Glacier Flexible Retrieval 提供灵活的检索时间，有助于您平衡成本，访问时间从几分钟到几小时不等，并且可以免费批量检索。此存储类非常适合备份和灾难恢复。

存储在 S3 Glacier Flexible Retrieval 中的对象已归档，无法实时访问。有关更多信息，请参阅 了解 S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 中的归档存储。要访问这些对象，首先启动还原请求，该请求会创建对象的临时副本，您可以在请求完成时访问该副本。有关信息，请参阅使用归档的对象。当您还原对象时，您可以选择一个检索层来满足您的使用案例，还原时间越长，成本越低。

以下检索层适用于 S3 Glacier Flexible Retrieval：

- 加速检索 - 通常在 1-5 分钟内还原对象。加速检索视需求而定，因此，为了确保您拥有可靠且可预测的还原时间，建议您购买预置检索容量。有关更多信息，请参阅 预调配容量。
- 标准检索 - 通常在 3-5 小时内还原对象，或者当使用 S3 批量操作时，在 1 分钟到 5 小时内还原对象。有关更多信息，请参阅 使用批量操作还原对象。
- 批量检索 - 通常在 5 到 12 小时内还原对象。批量检索是免费的。

S3 Glacier Flexible Retrieval 存储类中对象的最短存储持续时间为 90 天。

S3 Glacier Flexible Retrieval 对于每个对象需要 40 KB 的额外元数据。这包括识别和检索您的数据所需的 32 KB 元数据，按 S3 Glacier Flexible Retrieval 的默认费率计费。需要额外 8 KB 数据来维护归档对象的用户定义名称和元数据，按 S3 Standard 费率计费。

## S3 Glacier Deep Archive

对于每年访问不到一次的归档数据，我们建议使用 S3 Glacier Deep Archive。此存储类专为将数据集保留多年来满足合规性要求而设计，也可用于备份或灾难恢复，或任何不频繁访问的数据，您可能要等待多达 72 小时才能检索这些数据。S3 Glacier Deep Archive 是 Amazon 中成本最低的存储选项。

存储在 S3 Glacier Deep Archive 中的对象已归档，无法实时访问。有关更多信息，请参阅 了解 S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 中的归档存储。要访问这些对象，首先启动还原请求，该请求会创建对象的临时副本，您可以在请求完成时访问该副本。有关信息，请参阅使用归档的对象。当您还原对象时，您可以选择一个检索层来满足您的使用案例，还原时间越长，成本越低。

以下检索层适用 S3 Glacier Deep Archive：

- 标准检索 - 通常在 12 小时内还原对象，或者当使用 S3 批量操作时，在 9–12 小时内还原对象。有关更多信息，请参阅 使用批量操作还原对象。

- 批量检索 - 通常在 48 小时内还原对象，成本仅为标准检索层的一小部分。

S3 Glacier Deep Archive 存储类中对象的最短存储持续时间为 180 天。

S3 Glacier Deep Archive 对于每个对象需要 40 KB 的额外元数据。这包括识别和检索您的数据所需的 32 KB 元数据，按 S3 Glacier Deep Archive 的默认费率计费。需要额外 8 KB 数据来维护归档对象的用户定义名称和元数据，按 S3 Standard 费率计费。

## 了解 S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 中的归档存储

S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 为归档存储类。这意味着，当您将对象存储在这些存储类中时，该对象将归档，无法直接访问。要访问已归档的对象，您需要为其提交还原请求，然后等待服务还原该对象。还原请求会还原对象的临时副本，并且在超过您在请求中指定的持续时间之后，删除该副本。有关更多信息，请参阅使用归档的对象。

对象到 S3 Glacier Deep Archive 存储类的转换只能是单向的。

如果要将已存档对象的存储类更改为其他存储类，您必须首先使用还原操作制作该对象的临时副本。然后使用复制操作覆盖对象，并将 S3 Standard、S3 Intelligent-Tiering、S3 Standard-IA、S3 One Zone-IA、S3 Glacier Instant Retrieval、S3 Glacier Flexible Retrieval 或 Reduced Redundancy Storage 或低冗余指定为存储类。

> **Note**
>
> 在 Amazon S3 控制台中，对于 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储类中的对象，不支持对还原的对象执行复制操作。对于这种类型的复制操作，请使用 Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 REST API。

对于每个账户中的每个 Amazon Web Services 区域，在还原这些存储类中的对象时，处理对象还原请求数的速度可高达每秒 1000 个事务（TPS，Transactions Per Second）。

费用注意事项

如果您计划在数月或数年的时间内存档不经常访问的数据，则 S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 存储类可以降低您的存储成本。但是，为确保 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储类适合您，请考虑以下事项：

- 存储开销费用 – 每个归档对象需要 40 KB 的额外元数据。这包括识别和检索数据所需的 32 KB 元数据，按该存储类的默认费率计费。需要额外 8 KB 数据来维护归档对象的用户定义名称和元数据，按 S3 Standard 费率计费。

  如果您打算存档小对象，请考虑这些存储费用。还可以考虑将许多小型对象合并为少量大型对象，以便减少开销成本。
- 分段上传定价 – 当使用分段上传来上传 S3-storage-class-glacier; 和 S3 Glacier Deep Archive 中的对象时，将按 S3 Standard 存储类费率对这些对象进行计费。有关更多信息，请参阅 分段上传和定价。
- 最短 30 天存储费用 – S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 是长期归档解决方案。S3 Glacier Flexible Retrieval 存储类的最短存储持续期间是 90 天，S3 Glacier Deep Archive 是 180 天。如果您删除的对象的归档时间超过最短存储持续时间，则删除归档到这些存储类的数据不会引发费用。如果在最短持续时间内删除或覆盖归档的对象，则 Amazon S3 会对该持续时间的剩余部分收费。
- 数据检索费用 – 当您将归档的对象还原到 S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 时，将按请求收取数据检索费用。这些费用根据您在启动还原时选择的检索层而有所不同。有关定价信息，请参阅 Amazon S3 定价。
- S3 生命周期 – 当您将归档的对象还原到 S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 时，将按请求收取数据检索费用。这些费用根据您在启动还原时选择的检索层而有所不同。有关定价信息，请参阅 Amazon S3 定价。

### 还原存档对象

无法实时访问已归档对象。您必须首先启动恢复请求，然后耐心等待，直到对象的临时副本根据您在请求中指定的持续时间变为可用。收到已还原对象的临时副本后，对象的存储类仍保持为 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive。（HeadObject 或 GetObject API 操作请求将返回 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 作为存储类。）

> **Note**
>
> 在还原某个归档时，您同时为归档（以 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 费率）和临时还原的副本（S3 Standard 存储费率）付费。有关定价的信息，请参阅 Amazon S3 定价。

您可以采用编程方式或使用 Amazon S3 控制台恢复对象副本。Amazon S3 针对每个对象每次仅处理一个还原请求。有关更多信息，请参阅 恢复已归档的对象。

### 这些存储类与 S3 Glacier 服务有何不同

S3 Glacier 存储类是 Amazon S3 服务的一部分，将数据作为对象存储在 S3 存储桶中。您可以使用 S3 控制台，或使用 S3 API 或 SDK 以编程方式，来管理这些存储类中的对象。当您将对象存储在 S3 Glacier 存储类中时，您可以使用高级加密、对象标记和 S3 生命周期配置等 S3 功能，来协助管理数据可访问性和成本。

> **Important**
>
> 我们建议使用 Amazon S3 服务中的 S3 Glacier 存储类来存储所有长期数据。

Amazon S3 Glacier（S3 Glacier）服务是一项单独的服务，它将数据作为归档存储在保管库中。此服务不支持 Amazon S3 功能，也不为数据上传和下载操作提供控制台支持。我们建议不要使用 S3 Glacier 服务来存储您的长期数据。存储在 S3 Glacier 服务中的数据无法通过 Amazon S3 服务访问。如果您正在寻找有关 S3 Glacier 服务的信息，请参阅 Amazon S3 Glacier Developer Guide。要将数据从 Amazon S3 Glacier 服务传输到 Amazon S3 中的存储类，请参阅 Amazon 解决方案库中的将数据从 Amazon S3 Glacier 保管库传输到 Amazon S3。

## 使用归档的对象

要降低不经常访问的对象的存储成本，您可以对此类对象进行归档。当您归档对象时，它会被移动到低成本存储中，这意味着您无法实时访问它。

尽管无法实时访问归档对象，但您可以在几分钟或几小时内还原它们，具体取决于存储类。您可以使用 Amazon S3 控制台、S3 批量操作、REST API、Amazon SDK 和 Amazon Command Line Interface（Amazon CLI）还原归档的对象。有关说明，请参阅 恢复已归档的对象。

以下存储类或存储层中的 Amazon S3 对象已归档，无法实时访问：

- S3 Glacier Flexible Retrieval 存储类
- S3 Glacier Deep Archive 存储类
- S3 Intelligent-Tiering 归档访问层
- S3 Intelligent-Tiering 深度归档访问层

要还原归档对象，必须执行以下操作：

- 对于 S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 存储类中的对象，您必须启动还原请求，并等待对象的临时副本可用。当创建了还原对象的临时副本时，该对象的存储类保持不变。

（HeadObject 或 GetObject API 操作请求会返回 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 作为存储类。）

- 对于 S3 Intelligent-Tiering 归档访问层和 S3 Intelligent-Tiering 深度归档访问层中的对象，您必须启动还原请求，并等待对象移动到频繁访问层。

有关所有 Amazon S3 存储类的比较情况的更多信息，请参阅了解和管理 Amazon S3 存储类。有关 S3 Intelligent-Tiering 的更多信息，请参阅the section called “S3 Intelligent-Tiering 工作原理”。

完成还原任务所需的时间取决于您使用的归档存储类或存储层和您指定的检索选项：加速（仅适用于 S3 Glacier Flexible Retrieval 和 S3 Intelligent-Tiering 归档访问）、标准或批量。有关更多信息，请参阅 了解归档检索选项。

使用 Amazon S3 事件通知，您可以在还原完成时得到通知。有关更多信息，请参阅 Amazon S3 事件通知。

## 从 S3 Glacier 还原对象

当您使用 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 时，Amazon S3 仅在指定的持续时间内恢复对象的临时副本。在此之后，它会删除还原的对象副本。您可以通过重新发出还原请求来修改已还原副本的到期时间。在这种情况下，Amazon S3 会更新相对于当前时间的有效期。

> **Note**
>
> 当您从 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 还原归档对象时，您需要同时为归档对象和临时还原的副本付费。有关定价的信息，请参阅 Amazon S3 定价。

Amazon S3 通过将还原请求中指定的天数与所请求的还原的完成时间相加来计算还原的对象副本的到期时间。然后，Amazon S3 将得出的时间舍入至第二天的午夜协调世界时（UTC)。例如，假设还原的对象副本是在 2012 年 10 月 15 日上午 10:30 UTC 创建的，并且还原时段被指定为 3 天。在这种情况下，还原的副本将于 2012 年 10 月 19 日 00:00 UTC 到期，届时 Amazon S3 将删除对象副本。

## 从 S3 Intelligent-Tiering 还原对象

当您从 S3 Intelligent-Tiering 归档访问层或 S3 Intelligent-Tiering 深度归档访问层还原对象时，对象会移回到 S3 Intelligent-Tiering 频繁访问层中。如果对象在连续 30 天后仍未被访问，它会自动进入不频繁访问层。至少连续 90 天无访问后，对象将移动到 S3 Intelligent-Tiering 归档访问层。如果对象在至少连续 180 天后未被访问，则该对象将移动到深层归档访问层。

> **Note**
>
> 与 S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 存储类不同，S3 Intelligent-Tiering 对象的还原请求不接受该 `Days` 值。

## 结合使用 S3 批量操作与还原请求

要使用单个请求恢复多个 Amazon S3 对象，您可以使用 S3 分批操作。您为 S3 批量操作提供要操作的对象列表。S3 批量操作调用相应的 API 操作来执行指定的操作。单个批量操作任务可对包含 EB 级数据的数十亿个对象执行指定操作。

主题

- 了解归档检索选项
- 恢复已归档的对象

## 了解归档检索选项

以下是在 Amazon S3 中还原已归档对象时可用的检索选项：

- 加速 – 快速访问存储在 S3 Glacier Flexible Retrieval 存储类或 S3 Intelligent-Tiering 归档访问层中的数据。可以在偶尔需要紧急请求归档子集时使用此选项。对于除最大归档对象（250MB+）之外的所有其他归档对象，使用加速检索访问的数据通常在 1 到 5 分钟内可用。

  > **Note**
  >
  > 加速检索是一项高级特征，按加急请求和检索费率收费。
  > 有关 Amazon S3 定价的信息，请参阅 Amazon S3 定价。

  预配置容量帮助确保在您需要时，可以使用针对 S3 Glacier Flexible Retrieval 中的加速检索的检索容量。有关更多信息，请参阅 预调配容量。
- 标准 - 在数小时内访问您的任意归档对象。“标准”是未指定检索选项的检索请求的原定设置选项。对于存储在 S3 Glacier Flexible Retrieval 存储类或 S3 Intelligent-Tiering 归档访问层中的对象，标准检索通常在 3-5 小时内完成。对于存储在 S3 Glacier Deep Archive 存储类或 S3 Intelligent-Tiering 深度归档访问层中的对象，这些检索通常会在 12 小时内完成。对于存储在 S3 Intelligent-Tiering 中的对象，标准检索是免费的。

> **Note**
>
> - 对于存储在 S3 Glacier Flexible Retrieval 存储类或 S3 Intelligent-Tiering 存档访问层中的对象，使用 S3 批量操作还原操作启动的标准检索通常在几分钟内开始，并在 3-5 小时内完成。
> - 对于 S3 Glacier Deep Archive 存储类或 S3 Intelligent-Tiering 深度存档访问层中的对象，使用批量操作还原操作启动的标准检索通常在 9 小时内开始，并在 12 小时内完成。

- 批量 – 使用 Amazon S3 Glacier 中成本最低的检索选项访问您的数据。通过批量检索，您能够以低廉的成本检索大量数据，甚至达到 PB 级。

  对于存储在 S3 Glacier Flexible Retrieval 存储类或 S3 Intelligent-Tiering 存档访问层中的对象，批量检索通常在 5-12 小时内完成。对于存储在 S3 Glacier Deep Archive 存储类或 S3 Intelligent-Tiering 深度存档访问层中的对象，这些检索通常会在 48 小时内完成。

  对于存储在 S3 Glacier Flexible Retrieval 或 S3 Intelligent-Tiering 存储类中的对象，批量检索是免费的。

下表总结了归档检索选项。有关定价的信息，请参阅 Amazon S3 定价。

要进行 `Expedited`、`Standard` 或 `Bulk` 检索，请将 RestoreObject REST API 操作请求中的 `Tier` 请求元素设置为您需要的选项，或 Amazon Command Line Interface（Amazon CLI）或 Amazon SDK 中的等效选项。如果您购买了预配置容量，则所有加速检索都会通过您的预配置容量自动获得处理。

预调配容量

预调配容量的作用在于：当您从 S3 Glacier Flexible Retrieval 中进行加速检索时，它可帮助确保您在需要时获得检索容量。每个容量单位确保每 5 分钟至少可以执行 3 个加速检索，并提供高达 150MB/秒（MBps）的检索吞吐量。

如果您的工作负载要求在几分钟内对数据子集进行高度可靠和可预测的访问，应考虑购买预调配的检索容量。如果没有预配置容量，在高需求期间可能不会接受加速检索。如果您需要随时可以访问加速检索，建议您购买预配置检索容量。

预调配容量单位分配给 Amazon Web Services 账户。因此，加速数据检索的请求者（而不是桶拥有者）应购买预调配容量单位。

您可以使用 Amazon S3 控制台、Amazon S3 Glacier 控制台、购买预调配容量 REST API 操作、Amazon SDK 或 Amazon CLI 购买预调配容量。有关预调配容量的定价信息，请参阅 Amazon S3 定价。

S3 Glacier 还原启动请求速率

当您为存储在 S3 Glacier Flexible Retrieval 或 S3 Glacir Deep Archive 存储类中的对象启动还原请求时，将为您的 Amazon Web Services 账户应用检索请求限额。S3 Glacier 支持以每秒 1000 个事务的速率发出还原请求。如果超过此速率，则有效请求将受限制或被拒绝，而 Amazon S3 会返回 `ThrottlingException` 错误。

或者，您还可以使用 S3 批量操作通过单个请求检索存储在 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 中的大量对象。有关更多信息，请参阅 使用批量操作批量执行对象操作。

## 恢复已归档的对象

以下存储类或存储层中的 Amazon S3 对象已归档，无法实时访问：

- S3 Glacier Flexible Retrieval 存储类
- S3 Glacier Deep Archive 存储类
- S3 Intelligent-Tiering 归档访问层
- S3 Intelligent-Tiering 深度归档访问层

无法立即访问存储在 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储类中的 Amazon S3 对象。要访问这些存储类中的对象，您必须在指定的持续时间（天数）内将该对象的临时副本还原到其 S3 桶。如果您想要该对象的永久副本，请还原该对象，然后在 Amazon S3 桶中创建该对象的一个副本。Amazon S3 控制台不支持复制已还原的对象。对于这种类型的复制操作，请使用 Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 REST API。除非您制作副本并更改其存储类，否则对象仍将存储在 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储类中。有关使用这些存储类的信息，请参阅极少访问的对象的存储类。

要访问 S3 Intelligent-Tiering 归档访问层和深度归档访问层中的对象，您必须启动还原请求，并等待对象移动到频繁访问层。从归档访问层或深度归档访问层进行还原时，对象会转换回 频繁访问层中。有关使用这些存储类的信息，请参阅用于自动优化访问模式不断变化或未知的数据的存储类。

有关归档对象的一般信息，请参阅使用归档的对象。

> **Note**
>
> - 当您从 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储类还原存档对象时，您需要同时为存档对象和临时还原的副本付费。
> - 从 S3 Intelligent-Tiering 还原对象时，标准检索或批量检索不收取检索费用。
> - 对已还原的存档对象调用的后续还原请求将作为 GET 请求计费。有关定价的信息，请参阅 Amazon S3 定价。

恢复已归档的对象

您可以使用 Amazon S3 控制台、Amazon S3 REST API、Amazon SDK、Amazon Command Line Interface（Amazon CLI）或 S3 批量操作还原归档的对象。

使用 S3 控制台

使用 Amazon S3 控制台还原对象

使用以下过程还原已归档到 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储类或 S3 Intelligent-Tiering 归档访问或深度归档访问存储层的对象。

还原已归档的对象

1. 登录到Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在存储桶列表中，选择包含您想要还原的对象的存储桶的名称。
4. 在 Objects（对象）列表中，选择要还原的一个或多个对象，再选择 Actions（操作），然后选择 Initiate restore（启动还原）。
5. 如果要从 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 进行还原，请在还原的副本可用的天数框中输入您希望归档数据可供访问的天数。
6. 对于检索层，执行以下操作之一：

   - 选择批量检索或标准检索，然后选择启动还原。
   - 选择 Expedited retrieval（加急检索）（仅适用于 S3 Glacier Flexible Retrieval 或 S3 Intelligent-Tiering 归档访问）。如果您要还原 S3 Glacier Flexible Retrieval 中的对象，则可以

选择是否要购买预调配容量来进行加速检索。如果要购买预调配容量，请继续执行下一步。否则，请选择启动还原。

> **Note**
>
> S3 Intelligent-Tiering 归档访问层和深度归档访问层中的对象会自动还原到频繁访问层。

7. （可选）如果您要还原 S3 Glacier Flexible Retrieval 中的对象，并且您选择了加速检索，您可以选择是否购买预调配容量。预调配容量仅适用于 S3 Glacier Flexible Retrieval 中的对象。如果您已有预调配容量，请选择 启动还原以开始预调配检索。

   如果您有预调配容量，则您的预调配容量可处理您的所有加速检索。有关更多信息，请参阅 预调配容量。

   - 如果您没有预调配容量并且不想购买，请选择启动还原。
   - 如果您没有预调配容量，但要购买预调配容量单位（PCU），请选择购买 PCU。在购买 PCU 对话框中，选择要购买的 PCU 数量，确认购买，然后选择购买 PCU。在收到购买成功消息后，选择启动还原以开始预调配检索。

使用 Amazon CLI

从 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 还原对象

以下示例使用 `restore-object` 命令还原桶 *amzn-s3-demo-bucket* 中的对象 *dir1/example.obj*，时间为 25 天。

```
aws s3api restore-object --bucket amzn-s3-demo-bucket --key dir1/example.obj --restore-request '{"Days":25,"GlacierJobParameters":{"Tier":"Standard"}}'
```

如果示例中使用的 JSON 句法导致 Windows 客户端错误，则使用如下句法替换还原请求：

```
--restore-request Days=25,GlacierJobParameters={"Tier"="Standard"}
```

从 S3 Intelligent-Tiering 归档访问和深度归档访问还原对象

以下示例使用 `restore-object` 命令将桶 *amzn-s3-demo-bucket* 中的对象 *dir1/example.obj* 还原到频繁访问层

```
aws s3api restore-object --bucket amzn-s3-demo-bucket --key dir1/example.obj --restore-request '{}'
```

> **Note**
>
> 与 S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 存储类不同，S3 Intelligent-Tiering 对象的还原请求不接受该 `Days` 值。

监控还原状态

要监控 `restore-object` 请求的状态，请使用以下 `head-object` 命令：

```
aws s3api head-object --bucket amzn-s3-demo-bucket --key dir1/example.obj
```

有关更多信息，请参阅 Amazon CLI 命令参考 中的 restore-object。

使用 REST API

Amazon S3 向您提供了用于启动归档对象还原的 API 操作。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 RestoreObject。

使用 Amazon SDK

有关如何使用 Amazon SDK 还原 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 中的归档对象的示例，请参阅《Amazon S3 API 参考》中的 Code examples。

使用 S3 批量操作

要使用单个请求还原多个归档对象，您可以使用 S3 批量操作。您为 S3 批量操作提供要操作的对象列表。S3 批量操作调用相应的 API 操作来执行指定的操作。单个批量操作任务可对包含 EB 级数据的数十亿个对象执行指定操作。

要创建批量操作任务，您必须有一个仅包含要还原的对象的清单。您可以使用 S3 清单来创建清单，也可以提供包含必要信息的 CSV 文件。有关更多信息，请参阅 the section called “指定清单”。

在创建和运行 S3 批量操作任务之前，您必须向 Amazon S3 授予代表您执行 S3 批量操作的权限。有关所需的权限，请参阅the section called “授予权限”。

> **Note**
>
> 批量操作任务既可以在 S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 存储类对象上运行，也可以在 S3 Intelligent-Tiering 归档访问和深度归档访问存储层对象上运行。批量操作不能在同一个任务中对两种类型的归档对象进行操作。要还原两种类型的对象，必须创建单独的分批操作任务。
>
> 有关使用批量操作还原归档对象的更多信息，请参阅the section called “还原对象”。

创建 S3 启动还原对象批量操作任务

1. 登录到Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择批量操作。
3. 选择创建任务。
4. 对于 Amazon Web Services 区域，选择要在其中创建任务的区域。
5. 在清单格式下，请选择要使用的清单类型。
   - 如果您选择 S3 清单报告，请输入 Amazon S3 作为 CSV 格式清单报告的一部分生成的 `manifest.json` 对象的路径。如果要使用除最新版本之外的清单版本，请输入 `manifest.json` 对象的版本 ID。
   - 如果您选择 CSV，请输入 CSV 格式清单对象的路径。清单对象必须遵循控制台中描述的格式。如果要使用除最新版本之外的版本，则可以选择包含清单对象的版本 ID。
6. 选择下一步。
7. 在操作部分，选择还原。
8. 在还原部分，对于还原源，选择 Glacier Flexible Retrieval 或 Glacier Deep Archive 或 Intelligent-Tiering 归档访问层或深度归档访问层。

   如果您选择 Glacier Flexible Retrieval 或 Glacier Deep Archive，则为还原的副本可用的天数输入一个数字。

   对于检索层，选择要使用的层。
9. 选择下一步。
10. 在配置其他选项页面上，填写以下部分：

- 在其他选项部分，提供任务的描述并指定该任务的优先级编号。编号越大，优先级越高。有关更多信息，请参阅 the section called “分配任务优先级”。
- 在完成报告部分中，选择批量操作是否应创建完成报告。有关完成报告的更多信息，请参阅the section called “完成报告”。
- 在权限部分，您必须向 Amazon S3 授予代表您执行批量操作的权限。有关所需的权限，请参阅the section called “授予权限”。
- （可选）在任务标签部分，以键值对方式添加标签。有关更多信息，请参阅 the section called “使用标签”。

完成后，选择下一步。

11. 在 Review (审核) 页面上，验证设置。如果需要进行更改，请选择 Previous。否则，请选择创建任务。

有关批量操作的更多信息，请参阅使用批量操作还原对象和创建 S3 批量操作任务。

检查还原状态和到期日期

您可以使用 Amazon S3 控制台、Amazon S3 事件通知、Amazon CLI 或 Amazon S3 REST API 查看还原请求的状态或到期日期。

> **Note**
>
> 从 S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 存储类还原的对象仅存储您指定的天数。以下过程将返回这些副本的到期日期。
> 从 S3 Intelligent-Tiering 存档访问和深度存档访问存储层还原的对象没有到期日期，而是移回到频繁访问层。

使用 S3 控制台

在 Amazon S3 控制台中检查对象的还原状态和过期日期

1. 通过以下网址打开 Simple Storage Service（Amazon S3）控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在存储桶列表中，选择包含待还原对象的存储桶的名称。

4. 在对象列表中，选择要还原的对象。此时将显示对象的详细信息页面。

   - 如果还原未完成，则在页面顶部，您会看到一个部分显示正在还原。
   - 如果还原已完成，则在页面顶部，您会看到一个部分显示还原完成。如果您从 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 中进行还原，则此部分还会显示还原过期日期。在该日期，Amazon S3 将删除归档对象的已还原副本。

使用 Amazon S3 事件通知

通过使用 `s3:ObjectRestore:Completed` 操作与 Amazon S3 事件通知特征，您可以收到对象还原完成的通知。有关启用事件通知的更多信息，请参阅 Enabling notifications by using Amazon SQS, Amazon SNS, and Amazon Lambda。有关各种 `ObjectRestore` 事件类型的更多信息，请参阅the section called “SQS、SNS 和 Lambda 支持的事件类型”。

使用 Amazon CLI

使用 Amazon CLI 检查对象的还原状态和过期日期

以下示例使用 `head-object` 命令查看桶 *amzn-s3-demo-bucket* 中对象 *dir1/example.obj* 的元数据。当您对正在还原的对象运行此命令时，Amazon S3 会返回还原是否正在进行以及（如果适用）过期日期。

```
aws s3api head-object --bucket amzn-s3-demo-bucket --key dir1/example.obj
```

预期输出（还原正在进行中）：

```
{
    "Restore": "ongoing-request=\"true\"",
    "LastModified": "2020-06-16T21:55:22+00:00",
    "ContentLength": 405,
    "ETag": "\"b662d79adeb7c8d787ea7eafb9ef6207\"",
    "VersionId": "wbYaE2vtOV0iIBXrOqGAJt3fP1cHB8Wi",
    "ContentType": "binary/octet-stream",
    "ServerSideEncryption": "AES256",
    "Metadata": {},
    "StorageClass": "GLACIER"
}
```

预期输出（还原已完成）：

```
{
    "Restore": "ongoing-request=\"false\", expiry-date=\"Wed, 12 Aug 2020 00:00:00 GMT
\"",
    "LastModified": "2020-06-16T21:55:22+00:00",
    "ContentLength": 405,
    "ETag": "\"b662d79adeb7c8d787ea7eafb9ef6207\"",
    "VersionId": "wbYaE2vtOV0iIBXrOqGAJt3fP1cHB8Wi",
    "ContentType": "binary/octet-stream",
    "ServerSideEncryption": "AES256",
    "Metadata": {},
    "StorageClass": "GLACIER"
}
```

有关 `head-object` 的更多信息，请参阅《Amazon CLI 命令参考》中的 head-object。

使用 REST API

Amazon S3 提供了一个 API 操作供您检索对象元数据。要使用 REST API 检查归档对象的还原状态和过期日期，请参阅《Amazon Simple Storage Service API 参考》中的 HeadObject。

升级正在进行的还原的速度

在还原过程中，您可以升级还原的速度。

将正在进行的还原升级到更快的层级

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 在存储桶列表中，选择包含您想要还原的对象的桶的名称。
4. 在对象列表中，选择要还原的对象。此时将显示对象的详细信息页面。在对象的详细信息页面上，选择升级检索层。有关检查对象还原状态的信息，请参阅检查还原状态和到期日期。
5. 选择要升级到的层，然后选择启动还原。

# 管理对象的生命周期

S3 生命周期通过将对象转换到成本较低的存储类，或代表您删除到期的对象，协助您在对象的整个生命周期内经济高效地存储对象。要管理对象的生命周期，请为存储桶创建 S3 生命周期配置。S3 生命周期配置 是一组规则，用于定义 Amazon S3 对一组对象应用的操作。有两种类型的操作：

- Transition actions（转换操作）–这些操作将定义对象转换为另一个存储类的时间。例如，您可以选择在对象创建 30 天后将其转换为 S3 Standard-IA 存储类，或在对象创建 1 年后将其存档到 S3 Glacier 存储类。有关更多信息，请参阅 了解和管理 Amazon S3 存储类。

  存在与生命周期转换请求关联的成本。有关定价信息，请参阅 Amazon S3 定价。

- Expiration actions（过期操作）– 这些操作将定义对象的过期时间。Amazon S3 将代表您删除过期的对象。例如，您可能会选择在对象存储已达到监管合规期后使其到期。有关更多信息，请参阅 即将过期的对象。

  仅当您使存储期限最短的存储类中的对象过期时，才会产生与生命周期过期关联的潜在成本。有关更多信息，请参阅 最小存储持续时间收费。

> **Important**
>
> 通用存储桶：您不能使用存储桶策略来防止通过 S3 生命周期规则进行删除或转换。例如，即使您的存储桶策略拒绝所有主体的所有操作，您的 S3 生命周期配置也仍能正常发挥作用。

现有对象和新对象

当您向存储桶添加生命周期配置时，配置规则将应用到现有对象以及您在以后添加的对象。例如，如果您在今天添加带有过期操作的生命周期配置规则，而该规则使对象在创建 30 天后过期，Amazon S3 会将任何超过 30 天的现有对象加入移除队列。

账单的变化

如果在对象符合生命周期操作资格与 Amazon S3 转移或过期对象之间存在任何延迟，则在对象符合生命周期操作的资格后立即应用账单更改。例如，如果对象计划到期但 Amazon S3 没有立即使该对象到期，则不会在到期时间后向您收取存储费用。

此行为的一个例外情况是，如果您有一个生命周期规则转换为 S3 Intelligent-Tiering 存储类。在此类情况下，在对象转换为 S3 Intelligent-Tiering 存储类之前，账单不会发生更改。有关 S3 生命周期规则的更多信息，请参阅 生命周期配置元素。

> **Note**
>
> 生命周期转换不收取数据检索费用。但是，当使用 PUT、COPY 或生命周期规则将数据移至任何 S3 存储类时，将按请求收取摄取费用。在将对象移动到任何存储类之前，请考虑摄取或转换成本。有关成本考虑事项的更多信息，请参阅 Amazon S3 定价。

监控生命周期规则的影响

要监控由活动的生命周期规则进行的更新的效果，请参阅the section called “如何监控生命周期规则执行的操作？”。

## 管理对象的完整生命周期

利用 S3 生命周期配置规则，可以指示 Amazon S3 将对象转换到成本较低的存储类、将其归档或删除它们。例如：

- 如果您将定期日志上传到一个存储桶，您的应用程序可能需要使用这些日志一个星期或一个月。之后，您可能需要删除这些日志。
- 在限定的时间段内可能需要经常访问某些文档。自此之后，这些文档很少被访问。有时，您可能不需要对这些文档进行实时访问，但是您的组织或法规可能要求您将它们存档一段特定的时间。之后，您可以删除这些文档。
- 您可以主要为了存档目的而将一些类型的数据上传到 Amazon S3。例如，可以归档数字媒体、财务和健康记录、原始基因组序列数据、长期数据库备份，以及为遵从法规而必须保留的数据。

通过组合 S3 生命周期操作来管理对象的完整生命周期。例如，假设您创建了具有明确定义的生命周期的对象。最初，这些对象在 30 天的周期内可能被经常访问。紧接着，对象在长达 90 天内不常访问。之后，不再需要对象，您可能选择存档或删除对象。

在此方案中，您创建一个 S3 生命周期规则，用于指定到 S3 Intelligent-Tiering 、S3 Standard-IA 或 S3 One Zone-IA 存储的初始转换操作，并指定到用于存档的 S3 Glacier Flexible Retrieval 存储的另一个转换操作以及一个过期操作。在将对象从一个存储类移至另一个存储类时，可节省存储成本。有关成本考虑事项的更多信息，请参阅 Amazon S3 定价。

主题

- 使用 Amazon S3 生命周期转换对象
- 即将过期的对象

- 在存储桶上设置 S3 生命周期配置
- S3 生命周期如何与其它存储桶配置进行交互
- 配置 S3 生命周期事件通知
- 生命周期配置元素
- Amazon S3 如何处理生命周期配置中的冲突
- S3 生命周期配置的示例
- 排查 Amazon S3 生命周期问题

## 使用 Amazon S3 生命周期转换对象

可以向 S3 生命周期配置中添加转换操作，来指示 Amazon S3 将对象移到另一个 Amazon S3 存储类。有关存储类的更多信息，请参阅 了解和管理 Amazon S3 存储类。您何时可以以这种方式使用 S3 生命周期配置的一些示例包括以下内容：

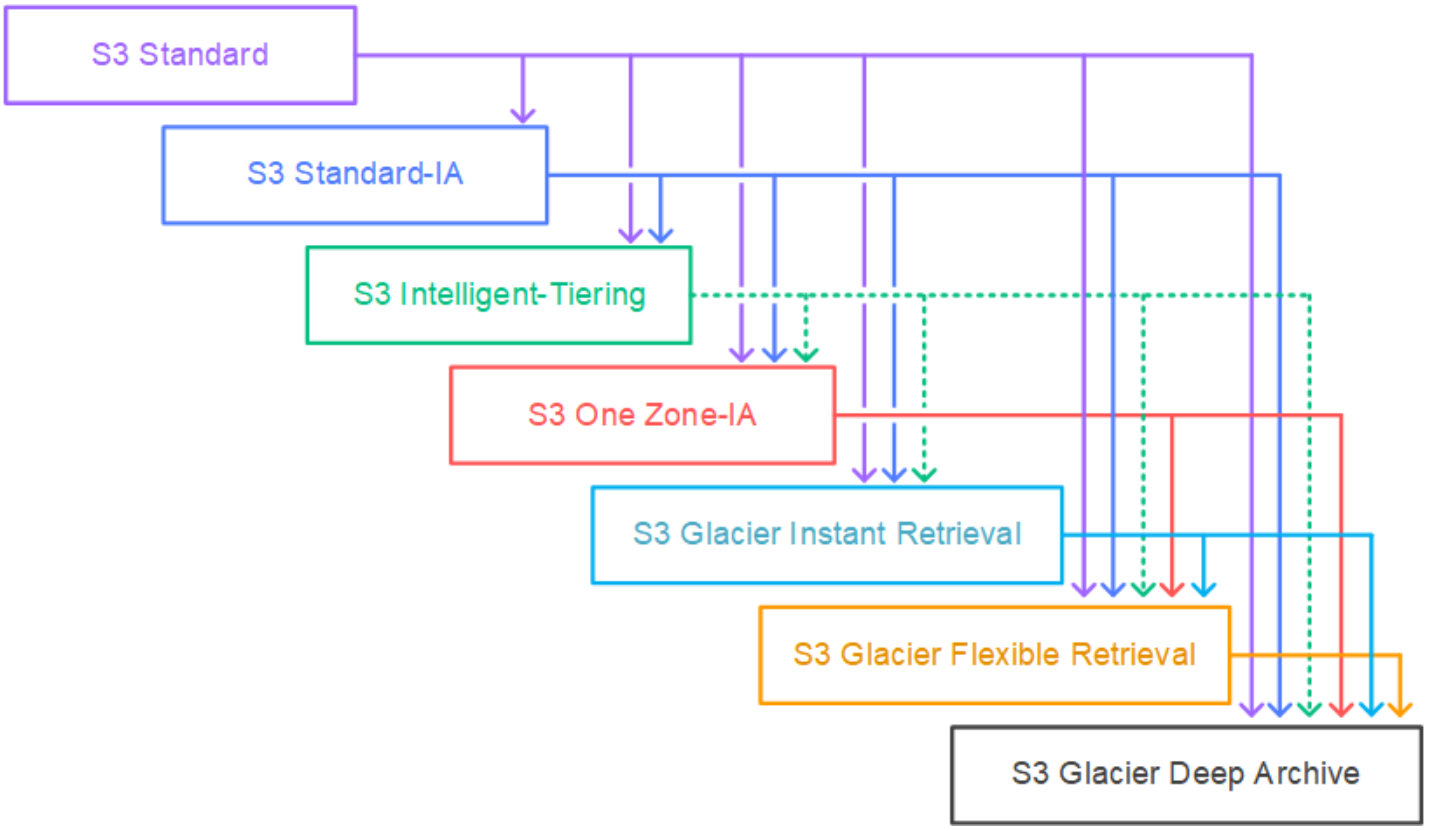
- 当您知道对象不常访问时，您可能会将其转换为 S3 Standard-IA 存储类。
- 您可能想要将不需要实时访问的对象归档到 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储类。

> **Note**
>
> 加密对象在整个存储类转换过程中保持加密状态。

### 支持的转换

在 S3 生命周期配置中，您可以定义用于将对象从一个存储类转换为另一个存储类的规则，以节省存储成本。如果您不了解对象的访问模式或访问模式不断变化，则可将对象转换为 S3 Intelligent-Tiering 存储类，以自动实现成本节省。有关存储类的信息，请参阅 了解和管理 Amazon S3 存储类。

Amazon S3 支持用于在存储类之间进行转换的瀑布模型，如下图所示。




支持的生命周期转换

Amazon S3 支持在使用 S3 生命周期配置的存储类之间进行以下生命周期转换。

- 从 S3 Standard 存储类转换为 S3 Standard-IA、S3 Intelligent-Tiering、S3 One Zone-IA、S3 Glacier Instant Retrieval、S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储类。
- 从 S3 Standard-IA 存储类转换为 S3 Intelligent-Tiering、S3 One Zone-IA、S3 Glacier Instant Retrieval、S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储类。
- S3 Intelligent-Tiering 存储类可以转换为不同的存储类，具体取决于 S3 Intelligent-Tiering 访问层。每个访问层都可以进行以下转换。
  - 从频繁访问层或不频繁访问层转换为 S3 One Zone-IA、S3 Glacier Instant Retrieval、S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储类。
  - 从归档即时访问层转换为 S3 Glacier Instant Retrieval、S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储类。
  - 从归档访问层转换为 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储类。
  - 从深度归档访问层转换为 S3 Glacier Deep Archive 存储类。
- 从 S3 One Zone-IA 存储类转换为 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储类。

- 从 S3 Glacier Instant Retrieval 存储类转换为 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储类。
- 从 S3 Glacier Flexible Retrieval 存储类转换为 S3 Glacier Deep Archive 存储类。

> **Note**
>
> 对于启用了版本控制或已暂停版本控制的存储桶，您无法转换具有 `Pending` 复制状态的对象。

## 转换的约束和注意事项

生命周期存储类转换具有以下约束：

默认情况下，小于 128 KB 的对象不会转换到任何存储类

Amazon S3 对 S3 生命周期配置应用默认行为，来防止将小于 128 KB 的对象转换到任何存储类。我们不建议转换小于 128 KB 的对象，因为会针对每个对象向您收取转换请求费用。这意味着，对于较小的对象，转换成本可能超过节省的存储成本。有关转换请求费用的更多信息，请参阅 Amazon S3 定价页面的存储和请求选项卡上的请求和数据检索。

要支持较小的对象进行转换，可以向生命周期转换规则中添加对象大小筛选条件，来指定自定义的最小大小 (`ObjectSizeGreaterThan`) 或最大大小 (`ObjectSizeLessThan`)。有关更多信息，请参阅 示例：支持转换小于 128 KB 的对象。

> **Note**
>
> 2024 年 9 月，Amazon S3 更新了小对象的默认转换行为，如下所示：
>
> - 更新了默认转换行为 — 从 2024 年 9 月起，默认行为禁止将小于 128 KB 的对象转换到任何存储类。
> - 之前的默认转换行为 — 在 2024 年 9 月之前，默认行为仅支持将小于 128 KB 的对象转换到 S3 Glacier 和 S3 Glacier Deep Archive 存储类。
>
> 2024 年 9 月之前创建的配置将保留之前的转换行为，除非您对其进行修改。也就是说，如果您创建、编辑或删除规则，则配置的默认转换行为会更改为更新的行为。如果用例需要，则可以更改默认转换行为，以便小于 128 KB 的对象将转换到 S3 Glacier 和 S3 Glacier

Deep Archive。为此，请在 PutBucketLifecycleConfiguration 请求中使用可选 `x-amz-transition-default-minimum-object-size` 标头。

对象必须存储至少达 30 天才能转换到 S3 Standard-IA 或 S3 One Zone-IA

在将对象转换为 S3 标准-IA 或 S3 单区-IA 之前，必须将它们存储在 Amazon S3 中至少达 30 天。例如，您无法创建用于在对象创建 1 天后将其转换为 S3 Standard-IA 存储类的生命周期规则。Amazon S3 在前 30 天内不支持此类转换，因为较新的对象的访问频率或删除速度通常高于适合 S3 标准-IA 或 S3 单区-IA 存储的值。

类似地，如果您在转换非当前对象（在受版本控制的存储桶中），则只能将至少在 30 天内是非当前版本的对象转换为 S3 Standard-IA 或 S3 One Zone-IA 存储。有关所有存储类的最短存储持续时间的列表，请参阅比较 Amazon S3 存储类。

在对象的最短存储持续时间之前转换对象需要付费

某些存储类具有最短对象存储持续时间。如果您在最短持续时间之前将对象从这些存储类中转换出来，则需要为该持续时间的剩余时间付费。有关哪些存储类具有最短存储持续时间的更多信息，请参阅比较 Amazon S3 存储类。

在最短存储持续时间到期之前，无法创建用于将对象从一种存储类转换到另一种存储类的单个生命周期规则。

例如，S3 Glacier Instant Retrieval 具有 90 天的最短存储持续时间。您无法指定这样一个生命周期规则：在 4 天后将对象转换到 S3 Glacier Instant Retrieval，然后在 20 天后将对象转换到 S3 Glacier Deep Archive。在这种情况下，S3 Glacier Deep Archive 转换必须在至少 94 天后才能进行。

可以指定两条规则来实现这一点，但需要支付最短持续时间的存储费用。有关成本考虑事项的更多信息，请参阅 Amazon S3 定价。

有关创建 S3 生命周期的更多信息，请参阅在存储桶上设置 S3 生命周期配置。

## 转换为 S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 存储类（对象存档）

通过使用 S3 生命周期配置，可以将对象转换为 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储类来进行存档。

在存档对象之前，请查看以下章节中的相关注意事项。

### 一般注意事项

下面是存档对象之前的一般注意事项：

- 加密对象在整个存储类转换过程中保持加密状态。
- 存储在 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储类中的对象无法实时可用。

  存档的对象是 Amazon S3 对象，但在您可以访问某个存档的对象之前，您必须首先恢复它的临时副本。根据您在还原请求内指定的持续时间，还原的对象副本仅在该期间内可用。在那之后，Amazon S3 将删除临时副本，并且对象将继续归档在 S3 Glacier Flexible Retrieval 中。

  您可以使用 Amazon S3 控制台还原对象，也可以在代码中使用 Amazon SDK 包装程序库或 Amazon S3 REST API 以编程方式还原对象。有关更多信息，请参阅 恢复已归档的对象。
- 存储在 S3 Glacier Flexible Retrieval 存储类中的对象只能转换为 S3 Glacier Deep Archive 存储类。

  您只能使用 S3 生命周期配置规则将对象的存储类从 S3 Glacier Flexible Retrieval 转换为 S3 Glacier Deep Archive 存储类。如果要将存储在 S3 Glacier Flexible Retrieval 中的对象的存储类更改为 S3 Glacier Deep Archive 以外的存储类，您必须首先使用还原操作制作该对象的临时副本。然后使用复制操作覆盖对象，并将 S3 Standard 、S3 Intelligent-Tiering 、S3 Standard-IA、S3 One Zone-IA 或低冗余指定为存储类。
- 对象到 S3 Glacier Deep Archive 存储类的转换只能是单向的。

  您无法使用 S3 生命周期配置规则将对象的存储类从 S3 Glacier Deep Archive 转换为任何其他存储类。如果要将已存档对象的存储类更改为其他存储类，您必须首先使用还原操作制作该对象的临时副本。然后使用复制操作覆盖对象，并将 S3 Standard、S3 Intelligent-Tiering、S3 Standard-IA、S3 One Zone-IA、S3 Glacier Instant Retrieval、S3 Glacier Flexible Retrieval 或 Reduced Redundancy Storage 或低冗余指定为存储类。

  > **Note**
  >
  > 在 Amazon S3 控制台中，对于 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储类中的对象，不支持对还原的对象执行复制操作。对于这种类型的复制操作，请使用 Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 REST API。

  存储在 S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 存储类中的对象仅通过 Amazon S3 可见和可用。它们不能通过单独的 Amazon S3 Glacier 服务进行使用。

这些是 Amazon S3 对象，您只能使用 Amazon S3 控制台或 Amazon S3 API 访问它们。您无法通过单独的 Amazon S3 Glacier 控制台或 Amazon S3 Glacier API 访问已存档的对象。

### 与成本相关的注意事项

如果您计划在数月或数年的时间内存档不经常访问的数据，则 S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 存储类可以降低您的存储成本。但是，为确保 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储类适合您，请考虑以下事项：

- 存储开销费用 – 将对象转换为 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 存储类时，需向每个对象添加固定存储量以容纳用于管理对象的元数据。
  - 对于存档到 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 的每个对象，Amazon S3 将 8 KB 存储用于对象的名称和其他元数据。Amazon S3 将存储此元数据，以便您可以使用 Amazon S3 API 获取已存档对象的实时列表。有关更多信息，请参阅获取存储桶（列出对象）。将按照 S3 Standard 标准费率对此附加存储收费。
  - 对于每个存档到 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 的对象，Amazon S3 添加 32 KB 的存储用于索引和相关元数据。标识和还原对象需要此额外数据。按照 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 费率对此附加存储收费。

  如果您打算存档小对象，请考虑这些存储费用。还可以考虑将许多小型对象合并为少量大型对象，以便减少开销成本。
- Number of days you plan to keep objects archived（计划归档对象的天数）– S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 是长期存档解决方案。S3 Glacier Flexible Retrieval 存储类的最短存储持续期间是 90 天，S3 Glacier Deep Archive 是 180 天。如果删除的对象的存档时间超过最短存储持续期间，则删除存档到 Amazon S3 Glacier 的数据是免费的。如果在最短持续期间内删除或覆盖存档的对象，则 Amazon S3 将收取按比例计算的提前删除费用。有关提前删除费用的信息，请参阅“删除存储在 Amazon S3 Glacier 中不足 90 天的对象时，如何收费？”问题（Amazon S3 常见问题）。
- S3 Glacier Flexible Retrieval and S3 Glacier Deep Archive transition request charges（S3 Glacier 和 S3 Glacier Deep Archive 转换请求费用）– 每个转换为 S3 Glacier 或 S3 Glacier Deep Archive 存储类的对象都构成一个转换请求。每个这类请求都有成本。如果您计划转换大量对象，则考虑这些请求费用。如果您归档的对象组合包括小对象，尤其是 128KB 以下的对象，我们建议您使用生命周期对象大小筛选条件从转换中筛选出小对象，以降低请求成本。
- S3 Glacier Flexible Retrieval and S3 Glacier Deep Archive data restore charges（S3 Glacier 和 S3 Glacier Deep Archive 数据还原费用）– S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 旨在用于长期存档您不经常访问的数据。有关数据还原费用的信息，请参阅“从 Amazon S3 Glacier 检

索数据如何收费？”问题（Amazon S3 常见问题）。有关如何从 Amazon S3 Glacier 还原数据的信息，请参阅恢复已归档的对象。

> **Note**
>
> S3 生命周期将对象异步转换到 S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive。S3 生命周期配置规则中的转换日期与实际转换日期之间可能存在延迟。在这种情况下，将根据在规则中指定的转换日期，按您从中转出的存储类的默认费率对您收费。

Amazon S3 产品详细信息页面针对存档 Amazon S3 对象提供了定价信息和示例计算。有关更多信息，请参阅以下主题：

- “将 Amazon S3 对象存档到 Amazon S3 Glacier 时，如何计算存储费用？”（Amazon S3 常见问题）。
- “删除存储在 Amazon S3 Glacier 中不足 90 天的对象时，如何收费？”（Amazon S3 常见问题）。
- “从 Amazon S3 Glacier 检索数据如何收费？”（Amazon S3 常见问题）。
- 针对不同存储类的存储成本的 Amazon S3 定价。

还原存档对象

无法实时访问已归档对象。您必须首先启动恢复请求，然后耐心等待，直到对象的临时副本根据您在请求中指定的持续时间变为可用。收到已还原对象的临时副本后，对象的存储类仍保持为 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive。（HeadObject 或 GetObject API 操作请求将返回 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 作为存储类。）

> **Note**
>
> 在还原某个归档时，您同时为归档（以 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 费率）和临时还原的副本（S3 Standard 存储费率）付费。有关定价的信息，请参阅 Amazon S3 定价。

您可以采用编程方式或使用 Amazon S3 控制台恢复对象副本。Amazon S3 针对每个对象每次仅处理一个还原请求。有关更多信息，请参阅 恢复已归档的对象。

# 即将过期的对象

可以向 S3 生命周期配置中添加转换操作，来指示 Amazon S3 在对象生命周期结束时删除对象。当对象根据其生命周期配置达到其生命周期结束时，Amazon S3 会根据存储桶所处的 S3 版本控制状态执行 Expiration 操作。

- 不受版本控制的存储桶 – Amazon S3 会将该对象加入移除队列并异步移除该对象，从而永久移除该对象。
- 受版本控制的存储桶 – 如果当前对象版本不是删除标记，Amazon S3 将添加具有唯一的版本 ID 的删除标记。这会使当前对象版本变为非当前版本，并使删除标记变为当前版本。
- 已暂停版本控制的存储桶 – Amazon S3 创建版本 ID 为 null 的删除标记。此删除标记会在版本层次结构中将任何对象版本替换为 null 版本 ID，从而实际上删除对象。

对于受版本控制的存储桶（也即，已启用版本控制或已暂停版本控制），有一些指导 Amazon S3 如何处理 Expiration 操作的注意事项。对于启用版本控制或暂停版本控制的存储桶，以下内容适用：

- 对象过期仅适用于对象的当前版本（它对非当前对象版本没有影响）。
- 如果有一个或多个对象版本，并且删除标记是当前版本，则 Amazon S3 不会执行任何操作。
- 如果当前对象版本是唯一的对象版本并且它还是删除标记（也称为过期对象删除标记，在这种情况下，所有对象版本都已删除，您只剩下一个删除标记），则 Amazon S3 将删除过期对象删除标记。还可以使用 Expiration 操作来指示 Amazon S3 移除所有到期对象删除标记。有关示例，请查看在启用了版本控制的存储桶中移除到期对象删除标记。
- 您可以使用 NoncurrentVersionExpiration 操作元素来指示 Amazon S3 何时永久删除对象的非当前版本。删除的对象无法恢复。您可以根据自对象变为非当前对象以来的一定天数来确定此到期日期。除了天数之外，还可以提供要保留的最大非当前版本数（介于 1 和 100 之间）。此值指定在 Amazon S3 可以对给定版本执行关联操作之前，必须存在多少较新的非当前版本。要指定最大非当前版本数量，您还必须提供 Filter 元素。如果您未指定 Filter 元素，Amazon S3 会在您提供最大数量的非当前版本时生成 InvalidRequest 错误。有关使用 NoncurrentVersionExpiration 操作元素的更多信息，请参阅the section called “用于描述生命周期操作的元素”。
- Amazon S3 不会对应用了 S3 对象锁定配置的非当前版本的对象采取任何操作。
- 对于具有 Pending 复制状态的对象，Amazon S3 不会对当前或非当前版本的对象采取任何操作。

有关更多信息，请参阅 使用 S3 版本控制保留对象的多个版本。

**Important**

当您在 S3 生命周期配置中有多个规则时，对象可能变得符合条件可在同一天执行多个 S3 生命周期操作。在这种情况下，Amazon S3 遵循以下一般规则：

- 永久删除优先于转换。
- 转换优先于删除标记的创建。
- 当对象符合条件可进行 S3 Glacier Flexible Retrieval 和 S3 Standard-IA（或 S3 One Zone-IA）转换时，Amazon S3 将选择 S3 Glacier Flexible Retrieval 转换。

有关示例，请参阅 重叠的筛选条件和冲突的生命周期操作的示例。

现有对象和新对象

当您向存储桶添加生命周期配置时，配置规则将应用到现有对象以及您在以后添加的对象。例如，如果您在今天添加带有过期操作的生命周期配置规则，而该规则使带有特定前缀的对象在创建 30 天后过期，Amazon S3 会将任何超过 30 天且具有指定前缀的现有对象加入移除队列。

**Important**

您不能使用存储桶策略来防止通过 S3 生命周期规则进行删除或转换。例如，即使您的存储桶策略拒绝所有主体的所有操作，您的 S3 生命周期配置也仍能正常发挥作用。

## 如何查找对象何时过期

要找出对象的当前版本计划到期的时间，请使用 HeadObject 或 GetObject API 操作。这些 API 操作返回的响应标头提供了对象的当前版本不再可供缓存的日期和时间。

**Note**

- 过期日期和 Amazon S3 删除对象的日期之间可能会有一段延迟。对象过期后，不会再向您收取相关的过期或存储时间费用。
- 在更新、禁用或删除生命周期规则之前，请使用 LIST API 操作（例如 ListObjectsV2、ListObjectVersions 和 ListMultipartUploads）或 使用 S3 清单对数据进行编目和分析，根据您的应用场景验证 Amazon S3 是否已转换符合条件的对象并使其到期。

### 最小存储持续时间收费

如果您创建的 S3 生命周期过期规则将促使在 S3 Standard-IA 或 S3 One Zone-IA 存储中存储不到 30 天的对象过期，则您需要支付 30 天的费用。如果您创建的生命周期过期规则将促使存储在 S3 Glacier Flexible Retrieval 存储中不到 90 天的对象过期，则您需要支付 90 天的费用。如果您创建的生命周期过期规则将促使存储在 S3 Glacier Deep Archive 存储中不到 180 天的对象过期，则您需要支付 180 天的费用。

有关更多信息，请参阅 Amazon S3 定价。

## 在存储桶上设置 S3 生命周期配置

可以使用 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 Amazon S3 REST API 在存储桶上设置 Amazon S3 生命周期配置。有关 S3 生命周期配置的信息，请参阅 管理对象的生命周期。

> **Note**
>
> 要查看或编辑目录存储桶的生命周期配置，请使用 Amazon CLI、Amazon SDK 或 Amazon S3 REST API。有关更多信息，请参阅 使用针对目录存储桶的 S3 生命周期。

在 S3 生命周期配置中，可以使用生命周期规则 来定义您希望 Amazon S3 在对象的生命周期内执行的操作。例如，您可以定义规则，来将对象转换到另一个存储类、归档对象或在指定时间段后使对象到期（将其删除）。

### S3 生命周期注意事项

在设置生命周期配置之前，请注意以下情况：

生命周期配置传播延时

将 S3 生命周期配置添加到存储桶时，在将新的或更新的生命周期配置完全传播到所有 Amazon S3 系统前通常存在一些滞后。在此配置完全生效之前，预计会有几分钟延迟。在删除 S3 生命周期配置时也可能出现这种延迟。

转换或到期延迟

从满足生命周期规则到规则操作完成之间会有延迟。例如，假设一组对象根据生命周期规则在 1 月 1 日到期。尽管已在 1 月 1 日满足到期规则，但 Amazon S3 可能要等到几天甚至几周后，才会真正删除这些对象。之所以出现这种延迟，是因为 S3 生命周期以异步方式将对象排入队列来执行转换或到期操

作。然而，当满足生命周期规则时，通常会应用账单的变化，即使操作尚未完成也是如此。有关更多信息，请参阅账单的变化。要监控由活动的生命周期规则进行的更新的效果，请参阅the section called “如何监控生命周期规则执行的操作？”

更新、禁用或删除生命周期规则

禁用或删除生命周期规则时，在短暂延迟后，Amazon S3 会停止安排新对象的删除或转换。已安排的任何对象都将被取消安排，并且不会被删除或转换。

> **Note**
>
> 在更新、禁用或删除生命周期规则之前，请使用 LIST API 操作（例如 ListObjectsV2、ListObjectVersions 和 ListMultipartUploads）或 使用 S3 清单对数据进行编目和分析，根据您的应用场景验证 Amazon S3 是否已转换符合条件的对象并使其到期。如果您在更新、禁用或删除生命周期规则时遇到任何问题，请参阅排查 Amazon S3 生命周期问题。

现有对象和新对象

当您向存储桶添加生命周期配置时，配置规则将应用到现有对象以及您在以后添加的对象。例如，如果您在今天添加带有过期操作的生命周期配置规则，而该规则使带有特定前缀的对象在创建 30 天后过期，Amazon S3 会将任何超过 30 天且具有指定前缀的现有对象加入移除队列。

监控生命周期规则的影响

要监控由活动的生命周期规则进行的更新的效果，请参阅the section called “如何监控生命周期规则执行的操作？”

账单的变化

当满足生命周期配置规则时，可能经过一些滞后才会触发相应的操作。但是，一旦满足生命周期配置规则，账单就会立即发生变化，无论是否执行操作。

例如，在对象到期后，即使没有立即删除对象，也不会向您收取存储费用。同样，只要对象转换时间一过，就会立即按照 S3 Glacier Flexible Retrieval 存储费率向您收费，即使没有立即将该对象转换为 S3 Glacier Flexible Retrieval 存储类也是如此。

但是，生命周期转换为 S3 Intelligent-Tiering 存储类是例外。在对象转换为 S3 Intelligent-Tiering 存储类之前，账单不会发生更改。

多个或相互冲突的规则

当您在 S3 生命周期配置中有多个规则时，对象可能变得符合条件可在同一天执行多个 S3 生命周期操作。在这种情况下，Amazon S3 遵循以下一般规则：

- 永久删除优先于转换。
- 转换优先于删除标记的创建。
- 当对象符合条件可进行 S3 Glacier Flexible Retrieval 和 S3 Standard-IA（或 S3 One Zone-IA）转换时，Amazon S3 将选择 S3 Glacier Flexible Retrieval 转换。

有关示例，请参阅 重叠的筛选条件和冲突的生命周期操作的示例。

## 如何设置 S3 生命周期配置

可以使用 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 Amazon S3 REST API 在通用存储桶上设置 Amazon S3 生命周期配置。

有关 Amazon CloudFormation 模板和示例的信息，请参阅《Amazon CloudFormation 用户指南》中的使用 Amazon CloudFormation 模板和 AWS::S3::Bucket。

### 使用 S3 控制台

您可以使用共享前缀（以通用字符串开头的对象名称）或标签为存储桶中的所有对象或一部分对象定义生命周期规则。在生命周期规则中，您可以定义特定于当前和非当前对象版本的操作。有关更多信息，请参阅下列内容：

- 管理对象的生命周期
- 使用 S3 版本控制保留对象的多个版本

### 创建生命周期规则

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在存储桶列表中，选择要为其创建生命周期规则的存储桶的名称。
4. 请选择 Management（管理）选项卡，然后选择 Create lifecycle rule（创建生命周期规则）。
5. 在 Lifecycle rule name (生命周期规则名称) 中，输入规则的名称。

   在该存储桶内，此名称必须是唯一的。
6. 请选择生命周期规则的范围：

- 要将此生命周期规则应用于所有带特定前缀或标签的对象，请选择将范围限制在特定前缀或标签。
  - 要按前缀限制范围，请在 Prefix (前缀) 中输入前缀。
  - 要按标签限制范围，请选择 Add tag (添加标签)，然后输入标签键和值。

  有关对象名称前缀的更多信息，请参阅 为 Amazon S3 对象命名。有关对象标签的更多信息，请参阅 使用标签对存储进行分类。
- 要将此生命周期规则应用于存储桶中的所有对象，请选择此规则适用于存储桶中的所有 对象，然后选择我确认此规则适用于存储桶中的所有对象。

7. 要按对象大小筛选规则，可以选择指定最小对象大小和/或指定最大对象大小选项。

   - 当您为最小对象大小或最大对象大小指定值时，该值必须大于 0 字节且不超过 5 TB。您可以以字节、KB、MB 或 GB 为单位指定此值。
   - 当您指定这两个值时，最大对象大小必须大于最小对象大小。

   > **Note**
   >
   > 最小对象大小和最大对象大小筛选条件不包含所指定的值。例如，如果您将筛选条件设置为使最小对象大小为 128 KB 的对象到期，则恰好为 128 KB 的对象不会到期。相反，该规则仅适用于大小超过 128 KB 的对象。

8. 在 Lifecycle rule actions (生命周期规则操作) 下，请选择希望生命周期规则执行的操作：

   - 在存储类之间转换对象的当前版本
   - 在存储类之间转换对象的先前版本
   - 使对象的当前版本过期

   > **Note**
   >
   > 对于未启用 S3 版本控制的存储桶，使当前版本到期会导致 Amazon S3 永久删除对象。有关更多信息，请参阅 the section called “生命周期操作与桶版本控制状态”。

   - 永久删除对象的先前版本
   - 删除过期的删除标记或未完成的分段上传

   根据您选择的操作，会显示不同的选项。

9. 要在存储类之间转换对象的当前 版本，请在在存储类之间转换对象的当前版本下，执行以下操作：

   a. 在存储类转换中，请选择要转换到的存储类。有关可能的转换的列表，请参阅the section called “支持的生命周期转换”。可从以下存储类中进行选择：

      - S3 标准 - IA
      - S3 智能分层
      - S3 单区 - IA
      - S3 Glacier Instant Retrieval
      - S3 Glacier Flexible Retrieval
      - S3 Glacier Deep Archive

   b. 在 Days after object creation (对象创建后的天数) 中，输入创建后转换对象的天数。

   有关存储类的更多信息，请参阅 了解和管理 Amazon S3 存储类。您可以为当前对象版本和/或之前的对象版本定义转换。版本控制允许您在一个存储桶中保留多个版本的对象。有关版本控制的更多信息，请参阅 使用 S3 控制台。

   > **Important**
   >
   > 如果选择 S3 Glacier Instant Retrieval、S3 Glacier Flexible Retrieval 或 Glacier Deep Archive 存储类，对象将保留在 Amazon S3 中。您无法直接通过单独的 Amazon S3 Glacier 服务访问它们。有关更多信息，请参阅 使用 Amazon S3 生命周期转换对象。

10. 要在存储类之间转换对象的非当前 版本，请在在存储类之间转换对象的非当前版本下，执行以下操作：

    a. 在存储类转换中，请选择要转换到的存储类。有关可能的转换的列表，请参阅the section called “支持的生命周期转换”。可从以下存储类中进行选择：

       - S3 标准 - IA
       - S3 智能分层
       - S3 单区 - IA
       - S3 Glacier Instant Retrieval
       - S3 Glacier Flexible Retrieval
       - S3 Glacier Deep Archive

b. 在对象成为非当前对象后的天数中，输入创建后转换对象的天数。

11. 要使对象的当前版本过期，请在 Expire current versions of objects（使对象的当前版本过期）下面的 Number of days after object creation（对象创建后的天数）中输入天数。

> **Important**
>
> 在不受版本控制的存储桶中，到期操作会导致 Amazon S3 永久移除该对象。有关生命周期操作的更多信息，请参阅 用于描述生命周期操作的元素。

12. 要永久删除对象的先前版本，请在 Permanently delete noncurrent versions of objects（永久删除对象的先前版本）下的 Days after objects become noncurrent（对象变为非当前对象后的天数）中输入天数。您可以选择在 Number of newer versions to retain（要保留的较新版本的数量）下输入一个值，从而指定要保留的较新版本数量。

13. 在 Delete expired delete markers or incomplete multipart uploads (删除过期的删除标记或未完成的分段上传) 下面，请选择 Delete expired object delete markers (删除过期对象的删除标记) 和 Delete incomplete multipart uploads (删除未完成的分段上传)。然后，输入您要在分段上传启动多少天后结束并清理未完成的分段上传。

    有关分段上传的更多信息，请参阅 在 Amazon S3 中使用分段上传来上传和复制对象。

14. 请选择 Create rule (创建规则)。

    如果规则没有任何错误，Amazon S3 会启用它，并且您可以在 Lifecycle rules (生命周期规则) 下的 Management (管理) 选项卡上看到它。

使用 Amazon CLI

您可以使用以下 Amazon CLI 命令管理 S3 生命周期配置：

- `put-bucket-lifecycle-configuration`
- `get-bucket-lifecycle-configuration`
- `delete-bucket-lifecycle`

有关设置 Amazon CLI 的说明，请参阅《Amazon S3 API 参考》中的 Developing with Amazon S3 using the Amazon CLI。

Amazon S3 生命周期配置是一个 XML 文件。但在使用 Amazon CLI 时，您不能指定 XML 格式。您必须改为指定 JSON 格式。以下是您可在 Amazon CLI 命令中指定的示例 XML 生命周期配置和等效 JSON 配置。

请考虑以下示例 S3 生命周期配置。

Example 示例 1

Example

XML

```
<LifecycleConfiguration>
    <Rule>
        <ID>ExampleRule</ID>
        <Filter>
           <Prefix>documents/</Prefix>
        </Filter>
        <Status>Enabled</Status>
        <Transition>
           <Days>365</Days>
           <StorageClass>GLACIER</StorageClass>
        </Transition>
        <Expiration>
             <Days>3650</Days>
        </Expiration>
    </Rule>
</LifecycleConfiguration>
```

JSON

```
{
    "Rules": [
        {
            "Filter": {
                "Prefix": "documents/"
            },
            "Status": "Enabled",
            "Transitions": [
                {
                    "Days": 365,
                    "StorageClass": "GLACIER"
```

```
                }
            ],
            "Expiration": {
                "Days": 3650
            },
            "ID": "ExampleRule"
        }
    ]
}
```

Example 示例 2

Example

XML

```
<LifecycleConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    <Rule>
        <ID>id-1</ID>
        <Expiration>
            <Days>1</Days>
        </Expiration>
        <Filter>
            <And>
                <Prefix>myprefix</Prefix>
                <Tag>
                    <Key>mytagkey1</Key>
                    <Value>mytagvalue1</Value>
                </Tag>
                <Tag>
                    <Key>mytagkey2</Key>
                    <Value>mytagvalue2</Value>
                </Tag>
            </And>
        </Filter>
        <Status>Enabled</Status>
    </Rule>
</LifecycleConfiguration>
```

JSON

```
{
    "Rules": [
        {
            "ID": "id-1",
            "Filter": {
                "And": {
                    "Prefix": "myprefix",
                    "Tags": [
                        {
                            "Value": "mytagvalue1",
                            "Key": "mytagkey1"
                        },
                        {
                            "Value": "mytagvalue2",
                            "Key": "mytagkey2"
                        }
                    ]
                }
            },
            "Status": "Enabled",
            "Expiration": {
                "Days": 1
            }
        }
    ]
}
```

您可以测试 put-bucket-lifecycle-configuration，如下所示。

测试配置

1. 将 JSON 生命周期配置保存在一个文件（例如 *lifecycle.json*）中。
2. 运行以下 Amazon CLI 命令以在存储桶上设置生命周期配置。将 *user input placeholders* 替换为您自己的信息。

```
$ aws s3api put-bucket-lifecycle-configuration  \
--bucket amzn-s3-demo-bucket  \
--lifecycle-configuration file://lifecycle.json
```

3. 要进行验证，请使用 `get-bucket-lifecycle-configuration` Amazon CLI 命令检索 S3 生命周期配置，如下所示：

```
$ aws s3api get-bucket-lifecycle-configuration  \
--bucket amzn-s3-demo-bucket
```

4. 要删除 S3 生命周期配置，请使用 `delete-bucket-lifecycle` Amazon CLI 命令，如下所示：

```
aws s3api delete-bucket-lifecycle \
--bucket amzn-s3-demo-bucket
```

使用 Amazon SDK

Java

您可以使用 适用于 Java 的 Amazon SDK 管理存储桶的 S3 生命周期配置。有关管理 S3 生命周期配置的更多信息，请参阅 管理对象的生命周期。

> **Note**
>
> 在将 S3 生命周期配置添加到存储桶时，Amazon S3 会替换存储桶的当前生命周期配置（如果有）。要更新一个配置，请检索它，进行所需的更改，然后向存储桶添加已修订的配置。

以下示例说明如何使用 适用于 Java 的 Amazon SDK 添加、更新和删除存储桶的生命周期配置。本示例执行以下操作：

- 向存储桶添加生命周期配置。
- 检索生命周期配置并通过添加其他规则来更新该配置。
- 向存储桶添加已修改的生命周期配置。Amazon S3 将替换现有配置。
- 再次检索配置，并通过输出规则数来验证它是否具有正确数量的规则。
- 删除生命周期配置并通过再次尝试检索它来验证它是否已被删除。

有关创建和测试有效示例的说明，请参阅《适用于 Java 的 Amazon SDK 开发人员指南》中的 Getting Started。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.BucketLifecycleConfiguration;
import com.amazonaws.services.s3.model.BucketLifecycleConfiguration.Transition;
import com.amazonaws.services.s3.model.StorageClass;
import com.amazonaws.services.s3.model.Tag;
import com.amazonaws.services.s3.model.lifecycle.LifecycleAndOperator;
import com.amazonaws.services.s3.model.lifecycle.LifecycleFilter;
import com.amazonaws.services.s3.model.lifecycle.LifecyclePrefixPredicate;
import com.amazonaws.services.s3.model.lifecycle.LifecycleTagPredicate;

import java.io.IOException;
import java.util.Arrays;

public class LifecycleConfiguration {

        public static void main(String[] args) throws IOException {
                Regions clientRegion = Regions.DEFAULT_REGION;
                String bucketName = "*** Bucket name ***";

                // Create a rule to archive objects with the "glacierobjects/"
 prefix to Glacier
                // immediately.
                BucketLifecycleConfiguration.Rule rule1 = new
 BucketLifecycleConfiguration.Rule()
                                .withId("Archive immediately rule")
                                .withFilter(new LifecycleFilter(new
 LifecyclePrefixPredicate("glacierobjects/")))
                                .addTransition(new
 Transition().withDays(0).withStorageClass(StorageClass.Glacier))
                                .withStatus(BucketLifecycleConfiguration.ENABLED);

                // Create a rule to transition objects to the Standard-Infrequent
 Access storage
                // class
                // after 30 days, then to Glacier after 365 days. Amazon S3 will
 delete the
                // objects after 3650 days.
                // The rule applies to all objects with the tag "archive" set to
 "true".
```

```
                BucketLifecycleConfiguration.Rule rule2 = new
BucketLifecycleConfiguration.Rule()
                                .withId("Archive and then delete rule")
                                .withFilter(new LifecycleFilter(new
LifecycleTagPredicate(new Tag("archive", "true"))))
                                .addTransition(new Transition().withDays(30)

.withStorageClass(StorageClass.StandardInfrequentAccess))
                                .addTransition(new
Transition().withDays(365).withStorageClass(StorageClass.Glacier))
                                .withExpirationInDays(3650)
                                .withStatus(BucketLifecycleConfiguration.ENABLED);

                // Add the rules to a new BucketLifecycleConfiguration.
                BucketLifecycleConfiguration configuration = new
BucketLifecycleConfiguration()
                                .withRules(Arrays.asList(rule1, rule2));

                try {
                        AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                                        .withCredentials(new
ProfileCredentialsProvider())
                                        .withRegion(clientRegion)
                                        .build();

                        // Save the configuration.
                        s3Client.setBucketLifecycleConfiguration(bucketName,
configuration);

                        // Retrieve the configuration.
                        configuration =
s3Client.getBucketLifecycleConfiguration(bucketName);

                        // Add a new rule with both a prefix predicate and a tag
predicate.
                        configuration.getRules().add(new
BucketLifecycleConfiguration.Rule().withId("NewRule")
                                        .withFilter(new LifecycleFilter(new
LifecycleAndOperator(
                                                        Arrays.asList(new
LifecyclePrefixPredicate("YearlyDocuments/"),
                                                                        new
LifecycleTagPredicate(new Tag(
```

```
   "expire_after",

   "ten_years"))))))
                                        .withExpirationInDays(3650)

.withStatus(BucketLifecycleConfiguration.ENABLED));

                        // Save the configuration.
                        s3Client.setBucketLifecycleConfiguration(bucketName,
configuration);

                        // Retrieve the configuration.
                        configuration =
s3Client.getBucketLifecycleConfiguration(bucketName);

                        // Verify that the configuration now has three rules.
                        configuration =
s3Client.getBucketLifecycleConfiguration(bucketName);
                        System.out.println("Expected # of rules = 3; found: " +
configuration.getRules().size());

                        // Delete the configuration.
                        s3Client.deleteBucketLifecycleConfiguration(bucketName);

                        // Verify that the configuration has been deleted by
attempting to retrieve it.
                        configuration =
s3Client.getBucketLifecycleConfiguration(bucketName);
                        String s = (configuration == null) ? "No configuration
found." : "Configuration found.";
                        System.out.println(s);
                } catch (AmazonServiceException e) {
                        // The call was transmitted successfully, but Amazon S3
couldn't process
                        // it, so it returned an error response.
                        e.printStackTrace();
                } catch (SdkClientException e) {
                        // Amazon S3 couldn't be contacted for a response, or the
client
                        // couldn't parse the response from Amazon S3.
                        e.printStackTrace();
                }
        }
```

```
}
```

.NET

您可以使用 适用于 .NET 的 Amazon SDK 管理存储桶上的 S3 生命周期配置。有关管理生命周期配置的更多信息，请参阅 管理对象的生命周期。

> **Note**
>
> 在添加生命周期配置时，Amazon S3 将替换指定存储桶上的现有配置。要更新配置，您必须先检索生命周期配置，进行更改，然后向存储桶添加已修订的生命周期配置。

以下示例说明如何使用 适用于 .NET 的 Amazon SDK 添加、更新和删除存储桶的生命周期配置。该代码示例执行以下操作：

- 向存储桶添加生命周期配置。
- 检索生命周期配置并通过添加其他规则来更新该配置。
- 向存储桶添加已修改的生命周期配置。Amazon S3 将替换现有生命周期配置。
- 再次检索配置并通过输出配置中的规则数进行验证。
- 删除生命周期配置并确认删除操作。

有关设置和运行代码示例的信息，请参阅《适用于 .NET 的 Amazon SDK 开发人员指南》中的 Getting Started with the 适用于 .NET 的 Amazon SDK。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class LifecycleTest
    {
        private const string bucketName = "*** bucket name ***";
        // Specify your bucket region (an example region is shown).
```

```
        private static readonly RegionEndpoint bucketRegion =
RegionEndpoint.USWest2;
        private static IAmazonS3 client;
        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            AddUpdateDeleteLifecycleConfigAsync().Wait();
        }

        private static async Task AddUpdateDeleteLifecycleConfigAsync()
        {
            try
            {
                var lifeCycleConfiguration = new LifecycleConfiguration()
                {
                    Rules = new List<LifecycleRule>
                        {
                            new LifecycleRule
                            {
                                 Id = "Archive immediately rule",
                                 Filter = new LifecycleFilter()
                                 {
                                     LifecycleFilterPredicate = new
LifecyclePrefixPredicate()
                                     {
                                         Prefix = "glacierobjects/"
                                     }
                                 },
                                 Status = LifecycleRuleStatus.Enabled,
                                 Transitions = new List<LifecycleTransition>
                                 {
                                      new LifecycleTransition
                                      {
                                           Days = 0,
                                           StorageClass = S3StorageClass.Glacier
                                      }
                                  },
                            },
                            new LifecycleRule
                            {
                                 Id = "Archive and then delete rule",
                                  Filter = new LifecycleFilter()
                                 {
```

```
                                    LifecycleFilterPredicate = new
LifecyclePrefixPredicate()
                                    {
                                        Prefix = "projectdocs/"
                                    }
                                },
                                Status = LifecycleRuleStatus.Enabled,
                                Transitions = new List<LifecycleTransition>
                                {
                                     new LifecycleTransition
                                     {
                                          Days = 30,
                                          StorageClass =
S3StorageClass.StandardInfrequentAccess
                                     },
                                     new LifecycleTransition
                                     {
                                       Days = 365,
                                       StorageClass = S3StorageClass.Glacier
                                     }
                                },
                                Expiration = new LifecycleRuleExpiration()
                                {
                                      Days = 3650
                                }
                            }
                        }
                };

                // Add the configuration to the bucket.
                await AddExampleLifecycleConfigAsync(client,
lifeCycleConfiguration);

                // Retrieve an existing configuration.
                lifeCycleConfiguration = await RetrieveLifecycleConfigAsync(client);

                // Add a new rule.
                lifeCycleConfiguration.Rules.Add(new LifecycleRule
                {
                    Id = "NewRule",
                    Filter = new LifecycleFilter()
                    {
                        LifecycleFilterPredicate = new LifecyclePrefixPredicate()
                        {
```

```
                            Prefix = "YearlyDocuments/"
                        }
                    },
                    Expiration = new LifecycleRuleExpiration()
                    {
                        Days = 3650
                    }
                });

                // Add the configuration to the bucket.
                await AddExampleLifecycleConfigAsync(client,
lifeCycleConfiguration);

                // Verify that there are now three rules.
                lifeCycleConfiguration = await RetrieveLifecycleConfigAsync(client);
                Console.WriteLine("Expected # of rulest=3; found:{0}",
lifeCycleConfiguration.Rules.Count);

                // Delete the configuration.
                await RemoveLifecycleConfigAsync(client);

                // Retrieve a nonexistent configuration.
                lifeCycleConfiguration = await RetrieveLifecycleConfigAsync(client);

            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered ***. Message:'{0}' when writing
an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
        }

        static async Task AddExampleLifecycleConfigAsync(IAmazonS3 client,
LifecycleConfiguration configuration)
        {

            PutLifecycleConfigurationRequest request = new
PutLifecycleConfigurationRequest
            {
```

```
                BucketName = bucketName,
                Configuration = configuration
            };
            var response = await client.PutLifecycleConfigurationAsync(request);
        }

        static async Task<LifecycleConfiguration>
 RetrieveLifecycleConfigAsync(IAmazonS3 client)
        {
            GetLifecycleConfigurationRequest request = new
 GetLifecycleConfigurationRequest
            {
                BucketName = bucketName
            };
            var response = await client.GetLifecycleConfigurationAsync(request);
            var configuration = response.Configuration;
            return configuration;
        }

        static async Task RemoveLifecycleConfigAsync(IAmazonS3 client)
        {
            DeleteLifecycleConfigurationRequest request = new
 DeleteLifecycleConfigurationRequest
            {
                BucketName = bucketName
            };
            await client.DeleteLifecycleConfigurationAsync(request);
        }
    }
}
```

Ruby

可以使用适用于 Ruby 的 Amazon SDK 通过 AWS::S3::BucketLifecycleConfiguration 类来管理存储桶上的 S3 生命周期配置。有关管理 S3 生命周期配置的更多信息，请参阅 管理对象的生命周期。

使用 REST API

《Amazon Simple Storage Service API 参考》中的以下主题描述了与 S3 生命周期配置相关的 REST API 操作：

- PutBucketLifecycleConfiguration

- GetBucketLifecycleConfiguration
- DeleteBucketLifecycle

### S3 生命周期问题排查

有关使用 S3 生命周期时可能出现的常见问题，请参阅the section called “排查生命周期问题”。

## S3 生命周期如何与其它存储桶配置进行交互

除了 S3 生命周期配置之外，您还可以将其他配置与存储桶关联。本部分解释了 S3 生命周期配置如何与其他存储桶配置相关。

### S3 生命周期和 S3 版本控制

您可以向不受版本控制的存储桶和启用了版本控制的存储桶添加 S3 生命周期配置。有关更多信息，请参阅 使用 S3 版本控制保留对象的多个版本。

启用了版本控制的存储桶会维护一个当前对象版本，以及零个或零个以上非当前对象版本。可以为当前和非当前对象版本定义单独的生命周期规则。

有关更多信息，请参阅 生命周期配置元素。

> **Important**
>
> 当您在 S3 生命周期配置中有多个规则时，对象可能变得符合条件可在同一天执行多个 S3 生命周期操作。在这种情况下，Amazon S3 遵循以下一般规则：
>
> - 永久删除优先于转换。
> - 转换优先于删除标记的创建。
> - 当对象有资格进行 S3 Glacier Flexible Retrieval 和 S3 Standard-IA（或 S3 One Zone-IA）转换时，Amazon S3 将选择 S3 Glacier Flexible Retrieval 转换。
>
> 有关示例，请参阅 重叠的筛选条件和冲突的生命周期操作的示例。

### 启用了 MFA 的存储桶上的 S3 生命周期配置

为删除 MFA 而配置的多重身份验证存储桶上不支持 S3 生命周期配置。有关更多信息，请参阅 配置 MFA 删除。

## S3 生命周期和日志记录

Amazon CloudTrail 对象级别日志记录不捕获 Amazon S3 生命周期操作。CloudTrail 捕获向外部 Amazon S3 端点发出的 API 请求，而 S3 生命周期操作通过使用内部 Amazon S3 端点来执行。

可以在 S3 存储桶中启用 Amazon S3 服务器访问日志，来捕获与 S3 生命周期相关的操作，例如，对象转换为另一个存储类以及对象到期（这会导致永久删除或逻辑删除）。有关更多信息，请参阅 the section called “记录服务器访问”。

如果您在存储桶上启用了日志记录，Amazon S3 服务器访问日志会报告以下操作的结果。

| 操作日志 | 描述 |
| --- | --- |
| S3.EXPIRE.OBJECT | Amazon S3 由于生命周期 Expiration 操作而永久删除对象。 |
| S3.CREATE.DELETEMARKER | Amazon S3 通过在启用版本控制的存储桶中添加删除标记，来在逻辑上删除当前版本。 |
| S3.TRANSITION_SIA.OBJECT | Amazon S3 将对象转换为 S3 Standard-IA 存储类。 |
| S3.TRANSITION_ZIA.OBJECT | Amazon S3 将对象转换为 S3 One Zone-IA 存储类。 |
| S3.TRANSITION_INT.OBJECT | Amazon S3 将对象转换为 S3 Intelligent-Tiering 存储类。 |
| S3.TRANSITION_GIR.OBJECT | Amazon S3 启动将对象转换为 S3 Glacier Instant Retrieval 存储类的过程。 |
| S3.TRANSITION.OBJECT | Amazon S3 启动将对象转换为 S3 Glacier Flexible Retrieval 存储类的过程。 |
| S3.TRANSITION_GDA.OBJECT | Amazon S3 启动将对象转换为 S3 Glacier Deep Archive 存储类的过程。 |
| S3.DELETE.UPLOAD | Amazon S3 中止未完成的分段上传。 |

> **Note**
>
> Amazon S3 服务器访问日志记录会尽最大努力记录信息，但不能用于完整记录所有 Amazon S3 请求。

## 配置 S3 生命周期事件通知

要在 Amazon S3 删除对象或因遵循 S3 生命周期规则而将对象转换为另一个 Amazon S3 存储类时接收通知，可以设置 Amazon S3 事件通知。

您可以收到以下 S3 生命周期事件的通知：

- 转换事件 – 通过使用 `s3:LifecycleTransition` 事件类型，当对象按照 S3 生命周期配置从一个 Amazon S3 存储类转换到另一个存储类时，您可以收到通知。
- 到期（删除）事件 – 通过使用 `LifecycleExpiration` 事件类型，每当 Amazon S3 基于 S3 生命周期配置删除对象时，您都可以收到通知。

  有两种到期事件类型：

  - 当删除不受版本控制的存储桶中的对象时，`s3:LifecycleExpiration:Delete` 事件类型会通知您。当 S3 生命周期配置永久删除对象版本时，`s3:LifecycleExpiration:Delete` 也会通知您。
  - 在删除受版本控制的存储桶中对象的当前版本后，如果 S3 生命周期创建删除标记，`s3:LifecycleExpiration:DeleteMarkerCreated` 事件类型会通知您。有关更多信息，请参阅 the section called “删除对象版本”。

Amazon S3 可以将事件通知发布到 Amazon Simple Notification Service (Amazon SNS) 主题、Amazon Simple Queue Service (Amazon SQS) 队列或 Amazon Lambda 函数。有关更多信息，请参阅 Amazon S3 事件通知。

有关如何配置 Amazon S3 事件通知的说明，请参阅使用 Amazon SQS、Amazon SNS 和 Amazon Lambda 启用事件通知。

以下是 Amazon S3 发送以发布 `s3:LifecycleExpiration:Delete` 事件的消息示例。有关更多信息，请参阅 the section called “事件消息结构”。

```
{
   "Records":[
```

```
      {
         "eventVersion":"2.3",
         "eventSource":"aws:s3",
         "awsRegion":"us-west-2",
         "eventTime":"1970-01-01T00:00:00.000Z",
         "eventName":"LifecycleExpiration:Delete",
         "userIdentity":{
            "principalId":"s3.amazonaws.com"
         },
         "requestParameters":{
            "sourceIPAddress":"s3.amazonaws.com"
         },
         "responseElements":{
            "x-amz-request-id":"C3D13FE58DE4C810",
            "x-amz-id-2":"FMyUVURIY8/IgAtTv8xRjskZQpcIZ9KG4V5Wp6S7S/
JRWeUWerMUE5JgHvANOjpD"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"testConfigRule",
            "bucket":{
               "name":"amzn-s3-demo-bucket",
               "ownerIdentity":{
                  "principalId":"A3NL1KOZZKExample"
               },
               "arn":"arn:aws:s3:::amzn-s3-demo-bucket"
            },
            "object":{
               "key":"expiration/delete",
               "sequencer":"0055AED6DCD90281E5",
            }
         }
      }
   ]
}
```

Amazon S3 为发布 `s3:LifecycleTransition` 事件而发送的消息中还包括以下信息：

```
"lifecycleEventData":{
    "transitionEventData": {
        "destinationStorageClass": the destination storage class for the object
    }
}
```

# 生命周期配置元素

S3 生命周期配置由生命周期规则组成，这些规则包括各种元素，而这些元素描述 Amazon S3 在对象生命周期内执行的操作。可以将 Amazon S3 生命周期配置指定为 XML，该配置包含一个或多个生命周期规则，其中每个规则由一个或多个元素组成。

```
<LifecycleConfiguration>
    <Rule>
         <Element>
    </Rule>
    <Rule>
         <Element>
         <Element>
    </Rule>
</LifecycleConfiguration>
```

每个规则由以下内容组成：

- 规则元数据，包含规则 ID 以及指示规则是已启用还是已禁用的状态。如果规则处于禁用状态，则 Amazon S3 不会执行规则中指定的任何操作。
- 标识规则应用到的对象的筛选条件。您可以通过使用对象大小、对象键前缀、一个或多个对象标签或者筛选条件的组合来指定筛选条件。
- 您希望 Amazon S3 执行指定操作时的一个或多个转换或过期操作，带有位于对象的生命周期内的日期或时间段。

主题


- ID 元素
- Status 元素
- Filter 元素
- 用于描述生命周期操作的元素
- 将筛选条件添加到生命周期规则


以下部分介绍了 S3 生命周期配置中的 XML 元素。有关示例配置，请参阅 S3 生命周期配置的示例。

### ID 元素

一个 S3 生命周期配置最多可以有 1000 个规则。此限制不可调整。<ID> 元素唯一地标识规则。ID 长度最多为 255 个字符。

### Status 元素

<Status> 元素值可以是 Enabled 或 Disabled。如果规则处于禁用状态，则 Amazon S3 不会执行规则中定义的任何操作。

### Filter 元素

S3 生命周期规则可以根据您在规则中指定的 <Filter> 元素，应用于存储桶中的所有对象或一部分对象。

您可以按键前缀、对象标签或二者的组合（在此情况下，Amazon S3 使用逻辑 AND 组合筛选条件）筛选对象。有关筛选条件的示例和更多信息，请参阅将筛选条件添加到生命周期规则。

- 使用键前缀指定筛选条件 – 此示例显示一个 S3 生命周期规则，此规则基于键名前缀（logs/）应用于一部分对象。例如，此生命周期规则应用于对象 logs/mylog.txt、logs/temp1.txt 和 logs/test.txt。此规则不应用于对象 example.jpg。

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
           <Prefix>logs/</Prefix>
        </Filter>
        transition/expiration actions
         ...
    </Rule>
    ...
</LifecycleConfiguration>
```

如果您要基于不同的键名称前缀将生命周期操作应用于一部分对象，可指定单独的规则。在每个规则中，指定基于前缀的筛选条件。例如，要描述具有键前缀 projectA/ 和 projectB/ 的对象的生命周期操作，可指定两个规则，如下所示：

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
           <Prefix>projectA/</Prefix>
```

```
        </Filter>
        transition/expiration actions
         ...
    </Rule>

    <Rule>
        <Filter>
           <Prefix>projectB/</Prefix>
        </Filter>
        transition/expiration actions
         ...
    </Rule>
</LifecycleConfiguration>
```

有关对象键的更多信息，请参阅 为 Amazon S3 对象命名。

- 指定基于对象标签的筛选条件 – 在以下示例中，此生命周期规则指定基于标签（*key*）和值（*value*）的筛选条件。随后，此规则仅应用于具有特定标签的一部分对象。

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
           <Tag>
              <Key>key</Key>
              <Value>value</Value>
           </Tag>
        </Filter>
        transition/expiration actions
        ...
    </Rule>
</LifecycleConfiguration>
```

您可以指定基于多个标签的筛选条件。您必须在 <And> 元素中包含标签，如以下示例所示。此规则指示 Amazon S3 对具有两个标签（带特定的标签键和值）的对象执行生命周期操作。

```
<LifecycleConfiguration>
    <Rule>
      <Filter>
         <And>
            <Tag>
               <Key>key1</Key>
               <Value>value1</Value>
```

```
            </Tag>
            <Tag>
               <Key>key2</Key>
               <Value>value2</Value>
            </Tag>
             ...
          </And>
      </Filter>
      transition/expiration actions
    </Rule>
</Lifecycle>
```

此生命周期规则应用于具有指定的两个标签的对象。Amazon S3 执行逻辑 AND。请注意以下几点：

- 每个标签的键和值都 必须完全匹配。如果您只指定 <Key> 元素而不指定 <Value> 元素，则该规则将仅应用于与标签键匹配而未 指定值的对象。
- 此规则应用于具有规则中指定的所有标签的一部分对象。如果某个对象指定了其他标签，则该规则仍将适用。

> **Note**
>
> 当您在筛选条件中指定多个标签时，每个标签键必须是唯一的。

- 指定基于前缀和一个或多个标签的筛选条件 – 在生命周期规则中，您可以指定基于键前缀和一个或多个标签的筛选条件。同样，您必须在 <And> 元素中包含所有这些筛选条件元素，如下所示：

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
          <And>
             <Prefix>key-prefix</Prefix>
             <Tag>
                <Key>key1</Key>
                <Value>value1</Value>
             </Tag>
             <Tag>
                <Key>key2</Key>
                <Value>value2</Value>
             </Tag>
              ...
          </And>
        </Filter>
```

```
        <Status>Enabled</Status>
        transition/expiration actions
    </Rule>
</LifecycleConfiguration>
```

Amazon S3 使用逻辑 AND 组合这些筛选条件。也就是说，该规则应用于具有指定键前缀和指定标签的对象子集。一个筛选条件只能有一个前缀以及零个或多个标签。

- 您可以指定 empty filter（空筛选条件），在此情况下，此规则应用于桶中的所有对象。

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
        </Filter>
        <Status>Enabled</Status>
        transition/expiration actions
    </Rule>
</LifecycleConfiguration>
```

- 要按照 object size（对象大小）筛选规则，您可以指定最小的大小 (ObjectSizeGreaterThan) 或最大大小 (ObjectSizeLessThan)，也可以指定一系列对象大小。

  对象大小值以字节为单位。默认情况下，除非您指定较小的最小大小 (ObjectSizeGreaterThan) 或最大大小 (ObjectSizeLessThan)，否则小于 128 KB 的对象不会转换到任何存储类。有关更多信息，请参阅 [示例：支持转换小于 128 KB 的对象]。

```
                    <LifecycleConfiguration>
    <Rule>
        <Filter>
            <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
        </Filter>
        <Status>Enabled</Status>
        transition/expiration actions
    </Rule>
</LifecycleConfiguration>
```

> **Note**
>
> ObjectSizeGreaterThan 和 ObjectSizeLessThan 筛选条件不包含所指定的值。例如，如果您将大小为 128 KB 到 1024 KB 的对象设置为从 S3 Standard 存储类移到 S3

Standard-IA 存储类，则大小精确为 1024 KB 和 128 KB 的对象将不会转换到 S3 Standard-IA。相反，该规则将仅适用于大小大于 128 KB 且小于 1024 KB 的对象。

如果要指定对象大小范围，ObjectSizeGreaterThan 整数必须小于 ObjectSizeLessThan 值。当使用多个筛选条件时，必须将筛选条件包装在 <And> 元素中。以下示例显示了如何指定范围在 500 字节到 64000 字节之间的对象。

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
            <And>
                <Prefix>key-prefix</Prefix>
                <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
                <ObjectSizeLessThan>64000</ObjectSizeLessThan>
            </And>
        </Filter>
        <Status>Enabled</Status>
        transition/expiration actions
    </Rule>
</LifecycleConfiguration>
```

## 用于描述生命周期操作的元素

通过在 S3 生命周期规则中指定一个或多个以下预定义操作，您可以指示 Amazon S3 在对象的生命周期内执行特定操作。这些操作的效果取决于桶的版本控制状态。

- **Transition** 操作元素 – 您指定 Transition 操作来将对象从一个存储类转换为另一个存储类。有关转换对象的更多信息，请参阅 支持的转换。达到对象生命周期内指定的日期或时间段后，Amazon S3 将执行该转换。

  对于受版本控制的桶（已启用版本控制或已暂停版本控制的桶），Transition 操作适用于当前对象版本。为了管理非当前版本，Amazon S3 定义了 NoncurrentVersionTransition 操作（本主题稍后会对此描述）。

- **Expiration** 操作元素 – Expiration 操作使规则中标识的对象到期，并且应用于任意 Amazon S3 存储类中符合条件的对象。有关存储类别的更多信息，请参阅 了解和管理 Amazon S3 存储类。Amazon S3 使所有过期的对象不可用。是否永久删除对象取决于桶的版本控制状态。

- 不受版本控制的存储桶 – Expiration 操作导致 Amazon S3 永久移除对象。
- 受版本控制的桶 – 对于受版本控制的桶（即，已启用版本控制或已暂停版本控制），有一些指导 Amazon S3 如何处理 Expiration 操作的注意事项。对于启用版本控制或暂停版本控制的桶，以下内容适用：
  - Expiration 操作仅适用于当前版本 (对非当前对象版本没有影响)。
  - 如果有一个或多个对象版本，并且删除标记是当前版本，则 Amazon S3 不会执行任何操作。
  - 如果当前对象版本是唯一的对象版本并且它还是删除标记（也称为过期对象删除标记，在这种情况下，所有对象版本都已删除，您只剩下一个删除标记），则 Amazon S3 将删除过期对象删除标记。还可以使用过期操作来指示 Amazon S3 移除所有到期对象删除标记。有关示例，请参阅在启用了版本控制的存储桶中移除到期对象删除标记。

  有关更多信息，请参阅 使用 S3 版本控制保留对象的多个版本。

  设置 Amazon S3 以管理过期时，还应该考虑以下各项：

  - 已启用版本控制的桶

    如果当前对象版本不是删除标记，Amazon S3 将添加具有唯一的版本 ID 的删除标记。这会使当前对象版本变为非当前版本，并使删除标记变为当前版本。

  - 已暂停版本控制的桶

    在已暂停版本控制的存储桶中，到期操作将使 Amazon S3 创建版本 ID 为 null 的删除标记。此删除标记会在版本层次结构中将任何对象版本替换为 null 版本 ID，从而实际上删除对象。

此外，Amazon S3 还提供可用于管理受版本控制的桶（即，启用了版本控制和暂停了版本控制的桶）中的非当前对象版本的以下操作。

- **NoncurrentVersionTransition** 操作元素 – 使用此操作可指定 Amazon S3 何时将对象转换到指定的存储类。您可以根据自对象变为非当前版本以来的一定天数 (<NoncurrentDays>) 来确定此转换。除了天数之外，还可以指定要保留的非当前版本的数量 (<NewerNoncurrentVersions>)（介于 1 和 100 之间）。此值确定在 Amazon S3 可以转换给定版本之前，必须存在多少个较新的非当前版本。Amazon S3 将转换超过要保留的指定数量的任何其它非当前版本。要进行转换，必须同时超过 <NoncurrentDays> 和 <NewerNoncurrentVersions> 的值。

  要指定要保留的非当前版本数量，还必须提供 <Filter> 元素。如果您未指定 <Filter> 元素，Amazon S3 会在您指定要保留的非当前版本数量时生成 InvalidRequest 错误。

有关转换对象的更多信息，请参阅 支持的转换。有关当您在 NoncurrentVersionTransition 操作中指定天数时 Amazon S3 如何计算日期的详细信息，请参阅 生命周期规则：基于对象的存在期限。

- **NoncurrentVersionExpiration** 操作元素 – 使用此操作可指示 Amazon S3 何时永久删除对象的非当前版本。删除的对象无法恢复。您可以根据自对象变为非当前对象以来的一定天数 (<NoncurrentDays>) 来确定此到期日期。除了天数之外，还可以指定要保留的非当前版本的数量 (<NewerNoncurrentVersions>)（介于 1 和 100 之间）。此值指定在 Amazon S3 可以使给定版本到期之前，必须存在多少较新的非当前版本。Amazon S3 将永久删除超过要保留的指定数量的任何其它非当前版本。要进行删除，必须同时超过 <NoncurrentDays> 和 <NewerNoncurrentVersions> 的值。

  要指定要保留的非当前版本数量，还必须提供 <Filter> 元素。如果您未指定 <Filter> 元素，Amazon S3 会在您指定要保留的非当前版本数量时生成 InvalidRequest 错误。

  当您需要更正任何意外删除或覆盖时，非当前对象的延时移除可能很有帮助。例如，您可以配置一个到期规则，以便在对象变为非当前版本五天后删除非当前版本。例如，假设在 2014 年 1 月 1 日上午 10:30 UTC，您创建了名为 photo.gif 的对象（版本 ID 111111）。在 2014 年 2 月 1 日上午 11:30 UTC，您意外删除了 photo.gif（版本 ID 111111），这将导致使用新版本 ID（如版本 ID 4857693）创建一个删除标记。您现在有五天时间可以在永久删除之前，恢复原始版本的 photo.gif (版本 ID 111111)。在 2014 年 1 月 8 日 00:00 UTC，有关到期的生命周期规则运行并永久删除 photo.gif（版本 ID 111111）（在它成为非当前版本五天之后）。

  有关当您在 NoncurrentVersionExpiration 操作中指定天数时 Amazon S3 如何计算日期的详细信息，请参阅 生命周期规则：基于对象的存在期限。

  > **Note**
  >
  > 对象到期生命周期配置不会移除未完成的分段上传。要移除未完成的分段上传，您必须使用 AbortIncompleteMultipartUpload 生命周期配置操作，如本节后面所述。

除了转换和到期操作之外，您还可以使用以下生命周期配置操作，来指示 Amazon S3 停止未完成的分段上传或移除到期的对象删除标记：

- **AbortIncompleteMultipartUpload** 操作元素 – 使用此元素可设置您希望允许分段上传保持运行的最长时间（天）。如果适用的分段上传（由生命周期规则中指定的键名称 prefix 确定）未在

预定义的时间段内成功完成，Amazon S3 将停止未完成的分段上传。有关更多信息，请参阅 中止分段上传。

> **Note**
>
> 如果规则具有使用对象标签的筛选条件，则您无法在此规则中指定此生命周期操作。

- **`ExpiredObjectDeleteMarker`** 操作元素 – 在启用了版本控制的存储桶中，包含零个非当前版本的删除标记称为到期对象删除标记。您可以使用此生命周期操作来指示 Amazon S3 移除到期对象移除标记。有关示例，请参阅在启用了版本控制的存储桶中移除到期对象删除标记。

> **Note**
>
> 如果规则具有使用对象标签的筛选条件，则您无法在此规则中指定此生命周期操作。

Amazon S3 如何计算对象已成为非当前版本的时间长度

在启用版本控制的桶中，您可以有一个对象的多个版本。当前版本始终有一个，以及零个或零个以上非当前版本。每次上传对象时，当前版本都保留为非当前版本，新添加的版本 (后继者) 会成为当前版本。为了确定对象成为非当前版本的天数，Amazon S3 会查看其后继者的创建时间。Amazon S3 使用自后继者创建以来的天数作为对象成为非当前版本的天数。

> **在使用 S3 生命周期配置时还原对象的以前版本**
>
> 按照还原早期版本中的详细说明，您可以使用以下两种方法中的任一种来检索对象的以前版本：
>
> - 方法 1 – 将对象的非当前版本复制到相同存储桶中。复制的对象将成为该对象的当前版本，且所有对象版本都保留。
> - 方法 2 – 永久删除对象的当前版本。当您删除当前对象版本时，实际上是将非当前版本转换为该对象的当前版本。
>
> 当您正在将 S3 生命周期配置规则用于启用版本控制的存储桶时，我们建议的最佳实践是使用方法 1。
> S3 生命周期在最终一致的模型下运行。在更改传播到所有 Amazon S3 系统之前，永久删除的当前版本可能不会消失。（因此，Amazon S3 可能暂时不知道此删除操作。）同时，您配置

用于使非当前对象过期的生命周期规则可能会永久删除非当前对象，包括您要还原的对象。因此，复制旧版本（按照方法 1 建议）是更安全的替代方法。

生命周期操作与桶版本控制状态

生命周期规则：基于对象的存在期限

您可以指定 Amazon S3 能够执行指定操作的时间段 [自对象创建（或修改）以来的天数]。

当您在 S3 生命周期配置中的 `Transition` 和 `Expiration` 操作中指定天数时，请注意以下事项：

- 您指定的值是自对象创建以来将发生此操作的天数。
- Amazon S3 按以下方式计算时间：将在规则中指定的天数与对象创建时间相加，然后将得出的时间四舍五入至下一日的午夜 UTC。例如，如果对象的创建时间是 2014 年 1 月 15 日上午 10:30 UTC，并且您在转换规则中指定了 3 天，则对象的转换日期将计算为 2014 年 1 月 19 日 00:00 UTC。

Note

Amazon S3 仅为每个对象保持上次修改日期。例如，Amazon S3 控制台在对象的属性窗格中显示上次修改日期。最初创建新对象时，此日期反映对象的创建日期。如果您替换对象，此日期会相应地更改。因此，创建日期与上次修改日期同义。

当在生命周期配置中的 `NoncurrentVersionTransition` 和 `NoncurrentVersionExpiration` 操作中指定天数时，请注意以下几点：

- 您指定的值是从对象版本变为非当前版本以来（即，当对象被覆盖或删除时）的天数，作为 Amazon S3 将对指定的对象执行操作的时间。
- Amazon S3 按以下方式计算时间：将在规则中指定的天数与创建对象的新后继版本的时间相加，然后将得出的时间四舍五入至下一日的午夜 UTC。例如，在您的存储桶中，假设某个对象的当前版本的创建时间是 2014 年 1 月 1 日上午 10:30 UTC。如果替换当前版本的对象新版本的创建时间是 2014 年 1 月 15 日上午 10:30 UTC，并且您在转换规则中指定了 3 天，则对象的转换日期计算为 2014 年 1 月 19 日 00:00 UTC。

生命周期规则：基于特定日期

当在 S3 生命周期规则中指定操作时，您可以指定希望 Amazon S3 执行此操作的日期。到达特定日期时，Amazon S3 会向所有合格对象应用该操作（基于筛选条件）。

如果为 S3 生命周期操作指定一个过去的日期，所有合格对象会立即符合该生命周期操作的条件。

> **Important**
>
> 基于日期的操作并非一次性操作。即使过了该日期后，只要规则状态为 `Enabled`，Amazon S3 仍会继续应用该基于日期的操作。
> 例如，假设您指定一个基于日期的 `Expiration` 操作来删除所有对象（假设规则中未指定任何筛选条件）。在指定日期，Amazon S3 会使桶中的所有对象过期。此外，Amazon S3 还会继续使您在存储桶中创建的所有新对象到期。要停止生命周期操作，您必须从生命周期规则中移除操作，禁用规则或从生命周期配置中删除规则。

此日期值必须符合 ISO 8601 格式。时间始终为午夜 UTC。

> **Note**
>
> 您无法使用 Amazon S3 控制台创建基于日期的生命周期规则，但是可以查看、禁用或删除这类规则。

## 将筛选条件添加到生命周期规则

筛选条件是一个可选的生命周期规则元素，可用于指定规则适用于哪些对象。

以下元素可用于筛选对象：

键前缀

可以基于前缀来筛选对象。如果要将生命周期操作应用于多个前缀下的对象子集，您可以指定单独的规则。在每个规则中，指定基于前缀的筛选条件。有关更多信息，请参阅 [示例]

对象标签

可以基于一个或多个标签来筛选对象。每个标签必须与键和值完全匹配，如果您指定多个标签，每个标签键必须是唯一的。具有多个对象标签的筛选条件应用于已指定了所有标签的对象子集。如果某个对象指定了其它标签，则该筛选条件仍将适用。

> **Note**
>
> 如果您只指定 Key 元素而未指定 Value 元素，则该规则将仅应用于与标签键匹配而未指定值的对象。

最小或最大对象大小

可以基于大小来筛选对象。可以指定最小大小 (ObjectSizeGreaterThan) 或最大大小 (ObjectSizeLessThan)，也可以在同一个筛选条件中指定一系列对象大小。对象大小值以字节为单位。最大筛选条件大小为 5TB。Amazon S3 对生命周期配置应用默认的最小对象大小。有关更多信息，请参阅 示例：支持转换小于 128 KB 的对象。

可以组合不同的筛选元素，在这种情况下，Amazon S3 使用逻辑 AND。

筛选示例

以下示例说明如何使用不同的筛选元素：

- 使用键前缀指定筛选条件 – 此示例显示一个 S3 生命周期规则，此规则基于键名前缀（logs/）应用于一部分对象。例如，此生命周期规则应用于对象 logs/mylog.txt、logs/temp1.txt 和 logs/test.txt。此规则不应用于对象 example.jpg。

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
           <Prefix>logs/</Prefix>
        </Filter>
        transition/expiration actions
         ...
    </Rule>
    ...
</LifecycleConfiguration>
```

> **Note**
>
> 如果您有一个或多个前缀以相同的字符开头，则可以通过在筛选条件中指定不带尾部斜杠 (/) 的部分前缀，来将所有这些前缀包含在规则中。例如，假设您有以下前缀：
>
> ```
> sales1999/
> ```

```
                sales2000/
                sales2001/
```

要在规则中包含所有三个前缀，请在生命周期规则中指定 `sales` 作为前缀。

如果您要基于不同的键名称前缀将生命周期操作应用于一部分对象，可指定单独的规则。在每个规则中，指定基于前缀的筛选条件。例如，要描述具有键前缀 `projectA/` 和 `projectB/` 的对象的生命周期操作，可指定两个规则，如下所示：

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
           <Prefix>projectA/</Prefix>
        </Filter>
        transition/expiration actions
         ...
    </Rule>

    <Rule>
        <Filter>
           <Prefix>projectB/</Prefix>
        </Filter>
        transition/expiration actions
         ...
    </Rule>
</LifecycleConfiguration>
```

有关对象键的更多信息，请参阅 为 Amazon S3 对象命名。

- 指定基于对象标签的筛选条件 – 在以下示例中，此生命周期规则指定基于标签（*key*）和值（*value*）的筛选条件。随后，此规则仅应用于具有特定标签的一部分对象。

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
           <Tag>
              <Key>key</Key>
              <Value>value</Value>
           </Tag>
        </Filter>
        transition/expiration actions
```

```
        ...
    </Rule>
</LifecycleConfiguration>
```

您可以指定基于多个标签的筛选条件。您必须在 <And> 元素中包含标签，如以下示例所示。此规则指示 Amazon S3 对具有两个标签（带特定的标签键和值）的对象执行生命周期操作。

```
<LifecycleConfiguration>
    <Rule>
      <Filter>
         <And>
            <Tag>
               <Key>key1</Key>
               <Value>value1</Value>
            </Tag>
            <Tag>
               <Key>key2</Key>
               <Value>value2</Value>
            </Tag>
             ...
         </And>
      </Filter>
      transition/expiration actions
    </Rule>
</Lifecycle>
```

此生命周期规则应用于具有指定的两个标签的对象。Amazon S3 执行逻辑 AND。请注意以下几点：

- 每个标签的键和值都 必须完全匹配。如果您只指定 <Key> 元素而不指定 <Value> 元素，则该规则将仅应用于与标签键匹配而未 指定值的对象。
- 此规则应用于具有规则中指定的所有标签的一部分对象。如果某个对象指定了其他标签，则该规则仍将适用。

> **Note**
>
> 当您在筛选条件中指定多个标签时，每个标签键必须是唯一的。

- 指定基于前缀和一个或多个标签的筛选条件 – 在生命周期规则中，您可以指定基于键前缀和一个或多个标签的筛选条件。同样，您必须在 <And> 元素中包含所有这些筛选条件元素，如下所示：

```
<LifecycleConfiguration>
```

```
    <Rule>
        <Filter>
          <And>
             <Prefix>key-prefix</Prefix>
             <Tag>
                <Key>key1</Key>
                <Value>value1</Value>
             </Tag>
             <Tag>
                <Key>key2</Key>
                <Value>value2</Value>
             </Tag>
              ...
          </And>
        </Filter>
        <Status>Enabled</Status>
        transition/expiration actions
    </Rule>
</LifecycleConfiguration>
```

Amazon S3 使用逻辑 AND 组合这些筛选条件。也就是说，该规则应用于具有指定键前缀和指定标签的对象子集。一个筛选条件只能有一个前缀以及零个或多个标签。

- 指定空筛选条件 – 可以指定空筛选条件，在此情况下，规则应用于存储桶中的所有对象。

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
        </Filter>
        <Status>Enabled</Status>
        transition/expiration actions
    </Rule>
</LifecycleConfiguration>
```

- 指定对象大小筛选条件 – 要按对象大小来筛选规则，可以指定最小大小 (ObjectSizeGreaterThan) 或最大大小 (ObjectSizeLessThan)，也可以指定一系列对象大小。

  对象大小值以字节为单位。最大筛选条件大小为 5TB。某些存储类具有最小对象大小限制。有关更多信息，请参阅 比较 Amazon S3 存储类。

```
<LifecycleConfiguration>
    <Rule>
```

```
        <Filter>
            <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
        </Filter>
        <Status>Enabled</Status>
        transition/expiration actions
    </Rule>
</LifecycleConfiguration>
```

> **Note**
>
> ObjectSizeGreaterThan 和 ObjectSizeLessThan 筛选条件不包含所指定的值。例如，如果您将大小为 128 KB 到 1024 KB 的对象设置为从 S3 Standard 存储类移到 S3 Standard-IA 存储类，则大小精确为 1024 KB 和 128 KB 的对象将不会转换到 S3 Standard-IA。相反，该规则将仅适用于大小大于 128 KB 且小于 1024 KB 的对象。

如果要指定对象大小范围，ObjectSizeGreaterThan 整数必须小于 ObjectSizeLessThan 值。当使用多个筛选条件时，必须将筛选条件包装在 <And> 元素中。以下示例显示了如何指定范围在 500 字节到 64000 字节之间的对象。

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
            <And>
                <Prefix>key-prefix</Prefix>
                <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
                <ObjectSizeLessThan>64000</ObjectSizeLessThan>
            </And>
        </Filter>
        <Status>Enabled</Status>
        transition/expiration actions
    </Rule>
</LifecycleConfiguration>
```

## Amazon S3 如何处理生命周期配置中的冲突

通常，Amazon S3 生命周期会针对成本进行优化。例如，如果两个过期策略重叠，将采用较短的过期策略，以便数据存储不会超过预期时间。同样，如果两个转换策略重叠，S3 生命周期将对象转换为较低成本的存储类。

在这两种情况下，S3 生命周期尝试选择最便宜的路径。该一般规则的一个例外情况是 S3 Intelligent-Tiering 存储类。S3 生命周期更青睐 S3 Intelligent-Tiering 而非任何其它存储类，但 S3 Glacier 和 S3 Glacier Deep Archive 存储类除外。

当您在 S3 生命周期配置中有多个规则时，对象可能变得符合条件可在同一天执行多个 S3 生命周期操作。在这种情况下，Amazon S3 遵循以下一般规则：

- 永久删除优先于转换。
- 转换优先于删除标记的创建。
- 当对象符合条件可进行 S3 Glacier Flexible Retrieval 和 S3 Standard-IA（或 S3 One Zone-IA）转换时，Amazon S3 将选择 S3 Glacier Flexible Retrieval 转换。

## 重叠的筛选条件和冲突的生命周期操作的示例

您可能会指定一个在其中指定了重叠的前缀或操作的 S3 生命周期配置。以下示例说明 Amazon S3 如何解决潜在的冲突。

Example 1：重叠的前缀（无冲突）

以下示例配置包含两个规则，它们指定了如下所示的重叠前缀：

- 第一个规则指定了一个空筛选条件，指示存储桶中的所有对象。
- 第二个规则指定了一个键名前缀 (`logs/`)，指示仅一部分对象。

规则 1 请求 Amazon S3 在所有对象创建一年后删除这些对象。规则 2 请求 Amazon S3 在创建 30 天后将对象子集转换为 S3 Standard-IA 存储类。

```
<LifecycleConfiguration>
  <Rule>
    <ID>Rule 1</ID>
    <Filter>
    </Filter>
    <Status>Enabled</Status>
    <Expiration>
      <Days>365</Days>
    </Expiration>
  </Rule>
  <Rule>
    <ID>Rule 2</ID>
    <Filter>
```

```
      <Prefix>logs/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <StorageClass>STANDARD_IA</StorageClass>
      <Days>30</Days>
    </Transition>
   </Rule>
</LifecycleConfiguration>
```

由于在这种情况下没有冲突，因此 Amazon S3 将在创建 30 天后将带有 `logs/` 前缀的对象转换为 S3 Standard-IA 存储类。当任何对象在创建一年后到达时，它将被删除。

Example 2：冲突的生命周期操作

本示例配置中有两个规则，它们指示 Amazon S3 在对象的生命周期中同时对同一组对象执行两个不同的操作：

- 两个规则指定了相同的键名前缀，因此两个规则都应用于同一组对象。
- 当应用两个规则时，它们指定了相同的“对象创建后的 365 天”。
- 一个规则指示 Amazon S3 将对象转换为 S3 Standard-IA 存储类，另一个规则希望 Amazon S3 使对象同时过期。

```
<LifecycleConfiguration>
  <Rule>
    <ID>Rule 1</ID>
    <Filter>
      <Prefix>logs/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Expiration>
      <Days>365</Days>
    </Expiration>
  </Rule>
  <Rule>
    <ID>Rule 2</ID>
    <Filter>
      <Prefix>logs/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
```

```
      <StorageClass>STANDARD_IA</StorageClass>
      <Days>365</Days>
    </Transition>
   </Rule>
</LifecycleConfiguration>
```

在这种情况下，由于您希望对象过期（要移除），因此在更改存储类时没有意义，因此 Amazon S3 在这些对象上选择过期操作。

Example 3：导致冲突的生命周期操作的重叠的前缀

在本示例中，配置包含两个指定重叠前缀的规则，如下所示：

- 规则 1 指定了一个空前缀 (指示所有对象)。
- 规则 2 指定了一个键名前缀 (logs/)，用于确定所有对象中的一部分。

对于带 logs/ 键名前缀的一部分对象，两个规则中的 S3 生命周期操作都适用。一个规则指示 Amazon S3 在对象创建 10 天后对其进行转换，另一个规则指示 Amazon S3 在对象创建 365 天后对其进行转换。

```
<LifecycleConfiguration>
  <Rule>
    <ID>Rule 1</ID>
    <Filter>
      <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <StorageClass>STANDARD_IA</StorageClass>
      <Days>10</Days>
    </Transition>
  </Rule>
  <Rule>
    <ID>Rule 2</ID>
    <Filter>
      <Prefix>logs/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <StorageClass>STANDARD_IA</StorageClass>
      <Days>365</Days>
    </Transition>
```

```
   </Rule>
</LifecycleConfiguration>
```

在这种情况下，Amazon S3 将选择在对象创建 10 天后转换它们。

Example 4：基于标签的筛选和随之出现的冲突的生命周期操作

假设您有包含两个规则（每个规则各指定一个标签筛选条件）的以下 S3 生命周期配置：

- 规则 1 指定了基于标签的筛选条件 (`tag1/value1`)。此规则指示 Amazon S3 在对象创建 365 天后将其转换为 S3 Glacier Flexible Retrieval 存储类。
- 规则 2 指定了基于标签的筛选条件 (`tag2/value2`)。此规则指示 Amazon S3 在对象创建 14 天后使其过期。

S3 生命周期配置如下所示。

```
<LifecycleConfiguration>
  <Rule>
    <ID>Rule 1</ID>
    <Filter>
      <Tag>
         <Key>tag1</Key>
         <Value>value1</Value>
      </Tag>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <StorageClass>GLACIER</StorageClass>
      <Days>365</Days>
    </Transition>
  </Rule>
  <Rule>
    <ID>Rule 2</ID>
    <Filter>
      <Tag>
         <Key>tag2</Key>
         <Value>value2</Value>
      </Tag>
    </Filter>
    <Status>Enabled</Status>
    <Expiration>
      <Days>14</Days>
```

```
    </Expiration>
   </Rule>
</LifecycleConfiguration>
```

如果对象有两个标签，那么 Amazon S3 必须决定要遵循哪个规则。在这种情况下，Amazon S3 将在对象创建 14 天后使其过期。该对象将被删除，因此转换操作不会起作用。

## S3 生命周期配置的示例

此部分提供 S3 生命周期配置的示例。每个示例演示如何在各个示例方案中指定 XML。

主题

- 在创建后的一天内归档所有对象
- 临时禁用生命周期规则
- 在对象的生命周期内逐步将存储类降级
- 指定多个规则
- 为启用了版本控制的存储桶指定生命周期规则
- 在启用了版本控制的存储桶中移除到期对象删除标记
- 用于中止分段上传的生命周期配置
- 使没有数据的非当前对象到期
- 示例：支持转换小于 128 KB 的对象

### 在创建后的一天内归档所有对象

每个 S3 生命周期规则都包含一个筛选条件，该筛选条件可用于确定存储桶中适用 S3 生命周期规则的一部分对象。以下 S3 生命周期配置显示了如何指定筛选条件的示例。

- 在此 S3 生命周期配置规则中，筛选条件指定了一个键前缀 (`tax/`)。因此，此规则应用于带键名前缀 `tax/` 的对象，例如 `tax/doc1.txt` 和 `tax/doc2.txt`。

  此规则指定两个指示 Amazon S3 完成以下任务的操作：

  - 在对象创建 365 天（一年）后将其转换为 S3 Glacier Flexible Retrieval 存储类。
  - 在对象创建 3650 天（10 年）后将其删除（`Expiration` 操作）。

```
<LifecycleConfiguration>
```

```
  <Rule>
    <ID>Transition and Expiration Rule</ID>
    <Filter>
       <Prefix>tax/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>365</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
    <Expiration>
      <Days>3650</Days>
    </Expiration>
  </Rule>
</LifecycleConfiguration>
```

您可以为每个操作指定一个日期，而不用以创建后的天数的形式指定对象期限。但是，您不能在同一规则中同时使用 `Date` 和 `Days`。

- 如果希望 S3 生命周期规则应用于存储桶中的所有对象，请指定一个空前缀。在下面的配置中，该规则指定了一个 `Transition` 操作，该操作将指示 Amazon S3 在创建后 0 天将对象转移到 S3 Glacier Flexible Retrieval 存储类。此规则意味着对象在创建后有资格在世界标准时间午夜归档到 S3 Glacier Flexible Retrieval。有关生命周期约束的更多信息，请参阅 转换的约束和注意事项。

```
<LifecycleConfiguration>
  <Rule>
    <ID>Archive all object same-day upon creation</ID>
    <Filter>
      <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

- 您可以在筛选条件中指定零或一个键名前缀以及零或多个对象标签。以下示例代码将 S3 生命周期规则应用于带 `tax/` 键前缀的一部分对象以及包含具有特定键和值的两个标签的对象。在指定多个筛选条件时，您必须按下面所示包含 <And>（Amazon S3 会应用逻辑 AND 以将指定筛选条件组合起来）。

```
...
<Filter>
   <And>
      <Prefix>tax/</Prefix>
      <Tag>
         <Key>key1</Key>
         <Value>value1</Value>
      </Tag>
      <Tag>
         <Key>key2</Key>
         <Value>value2</Value>
      </Tag>
    </And>
</Filter>
...
```

- 您可以仅基于标签筛选对象。例如，以下 S3 生命周期规则应用于具有两个指定标签的对象（该规则未指定任何前缀）。

```
...
<Filter>
   <And>
      <Tag>
         <Key>key1</Key>
         <Value>value1</Value>
      </Tag>
      <Tag>
         <Key>key2</Key>
         <Value>value2</Value>
      </Tag>
    </And>
</Filter>
...
```

**Important**

当您在 S3 生命周期配置中有多个规则时，对象可能变得符合条件可在同一天执行多个 S3 生命周期操作。在这种情况下，Amazon S3 遵循以下一般规则：

- 永久删除优先于转换。
- 转换优先于删除标记的创建。
- 当对象有资格进行 S3 Glacier Flexible Retrieval 和 S3 Standard-IA（或 S3 One Zone-IA）转换时，Amazon S3 将选择 S3 Glacier Flexible Retrieval 转换。

有关示例，请参阅 重叠的筛选条件和冲突的生命周期操作的示例。

## 临时禁用生命周期规则

可以使用 `status` 元素临时禁用 S3 生命周期规则。如果您想在不覆盖现有规则的情况下测试新规则或排查配置问题，这可能很有用。以下 S3 生命周期配置指定了两个规则：

- 规则 1 指示 Amazon S3 在带 `logs/` 前缀的对象创建后立即将其转换为 S3 Glacier Flexible Retrieval 存储类。
- 规则 2 指示 Amazon S3 在带 `documents/` 前缀的对象创建后立即将其转换为 S3 Glacier Flexible Retrieval 存储类。

在此配置中，启用了规则 1 但禁用了规则 2。Amazon S3 忽略禁用的规则。

```
<LifecycleConfiguration>
  <Rule>
    <ID>Rule1</ID>
    <Filter>
      <Prefix>logs/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
  <Rule>
    <ID>Rule2</ID>
    <Filter>
      <Prefix>documents/</Prefix>
    </Filter>
```

```
    <Status>Disabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

## 在对象的生命周期内逐步将存储类降级

在本示例中，您使用 S3 生命周期配置在对象的生命周期内逐步将存储类降级。级别降低可帮助减少存储成本。有关定价的更多信息，请参阅 Amazon S3 定价。

以下 S3 生命周期配置指定了应用于带键名前缀 `logs/` 的对象的规则。该规则指定了以下操作：

- 两个转换操作：
  - 在对象创建 30 天后将其转换为 S3 Standard-IA 存储类。
  - 在对象创建 90 天后将其转换为 S3 Glacier Flexible Retrieval 存储类。
- 一个过期操作，指示 Amazon S3 在对象创建一年后将其删除。

```
<LifecycleConfiguration>
  <Rule>
    <ID>example-id</ID>
    <Filter>
       <Prefix>logs/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>30</Days>
      <StorageClass>STANDARD_IA</StorageClass>
    </Transition>
    <Transition>
      <Days>90</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
    <Expiration>
      <Days>365</Days>
    </Expiration>
  </Rule>
</LifecycleConfiguration>
```

> **Note**
>
> 如果所有 S3 生命周期操作都应用于同一组对象（由筛选条件标识），您可以使用一个规则来描述这些操作。或者，您也可以添加多个规则，每个规则指定一个不同的筛选条件。

> **Important**
>
> 当您在 S3 生命周期配置中有多个规则时，对象可能变得符合条件可在同一天执行多个 S3 生命周期操作。在这种情况下，Amazon S3 遵循以下一般规则：
>
> - 永久删除优先于转换。
> - 转换优先于删除标记的创建。
> - 当对象有资格进行 S3 Glacier Flexible Retrieval 和 S3 Standard-IA（或 S3 One Zone-IA）转换时，Amazon S3 将选择 S3 Glacier Flexible Retrieval 转换。
>
> 有关示例，请参阅 重叠的筛选条件和冲突的生命周期操作的示例。

## 指定多个规则

如果您希望不同的对象有不同的 S3 生命周期操作，则可以指定多个规则。以下 S3 生命周期配置有两个规则：

- 规则 1 应用于带键名前缀 `classA/` 的对象。它指示 Amazon S3 在对象创建一年后将其转换为 S3 Glacier Flexible Retrieval 存储类，并在对象创建 10 年后使它们过期。
- 规则 2 应用于带键名前缀 `classB/` 的对象。它指示 Amazon S3 在对象创建 90 天后将其转换为 S3 Standard-IA 存储类，并在对象创建 1 年后将其删除。

```
<LifecycleConfiguration>
    <Rule>
        <ID>ClassADocRule</ID>
        <Filter>
           <Prefix>classA/</Prefix>
        </Filter>
        <Status>Enabled</Status>
```

```
        <Transition>
           <Days>365</Days>
           <StorageClass>GLACIER</StorageClass>
        </Transition>
        <Expiration>
             <Days>3650</Days>
        </Expiration>
    </Rule>
    <Rule>
        <ID>ClassBDocRule</ID>
        <Filter>
            <Prefix>classB/</Prefix>
        </Filter>
        <Status>Enabled</Status>
        <Transition>
           <Days>90</Days>
           <StorageClass>STANDARD_IA</StorageClass>
        </Transition>
        <Expiration>
             <Days>365</Days>
        </Expiration>
    </Rule>
</LifecycleConfiguration>
```

**Important**

当您在 S3 生命周期配置中有多个规则时，对象可能变得符合条件可在同一天执行多个 S3 生命周期操作。在这种情况下，Amazon S3 遵循以下一般规则：

- 永久删除优先于转换。
- 转换优先于删除标记的创建。
- 当对象有资格进行 S3 Glacier Flexible Retrieval 和 S3 Standard-IA（或 S3 One Zone-IA）转换时，Amazon S3 将选择 S3 Glacier Flexible Retrieval 转换。

有关示例，请参阅 重叠的筛选条件和冲突的生命周期操作的示例。

## 为启用了版本控制的存储桶指定生命周期规则

假设您有一个启用了版本控制的存储桶，这意味着对于每个对象，您都有一个当前版本以及零个或零个以上的非当前版本。（有关 S3 版本控制的更多信息，请参阅 使用 S3 版本控制保留对象的多个版本。）

在下面的示例中，您想要保留一年的历史记录，然后保留 5 个非当前版本。S3 生命周期配置支持保留任何对象的 1 至 100 个版本。请注意，在 Amazon S3 可以使给定版本到期之前，必须存在超过 5 个较新的非当前版本。Amazon S3 将永久删除超过要保留的指定数量的任何其它非当前版本。要进行删除，必须同时超过 NoncurrentDays 和 NewerNoncurrentVersions 的值。

为了节省存储开销，您希望在非现行的版本成为非现行（假设这些非现行的对象是不需要实时访问的冷数据）后 30 天将非现行的版本移至 S3 Glacier Flexible Retrieval。此外，您还期望在对象创建 90 天后降低当前版本的访问频率，因此您可能会选择将这些对象移动到 S3 Standard-IA 存储类。

```
<LifecycleConfiguration>
    <Rule>
        <ID>sample-rule</ID>
        <Filter>
           <Prefix></Prefix>
        </Filter>
        <Status>Enabled</Status>
        <Transition>
           <Days>90</Days>
           <StorageClass>STANDARD_IA</StorageClass>
        </Transition>
        <NoncurrentVersionTransition>
            <NoncurrentDays>30</NoncurrentDays>
            <StorageClass>GLACIER</StorageClass>
        </NoncurrentVersionTransition>
       <NoncurrentVersionExpiration>
            <NewerNoncurrentVersions>5</NewerNoncurrentVersions>
            <NoncurrentDays>365</NoncurrentDays>
       </NoncurrentVersionExpiration>
    </Rule>
</LifecycleConfiguration>
```

## 在启用了版本控制的存储桶中移除到期对象删除标记

已启用版本控制的存储桶的每个对象有一个当前版本，以及零个或多个非当前版本。在删除对象时，请注意以下几点：

- 如果您在删除请求中未指定版本 ID，Amazon S3 将添加一个删除标记，而不是删除对象。当前对象版本将变为非当前版本，然后删除标记将变为当前版本。
- 如果在删除请求中指定了版本 ID，Amazon S3 将永久删除对象版本（不会创建删除标记）。
- 包含零个非当前版本的删除标记称为过期对象删除标记。

此示例演示了可在存储桶中创建过期对象删除标记的场景，以及如何使用 S3 生命周期配置指示 Amazon S3 删除过期对象删除标记。

假设您编写了一个 S3 生命周期配置，该配置使用 `NoncurrentVersionExpiration` 操作以在对象变为非当前版本 30 天之后移除这些非当前版本，并保留 10 个非当前版本，如下面的示例所示。请注意，在 Amazon S3 可以使给定版本到期之前，必须存在超过 10 个较新的非当前版本。Amazon S3 将永久删除超过要保留的指定数量的任何其它非当前版本。要进行删除，必须同时超过 `NoncurrentDays` 和 `NewerNoncurrentVersions` 的值。

```
<LifecycleConfiguration>
    <Rule>
        ...
        <NoncurrentVersionExpiration>
            <NewerNoncurrentVersions>10</NewerNoncurrentVersions>
            <NoncurrentDays>30</NoncurrentDays>
        </NoncurrentVersionExpiration>
    </Rule>
</LifecycleConfiguration>
```

`NoncurrentVersionExpiration` 操作不应用于当前的对象版本。它只会移除非当前版本。

对于当前对象版本，您可以根据当前对象版本是否遵循了明确定义的生命周期，通过以下方式管理其生命周期：

- 当前对象版本遵循明确定义的生命周期。

  在这种情况下，您可以将 S3 生命周期配置与 `Expiration` 操作结合使用，以指示 Amazon S3 移除当前版本，如以下示例所示。

```
<LifecycleConfiguration>
    <Rule>
        ...
        <Expiration>
           <Days>60</Days>
        </Expiration>
```

```
        <NoncurrentVersionExpiration>
            <NewerNoncurrentVersions>10</NewerNoncurrentVersions>
            <NoncurrentDays>30</NoncurrentDays>
        </NoncurrentVersionExpiration>
    </Rule>
</LifecycleConfiguration>
```

在此示例中，Amazon S3 将在每个当前对象版本创建 60 天之后通过为其添加删除标记来移除它们。这过程会使当前对象版本变为非当前版本，并使删除标记变为当前版本。有关更多信息，请参阅使用 S3 版本控制保留对象的多个版本。

> **Note**
>
> 不能在同一规则中同时指定 `Days` 和 `ExpiredObjectDeleteMarker` 标签。当您指定 `Days` 标记时，Amazon S3 将于删除标记过旧而无法满足年限条件时自动执行 `ExpiredObjectDeleteMarker` 清理。要在删除标记成为唯一版本时立刻清理，只能使用 `ExpiredObjectDeleteMarker` 标签创建单独的规则。

同一 S3 生命周期配置中的 `NoncurrentVersionExpiration` 操作将在对象变为非当前对象 30 天后删除它们。因此，在此示例中，所有对象版本在对象创建 90 天后被永久删除。请注意，在此示例中，在 Amazon S3 可以使给定版本到期之前，必须存在超过 10 个较新的非当前版本。Amazon S3 将永久删除超过要保留的指定数量的任何其它非当前版本。要进行删除，必须同时超过 `NoncurrentDays` 和 `NewerNoncurrentVersions` 的值。

虽然您可以在此过程中创建过期的对象删除标记，但 Amazon S3 会为您检测并移除过期对象删除标记。

- 当前对象版本没有明确定义的生命周期。

  在这种情况下，您可以在不需要对象时手动删除它们，从而创建具有一个或多个非当前版本的删除标记。如果使用 `NoncurrentVersionExpiration` 操作的 S3 生命周期配置删除了所有非当前版本，则您现在会获得过期对象删除标记。

  特别针对这种情况，S3 生命周期配置提供了 `Expiration` 操作，让您可以请求移除过期对象删除标记。

```
<LifecycleConfiguration>
    <Rule>
```

```
        <ID>Rule 1</ID>
         <Filter>
           <Prefix>logs/</Prefix>
         </Filter>
         <Status>Enabled</Status>
         <Expiration>
            <ExpiredObjectDeleteMarker>true</ExpiredObjectDeleteMarker>
         </Expiration>
         <NoncurrentVersionExpiration>
             <NewerNoncurrentVersions>10</NewerNoncurrentVersions>
             <NoncurrentDays>30</NoncurrentDays>
         </NoncurrentVersionExpiration>
     </Rule>
</LifecycleConfiguration>
```

通过在 Expiration 操作中将 ExpiredObjectDeleteMarker 元素设为 true，您可以指示 Amazon S3 移除过期对象删除标记。

> **Note**
>
> 当您使用 ExpiredObjectDeleteMarker S3 生命周期操作时，该规则无法指定基于标签的筛选条件。

## 用于中止分段上传的生命周期配置

您可以使用 Amazon S3 的分段上传 REST API 操作来在分段中上载大型对象。有关分段上传的更多信息，请参阅 在 Amazon S3 中使用分段上传来上传和复制对象。

通过使用 S3 生命周期配置，当分段上传在指定的启动后的天数内未完成时，您可以指示 Amazon S3 停止未完成的分段上传（通过在规则中指定的键名称前缀确定）。当 Amazon S3 中止分段上传时，它将删除与分段上传关联的所有分段。此流程通过确保您没有包含存储在 Amazon S3 中的分段的未完成分段上传，从而帮助控制存储成本。

> **Note**
>
> 当您使用 AbortIncompleteMultipartUpload S3 生命周期操作时，该规则无法指定基于标签的筛选条件。

下面是使用 AbortIncompleteMultipartUpload 操作指定规则的示例 S3 生命周期配置。此操作将指引 Amazon S3 在分段上传启动 7 天后停止未完成的分段上传。

```
<LifecycleConfiguration>
    <Rule>
        <ID>sample-rule</ID>
        <Filter>
           <Prefix>SomeKeyPrefix/</Prefix>
        </Filter>
        <Status>rule-status</Status>
        <AbortIncompleteMultipartUpload>
          <DaysAfterInitiation>7</DaysAfterInitiation>
        </AbortIncompleteMultipartUpload>
    </Rule>
</LifecycleConfiguration>
```

## 使没有数据的非当前对象到期

您可以创建仅根据对象的大小转换对象的规则。您可以指定最小大小（ObjectSizeGreaterThan）或最大大小（ObjectSizeLessThan），也可以指定一个对象大小范围，单位为字节。当使用多个筛选条件（如前缀和大小规则）时，必须将筛选条件包装在 <And> 元素中。

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition with a prefix and based on size</ID>
    <Filter>
       <And>
          <Prefix>tax/</Prefix>
          <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
       </And>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>365</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

当通过同时使用 ObjectSizeGreaterThan 和 ObjectSizeLessThan 元素指定范围时，最大对象大小必须大于最小对象大小。当使用多个筛选条件时，必须将筛选条件包装在 <And> 元素中。以下示例显示了如何指定范围在 500 字节到 64000 字节之间的对象。指定范围

时，ObjectSizeGreaterThan 和 ObjectSizeLessThan 筛选条件不包含所指定的值。有关更多信息，请参阅 the section called “Filter 元素”。

```
<LifecycleConfiguration>
    <Rule>
        ...
          <And>
             <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
             <ObjectSizeLessThan>64000</ObjectSizeLessThan>
          </And>
    </Rule>
</LifecycleConfiguration>
```

您还可以创建规则，专门使没有数据的非当前对象过期，包括在启用版本控制的存储桶中创建的非当前删除标记对象。以下示例使用 NoncurrentVersionExpiration 操作，在对象变为非当前版本 30 天之后移除这些非当前版本，并保留 10 个非当前对象版本。本示例还使用 ObjectSizeLessThan 元素来只筛选没有数据的对象。

请注意，在 Amazon S3 可以使给定版本到期之前，必须存在超过 10 个较新的非当前版本。Amazon S3 将永久删除超过要保留的指定数量的任何其它非当前版本。要进行删除，必须同时超过 NoncurrentDays 和 NewerNoncurrentVersions 的值。

```
<LifecycleConfiguration>
  <Rule>
    <ID>Expire noncurrent with size less than 1 byte</ID>
    <Filter>
       <ObjectSizeLessThan>1</ObjectSizeLessThan>
    </Filter>
    <Status>Enabled</Status>
    <NoncurrentVersionExpiration>
       <NewerNoncurrentVersions>10</NewerNoncurrentVersions>
       <NoncurrentDays>30</NoncurrentDays>
    </NoncurrentVersionExpiration>
  </Rule>
</LifecycleConfiguration>
```

## 示例：支持转换小于 128 KB 的对象

Amazon S3 对生命周期配置应用默认行为，来防止将小于 128 KB 的对象转换到任何存储类。可以通过向配置中添加最小大小 (ObjectSizeGreaterThan) 或最大大小 (ObjectSizeLessThan) 筛选条

件来指定更小的大小，从而支持转换更小的对象。以下示例支持将任何小于 128 KB 的对象转换到 S3 Glacier Instant Retrieval 存储类：

```
<LifecycleConfiguration>
  <Rule>
    <ID>Allow small object transitions</ID>
    <Filter>
          <ObjectSizeGreaterThan>1</ObjectSizeGreaterThan>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>365</Days>
      <StorageClass>GLACIER_IR</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

> **Note**
>
> 2024 年 9 月，Amazon S3 更新了小对象的默认转换行为，如下所示：
>
> - 更新了默认转换行为 — 从 2024 年 9 月起，默认行为禁止将小于 128 KB 的对象转换到任何存储类。
> - 之前的默认转换行为 — 在 2024 年 9 月之前，默认行为仅支持将小于 128 KB 的对象转换到 S3 Glacier 和 S3 Glacier Deep Archive 存储类。
>
> 2024 年 9 月之前创建的配置将保留之前的转换行为，除非您对其进行修改。也就是说，如果您创建、编辑或删除规则，则配置的默认转换行为会更改为更新的行为。如果用例需要，则可以更改默认转换行为，以便小于 128 KB 的对象将转换到 S3 Glacier 和 S3 Glacier Deep Archive。为此，请在 PutBucketLifecycleConfiguration 请求中使用可选 `x-amz-transition-object-size-minimum-default` 标头。

以下示例说明如何在 PutBucketLifecycleConfiguration 请求中使用 `x-amz-transition-object-size-minimum-default` 标头，来将 `varies_by_storage_class` 默认转换行为应用于 S3 生命周期配置。此行为支持将小于 128 KB 的对象转换到 S3 Glacier 或 S3 Glacier Deep Archive 存储类。默认情况下，所有其它存储类都将阻止小于 128 KB 的转换。您仍然可以使用自定义筛选条件来更改任何存储类的最小转换大小。自定义筛选条件始终优先于默认转换行为：

```
HTTP/1.1 200
x-amz-transition-object-size-minimum-default: varies_by_storage_class
<?xml version="1.0" encoding="UTF-8"?>
...
```

# 排查 Amazon S3 生命周期问题

以下信息可以帮助您排查 Amazon S3 生命周期规则的常见问题。

主题


- 我对我的桶运行了一个列表操作，看到了我认为已按生命周期规则过期或转换的对象。
- 如何监控生命周期规则执行的操作？
- 即使在启用了版本控制的存储桶上设置了生命周期规则之后，我的 S3 对象计数仍增加。
- 如何使用生命周期规则清空 S3 桶？
- 在将对象转换到成本较低的存储类后，我的 Amazon S3 账单增加了。
- 我已经更新了我的桶策略，但我的 S3 对象仍会被过期的生命周期规则删除。
- 我能否恢复由 S3 生命周期规则过期的 S3 对象？
- 为什么我的到期和转换生命周期操作没有发生？
- 如何从我的生命周期规则中排除前缀？
- 如何在我的生命周期规则中包含多个前缀？


## 我对我的桶运行了一个列表操作，看到了我认为已按生命周期规则过期或转换的对象。

S3 生命周期对象转换和对象过期是异步操作。因此，在对象符合过期或转换条件的时间与它们实际转换或过期的时间之间可能会有延迟。一旦满足生命周期规则，即使操作尚未完成，也会立即应用账单的变化。此行为的例外情况是，如果您有一个生命周期规则集转换为 S3 Intelligent-Tiering 存储类。在此类情况下，在对象转换为 S3 Intelligent-Tiering 存储类之前，账单不会发生更改。有关账单变化的更多信息，请参阅设置桶的生命周期配置。

> **Note**
>
> Amazon S3 不会将小于 128KB 的对象从 S3 Standard 或 S3 Standard-IA 存储类转换为 S3 Intelligent-Tiering、S3 Standard-IA 或 S3 One Zone-IA 存储类。

## 如何监控生命周期规则执行的操作？

要监控生命周期规则执行的操作，可以使用以下功能：

- S3 事件通知：您可以设置 S3 事件通知，以便收到有关任何 S3 生命周期到期或转换事件的通知。
- S3 服务器访问日志：您可以为 S3 存储桶启用服务器访问日志，以捕获 S3 生命周期操作，例如对象转换到另一个存储类或对象到期。有关更多信息，请参阅生命周期和日志记录。

要每天查看由生命周期操作引起的存储更改，我们建议使用 S3 Storage Lens 存储统计管理工具控制面板，而不是使用 Amazon CloudWatch 指标。在 Storage Lens 存储分析功能控制面板中，可以查看以下指标，这些指标监控对象计数或大小：

- 当前版本字节数
- 当前版本对象计数
- 非当前版本字节数
- 非当前版本对象计数
- 删除标记对象计数
- 删除标记存储字节数
- 未完成的分段上传字节数
- 未完成的分段上传对象计数

## 即使在启用了版本控制的存储桶上设置了生命周期规则之后，我的 S3 对象计数仍增加。

在启用了版本控制的存储桶中，当对象到期时，不会从存储桶中完全删除该对象。而是创建删除标记作为对象的最新版本。删除标记仍算作对象。因此，如果创建的生命周期规则仅使当前版本过期，则 S3 桶中的对象计数实际上会增加而不是减少。

例如，假设一个包含 100 个对象的 S3 桶启用了版本控制，并且生命周期规则设置为在 7 天后使对象的当前版本过期。第七天之后，对象计数增加到 200，这是因为除了 100 个原始对象（现在是非当前版本）之外，还创建了 100 个删除标记。有关启用版本控制的桶的 S3 生命周期配置规则操作的更多信息，请参阅对于桶设置生命周期配置。

要永久删除对象，请添加额外的生命周期配置以删除对象的先前版本、过期的删除标记和未完成的分段上传。有关如何创建新的生命周期规则的说明，请参阅对于桶设置生命周期配置。

> **Note**
>
> - Amazon S3 将对象的转换或过期日期舍入到第二天的世界标准时间午夜。
>
>  在评估对象的生命周期操作时，Amazon S3 使用以 UTC 表示的对象创建时间。例如，假设一个不受版本控制的存储桶，其生命周期规则配置为在一天后对象就会到期。假设一个对象是在太平洋夏令时（PDT）的 1 月 1 日 17:05 创建的，该时间对应于 UTC 时间 1 月 2 日 00:05。该对象在 UTC 时间 1 月 3 日 00:05 时已存在一天，因此，当 S3 生命周期在 UTC 时间 1 月 4 日 00:00 评估对象时，该对象符合到期条件。
>
>  由于 Amazon S3 生命周期操作是异步发生的，因此，在生命周期规则中指定的日期与对象的实际物理转换之间可能会有一些延迟。有关更多信息，请参阅转换或到期延迟。
>
>  有关更多信息，请参阅生命周期规则：基于对象的存在期限。
> - 对于受对象锁定保护的 S3 对象，不会永久删除当前版本。而是向对象添加删除标记，使其成为非当前对象。非当前版本将被保留，并且不会永久过期。

## 如何使用生命周期规则清空 S3 桶？

S3 生命周期规则是清空包含数百万个对象的 S3 桶的有效工具。要从 S3 存储桶中删除大量对象，请确保使用以下两对生命周期规则：

- 将对象的当前版本设为过期和永久删除对象的先前版本
- 删除过期的删除标记和删除未完成的分段上传

有关如何创建生命周期配置规则的步骤，请参阅对于桶设置生命周期配置。

> **Note**
>
> 对于受对象锁定保护的 S3 对象，不会永久删除当前版本。而是向对象添加删除标记，使其成为非当前对象。非当前版本将被保留，并且不会永久过期。

## 在将对象转换到成本较低的存储类后，我的 Amazon S3 账单增加了。

将对象转换为成本较低的存储类后，您的账单可能会增加，原因有很多：

- 小型对象的 S3 Glacier 开销费用

  对于每个转换为 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 的对象，与此存储更新关联的总开销为 40KB。作为 40KB 开销的一部分，8KB 用于存储元数据和对象的名称。此 8KB 按照 S3 Standard 费率收费。剩余的 32KB 用于编制索引和相关的元数据。这 32KB 按照 S3 Glacier Flexible Retrieval 或 S3 Glacier Deep Archive 定价收费。

  因此，如果您要存储许多大小较小的对象，我们不建议使用生命周期转换。相反，为了减少任何开销费用，请考虑在将许多较小的对象存储到 Amazon S3 中之前，将它们聚合为数量较少的大型对象。有关成本注意事项的更多信息，请参阅转换为 S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 存储类（对象存档）。

- 最低存储费用

  某些 S3 存储类有最短存储持续时间要求。在满足最短持续时间之前从这些类中删除、覆盖或转换的对象将按比例收取提前转换或删除费用。这些最短存储持续时间要求如下所示：

  - S3 Standard-IA 和 S3 One Zone-IA – 30 天
  - S3 Glacier Flexible Retrieval 和 S3 Glacier Instant Retrieval – 90 天
  - S3 Glacier Deep Archive – 180 天

  有关这些要求的更多信息，请参阅使用 S3 生命周期转换对象的约束部分。有关一般 S3 定价信息，请参阅 Amazon S3 定价和 Amazon 定价计算器。

- 生命周期转换成本

  每次通过生命周期规则将对象转换到不同的存储类时，Amazon S3 都会将该转换视为一个转换请求。这些转换请求的成本未包含在这些存储类的成本中。如果计划转换大量对象，请在转换到较低层时考虑请求成本。有关更多信息，请参阅 Amazon S3 定价。

## 我已经更新了我的桶策略，但我的 S3 对象仍会被过期的生命周期规则删除。

桶策略中的 `Deny` 语句不会阻止在生命周期规则中定义的对象过期。生命周期操作（例如转换或过期）不使用 S3 `DeleteObject` 操作。相反，S3 生命周期操作是使用内部 S3 端点执行的。（有关更多信息，请参阅生命周期和日志记录。）

要防止您的生命周期规则采取任何操作，您必须编辑、删除或禁用该规则。

## 我能否恢复由 S3 生命周期规则过期的 S3 对象？

恢复由 S3 生命周期过期的对象的唯一方法是通过版本控制，版本控制必须在对象符合过期条件之前就位。您无法撤消由生命周期规则执行的过期操作。如果现有的 S3 生命周期规则永久删除了对象，则无法恢复这些对象。要对桶启用版本控制，请参阅the section called “保留对象的多个版本”。

如果您已对桶应用了版本控制，并且对象的非当前版本仍然完好无损，则可以恢复过期对象的先前版本。有关 S3 生命周期规则操作的行为和版本控制状态的更多信息，请参阅描述生命周期操作的元素中的生命周期操作和桶版本控制状态表。

> **Note**
>
> 如果 S3 桶受 Amazon Backup 或 S3 复制保护，则您也可以使用这些功能来恢复过期的对象。

## 为什么我的到期和转换生命周期操作没有发生？

对于已启用版本控制或已暂停版本控制的存储桶，以下注意事项决定了 Amazon S3 如何处理到期操作：

- 对象过期仅适用于对象的当前版本（它对非当前对象版本没有影响）。
- 如果有一个或多个对象版本，并且删除标记是当前版本，则 Amazon S3 不会执行任何操作。
- Amazon S3 不会对应用了 S3 对象锁定的非当前版本的对象执行任何操作。
- 对于具有 PENDING 复制状态的对象，Amazon S3 不会对当前或非当前版本的对象执行任何操作。

生命周期存储类转换具有以下约束：

- 默认情况下，小于 128 KB 的对象不会转换到任何存储类。
- 对象必须存储至少达 30 天，才能转换到 S3 Standard-IA 或 S3 One Zone-IA。
- 对于启用了版本控制或已暂停版本控制的存储桶，无法转换具有 PENDING 复制状态的对象。

## 如何从我的生命周期规则中排除前缀？

S3 生命周期不支持在规则中排除前缀。而是，使用标签来标记要包含在规则中的所有对象。有关在生命周期规则中使用标签的更多信息，请参阅the section called “在创建后的一天内归档所有对象”。

## 如何在我的生命周期规则中包含多个前缀？

S3 生命周期不支持在规则中包含多个前缀。而是，使用标签来标记要包含在规则中的所有对象。有关在生命周期规则中使用标签的更多信息，请参阅the section called “在创建后的一天内归档所有对象”。

但是，如果您有一个或多个前缀以相同的字符开头，则可以通过在筛选条件中指定不带尾部斜杠 (/) 的部分前缀，来将所有这些前缀包含在规则中。例如，假设您有以下前缀：

```
sales1999/
sales2000/
sales2001/
```

要在规则中包含所有三个前缀，请在生命周期规则中指定 `<Prefix>sales</Prefix>`。

# Amazon S3 中的日志记录和监控

监控是保持 Amazon S3 和您的 Amazon 解决方案的可靠性、可用性和性能的重要方面。我们推荐您从 Amazon 解决方案的所有方面收集监控数据，以便更轻松地调试出现的多点故障。在开始监控 Amazon S3 之前，创建一个监控计划，解决以下问题：

- 监控目的是什么？
- 您将监控哪些资源？
- 监控这些资源的频率如何？
- 您将使用哪些监控工具？
- 谁负责执行监控任务？
- 出现错误时应通知谁？

有关 Amazon S3 中的日志记录和监控的更多信息，请参阅以下主题。

> **Note**
>
> 有关将 Amazon S3 Express One Zone 存储类与目录存储桶配合使用的更多信息，请参阅 S3 Express One Zone 和使用目录存储桶。

监控是保持 Amazon S3 和您的 Amazon 解决方案的可靠性、可用性和性能的重要方面。您应该从 Amazon 解决方案的各个部分收集监控数据，以便您可以更轻松地调试多点故障（如果发生）。Amazon 提供了多种工具来监控您的 Amazon S3 资源并对潜在事件做出响应。

Amazon CloudWatch 警报

使用 Amazon CloudWatch 警报，您可以在指定时间段内监控某个指标。如果指标超过给定阈值，则会向 Amazon SNS 主题或 Amazon Auto Scaling 策略发送通知。CloudWatch 警报将不会调用操作，因为这些操作处于特定状态。而是必须在状态已改变并在指定的若干个时间段内保持不变后才调用。有关更多信息，请参阅 使用 Amazon CloudWatch 监控指标。

Amazon CloudTrail 日志

CloudTrail 提供了用户、角色或 Amazon 服务在 Amazon S3 中所执行操作的记录。使用 CloudTrail 收集的信息，您可以确定向 Amazon S3 发出了什么请求、发出请求的 IP 地址、何人发

出的请求、请求的发出时间以及其他详细信息。有关更多信息，请参阅 使用 Amazon CloudTrail 记录 Amazon S3 API 调用。

Amazon GuardDuty

Amazon GuardDuty 是一项威胁检测服务，可持续监控您的账户、容器、工作负载和 Amazon 环境中的数据，以识别 S3 存储桶面临的潜在威胁或安全风险。GuardDuty 还提供了有关所检测到的威胁的丰富上下文信息。GuardDuty 会监控 Amazon CloudTrail 管理日志中是否存在威胁，并显示与安全相关的信息。例如，GuardDuty 会将 API 请求的各个因素纳入考量，如发出请求的用户、发出请求的位置以及请求的特定 API，而这些因素在您的环境中可能存在异常。GuardDuty S3 Protection 会监控 CloudTrail 收集的 S3 数据事件，并识别您环境中所有 S3 存储桶中可能存在的异常和恶意行为。

Amazon S3 访问日志

服务访问日志提供有关对存储桶做出的请求的详细记录。对于许多应用程序而言，服务器访问日志很有用。例如，访问日志信息可能在安全和访问权限审核方面很有用。有关更多信息，请参阅 使用服务器访问日志记录来记录请求。

Amazon Trusted Advisor

Trusted Advisor 凝聚了从为数十万 Amazon 客户提供服务中总结的最佳实践。Trusted Advisor 可检查您的 Amazon 环境，然后在有可能节省开支、提高系统可用性和性能或弥补安全漏洞时为您提供建议。所有 Amazon 客户均有权访问五个 Trusted Advisor 检查。使用“商业”和“企业”支持计划的客户可以查看所有 Trusted Advisor 检查。

Trusted Advisor 有以下与 Amazon S3 相关的检查：

- Amazon S3 存储桶的日志记录配置。
- 具有开放访问权限的 Amazon S3 存储桶的安全性检查。
- 未启用版本控制或已暂停版本控制的 Amazon S3 存储桶的容错检查。

有关更多信息，请参阅 Amazon Web Services 支持 用户指南中的 Amazon Trusted Advisor。

Amazon S3 Storage Lens 存储统计管理工具

Amazon S3 Storage Lens 存储统计管理工具是一项云存储分析功能，您可以使用它在整个组织范围内了解对象存储的使用情况和活动。您可以使用 S3 Storage Lens 存储统计管理工具指标生成摘要见解，例如，了解整个组织中有多少存储空间，或增长最快的桶和前缀是哪些。您还可以使用 S3 Storage Lens 存储统计管理工具指标来识别成本优化机会，实施数据保护和安全最佳实践，并提高应用程序工作负载的性能。

S3 Storage Lens 存储统计管理工具聚合您的指标，并在 Amazon S3 控制台的存储桶页上的“账户快照”部分中显示此信息。S3 Storage Lens 存储统计管理工具还提供了一个交互式控制面板，您可以使用它来可视化见解和趋势，标记异常值，并接收有关优化存储成本和应用数据保护最佳实践的建议。控制面板提供深入分析选项，用于在组织、账户、Amazon Web Services 区域、存储类、存储桶、前缀或 Storage Lens 组级别生成和可视化见解。有关更多信息，请参阅 了解 Amazon S3 Storage Lens 存储统计管理工具。

Amazon S3 清单

Amazon S3 清单会生成一个对象和元数据列表，您可以使用它们来查询和管理您的对象。您可以使用此清单报告来生成细粒度数据，例如对象大小、上次修改日期、加密状态和其它字段。这些报告每天或每周都可用，可自动提供最新的列表。

例如，出于业务、合规性和法规要求，您可以使用 Amazon S3 清单来审计和报告对象的复制和加密状态。您还可以使用 Amazon S3 清单来简化和加快业务工作流和大数据任务，这可以有计划地取代 Amazon S3 同步 `List` API 操作。Amazon S3 清单不使用 `List` API 操作来审计对象，且不会影响存储桶的请求速率。有关更多信息，请参阅 使用 S3 清单对数据进行编目和分析。

Amazon S3 事件通知

通过 Amazon S3 事件通知功能，您可以在 S3 存储桶中发生某些事件时接收通知。要启用通知，请添加一个通知配置，该配置标识您希望 Amazon S3 发布的事件。有关更多信息，请参阅 Amazon S3 事件通知。

Amazon S3 和 Amazon X-Ray

Amazon X-Ray 与 Amazon S3 集成以跟踪更新应用程序 S3 存储桶的上游请求。如果某项服务使用 X-Ray SDK 跟踪请求，则 Amazon S3 可以将跟踪标头发送给 Λ、Amazon SQS 和 Amazon SNS 等下游事件订阅用户。X-Ray 支持跟踪消息以实现 Amazon S3 事件通知。您可以使用 X-Ray 跟踪地图查看 Amazon S3 与应用程序所用其他服务之间的连接。有关更多信息，请参阅 Amazon S3 and X-Ray。

下面的安全最佳实践也处理日志记录和监控：

- Identify and audit all your Amazon S3 buckets
- Implement monitoring using Amazon Web Services monitoring tools
- Enable Amazon Config（启用 Gem）
- Enable Amazon S3 server access logging
- Use CloudTrail
- Monitor Amazon Web Services security advisories

主题


- 监控工具
- Amazon S3 的日志记录选项
- 使用 Amazon CloudTrail 记录 Amazon S3 API 调用
- 使用服务器访问日志记录来记录请求
- 使用 Amazon CloudWatch 监控指标
- Amazon S3 事件通知
- 使用 Amazon S3 Storage Lens 存储统计管理工具评估您的存储活动和使用情况
- 使用 S3 清单对数据进行编目和分析


# 监控工具

Amazon 为您提供了各种可用于监控 Amazon S3 的工具。您可以配置其中的一些工具来为您执行监控任务，但有些工具需要手动干预。建议您尽可能实现监控任务自动化。

## 自动监控工具

您可以使用以下自动化监控工具来监控 Amazon S3，并在出现错误时进行报告：

- Amazon CloudWatch 警报 – 按您指定的时间段观察单个指标，并根据相对于给定阈值的指标值在若干时间段内执行一项或多项操作。操作是一个发送到 Amazon Simple Notification Service (Amazon SNS) 主题或 Amazon EC2 Auto Scaling 策略的通知。CloudWatch 警报将不会调用操作，因为这些操作处于特定状态。该状态必须已改变并在指定的若干个时间段内保持不变。有关更多信息，请参阅使用 Amazon CloudWatch 监控指标。
- Amazon CloudTrail 日志监控 – 在账户间共享日志文件，通过将 CloudTrail 日志文件发送到 CloudWatch Logs 对它们进行实时监控，在 Java 中编写日志处理应用程序，以及验证您的日志文件在由 CloudTrail 交付后未发生更改。有关更多信息，请参阅 使用 Amazon CloudTrail 记录 Amazon S3 API 调用。

## 手动监控工具

监控 Amazon S3 的另一个重要环节是手动监控 CloudWatch 警报未涵盖的那些项。Amazon S3、CloudWatch、Trusted Advisor 和其他 Amazon Web Services Management Console 控制面板提供您的 Amazon 环境状态的概览视图。您可能要启用服务器访问日志记录，以跟踪针对存储桶的访问

请求。每个访问日志记录都提供有关单个访问请求的详细信息，如请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果有）。有关更多信息，请参阅 使用服务器访问日志记录来记录请求。

- Amazon S3 控制面板显示以下内容：
  - 您的存储桶及其包含的对象和属性
- CloudWatch 主页显示以下内容：
  - 当前警报和状态
  - 告警和资源图表
  - 服务运行状况

  此外，您还可以使用 CloudWatch 执行以下操作：
  - 创建自定义控制面板以监控您关心的服务。
  - 绘制指标数据图，以排除问题并弄清楚趋势。
  - 搜索并浏览您所有的 Amazon 资源指标。
  - 创建和编辑警报以接收有关问题的通知。
- Amazon Trusted Advisor 可以帮助您监控 Amazon 资源以提高性能、可靠性、安全性和成本效益。四个 Trusted Advisor 检查可供所有用户使用；超过 50 个检查可供具有“商业”或“企业”支持计划的用户使用。有关更多信息，请参阅 Amazon Trusted Advisor。

  Trusted Advisor 具有与 Amazon S3 相关的以下检查：
  - 检查 Amazon S3 存储桶的日志记录配置。
  - 具有开放访问权限的 Amazon S3 存储桶的安全性检查。
  - 未启用版本控制或已暂停版本控制的 Amazon S3 存储桶的容错检查。

# Amazon S3 的日志记录选项

您可以记录用户、角色或 Amazon Web Services 服务对 Amazon S3 资源所采取的操作，并维护日志记录以满足审计和合规性目的。为此，您可以使用服务器访问日志记录、Amazon CloudTrail 日志记录，或两者的组合。我们建议您使用 CloudTrail 为您的 Amazon S3 资源记录存储桶级和对象级操作的日志。请参阅下面几节，了解有关每个选项的更多信息：

- 使用服务器访问日志记录来记录请求
- 使用 Amazon CloudTrail 记录 Amazon S3 API 调用

下表列出了 CloudTrail 日志和 Amazon S3 服务器访问日志的关键属性。要确保 CloudTrail 满足您的安全要求，请查看表和注释。

| 日志属性 | Amazon CloudTrail | Amazon S3 服务器日志 |
| --- | --- | --- |
| 可以转发到其他系统（Amazon CloudWatch Logs、Amazon CloudWatch Events） | 是 | No |
| 将日志传输到多个目标（例如，将相同的日志发送到两个不同的存储桶） | 是 | No |
| 对对象的子级开启日志（前缀） | 是 | No |
| 跨账户日志传输（不同账户拥有的目标和源存储桶） | 是 | No |
| 使用数字签名或哈希对日志文件进行完整性验证 | 是 | No |
| 默认或选择加密日志文件 | 是 | No |
| 对象操作（使用 Amazon S3 API） | 支持 | 是 |
| 存储桶操作（使用 Amazon S3 API） | 支持 | 是 |
| 日志的可搜索 UI | 是 | No |
| 对象锁定参数的字段，Amazon S3 选择日志记录的属性 | 是 | No |
| 日志记录的 `Object Size`、`Total Time`、`Turn-Around Time` 和 `HTTP Referer` 的字段 | 否 | 是 |

| 日志属性 | Amazon CloudTrail | Amazon S3 服务器日志 |
| --- | --- | --- |
| 生命周期转换，过期，还原 | 否 | 是 |
| 批处理删除操作中键的日志记录 | 否 | 是 |
| 身份验证失败[1] | 否 | 是 |
| 日志得到传输的账户 | 存储桶拥有者[2] 以及请求者 | 仅限存储桶拥有者 |
| Performance and Cost | Amazon CloudTrail | Amazon S3 Server Logs |
| 价格 | 管理事件（第一次传输）免费；数据事件引发费用，此外还有日志存储 | 除日志存储之外，没有其他费用 |
| 日志传输的速度 | 每 5 分钟传输数据事件；每 15 分钟传输管理事件 | 几个小时内 |
| 日志格式 | JSON | 具有以空格分隔、新行分隔的记录的日志文件 |

备注

1. CloudTrail 对于未通过身份验证（其中，提供的凭证无效）或由于重定向而失败（错误代码 `301 Moved Permanently`）的请求不传输日志。但是，对于授权失败的请求 (`AccessDenied`) 和匿名用户发出的请求，它的确包括日志。
2. 当账户对请求中的此对象没有完全访问权限时，S3 存储桶拥有者将接收 CloudTrail 日志。有关更多信息，请参阅 跨账户情形中的 Amazon S3 对象级操作。
3. 对于 VPC 端点策略拒绝的 VPC 端点请求，或者对于在评估 VPC 策略之前失败的请求，S3 不支持向请求者或存储桶拥有者传输 CloudTrail 日志或服务器访问日志。

# 使用 Amazon CloudTrail 记录 Amazon S3 API 调用

Amazon S3 与 Amazon CloudTrail 集成，后者是一项提供用户、角色或 Amazon Web Services 服务所采取操作的记录的服务。CloudTrail 将 Amazon S3 的所有 API 调用作为事件捕获。捕获的调用中包括通过 Amazon S3 控制台的调用和对 Amazon S3 API 操作的代码调用。借助通过 CloudTrail 收集的

信息，您可以确定向 Amazon S3 发出哪些请求、发出请求的 IP 地址、请求的发出时间以及其它详细信息。

每个事件或日志条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是使用根用户凭证还是用户凭证发出的。
- 请求是否代表 IAM Identity Center 用户发出。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 Amazon Web Services 服务 发出。

当您创建账户并可以自动访问 CloudTrail 事件历史记录时，CloudTrail 在您的 Amazon Web Services 账户 中处于活动状态。CloudTrail 事件历史记录提供对 Amazon Web Services 区域 中过去 90 天的已记录管理事件的可查看、可搜索、可下载和不可变记录。有关更多信息，请参见《Amazon CloudTrail 用户指南》的 使用 CloudTrail 事件历史记录。查看事件历史记录不会收取 CloudTrail 费用。

要持续记录您的 Amazon Web Services 账户 过去 90 天的事件，请创建跟踪或 CloudTrail Lake 事件数据存储。

CloudTrail 跟踪

通过跟踪记录，CloudTrail 可将日志文件传送至 Simple Storage Service (Amazon S3) 存储桶。使用 Amazon Web Services Management Console 创建的所有跟踪均具有多区域属性。您可以通过使用 Amazon CLI 创建单区域或多区域跟踪。建议创建多区域跟踪，因为您可记录您账户中的所有 Amazon Web Services 区域 的活动。如果您创建单区域跟踪，则只能查看跟踪的 Amazon Web Services 区域 中记录的事件。有关跟踪的更多信息，请参阅《Amazon CloudTrail 用户指南》中的为您的 Amazon Web Services 账户 创建跟踪和为组织创建跟踪。

通过创建跟踪，您可以从 CloudTrail 免费向您的 Amazon S3 存储桶传送一份正在进行的管理事件的副本，但会收取 Amazon S3 存储费用。有关 CloudTrail 定价的更多信息，请参阅 Amazon CloudTrail 定价。有关 Amazon S3 定价的信息，请参阅 Amazon S3 定价。

CloudTrail Lake 事件数据存储

CloudTrail Lake 允许您对事件运行基于 SQL 的查询。CloudTrail Lake 可将基于行的 JSON 格式的现有事件转换为 Apache ORC 格式。ORC 是一种针对快速检索数据进行优化的列式存储格式。事件将被聚合到事件数据存储中，它是基于您通过应用高级事件选择器选择的条件的不可变的事件集合。应用于事件数据存储的选择器用于控制哪些事件持续存在并可供您查询。有关 CloudTrail Lake 的更多信息，请参阅《Amazon CloudTrail 用户指南》中的使用 Amazon CloudTrail Lake。

CloudTrail Lake 事件数据存储和查询会产生费用。创建事件数据存储时，您可以选择要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及事件数据存储的默认和最长保留期。有关 CloudTrail 定价的更多信息，请参阅 Amazon CloudTrail 定价。

日志文件可以在存储桶中存储任意长时间，不过您也可以定义 Amazon S3 生命周期规则以自动归档或删除日志文件。默认情况下，将使用 Amazon S3 服务器端加密 (SSE) 对日志文件进行加密。

## 将 CloudTrail 日志与 Amazon S3 服务器访问日志和 CloudWatch Logs 结合使用

Amazon CloudTrail 日志记录用户、角色或 Amazon 服务在 Amazon S3 中执行的操作，而 Amazon S3 服务器访问日志提供向 S3 存储桶发出的请求的详细记录。有关不同日志的工作方式及其属性、性能和成本的更多信息，请参阅 the section called “日志记录选项”。

您可以将 Amazon CloudTrail 日志与 Amazon S3 的服务器访问日志搭配使用。CloudTrail 日志为您提供了 Amazon S3 存储桶级别和对象级操作的详细 API 跟踪。Amazon S3 的服务器访问日志可让您了解对于 Amazon S3 中您的数据的对象级操作。有关服务器访问日志的更多信息，请参阅 使用服务器访问日志记录来记录请求。

您还可以将 CloudTrail 日志与 Amazon S3 的 Amazon CloudWatch 一起使用。CloudTrail 与 CloudWatch Logs 集成可将 CloudTrail 捕获到的 S3 存储桶级 API 活动传送给您指定的 CloudWatch 日志组中的 CloudWatch 日志流。您可以创建用于监控特定 API 活动的 CloudWatch 警报，并在此特定 API 活动发生时收到电子邮件通知。有关用于监控特定 API 活动的 CloudWatch 警报的更多信息，请参阅 Amazon CloudTrail 用户指南。有关将 CloudWatch 与 Amazon S3 结合使用的更多信息，请参阅 使用 Amazon CloudWatch 监控指标。

> **Note**
>
> 当 VPC 端点策略拒绝时，S3 不支持向 VPC 端点请求的请求者或存储桶拥有者传输 CloudTrail 日志。

## 使用 Amazon S3 SOAP API 调用进行 CloudTrail 跟踪

CloudTrail 跟踪 Amazon S3 SOAP API 调用。Amazon S3 HTTP 上的 SOAP 支持已弃用，但是仍可在 HTTPS 上使用。有关 Amazon S3 SOAP 支持的更多信息，请参阅《Amazon S3 API 参考》中的 Appendix: SOAP API。

> **Important**
>
> SOAP 不支持较新的 Amazon S3 特征。我们建议您使用 REST API 或 Amazon SDK。

下表显示了 CloudTrail 日志记录所跟踪的 Amazon S3 SOAP 操作。

| SOAP API 名称 | CloudTrail 日志中使用的 API 事件名称 |
| --- | --- |
| ListAllMyBuckets | `ListBuckets` |
| CreateBucket | `CreateBucket` |
| DeleteBucket | `DeleteBucket` |
| GetBucketAccessControlPolicy | `GetBucketAcl` |
| SetBucketAccessControlPolicy | `PutBucketAcl` |
| GetBucketLoggingStatus | `GetBucketLogging` |
| SetBucketLoggingStatus | `PutBucketLogging` |

有关 CloudTrail 和 Amazon S3 的更多信息，请参阅以下主题：

主题

- Amazon S3 CloudTrail 事件
- Amazon S3 和 S3 on Outposts 的 CloudTrail 日志文件条目
- 为 S3 存储桶和对象启用 CloudTrail 事件日志记录
- 使用 CloudTrail 识别 Amazon S3 请求

## Amazon S3 CloudTrail 事件

> **Important**
>
> Amazon S3 现在将具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）作为 Amazon S3 中每个存储桶的基本加密级别。从 2023 年 1 月 5 日起，上传到 Amazon S3 的所有新对象都

将自动加密，不会产生额外费用，也不会影响性能。S3 存储桶默认加密配置和上传的新对象的自动加密状态可在 Amazon CloudTrail 日志、S3 清单、S3 Storage Lens 存储统计管理工具、Amazon S3 控制台中获得，并可用作 Amazon Command Line Interface 和 Amazon SDK 中的附加 Amazon S3 API 响应标头。有关更多信息，请参阅默认加密常见问题解答。

本节提供有关 S3 记录到 CloudTrail 的事件的信息。

## CloudTrail 中的 Amazon S3 数据事件

数据事件可提供对资源或在资源中所执行资源操作（例如，读取或写入 Amazon S3 对象）的相关信息。这些也称为数据层面操作。数据事件通常是高容量活动。默认情况下，CloudTrail 不记录数据事件。CloudTrail 事件历史记录不记录数据事件。

记录数据事件将收取额外费用。有关 CloudTrail 定价的更多信息，请参阅 Amazon CloudTrail 定价。

您可以使用 CloudTrail 控制台、Amazon CLI 或 CloudTrail API 操作记录 Amazon S3 资源类型的数据事件。有关如何记录数据事件的更多信息，请参阅《Amazon CloudTrail 用户指南》中的使用 Amazon Web Services Management Console 记录数据事件和使用 Amazon Command Line Interface 记录数据事件。

下表列出了您可以为其记录数据事件的 Amazon S3 资源类型。数据事件类型（控制台）列显示可从 CloudTrail 控制台上的数据事件类型列表中选择的值。resources.type 值列显示了您在使用 Amazon CLI 或 CloudTrail API 配置高级事件选择器时需要指定的 `resources.type` 值。记录到 CloudTrail 的数据 API 列显示了针对该资源类型记录到 CloudTrail 的 API 调用。

| 数据事件类型（控制台） | resources.type 值 | 记录至 CloudTrail 的数据 API |
| --- | --- | --- |
| S3 | `Amazon::S3::Object` | • AbortMultipartUpload<br>• CompleteMultipartUpload<br>• CopyObject<br>• CreateMultipartUpload<br>• DeleteObject<br>• DeleteObjectTagging<br>• DeleteObjects<br>• GetObject |

| 数据事件类型（控制台） | resources.type 值 | 记录至 CloudTrail 的数据 API |
| --- | --- | --- |
| | | • GetObjectAcl<br>• GetObjectAttributes<br>• GetObjectLegalHold<br>• GetObjectRetention<br>• GetObjectTagging<br>• GetObjectTorrent<br>• HeadObject<br>• HeadBucket<br>• ListMultipartUploads<br>• ListObjectVersions<br>• ListObjects<br>• ListParts<br>• PutObject<br>• PutObjectAcl<br>• PutObjectLegalHold<br>• PutObjectRetention<br>• PutObjectTagging<br>• RestoreObject<br>• SelectObjectContent<br>• UploadPart<br>• UploadPartCopy |

| 数据事件类型（控制台） | resources.type 值 | 记录至 CloudTrail 的数据 API |
| --- | --- | --- |
| S3 Express One Zone | `Amazon::S3Express::Object` | • AbortMultipartUpload<br>• CompleteMultipartUpload<br>• CreateSession<br>• CopyObject<br>• CreateMultipartUpload<br>• DeleteObject<br>• DeleteObjects<br>• GetObject<br>• GetObjectAttributes<br>• HeadBucket<br>• HeadObject<br>• ListObjectsV2<br>• ListParts<br>• PutObject<br>• UploadPart<br>• UploadPartCopy |

| 数据事件类型（控制台） | resources.type 值 | 记录至 CloudTrail 的数据 API |
| --- | --- | --- |
| S3 接入点 | `Amazon::S3::AccessPoint` | • AbortMultipartUpload<br>• CompleteMultipartUpload<br>• CopyObject（仅限同区域副本）<br>• CreateMultipartUpload<br>• DeleteObject<br>• DeleteObjectTagging<br>• GetBucketAcl<br>• GetBucketCors<br>• GetBucketLocation<br>• GetBucketNotificationConfiguration<br>• GetBucketPolicy<br>• GetObject<br>• GetObjectAcl<br>• GetObjectAttributes<br>• GetObjectLegalHold<br>• GetObjectRetention<br>• GetObjectTagging<br>• HeadBucket<br>• HeadObject<br>• ListMultipartUploads<br>• ListObjects<br>• ListObjectsV2<br>• ListObjectVersions<br>• ListParts<br>• Presign<br>• PutObject<br>• PutObjectLegalHold |

| 数据事件类型（控制台） | resources.type 值 | 记录至 CloudTrail 的数据 API |
| --- | --- | --- |
| | | • PutObjectRetention<br>• PutObjectAcl<br>• PutObjectTagging<br>• RestoreObject<br>• UploadPart<br>• UploadPartCopy（仅限同区域副本） |

| 数据事件类型（控制台） | resources.type 值 | 记录至 CloudTrail 的数据 API |
| --- | --- | --- |
| S3 对象 Lambda | `Amazon::S3ObjectLambda::AccessPoint` | • AbortMultipartUpload<br>• CompleteMultipartUpload<br>• CopyObject（仅限同区域副本）<br>• CreateMultipartUpload<br>• DeleteObject<br>• DeleteObjectTagging<br>• GetObject<br>• GetObjectAcl<br>• GetObjectLegalHold<br>• GetObjectRetention<br>• GetObjectTagging<br>• HeadObject<br>• ListMultipartUploads<br>• ListObjects<br>• ListObjectVersions<br>• ListParts<br>• PutObject<br>• PutObjectLegalHold<br>• PutObjectRetention<br>• PutObjectAcl<br>• PutObjectTagging<br>• RestoreObject<br>• UploadPart<br>• WriteGetObjectResponse |

| 数据事件类型（控制台） | resources.type 值 | 记录至 CloudTrail 的数据 API |
| --- | --- | --- |
| S3 Outposts | `Amazon::S3Outposts::Object` | • AbortMultipartUpload<br>• CompleteMultipartUpload<br>• CopyObject（仅限同区域副本）<br>• CreateMultipartUpload<br>• DeleteObject<br>• DeleteObjectTagging<br>• GetObject<br>• GetObjectTagging<br>• HeadObject<br>• ListMultipartUploads<br>• ListObjects<br>• ListObjectsV2<br>• ListParts<br>• PutObject<br>• PutObjectTagging<br>• UploadPart<br>• UploadPartCopy |

您可以将高级事件选择器配置为在 `eventName`、`readOnly` 和 `resources.ARN` 字段上进行筛选，从而仅记录那些对您很重要的事件。有关这些字段的更多信息，请参阅《Amazon CloudTrail API 参考》中的 AdvancedFieldSelector。

## CloudTrail 中的 Amazon S3 管理事件

Amazon S3 将所有控制面板操作记录为管理事件。有关 S3 API 操作的更多信息，请参阅 Amazon S3 API Reference。

## CloudTrail 如何捕获向 Amazon S3 发出的请求

默认情况下，CloudTrail 会记录在过去 90 天内进行的 S3 存储桶级别 API 调用，但不会记录向对象发出的请求。存储桶级调用包括诸如

`CreateBucket`、`DeleteBucket`、`PutBucketLifecycle`、`PutBucketPolicy` 等事件。您可以在 CloudTrail 控制台上看到存储桶级事件。但是，您无法在此查看数据事件（Amazon S3 对象级调用），您必须解析或查询它们的 CloudTrail 日志。

## CloudTrail 日志记录跟踪的 Amazon S3 账户级操作

CloudTrail 会记录账户级操作。Amazon S3 记录与其他 Amazon Web Services 服务记录一起写入日志文件。CloudTrail 基于时间段和文件大小来确定何时创建并写入新文件。

本节中的表格列出了可用于 CloudTrail 日志记录的 Amazon S3 账户级操作。

CloudTrail 日志记录跟踪的 Amazon S3 账户级 API 操作显示为以下事件名称。CloudTrail 事件名称与 API 操作名称不同。例如，DeletePublicAccessBlock 是 DeleteAccountPublicAccessBlock。

- DeleteAccountPublicAccessBlock
- GetAccountPublicAccessBlock
- PutAccountPublicAccessBlock

## CloudTrail 日志记录跟踪的 Amazon S3 存储桶级操作

默认情况下，CloudTrail 将记录通用存储桶的存储桶级操作。Amazon S3 记录与其他 Amazon 服务记录一起写入日志文件。CloudTrail 基于时间段和文件大小来确定何时创建并写入新文件。

此部分列出了可用于 CloudTrail 日志记录的 Amazon S3 存储桶级操作。

CloudTrail 日志记录跟踪的 Amazon S3 存储桶级 API 操作显示为以下事件名称。在某些情况下，CloudTrail 事件名称与 API 操作名称不同。例如，`PutBucketLifecycleConfiguration` 为 `PutBucketLifecycle`。

- CreateBucket
- CreateBucketMetadataTableConfiguration
- DeleteBucket
- DeleteBucketAnalyticsConfiguration
- DeleteBucketCors
- DeleteBucketEncryption
- DeleteBucketIntelligentTieringConfiguration

- DeleteBucketInventoryConfiguration
- DeleteBucketLifecycle
- DeleteBucketMetadataTableConfiguration
- DeleteBucketMetricsConfiguration
- DeleteBucketOwnershipControls
- DeleteBucketPolicy
- DeleteBucketPublicAccessBlock
- DeleteBucketReplication
- DeleteBucketTagging
- GetAccelerateConfiguration
- GetBucketAcl
- GetBucketAnalyticsConfiguration
- GetBucketCors
- GetBucketEncryption
- GetBucketIntelligentTieringConfiguration
- GetBucketInventoryConfiguration
- GetBucketLifecycle
- GetBucketLocation
- GetBucketLogging
- GetBucketMetadataTableConfiguration
- GetBucketMetricsConfiguration
- GetBucketNotification
- GetBucketObjectLockConfiguration
- GetBucketOwnershipControls
- GetBucketPolicy
- GetBucketPolicyStatus
- GetBucketPublicAccessBlock
- GetBucketReplication

- GetBucketRequestPayment
- GetBucketTagging
- GetBucketVersioning
- GetBucketWebsite
- HeadBucket
- ListBuckets
- PutAccelerateConfiguration
- PutBucketAcl
- PutBucketAnalyticsConfiguration
- PutBucketCors
- PutBucketEncryption
- PutBucketIntelligentTieringConfiguration
- PutBucketInventoryConfiguration
- PutBucketLifecycle
- PutBucketLogging
- PutBucketMetricsConfiguration
- PutBucketNotification
- PutBucketObjectLockConfiguration
- PutBucketOwnershipControls
- PutBucketPolicy
- PutBucketPublicAccessBlock
- PutBucketReplication
- PutBucketRequestPayment
- PutBucketTagging
- PutBucketVersioning
- PutBucketWebsite

除了这些 API 操作之外，还可以使用 OPTIONS object 对象级操作。由于此操作将检查存储桶的 CORS 配置，因此它被视为 CloudTrail 日志记录中的存储桶级操作。

## CloudTrail 日志记录跟踪的 Amazon S3 Express One Zone 存储类存储桶级别（区域 API 端点）操作

默认情况下，CloudTrail 将目录存储桶的存储桶级操作记录为管理事件。S3 Express One Zone 的 CloudTrail 管理事件的 `eventsource` 为 `s3express.amazonaws.com`。

以下区域端点 API 操作将记录到 CloudTrail 中。

- CreateBucket
- DeleteBucket
- DeleteBucketPolicy
- GetBucketPolicy
- PutBucketPolicy
- ListDirectoryBuckets
- PutBucketEncryption
- GetBucketEncryption
- DeleteBucketEncryption

有关更多信息，请参阅使用 Amazon CloudTrail 为 S3 Express One Zone 记录日志

## 跨账户情形中的 Amazon S3 对象级操作

下面是涉及跨账户情形中的对象级 API 调用的特殊使用案例以及报告 CloudTrail 日志的方法。CloudTrail 会将日志提供给申请方（进行 API 调用的账户），除非在某些拒绝访问的情况下，其中日志条目被编辑或省略。在设置跨账户访问时，请考虑本部分中的示例。

> **Note**
>
> 这些示例假定 CloudTrail 日志已适当配置。

示例 1：CloudTrail 将日志提供给存储桶拥有者

即使存储桶拥有者不具有执行相同对象 API 操作的权限，CloudTrail 也会将日志传递给存储桶拥有者。请考虑以下跨账户情形：

- 账户 A 拥有该存储桶。

- 账户 B（请求者）尝试访问该存储桶中的对象。
- 账户 C 拥有该对象。账户 C 可能与账户 A 是同一个账户，也可能不是同一个账户。

> **Note**
>
> CloudTrail 始终将对象级 API 日志提供给请求者（账户 B）。此外，即使存储桶拥有者不拥有该对象（账户 C）或对该对象不具有执行相同 API 操作的权限，CloudTrail 也会向存储桶拥有者（账户 A）提供相同的日志。

示例 2：CloudTrail 没有使设置对象 ACL 时使用的电子邮件地址激增

请考虑以下跨账户情形：

- 账户 A 拥有该存储桶。
- 账户 B（请求者）使用电子邮件地址发送了一个设置对象 ACL 授权的请求。有关 ACL 的更多信息，请参阅 访问控制列表 (ACL) 概述。

该请求方将获取日志以及电子邮件信息。但是，存储桶拥有者（如果他们像在示例 1 中一样有资格接收日志）将获取报告该事件的 CloudTrail 日志。但是，存储桶拥有者不会获取 ACL 配置信息，尤其是被授权者电子邮件地址和授权。日志为存储桶拥有者提供的唯一信息是账户 B 进行了 ACL API 调用。

## Amazon S3 和 S3 on Outposts 的 CloudTrail 日志文件条目

> **Important**
>
> Amazon S3 现在将具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）作为 Amazon S3 中每个存储桶的基本加密级别。从 2023 年 1 月 5 日起，上传到 Amazon S3 的所有新对象都将自动加密，不会产生额外费用，也不会影响性能。S3 存储桶默认加密配置和上传的新对象的自动加密状态可在 Amazon CloudTrail 日志、S3 清单、S3 Storage Lens 存储统计管理工具、Amazon S3 控制台中获得，并可用作 Amazon Command Line Interface 和 Amazon SDK 中的附加 Amazon S3 API 响应标头。有关更多信息，请参阅默认加密常见问题解答。

一个事件表示一个来自任何源的请求，包括有关所请求的 API 操作、操作的日期和时间、请求参数等方面的信息。CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此事件不会按任何特定顺序显示。

> **Note**
>
> 要查看 Amazon S3 Express One Zone 存储类的 CloudTrail 日志文件示例，请参阅 CloudTrail log file examples for S3 Express One Zone。

有关更多信息，请参阅以下示例。

主题

- 示例：Amazon S3 的 CloudTrail 日志文件条目

## 示例：Amazon S3 的 CloudTrail 日志文件条目

下面的示例显示了一个 CloudTrail 日志条目，该条目说明了 GET 服务、PutBucketAcl 和 GetBucketVersioning 操作。


```
{
    "Records": [
    {
        "eventVersion": "1.03",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "111122223333",
            "arn": "arn:aws:iam::111122223333:user/myUserName",
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "userName": "myUserName"
        },
        "eventTime": "2019-02-01T03:18:19Z",
        "eventSource": "s3.amazonaws.com",
        "eventName": "ListBuckets",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "[]",
        "requestParameters": {
            "host": [
                "s3.us-west-2.amazonaws.com"
            ]
        },
        "responseElements": null,
        "additionalEventData": {
```

```
            "SignatureVersion": "SigV2",
            "AuthenticationMethod": "QueryString",
            "aclRequired": "Yes"
    },
        "requestID": "47B8E8D397DCE7A6",
        "eventID": "cdc4b7ed-e171-4cef-975a-ad829d4123e8",
        "eventType": "AwsApiCall",
        "recipientAccountId": "444455556666",
        "tlsDetails": {
            "tlsVersion": "TLSv1.2",
            "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
            "clientProvidedHostHeader": "s3.amazonaws.com"
    }
    },
    {
       "eventVersion": "1.03",
       "userIdentity": {
            "type": "IAMUser",
            "principalId": "111122223333",
            "arn": "arn:aws:iam::111122223333:user/myUserName",
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "userName": "myUserName"
        },
      "eventTime": "2019-02-01T03:22:33Z",
      "eventSource": "s3.amazonaws.com",
      "eventName": "PutBucketAcl",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "",
      "userAgent": "[]",
      "requestParameters": {
          "bucketName": "",
          "AccessControlPolicy": {
              "AccessControlList": {
                  "Grant": {
                      "Grantee": {
                          "xsi:type": "CanonicalUser",
                          "xmlns:xsi": "http://www.w3.org/2001/XMLSchema-instance",
                          "ID":
"d25639fbe9c19cd30a4c0f43fbf00e2d3f96400a9aa8dabfbbebe1906Example"
                       },
                      "Permission": "FULL_CONTROL"
                  }
              },
```

```
            "xmlns": "http://s3.amazonaws.com/doc/2006-03-01/",
            "Owner": {
                "ID":
"d25639fbe9c19cd30a4c0f43fbf00e2d3f96400a9aa8dabfbbebe1906Example"
            }
        },
        "host": [
            "s3.us-west-2.amazonaws.com"
        ],
        "acl": [
            ""
        ]
    },
    "responseElements": null,
    "additionalEventData": {
        "SignatureVersion": "SigV4",
        "CipherSuite": "ECDHE-RSA-AES128-SHA",
        "AuthenticationMethod": "AuthHeader"
    },
    "requestID": "BD8798EACDD16751",
    "eventID": "607b9532-1423-41c7-b048-ec2641693c47",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333",
    "tlsDetails": {
          "tlsVersion": "TLSv1.2",
          "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
          "clientProvidedHostHeader": "s3.amazonaws.com"
  }
  },
  {
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "111122223333",
        "arn": "arn:aws:iam::111122223333:user/myUserName",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "myUserName"
      },
    "eventTime": "2019-02-01T03:26:37Z",
    "eventSource": "s3.amazonaws.com",
    "eventName": "GetBucketVersioning",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "",
```

```
      "userAgent": "[]",
      "requestParameters": {
          "host": [
              "s3.us-west-2.amazonaws.com"
          ],
          "bucketName": "amzn-s3-demo-bucket1",
          "versioning": [
              ""
          ]
      },
      "responseElements": null,
      "additionalEventData": {
          "SignatureVersion": "SigV4",
          "CipherSuite": "ECDHE-RSA-AES128-SHA",
          "AuthenticationMethod": "AuthHeader"
    },
      "requestID": "07D681279BD94AED",
      "eventID": "f2b287f3-0df1-4961-a2f4-c4bdfed47657",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333",
      "tlsDetails": {
            "tlsVersion": "TLSv1.2",
            "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
            "clientProvidedHostHeader": "s3.amazonaws.com"
    }
    }
  ]
}
```


## 为 S3 存储桶和对象启用 CloudTrail 事件日志记录

您可以使用 CloudTrail 数据事件获取有关 Amazon S3 中存储桶和对象级别请求的信息。要为您的所有存储桶或特定存储桶列表启用 CloudTrail 数据事件，您必须在 CloudTrail 中手动创建跟踪记录。

> **Note**
>
> - CloudTrail 的默认设置是仅查找管理事件。请检查以确保已为您的账户启用数据事件。
> - 利用正在生成高工作负载的 S3 存储桶，您可以在很短时间内快速生成数千条日志。请注意您为某个繁忙存储桶启用 CloudTrail 数据事件所选择的时长。

CloudTrail 将 Amazon S3 数据事件日志存储在您选择的 S3 存储桶中。考虑在单独的 Amazon Web Services 账户中使用一个存储桶将多个存储桶中您可能拥有的事件整理到一个集中位置，以便更轻松地进行查询和分析。Amazon Organizations 可帮助您创建与拥有您所监控的存储桶的账户关联的 Amazon Web Services 账户。有关更多信息，请参阅《Amazon Organizations 用户指南》中的什么是 Amazon Organizations？。

在 CloudTrail 中记录跟踪的数据事件时，您可以选择使用高级事件选择器或基本事件选择器，来记录存储在通用存储桶中的对象的数据事件。要记录存储在目录存储桶中的对象的数据事件，必须使用高级事件选择器。有关更多信息，请参阅使用 Amazon CloudTrail 为 S3 Express One Zone 记录日志。

在 CloudTrail 控制台中使用高级事件选择器创建跟踪时，在数据事件部分中，您可以在记录选择器模板中选择记录所有事件，来记录所有对象级事件。在 CloudTrail 中使用基本事件选择器创建跟踪时，在数据事件部分中，您可以选中选择您账户中的所有 S3 存储桶复选框以记录所有对象级事件。

> **Note**
>
> - 最佳实践是为 Amazon CloudTrail 数据事件存储桶创建生命周期配置。配置生命周期配置，以便在您认为需要审计日志文件的时间段之后定期删除这些日志文件。这样做可以减少 Athena 为每个查询分析的数据量。有关更多信息，请参阅 在存储桶上设置 S3 生命周期配置。
> - 有关日志记录格式的更多信息，请参阅使用 Amazon CloudTrail 记录 Amazon S3 API 调用。
> - 有关如何查询 CloudTrail 日志的示例，请参阅 Amazon 大数据博客文章使用 Amazon CloudTrail 和 Amazon Athena 分析安全性、合规性和操作活动。

## 使用控制台为存储桶中的对象启用日志记录功能

您可以使用 Amazon S3 控制台配置 Amazon CloudTrail 跟踪来记录 S3 存储桶中的对象的数据事件。CloudTrail 支持记录 Amazon S3 对象级别 API 操作，例如 `GetObject`、`DeleteObject` 和 `PutObject`。这些事件称为数据事件。

默认情况下，CloudTrail 跟踪不会记录数据事件，但您可以将跟踪配置为记录您指定的 S3 存储桶的数据事件，或记录 Amazon Web Services 账户 中所有 Amazon S3 存储桶的数据事件。有关更多信息，请参阅 使用 Amazon CloudTrail 记录 Amazon S3 API 调用。

CloudTrail 不会在 CloudTrail 事件历史记录中填充数据事件。此外，并非所有存储桶级别的操作都会填充在 CloudTrail 事件历史记录中。有关 CloudTrail 日志记录跟踪的 Amazon S3 存储桶级 API 操作

的更多信息，请参阅CloudTrail 日志记录跟踪的 Amazon S3 存储桶级操作。有关如何查询 CloudTrail 日志的更多信息，请参阅关于使用 Amazon CloudWatch Logs 筛选条件模式和 Amazon Athena 查询 CloudTrail 日志的 Amazon 知识中心文章。

要配置跟踪以记录某个 S3 存储桶的数据事件，您可以使用 Amazon CloudTrail 控制台或 Amazon S3 控制台。如果您要配置跟踪以记录您的 Amazon Web Services 账户 中所有 Amazon S3 存储桶的数据事件，使用 CloudTrail 控制台会更轻松。有关使用 CloudTrail 控制台配置跟踪以记录 S3 数据事件的信息，请参阅 Amazon CloudTrail 用户指南中的数据事件。

> **Important**
>
> 记录数据事件将收取额外费用。有关更多信息，请参阅 Amazon CloudTrail 定价。

以下过程演示如何使用 Amazon S3 控制台配置 CloudTrail 跟踪来记录 S3 存储桶的数据事件。

为 S3 通用存储桶或 S3 目录存储桶中的对象启用 CloudTrail 数据事件日志记录

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets（存储桶）列表中，请选择存储桶的名称。
3. 选择 Properties (属性)。
4. 在 Amazon CloudTrail data events (Amazon CloudTrail 数据事件) 下，请选择 Configure in CloudTrail (在 CloudTrail 中配置)。

   您可以创建新的 CloudTrail 跟踪或重复使用现有跟踪，并配置要在跟踪中记录的 Amazon S3 数据事件。有关如何在 CloudTrail 控制台中创建跟踪的信息，请参阅 Amazon CloudTrail 用户指南中的使用控制台创建和更新跟踪。有关如何在 CloudTrail 控制台中配置 Amazon S3 数据事件日志记录的信息，请参阅 Amazon CloudTrail 用户指南中的记录 Amazon S3 对象的数据事件。

   > **Note**
   >
   > 如果您使用 CloudTrail 控制台或 Amazon S3 控制台配置某个跟踪以记录 S3 存储桶的数据事件，Amazon S3 控制台将显示已为该存储桶启用对象级别日志记录。

为 S3 存储桶中的对象禁用 CloudTrail 数据事件日志记录

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 CloudTrail 控制台：https://console.aws.amazon.com/cloudtrail。
2. 在左侧导航窗格中，选择跟踪。
3. 选择您创建用于记录存储桶的事件的跟踪名称。
4. 在跟踪的详细信息页面上，选择右上角的停止记录。
5. 在随后显示的对话框中，选择停止记录。

有关创建 S3 存储桶时启用对象级别日志记录的信息，请参阅 创建通用存储桶。

有关使用 S3 存储桶进行 CloudTrail 日志记录的更多信息，请参阅以下主题：

- 查看 S3 通用存储桶的属性
- 使用 Amazon CloudTrail 记录 Amazon S3 API 调用
- Amazon CloudTrail 用户指南中的使用 CloudTrail 日志文件

## 使用 CloudTrail 识别 Amazon S3 请求

在 Amazon S3 中，可以使用 Amazon CloudTrail 事件日志识别请求。Amazon CloudTrail 是识别 Amazon S3 请求的首选方法，但是如果您使用的是 Amazon S3 服务器访问日志，请参阅the section called “识别 S3 请求”。

主题

- 识别 CloudTrail 日志中向 Amazon S3 发出的请求
- 使用 CloudTrail 识别 Amazon S3 签名版本 2 请求
- 使用 CloudTrail 识别对 S3 对象的访问权限

### 识别 CloudTrail 日志中向 Amazon S3 发出的请求

在设置 CloudTrail 以将事件传输到存储桶后，您应开始看到对象进入您在 Amazon S3 控制台上的目标存储桶。其格式如下所示：

```
s3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/Region/yyyy/mm/dd
```

由 CloudTrail 记录的事件作为使用 gzipped 进行压缩的 JSON 对象存储在您的 S3 存储桶中。要高效地查找请求，您应使用 Amazon Athena 等服务来为 CloudTrail 日志建立索引并查询。

有关 CloudTrail 和 Athena 的更多信息，请参阅《Amazon Athena 用户指南》中的使用分区投影在 Athena 中创建 Amazon CloudTrail 日志表。

## 使用 CloudTrail 识别 Amazon S3 签名版本 2 请求

您可以使用 CloudTrail 事件日志来确定已用于在 Amazon S3 中签署请求的 API 签名版本。此功能非常重要，因为对 Signature Version 2 的支持将会关闭（弃用）。之后，Amazon S3 将不再接受使用 Signature Version 2 的请求，并且所有请求必须使用 Signature Version 4 进行签署。

我们强烈建议您使用 CloudTrail 来帮助确定您的任何工作流是否正在使用 Signature Version 2 进行签署。请通过将您的库和代码升级为使用 Signature Version 4 进行纠正，以防对您的业务产生任何影响。

有关更多信息，请参阅 Amazon Web Services re:Post 中的公告：适用于 Amazon S3 的 Amazon CloudTrail 为增强安全性审计添加了新字段。

> **Note**
>
> Amazon S3 的 CloudTrail 事件在请求详细信息中的键名称“`additionalEventData`”之下包含签名版本。要针对为 Amazon S3 中的对象发出的请求（如 `GET`、`PUT` 和 `DELETE` 请求）查找签名版本，您必须启用 CloudTrail 数据事件。（默认情况下，此特征处于关闭状态。）

Amazon CloudTrail 是确定签名版本 2 请求的首选方法。如果您使用的是 Amazon S3 服务器访问日志，请参阅使用 Amazon S3 访问日志确定签名版本 2 请求。

主题

- 用于识别 Amazon S3 签名版本 2 请求的 Athena 查询示例
- 对签名版本 2 数据进行分区

### 用于识别 Amazon S3 签名版本 2 请求的 Athena 查询示例

Example — 选择所有签名版本 2 事件，并仅打印 **`EventTime`**、**`S3_Action`**、**`Request_Parameters`**、**`Region`**、**`SourceIP`** 和 **`UserAgent`**

在以下 Athena 查询中，将 *`s3_cloudtrail_events_db.cloudtrail_table`* 替换为您的 Athena 详细信息，并根据需要增加或删除限制。

```
SELECT EventTime, EventName as S3_Action, requestParameters as Request_Parameters,
 awsregion as AWS_Region, sourceipaddress as Source_IP, useragent as User_Agent
FROM s3_cloudtrail_events_db.cloudtrail_table
WHERE eventsource='s3.amazonaws.com'
AND json_extract_scalar(additionalEventData, '$.SignatureVersion')='SigV2'
LIMIT 10;
```

Example — 选择发送签名版本 2 流量的所有请求者

```
SELECT useridentity.arn, Count(requestid) as RequestCount
FROM s3_cloudtrail_events_db.cloudtrail_table
WHERE eventsource='s3.amazonaws.com'
    and json_extract_scalar(additionalEventData, '$.SignatureVersion')='SigV2'
Group by useridentity.arn
```

对签名版本 2 数据进行分区

如果您有大量要查询的数据，则可以通过创建分区表来减少 Athena 的成本和运行时间。

为此，创建一个包含分区的新表，如下所示。

```
  CREATE EXTERNAL TABLE s3_cloudtrail_events_db.cloudtrail_table_partitioned(
       eventversion STRING,
       userIdentity STRUCT<
           type:STRING,
           principalid:STRING,
           arn:STRING,
           accountid:STRING,
           invokedby:STRING,
           accesskeyid:STRING,
           userName:STRING,
        sessioncontext:STRUCT<
                   attributes:STRUCT<
                   mfaauthenticated:STRING,
                   creationdate:STRING>,
                   sessionIssuer:STRUCT<
                   type:STRING,
```

```
                    principalId:STRING,
                    arn:STRING,
                    accountId:STRING,
                    userName:STRING>
                >
            >,
        eventTime STRING,
        eventSource STRING,
        eventName STRING,
        awsRegion STRING,
        sourceIpAddress STRING,
        userAgent STRING,
        errorCode STRING,
        errorMessage STRING,
        requestParameters STRING,
        responseElements STRING,
        additionalEventData STRING,
        requestId STRING,
        eventId STRING,
        resources ARRAY<STRUCT<ARN:STRING,accountId: STRING,type:STRING>>,
        eventType STRING,
        apiVersion STRING,
        readOnly STRING,
        recipientAccountId STRING,
        serviceEventDetails STRING,
        sharedEventID STRING,
        vpcEndpointId STRING
    )
    PARTITIONED BY (region string, year string, month string, day string)
    ROW FORMAT SERDE 'org.apache.hadoop.hive.ql.io.orc.OrcSerde'
    STORED AS INPUTFORMAT 'org.apache.hadoop.hive.ql.io.SymlinkTextInputFormat'
    OUTPUTFORMAT 'org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat'
    LOCATION 's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/';
```

然后，单独创建分区。您无法从尚未创建的日期获取结果。

```
ALTER TABLE s3_cloudtrail_events_db.cloudtrail_table_partitioned ADD
    PARTITION (region= 'us-east-1', year= '2019', month= '02', day= '19') LOCATION
 's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/us-east-1/2019/02/19/'
    PARTITION (region= 'us-west-1', year= '2019', month= '02', day= '19') LOCATION
 's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/us-west-1/2019/02/19/'
```

```
    PARTITION (region= 'us-west-2', year= '2019', month= '02', day= '19') LOCATION
's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/us-west-2/2019/02/19/'
    PARTITION (region= 'ap-southeast-1', year= '2019', month= '02', day= '19') LOCATION
's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/ap-southeast-1/2019/02/19/'
    PARTITION (region= 'ap-southeast-2', year= '2019', month= '02', day= '19') LOCATION
's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/ap-southeast-2/2019/02/19/'
    PARTITION (region= 'ap-northeast-1', year= '2019', month= '02', day= '19') LOCATION
's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/ap-northeast-1/2019/02/19/'
    PARTITION (region= 'eu-west-1', year= '2019', month= '02', day= '19') LOCATION
's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/eu-west-1/2019/02/19/'
    PARTITION (region= 'sa-east-1', year= '2019', month= '02', day= '19') LOCATION
's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/sa-east-1/2019/02/19/';
```

然后，您可以根据这些分区发出请求，并且无需加载完整的存储桶。

```
SELECT useridentity.arn,
Count(requestid) AS RequestCount
FROM s3_cloudtrail_events_db.cloudtrail_table_partitioned
WHERE eventsource='s3.amazonaws.com'
AND json_extract_scalar(additionalEventData, '$.SignatureVersion')='SigV2'
AND region='us-east-1'
AND year='2019'
AND month='02'
AND day='19'
Group by useridentity.arn
```

## 使用 CloudTrail 识别对 S3 对象的访问权限

您可以使用 Amazon CloudTrail 事件日志确定对于诸如 `GetObject`、`DeleteObject` 和 `PutObject` 等数据事件的 Amazon S3 对象访问请求，并发现有关这些请求的进一步信息。

以下示例说明如何从 Amazon CloudTrail 事件日志获取对于 Amazon S3 的所有 PUT 对象请求。

主题

- 用于识别 Amazon S3 对象访问请求的 Athena 查询示例

用于识别 Amazon S3 对象访问请求的 Athena 查询示例

在以下 Athena 查询示例中，将 *s3_cloudtrail_events_db.cloudtrail_table* 替换为您的 Athena 详细信息，并根据需要修改日期范围。

Example — 选择所有具有 **PUT** 对象访问请求的事件，并仅打印 **EventTime**、**EventSource**、**SourceIP**、**UserAgent**、**BucketName**、**object** 和 **UserARN**

```
SELECT
  eventTime,
  eventName,
  eventSource,
  sourceIpAddress,
  userAgent,
  json_extract_scalar(requestParameters, '$.bucketName') as bucketName,
  json_extract_scalar(requestParameters, '$.key') as object,
  userIdentity.arn as userArn
FROM
  s3_cloudtrail_events_db.cloudtrail_table
WHERE
  eventName = 'PutObject'
  AND eventTime BETWEEN '2019-07-05T00:00:00Z' and '2019-07-06T00:00:00Z'
```

Example — 选择所有具有 **GET** 对象访问请求的事件，并仅打印 **EventTime**、**EventSource**、**SourceIP**、**UserAgent**、**BucketName**、**object** 和 **UserARN**

```
SELECT
  eventTime,
  eventName,
  eventSource,
  sourceIpAddress,
  userAgent,
  json_extract_scalar(requestParameters, '$.bucketName') as bucketName,
  json_extract_scalar(requestParameters, '$.key') as object,
  userIdentity.arn as userArn
FROM
  s3_cloudtrail_events_db.cloudtrail_table
WHERE
  eventName = 'GetObject'
  AND eventTime BETWEEN '2019-07-05T00:00:00Z' and '2019-07-06T00:00:00Z'
```

Example — 选择特定时段内向存储桶发送的所有匿名请求者事件，并仅打印 **EventTime**、**EventName**、**EventSource**、**SourceIP**、**UserAgent**、**BucketName**、**UserARN** 和 **AccountID**

```
SELECT
  eventTime,
  eventName,
  eventSource,
  sourceIpAddress,
  userAgent,
  json_extract_scalar(requestParameters, '$.bucketName') as bucketName,
  userIdentity.arn as userArn,
  userIdentity.accountId
FROM
  s3_cloudtrail_events_db.cloudtrail_table
WHERE
  userIdentity.accountId = 'anonymous'
  AND eventTime BETWEEN '2019-07-05T00:00:00Z' and '2019-07-06T00:00:00Z'
```

Example — 识别所有需要 ACL 进行授权的请求

以下 Amazon Athena 查询示例说明如何识别向 S3 存储桶发出的所有请求，这些请求需要访问控制列表（ACL）进行授权。如果请求需要 ACL 进行授权，则 additionalEventData 中的 aclRequired 值为 Yes。如果不需要 ACL，则 aclRequired 不存在。您可以使用此信息将这些 ACL 权限迁移到相应的存储桶策略。创建这些存储桶策略后，您可以对这些存储桶禁用 ACL。有关禁用 ACL 的更多信息，请参阅禁用 ACL 的先决条件。

```
SELECT
  eventTime,
  eventName,
  eventSource,
  sourceIpAddress,
  userAgent,
  userIdentity.arn as userArn,
  json_extract_scalar(requestParameters, '$.bucketName') as bucketName,
  json_extract_scalar(requestParameters, '$.key') as object,
  json_extract_scalar(additionalEventData, '$.aclRequired') as aclRequired
FROM
  s3_cloudtrail_events_db.cloudtrail_table
WHERE
  json_extract_scalar(additionalEventData, '$.aclRequired') = 'Yes'
```

```
  AND eventTime BETWEEN '2022-05-10T00:00:00Z' and '2022-08-10T00:00:00Z'
```

> **Note**
>
> - 也可以使用这些查询示例进行安全监控。您可以查看意外或未经授权的 IP 地址或请求者发出的 PutObject 或 GetObject 调用的结果，以及确定向存储桶发出的任何匿名请求。
> - 此查询仅从启用了日志记录的时间检索信息。

如果您使用的是 Amazon S3 服务器访问日志，请参阅 使用 Amazon S3 访问日志确定对象访问请求。

# 使用服务器访问日志记录来记录请求

服务器访问日志记录详细地记录对存储桶提出的各种请求。对于许多应用程序而言，服务器访问日志很有用。例如，访问日志信息可能在安全和访问权限审核方面很有用。此信息还有助于您了解客户群以及您的 Amazon S3 账单。

> **Note**
>
> 服务器访问日志不会记录 2019 年 3 月 20 日之后发布的区域的不正确区域重定向错误的相关信息。在存储桶所在区域的外部发出对象或存储桶的请求时，会发生不正确区域重定向错误。

## 如何启用日志传送？

要启用日志传输，请执行以下基本步骤。有关更多信息，请参阅 启用 Amazon S3 服务器访问日志记录。

1. 提供目的地存储桶（也称为目标存储桶）的名称。此存储桶是您希望 Amazon S3 用于将访问日志保存为对象的位置。源存储桶和目标存储桶必须位于同一个 Amazon Web Services 区域，并且由同一个账户拥有。目标存储桶不得具有 S3 对象锁定默认保留期配置。目标存储桶也不得启用申请方付款。

   您可以让日志传输至您拥有的且与源存储桶位于同一区域中的任何存储桶，包括源存储桶本身。不过，为了更方便地管理日志，我们建议您将访问日志保存在不同的存储桶中。

当源存储桶和目标存储桶是同一存储桶时，将为写入该存储桶的日志创建额外的日志，从而形成日志的无限循环。我们不建议这样做，因为它会导致您的存储账单金额小幅增加。此外，有关日志的额外日志可能会导致更难以找到您所查找的日志。

如果您选择将访问日志保存在源存储桶中，建议您为所有日志对象键指定目的地前缀（也称为目标前缀）。指定前缀时，所有日志对象名称都以公共字符串开头，从而使日志对象更易识别。

2. （可选）将一个目标前缀分配给所有 Amazon S3 日志对象键。利用目的地前缀（也称作目标前缀），可更轻松地找到日志对象。例如，如果您指定前缀值 `logs/`，则 Amazon S3 创建的每个日志对象的键均以 `logs/` 前缀开头，例如：

```
logs/2013-11-01-21-32-16-E568B2907131C0C0
```

如果指定前缀值 `logs`，则日志对象如下所示：

```
logs2013-11-01-21-32-16-E568B2907131C0C0
```

当同一目标存储桶有多个存储桶日志时，键前缀也可用于区分源存储桶。

当您删除日志时，此前缀也很有用。例如，您可以设置一个生命周期配置规则，让 Amazon S3 删除具有特定前缀的对象。有关更多信息，请参阅 删除 Amazon S3 日志文件。

3. （可选）设置权限以使其他人能够访问生成的日志。默认情况下，仅存储桶拥有者始终拥有日志对象的完全访问权限。如果您的目标存储桶使用 S3 对象所有权的强制存储桶拥有者设置来禁用访问控制列表（ACL），则无法在使用 ACL 的目的地授权（也称作目标授权）中授予权限。但是，您可以更新目标存储桶的存储桶策略以向其他存储桶授予访问权限。有关更多信息，请参阅Amazon S3 的身份和访问管理和日志传输的权限。

4. （可选）为日志文件设置日志对象键格式。对于日志对象键格式（也称为目标对象键格式），有两个选项：

   - 非基于日期的分区 - 这是原始日志对象键格式。如果选择此格式，则日志文件键格式如下所示：

     ```
     [DestinationPrefix][YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
     ```

     例如，如果您指定 `logs/` 作为前缀，则日志对象将按以下方式命名：

     ```
     logs/2013-11-01-21-32-16-E568B2907131C0C0
     ```

- 基于日期的分区 - 如果选择基于日期的分区，则可以选择日志文件的事件时间或传输时间作为日志格式中使用的日期源。此格式让查询日志变得更轻松。

  如果选择基于日期的分区，则日志文件键格式如下所示：

  ```
  [DestinationPrefix][SourceAccountId]/[SourceRegion]/[SourceBucket]/[YYYY]/[MM]/
  [DD]/[YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
  ```

  例如，如果您指定 `logs/` 作为目标前缀，则日志对象将按以下方式命名：

  ```
  logs/123456789012/us-west-2/amzn-s3-demo-source-
  bucket/2023/03/01/2023-03-01-21-32-16-E568B2907131C0C0
  ```

  对于传输时间传送，日志文件名中的时间与日志文件的传输时间对应。

  对于事件时间传送，年、月和日对应于事件的发生日期，小时、分钟和秒设置为键中的 `00`。这些日志文件中传送的日志仅针对特定日期。

如果您通过 Amazon Command Line Interface（Amazon CLI）、Amazon SDK 或 Amazon S3 REST API 配置日志，请使用 `TargetObjectKeyFormat` 指定日志对象键格式。要指定非基于日期的分区，请使用 `SimplePrefix`。要指定基于日期的分区，请使用 `PartitionedPrefix`。如果使用 `PartitionedPrefix`，则使用 `PartitionDateSource` 来指定 `EventTime` 或 `DeliveryTime`。

对于 `SimplePrefix`，日志文件键格式如下所示：

```
[TargetPrefix][YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
```

对于带事件时间或传输时间的 `PartitionedPrefix`，日志文件键格式如下所示：

```
[TargetPrefix][SourceAccountId]/[SourceRegion]/[SourceBucket]/[YYYY]/[MM]/[DD]/
[YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
```

## 日志对象密钥格式

Amazon S3 将以下对象键格式用于在目标存储桶中上传的日志对象：

- 非基于日期的分区 - 这是原始日志对象键格式。如果选择此格式，则日志文件键格式如下所示：

```
[DestinationPrefix][YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
```

- 基于日期的分区 - 如果选择基于日期的分区，则可以选择日志文件的事件时间或传输时间作为日志格式中使用的日期源。此格式让查询日志变得更轻松。

  如果选择基于日期的分区，则日志文件键格式如下所示：

```
[DestinationPrefix][SourceAccountId]/[SourceRegion]/[SourceBucket]/[YYYY]/[MM]/[DD]/
[YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
```

在日志对象键中，YYYY、MM、DD、hh、mm 和 ss 分别是表示年、月、日、小时、分钟和秒的数字。这些日期和时间采用协调世界时 (UTC)。

在特定时间传输的日志文件可包含在该时间前的任何时刻编写的记录。无法知道是否已传输特定时间间隔内的所有日志记录。

键的 UniqueString 部分用于防止覆盖文件。它没有意义，日志处理软件应忽略它。

## 如何传输日志？

Amazon S3 定期收集访问日志记录，在日志文件中整合这些记录，然后将日志文件作为日志对象上传到目标存储桶。如果多个启用了日志记录的源存储桶使用相同的目标存储桶，此目标存储桶中将保留所有这些源存储桶的访问日志。但是，每个日志对象只会报告特定源存储桶的访问日志记录。

Amazon S3 使用特殊的日志传输账户写入服务器访问日志。这些写入受常规的访问控制限制。我们建议您更新目标存储桶上的存储桶策略，以授予对日志记录服务主体（logging.s3.amazonaws.com）的访问权限来进行访问日志传输。您也可以通过存储桶访问控制列表（ACL）向 S3 日志传输组授予访问日志传输的访问权限。但是，建议不要使用存储桶 ACL 授予对 S3 日志传输组的访问权限。

当您启用服务器访问日志记录并通过目标存储桶策略授予访问日志传输的访问权限时，您必须更新该策略，以允许日志记录服务主体访问 s3:PutObject。如果您使用 Amazon S3 控制台启用服务器访问日志录入，该控制台会自动更新目标存储桶策略，以便将这些权限授予日志记录服务主体。有关授予服务器访问日志传输的权限的更多信息，请参阅 日志传输的权限。

> **Note**
>
> 对于 VPC 端点策略拒绝的 VPC 端点请求，或者对于在评估 VPC 策略之前失败的请求，S3 不支持向请求者或存储桶拥有者传输 CloudTrail 日志或服务器访问日志。

S3 对象所有权的强制存储桶拥有者设置

如果目标存储桶使用对象所有权的强制存储桶拥有者设置，ACL 将被禁用，并且不再影响权限。您必须更新目标存储桶上的存储桶策略，以授予对日志记录服务主体的访问权。有关对象所有权的更多信息，请参阅为服务器访问日志记录授予对 S3 日志传输组的访问权限。

## 最大努力服务器日志传输

服务器访问日志记录会以最大努力进行传输。针对已正确配置了日志记录的存储桶的大多数请求会导致传输一条日志记录。大多数日志记录将在记录后的几小时内传输，但可以更频繁地传输这些记录。

因此不能保证服务器日志记录的完整性和即时性。特殊请求的日志记录可能会在实际处理了请求之后进行传输，也可能根本不会传输。您甚至可能会看到日志记录的副本。服务器日志的用途在于向您提供有关存储桶流量性质方面的信息。虽然日志记录丢失或重复的情况十分少见，但请注意，服务器日志记录并不旨在完整记录所有请求。

由于服务器日志记录特征的最大努力性质，使用情况报告中可能有一个或多个访问请求不会出现在传输的服务器日志中。您可以在 Amazon 账单与成本管理 控制台的成本和使用情况报告下找到这些使用情况报告。

## 存储桶日志记录状态更改将逐渐生效

存储桶日志记录状态的更改需要一定时间才能实际影响日志文件的传输。例如，如果您为某个存储桶启用了日志记录，那么将记录在以下时间内发送的请求，而不会记录其他请求。假定您将日志记录的目标存储桶从存储桶 A 更改为存储桶 B，则在接下来的一个小时里仍可能有一些日志传输到存储桶 A，但其他日志则会传输到新的目标存储桶 B。无论如何，新的设置将最终生效，并且您无需执行任何操作。

有关日志记录和日志文件的更多信息，请参阅以下各部分：

主题

- 启用 Amazon S3 服务器访问日志记录
- Amazon S3 服务器访问日志格式
- 删除 Amazon S3 日志文件

- 使用 Amazon S3 服务器访问日志来确定请求
- 排查服务器访问日志记录问题

# 启用 Amazon S3 服务器访问日志记录

服务器访问日志记录详细地记录对 Amazon S3 存储桶提出的各种请求。对于许多应用程序而言，服务器访问日志很有用。例如，访问日志信息可能在安全和访问权限审核方面很有用。此信息还有助于您了解客户群以及您的 Amazon S3 账单。

默认情况下，Amazon S3 不会收集服务器访问日志。在您启用日志记录后，Amazon S3 会将源存储桶的访问日志传输到您选择的目的地存储桶（也称作目标存储桶）。目标存储桶必须位于源存储桶所在的 Amazon Web Services 区域和 Amazon Web Services 账户中。

访问日志记录包含有关对存储桶做出的请求的详细信息。这些信息可能包括请求类型、请求中指定的资源以及处理请求的时间和日期。有关日志记录基本知识的更多信息，请参阅 使用服务器访问日志记录来记录请求。

**Important**

- 在 Amazon S3 存储桶上启用服务器访问日志记录不收取额外费用。但是，系统提交给您的任何日志文件都会产生普通存储费用。(您可以随时删除日志文件。) 我们不会估计传输日志文件的数据传输费，但会按正常数据传输费率对访问日志文件收费。
- 您的目标存储桶不应启用服务器访问日志记录。您可以让日志传输至您拥有的且与源存储桶位于同一区域中的任何存储桶，包括源存储桶本身。但是，将日志传输到源存储桶会导致日志的无限循环，因此不建议这样做。为了更方便地管理日志，我们建议您将访问日志保存在不同的存储桶中。有关更多信息，请参阅 如何启用日志传送？。
- 已启用 S3 对象锁定的 S3 存储桶不能用作服务器访问日志的目标存储桶。目标存储桶不得具有默认保留期配置。
- 目标存储桶不得启用“申请方付款”。
- 仅当使用具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）（该加密方式使用 256 位高级加密标准（AES-256））时，才能对目标存储桶使用默认存储桶加密。不支持默认的具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）。

您可以使用 Amazon S3 控制台、Amazon S3 API、Amazon Command Line Interface（Amazon CLI）或 Amazon SDK 启用或禁用服务器访问日志记录。

## 日志传输的权限

Amazon S3 使用特殊的日志传输账户写入服务器访问日志。这些写入受常规的访问控制限制。对于访问日志传输，您必须向日志记录服务主体（`logging.s3.amazonaws.com`）授予对目标存储桶的访问权限。

要向 Amazon S3 授予日志传输权限，您可以使用存储桶策略或存储桶访问控制列表（ACL），具体取决于目标存储桶的 S3 对象所有权设置。但是，建议您使用存储桶策略，而不是 ACL。

### S3 对象所有权的强制存储桶拥有者设置

如果目标存储桶使用对象所有权的强制存储桶拥有者设置，ACL 将被禁用，并且不再影响权限。在这种情况下，您必须更新目标存储桶的存储桶策略，以向日志记录服务主体授予访问权限。您无法更新存储桶 ACL 以授予对 S3 日志传输组的访问权限。您也无法在 PutBucketLogging 配置中包含目的地授权（也称为目标授权）。

有关将现有存储桶 ACL 以便将访问日志传输迁移到存储桶策略的信息，请参阅 为服务器访问日志记录授予对 S3 日志传输组的访问权限。有关对象所有权的更多信息，请参阅为您的存储桶控制对象所有权和禁用 ACL。。当您创建新存储桶时，默认情况下 ACL 处于禁用状态。

### 使用存储桶策略授予访问权限

要使用目标存储桶的存储桶策略授予访问权限，请更新存储桶策略以向日志记录服务主体授予 `s3:PutObject` 权限。如果您使用 Amazon S3 控制台启用服务器访问日志记录，该控制台会自动更新目标存储桶的存储桶策略，以便将此权限授予日志记录服务主体。如果以编程方式启用服务器访问日志记录，则必须手动更新目标存储桶的存储桶策略以向日志记录服务主体授予访问权限。

有关向日志服务主体授予访问权限的存储桶策略示例，请参阅the section called “使用存储桶策略向日志记录服务主体授予权限”。

### 使用存储桶 ACL 授予访问权限

您也可以使用存储桶 ACL 授予访问日志传输的访问权限。您可以在存储桶 ACL 中添加一个授予条目，以授予对 S3 日志传输组的 `WRITE` 和 `READ_ACP` 权限。但是，不建议使用存储桶 ACL 授予对 S3 日志传输组的访问权限。有关更多信息，请参阅 为您的存储桶控制对象所有权和禁用 ACL。。有关将现有存储桶 ACL 以便将访问日志传输迁移到存储桶策略的信息，请参阅 为服务器访问日志记录授予对 S3 日志传输组的访问权限。有关向日志记录服务主体授予访问权限的示例 ACL，请参阅the section called “使用存储桶 ACL 向日志传输组授予权限”。

使用存储桶策略向日志记录服务主体授予权限

此示例存储桶策略向日志记录服务主体（logging.s3.amazonaws.com）授予 s3:PutObject 权限。要使用这一存储桶策略，请将 *user input placeholders* 替换为您自己的信息。在以下策略中，*amzn-s3-demo-destination-bucket* 是将服务器访问日志传输到的目标存储桶，*amzn-s3-demo-source-bucket* 是源存储桶。*EXAMPLE-LOGGING-PREFIX* 是要用于日志对象的可选目的地前缀（也称为目标前缀）。*SOURCE-ACCOUNT-ID* 是拥有源存储桶的 Amazon Web Services 账户。

> **Note**
>
> 如果存储桶策略中有 Deny 语句，请确保这些语句不会阻止 Amazon S3 传输访问日志。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3ServerAccessLogsPolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "logging.s3.amazonaws.com"
            },
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/EXAMPLE-LOGGING-PREFIX*",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:::amzn-s3-demo-source-bucket"
                },
                "StringEquals": {
                    "aws:SourceAccount": "SOURCE-ACCOUNT-ID"
                }
            }
        }
    ]
}
```

使用存储桶 ACL 向日志传输组授予权限

> **Note**
>
> 作为安全最佳实践，默认情况下，Amazon S3 在所有新存储桶中禁用访问控制列表（ACL）。有关使用 Amazon S3 控制台 ACL 权限的更多信息，请参阅 配置 ACL。

我们建议您不要使用此方法，而是使用存储桶 ACL 向日志传输组授予权限。但是，如果目标存储桶使用对象所有权的强制存储桶拥有者设置，则无法设置存储桶或对象 ACL。您也无法在 PutBucketLogging 配置中包含目的地授权（也称为目标授权）。而是必须使用存储桶策略向日志记录服务主体（`logging.s3.amazonaws.com`）授予访问权限。有关更多信息，请参阅 日志传输的权限。

在存储桶 ACL 中，日志传输组通过以下 URL 表示：

```
http://acs.amazonaws.com/groups/s3/LogDelivery
```

要授予 `WRITE` 和 `READ_ACP`（ACL 读取）权限，请将以下授权添加到目标存储桶 ACL：

```
<Grant>
    <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  xsi:type="Group">
        <URI>http://acs.amazonaws.com/groups/s3/LogDelivery</URI>
    </Grantee>
    <Permission>WRITE</Permission>
</Grant>
<Grant>
    <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  xsi:type="Group">
        <URI>http://acs.amazonaws.com/groups/s3/LogDelivery</URI>
    </Grantee>
    <Permission>READ_ACP</Permission>
</Grant>
```

有关以编程方式添加 ACL 授权的示例，请参阅 配置 ACL。

> **Important**
>
> 当您对存储桶使用 Amazon CloudFormation 来启用 Amazon S3 服务器访问日志记录，并使用 ACL 向 S3 日志传输组授予访问权限时，您还必须向 CloudFormation 模板添加 `"AccessControl": "LogDeliveryWrite"`。这样做非常重要，因为您只能通过为存储桶

创建 ACL 来授予这些权限，而无法在 CloudFormation 中为存储桶创建自定义 ACL。您只能将标准 ACL 与 CloudFormation 结合使用。

## 要启用服务器访问日志记录

要使用 Amazon S3 控制台、Amazon S3 REST API、Amazon SDK 和 Amazon CLI 启用服务器访问日志记录，请使用以下过程。

使用 S3 控制台

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在存储桶列表中，选择要为其启用服务器访问日志记录的存储桶的名称。
4. 选择 Properties (属性)。
5. 在 Server access logging (服务器访问日志记录) 部分中，请选择 Edit (编辑)。
6. 在服务器访问日志记录下，选择启用。
7. 在目标存储桶下，指定存储桶和可选前缀。如果您指定前缀，建议您在前缀后面加上正斜杠（/），以便更轻松地查找日志。

   **Note**

   通过斜杠（/）指定前缀可让您更轻松地查找日志对象。例如，如果您指定前缀值 `logs/`，则 Amazon S3 创建的每个日志对象的键均以 `logs/` 前缀开头，如下所示：

   ```
   logs/2013-11-01-21-32-16-E568B2907131C0C0
   ```

   如果指定前缀值 `logs`，则日志对象如下所示：

   ```
   logs2013-11-01-21-32-16-E568B2907131C0C0
   ```

8. 在日志对象件格式下，执行下列操作之一：

   - 要选择非基于日期的分区，请选择 [DestinationPrefix][YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]。

- 要选择基于日期的分区，请选择 [DestinationPrefix][SourceAccountId]/[SourceRegion]/[SourceBucket]/[YYYY]/[MM]/[DD]/[YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]，然后选择 S3 事件时间或日志文件传输时间。

9. 选择保存更改。

   当您在存储桶上启用服务器访问日志记录时，控制台会在源存储桶上启用日志记录并更新目标存储桶的存储桶策略，以便向日志记录服务主体（`logging.s3.amazonaws.com`）授予 `s3:PutObject` 权限。有关存储桶策略的更多信息，请参阅 使用存储桶策略向日志记录服务主体授予权限。

   您可以查看目标存储桶中的日志。启用服务器访问日志记录后，可能需要数小时，日志才会传输到目标存储桶。有关如何以及何时传输日志的更多信息，请参阅如何传输日志？。

有关更多信息，请参阅 查看 S3 通用存储桶的属性。

使用 REST API

要启用日志记录，请提交 PutBucketLogging 请求，以在源存储桶上添加日志记录配置。该请求指定目的地存储桶（也称作目标存储桶），并（可选）指定要用于所有日志对象键的前缀。

以下示例将 *amzn-s3-demo-destination-bucket* 标识为目标存储桶，将 *logs/* 标识为前缀。

```
<BucketLoggingStatus xmlns="http://doc.s3.amazonaws.com/2006-03-01">
  <LoggingEnabled>
    <TargetBucket>amzn-s3-demo-destination-bucket</TargetBucket>
    <TargetPrefix>logs/</TargetPrefix>
  </LoggingEnabled>
</BucketLoggingStatus>
```

以下示例将 *amzn-s3-demo-destination-bucket* 标识为目标存储桶，将 *logs/* 标识为前缀，并将 `EventTime` 标识为日志对象键格式。

```
<BucketLoggingStatus xmlns="http://doc.s3.amazonaws.com/2006-03-01">
  <LoggingEnabled>
    <TargetBucket>amzn-s3-demo-destination-bucket</TargetBucket>
    <TargetPrefix>logs/</TargetPrefix>
    <TargetObjectKeyFormat>
      <PartitionedPrefix>
         <PartitionDateSource>EventTime</PartitionDateSource>
      </PartitionedPrefix>
```

```
  </TargetObjectKeyFormat>
  </LoggingEnabled>
</BucketLoggingStatus>
```

日志对象由 S3 日志传递账户编写并拥有，存储桶拥有者对日志对象授予完全权限。您可以选择性地使用目的地授权（也称作目标授权）向其他用户授予权限，以便他们能够访问日志。有关更多信息，请参阅 PutBucketLogging。

> **Note**
>
> 如果目标存储桶使用对象所有权的强制存储桶拥有者设置，则您无法使用目标授权向其他用户授予权限。要向其他用户授予权限，您可以更新目标存储桶的存储桶策略。有关更多信息，请参阅 日志传输的权限。

要检索存储桶上的日志记录配置，请使用 GetBucketLogging API 操作。

要删除日志记录配置，请发送带空白 `BucketLoggingStatus` 的 `PutBucketLogging` 请求：

```
<BucketLoggingStatus xmlns="http://doc.s3.amazonaws.com/2006-03-01">
</BucketLoggingStatus>
```

要对存储桶启用日志记录，您可以使用 Amazon S3 API 或 Amazon SDK 包装程序库。

使用 Amazon SDK

以下示例对存储桶启用日志记录。您必须创建两个存储桶，即一个源存储桶和一个目的地（目标）存储桶。这些示例首先更新目标存储桶上的存储桶 ACL。之后，向日志传输组授予向目标存储桶写入日志所需的权限，然后在源存储桶上启用日志记录。

这些示例不适用于使用对象所有权的强制存储桶拥有者设置的目标存储桶。

如果目的地（目标）存储桶使用对象所有权的强制存储桶拥有者设置，则无法设置存储桶或对象 ACL。您也不能将目的地（目标）授权包含在 PutBucketLogging 配置中。您必须使用存储桶策略向日志服务主体（`logging.s3.amazonaws.com`）授予访问权限。有关更多信息，请参阅 日志传输的权限。

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 查看 GitHub，了解更多信息。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
using System;
using System.IO;
using System.Threading.Tasks;
using Amazon.S3;
using Amazon.S3.Model;
using Microsoft.Extensions.Configuration;

/// <summary>
/// This example shows how to enable logging on an Amazon Simple Storage
/// Service (Amazon S3) bucket. You need to have two Amazon S3 buckets for
/// this example. The first is the bucket for which you wish to enable
/// logging, and the second is the location where you want to store the
/// logs.
/// </summary>
public class ServerAccessLogging
{
    private static IConfiguration _configuration = null!;

    public static async Task Main()
    {
        LoadConfig();

        string bucketName = _configuration["BucketName"];
        string logBucketName = _configuration["LogBucketName"];
        string logObjectKeyPrefix = _configuration["LogObjectKeyPrefix"];
        string accountId = _configuration["AccountId"];

        // If the AWS Region defined for your default user is different
        // from the Region where your Amazon S3 bucket is located,
        // pass the Region name to the Amazon S3 client object's constructor.
        // For example: RegionEndpoint.USWest2 or RegionEndpoint.USEast2.
        IAmazonS3 client = new AmazonS3Client();
```

```
            try
            {
                // Update bucket policy for target bucket to allow delivery of
logs to it.
                await SetBucketPolicyToAllowLogDelivery(
                    client,
                    bucketName,
                    logBucketName,
                    logObjectKeyPrefix,
                    accountId);

                // Enable logging on the source bucket.
                await EnableLoggingAsync(
                    client,
                    bucketName,
                    logBucketName,
                    logObjectKeyPrefix);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine($"Error: {e.Message}");
            }
        }

        /// <summary>
        /// This method grants appropriate permissions for logging to the
        /// Amazon S3 bucket where the logs will be stored.
        /// </summary>
        /// <param name="client">The initialized Amazon S3 client which will be
used
        /// to apply the bucket policy.</param>
        /// <param name="sourceBucketName">The name of the source bucket.</param>
        /// <param name="logBucketName">The name of the bucket where logging
        /// information will be stored.</param>
        /// <param name="logPrefix">The logging prefix where the logs should be
delivered.</param>
        /// <param name="accountId">The account id of the account where the
source bucket exists.</param>
        /// <returns>Async task.</returns>
        public static async Task SetBucketPolicyToAllowLogDelivery(
            IAmazonS3 client,
            string sourceBucketName,
            string logBucketName,
```

```
            string logPrefix,
            string accountId)
        {
            var resourceArn = @"""arn:aws:s3:::" + logBucketName + "/" +
logPrefix + @"*""";

            var newPolicy = @"{
                                ""Statement"":[{
                                ""Sid"": ""S3ServerAccessLogsPolicy"",
                                ""Effect"": ""Allow"",
                                ""Principal"": { ""Service"":
""logging.s3.amazonaws.com"" },
                                ""Action"": [""s3:PutObject""],
                                ""Resource"": [" + resourceArn + @"],
                                ""Condition"": {
                                ""ArnLike"": { ""aws:SourceArn"":
""arn:aws:s3:::" + sourceBucketName + @""" },
                                ""StringEquals"": { ""aws:SourceAccount"": """ +
accountId + @""" }
                                        }
                                    }]
                                }";
            Console.WriteLine($"The policy to apply to bucket {logBucketName} to
enable logging:");
            Console.WriteLine(newPolicy);

            PutBucketPolicyRequest putRequest = new PutBucketPolicyRequest
            {
                BucketName = logBucketName,
                Policy = newPolicy,
            };
            await client.PutBucketPolicyAsync(putRequest);
            Console.WriteLine("Policy applied.");
        }

        /// <summary>
        /// This method enables logging for an Amazon S3 bucket. Logs will be
stored
        /// in the bucket you selected for logging. Selected prefix
        /// will be prepended to each log object.
        /// </summary>
        /// <param name="client">The initialized Amazon S3 client which will be
used
```

```
        /// to configure and apply logging to the selected Amazon S3 bucket.</
param>
        /// <param name="bucketName">The name of the Amazon S3 bucket for which
 you
        /// wish to enable logging.</param>
        /// <param name="logBucketName">The name of the Amazon S3 bucket where
 logging
        /// information will be stored.</param>
        /// <param name="logObjectKeyPrefix">The prefix to prepend to each
        /// object key.</param>
        /// <returns>Async task.</returns>
        public static async Task EnableLoggingAsync(
            IAmazonS3 client,
            string bucketName,
            string logBucketName,
            string logObjectKeyPrefix)
        {
            Console.WriteLine($"Enabling logging for bucket {bucketName}.");
            var loggingConfig = new S3BucketLoggingConfig
            {
                TargetBucketName = logBucketName,
                TargetPrefix = logObjectKeyPrefix,
            };

            var putBucketLoggingRequest = new PutBucketLoggingRequest
            {
                BucketName = bucketName,
                LoggingConfig = loggingConfig,
            };
            await client.PutBucketLoggingAsync(putBucketLoggingRequest);
            Console.WriteLine($"Logging enabled.");
        }

        /// <summary>
        /// Loads configuration from settings files.
        /// </summary>
        public static void LoadConfig()
        {
            _configuration = new ConfigurationBuilder()
                .SetBasePath(Directory.GetCurrentDirectory())
                .AddJsonFile("settings.json") // Load settings from .json file.
                .AddJsonFile("settings.local.json", true) // Optionally, load
 local settings.
                .Build();
```

```
        }
    }
```

- 有关更多信息，请参阅《适用于 .NET 的 Amazon SDK API 参考》中的 PutBucketLogging。

Java

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.BucketLoggingStatus;
import software.amazon.awssdk.services.s3.model.LoggingEnabled;
import software.amazon.awssdk.services.s3.model.PartitionedPrefix;
import software.amazon.awssdk.services.s3.model.PutBucketLoggingRequest;
import software.amazon.awssdk.services.s3.model.TargetObjectKeyFormat;

// Class to set a bucket policy on a target S3 bucket and enable server access
 logging on a source S3 bucket.
public class ServerAccessLogging {
    private static S3Client s3Client;

    public static void main(String[] args) {
        String sourceBucketName = "SOURCE-BUCKET";
        String targetBucketName = "TARGET-BUCKET";
        String sourceAccountId = "123456789012";
        String targetPrefix = "logs/";

        // Create S3 Client.
        s3Client = S3Client.builder().
                region(Region.US_EAST_2)
                .build();

        // Set a bucket policy on the target S3 bucket to enable server access
 logging by granting the
        // logging.s3.amazonaws.com principal permission to use the PutObject
 operation.
        ServerAccessLogging serverAccessLogging = new ServerAccessLogging();
        serverAccessLogging.setTargetBucketPolicy(sourceAccountId, sourceBucketName,
 targetBucketName);

        // Enable server access logging on the source S3 bucket.
```

```
        serverAccessLogging.enableServerAccessLogging(sourceBucketName,
 targetBucketName,
                targetPrefix);

    }

    // Function to set a bucket policy on the target S3 bucket to enable server
 access logging by granting the
    // logging.s3.amazonaws.com principal permission to use the PutObject operation.
    public void setTargetBucketPolicy(String sourceAccountId, String
 sourceBucketName, String targetBucketName) {
        String policy = "{\n" +
                "    \"Version\": \"2012-10-17\",\n" +
                "    \"Statement\": [\n" +
                "        {\n" +
                "            \"Sid\": \"S3ServerAccessLogsPolicy\",\n" +
                "            \"Effect\": \"Allow\",\n" +
                "            \"Principal\": {\"Service\": \"logging.s3.amazonaws.com
\"},\n" +
                "            \"Action\": [\n" +
                "                \"s3:PutObject\"\n" +
                "            ],\n" +
                "            \"Resource\": \"arn:aws:s3:::" + targetBucketName + "/*
\",\n" +
                "            \"Condition\": {\n" +
                "                \"ArnLike\": {\n" +
                "                    \"aws:SourceArn\": \"arn:aws:s3:::" +
 sourceBucketName + "\"\n" +
                "                },\n" +
                "                \"StringEquals\": {\n" +
                "                    \"aws:SourceAccount\": \"" + sourceAccountId +
 "\"\n" +
                "                }\n" +
                "            }\n" +
                "        }\n" +
                "    ]\n" +
                "}";
        s3Client.putBucketPolicy(b -> b.bucket(targetBucketName).policy(policy));
    }

    // Function to enable server access logging on the source S3 bucket.
    public void enableServerAccessLogging(String sourceBucketName, String
 targetBucketName,
            String targetPrefix) {
```

```
        TargetObjectKeyFormat targetObjectKeyFormat =
TargetObjectKeyFormat.builder()

.partitionedPrefix(PartitionedPrefix.builder().partitionDateSource("EventTime").build())
                .build();
        LoggingEnabled loggingEnabled = LoggingEnabled.builder()
                .targetBucket(targetBucketName)
                .targetPrefix(targetPrefix)
                .targetObjectKeyFormat(targetObjectKeyFormat)
                .build();
        BucketLoggingStatus bucketLoggingStatus = BucketLoggingStatus.builder()
                .loggingEnabled(loggingEnabled)
                .build();
        s3Client.putBucketLogging(PutBucketLoggingRequest.builder()
                .bucket(sourceBucketName)
                .bucketLoggingStatus(bucketLoggingStatus)
                .build());
    }

}
```

使用 Amazon CLI

我们建议您在其中放置 S3 存储桶的每个 Amazon Web Services 区域 中都创建一个专用日志记录存储桶。然后，将 Amazon S3 访问日志传输到该 S3 存储桶。有关更多信息和示例，请参阅《Amazon CLI 参考》中的 put-bucket-logging。

如果目的地（目标）存储桶使用对象所有权的强制存储桶拥有者设置，则无法设置存储桶或对象 ACL。您也不能将目的地（目标）授权包含在 PutBucketLogging 配置中。您必须使用存储桶策略向日志服务主体（`logging.s3.amazonaws.com`）授予访问权限。有关更多信息，请参阅 日志传输的权限。

Example — 为跨两个区域的五个存储桶启用访问日志

在本示例中，您有以下 5 个存储桶：

- *amzn-s3-demo-source-bucket*-us-east-1
- *amzn-s3-demo-source-bucket1*-us-east-1
- *amzn-s3-demo-source-bucket2*-us-east-1
- *amzn-s3-demo-bucket1*-us-west-2

- *amzn-s3-demo-bucket2*-us-west-2

> **Note**
>
> 以下过程的最后一步提供了示例 bash 脚本，可使用这些脚本来创建日志记录存储桶，并在这些存储桶上启用服务器访问日志记录。要使用这些脚本，必须创建 policy.json 和 logging.json 文件，如以下过程所述。

1. 在美国西部（俄勒冈州）和美国东部（弗吉尼亚州北部）区域创建两个日志记录存储桶，并为其指定以下名称：
   - *amzn-s3-demo-destination-bucket*-logs-us-east-1
   - *amzn-s3-demo-destination-bucket1*-logs-us-west-2
2. 稍后，在这些步骤中，您将启用服务器访问日志记录，如下所示：
   - *amzn-s3-demo-source-bucket*-us-east-1 记录到带有前缀 *amzn-s3-demo-source-bucket*-us-east-1 的 S3 存储桶 *amzn-s3-demo-destination-bucket*-logs-us-east-1
   - *amzn-s3-demo-source-bucket1*-us-east-1 记录到带有前缀 *amzn-s3-demo-source-bucket1*-us-east-1 的 S3 存储桶 *amzn-s3-demo-destination-bucket*-logs-us-east-1
   - *amzn-s3-demo-source-bucket2*-us-east-1 记录到带有前缀 *amzn-s3-demo-source-bucket2*-us-east-1 的 S3 存储桶 *amzn-s3-demo-destination-bucket*-logs-us-east-1
   - *amzn-s3-demo-bucket1*-us-west-2 记录到带有前缀 *amzn-s3-demo-bucket1*-us-west-2 的 S3 存储桶 *amzn-s3-demo-destination-bucket1*-logs-us-west-2
   - *amzn-s3-demo-bucket2*-us-west-2 记录到带有前缀 *amzn-s3-demo-bucket2*-us-west-2 的 S3 存储桶 *amzn-s3-demo-destination-bucket1*-logs-us-west-2
3. 对于每个目标日志记录存储桶，使用存储桶 ACL 或存储桶策略授予服务器访问日志传输的权限：
   - 更新存储桶策略（建议）– 要向日志记录服务主体授予权限，请使用以下 put-bucket-policy 命令：将 *amzn-s3-demo-destination-bucket*-logs 替换为您的目标存储桶的名称。

```
aws s3api put-bucket-policy --bucket amzn-s3-demo-destination-bucket-logs --
policy file://policy.json
```

Policy.json 是当前文件夹中包含以下存储桶策略的 JSON 文档。要使用这一存储桶策略，请将 *user input placeholders* 替换为您自己的信息。在以下策略中，*amzn-s3-demo-destination-bucket-logs* 是要将服务器访问日志传输到的目标存储桶，*amzn-s3-demo-source-bucket* 是源存储桶。*SOURCE-ACCOUNT-ID* 是拥有源存储桶的 Amazon Web Services 账户。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3ServerAccessLogsPolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "logging.s3.amazonaws.com"
            },
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket-logs/*",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:::amzn-s3-demo-source-bucket"
                },
                "StringEquals": {
                    "aws:SourceAccount": "SOURCE-ACCOUNT-ID"
                }
            }
        }
    ]
}
```

- 更新存储桶 ACL –要向 S3 日志传输组授予权限，请使用以下 put-bucket-acl 命令。将 *amzn-s3-demo-destination-bucket-logs* 替换为您的目的地（目标）存储桶的名称。

```
aws s3api put-bucket-acl --bucket amzn-s3-demo-destination-bucket-logs  --
grant-write URI=http://acs.amazonaws.com/groups/s3/LogDelivery --grant-read-acp
 URI=http://acs.amazonaws.com/groups/s3/LogDelivery
```

4. 然后，创建一个包含日志记录配置的 logging.json 文件（基于以下三个示例之一）。创建 logging.json 文件后，可以使用以下 put-bucket-logging 命令应用日志记录配置。将 *amzn-s3-demo-destination-bucket-logs* 替换为您的目的地（目标）存储桶的名称。

```
aws s3api put-bucket-logging --bucket amzn-s3-demo-destination-bucket-logs --
bucket-logging-status file://logging.json
```

> **Note**
>
> 您可以使用下一步中提供的 bash 脚本之一，而不是使用此 put-bucket-logging 命令在每个目标存储桶上应用日志记录配置。要使用这些脚本，您必须创建 policy.json 和 logging.json 文件，如该过程所述。

logging.json 文件是当前文件夹中包含日志记录配置的 JSON 文档。如果目标存储桶使用对象所有权的强制存储桶拥有者设置，则您的日志记录配置不能包含目的地（目标）授权。有关更多信息，请参阅 日志传输的权限。

Example – **logging.json**，不带目的地（目标）授权

以下示例 logging.json 文件不包含目的地（目标）授权。因此，您可以将此配置应用于使用对象所有权的强制存储桶拥有者设置的目的地（目标）存储桶。

```
{
    "LoggingEnabled": {
        "TargetBucket": "amzn-s3-demo-destination-bucket-logs",
        "TargetPrefix": "amzn-s3-demo-destination-bucket/"
     }
 }
```

Example – **`logging.json`**，带目的地（目标）授权

以下示例 `logging.json` 文件包含目的地（目标）授权。

如果目标存储桶使用对象所有权的强制存储桶拥有者设置，则您无法在 PutBucketLogging 配置中包含目的地（目标）授权。有关更多信息，请参阅 日志传输的权限。

```
{
    "LoggingEnabled": {
        "TargetBucket": "amzn-s3-demo-destination-bucket-logs",
        "TargetPrefix": "amzn-s3-demo-destination-bucket/",
        "TargetGrants": [
             {
                "Grantee": {
                    "Type": "AmazonCustomerByEmail",
                    "EmailAddress": "user@example.com"
                 },
                "Permission": "FULL_CONTROL"
             }
         ]
     }
 }
```

被授权者值

您可以通过以下方式（使用请求元素）指定要向其分配访问权限的人员（被授权者）：

- 按人员的 ID：

```
{
  "Grantee": {
    "Type": "CanonicalUser",
    "ID": "ID",
    "DisplayName": "GranteesEmail"
  }
}
```

  `DisplayName` 是可选的，在请求中被忽略。

- 按电子邮件地址：

```
{
  "Grantee": {
    "Type": "AmazonCustomerByEmail",
    "EmailAddress": "username@example.com"
  }
}
```

被授予者解析为 CanonicalUser，并在对 GetObjectAcl 请求的响应中显示为 CanonicalUser。

> **Note**
>
> 仅在某些 Amazon Web Services 区域中支持使用电子邮件地址指定被授权者：有关更多信息，请参阅《Amazon S3 API 参考》中的 Grantee。

- 按 URI：

```
{
  "Grantee": {
    "Type": "Group",
    "URI": "http://acs.amazonaws.com/groups/global/AuthenticatedUsers"
  }
}
```

Example – **logging.json**，日志对象键格式设置为 S3 事件时间

以下 logging.json 文件将日志对象键格式更改为 S3 事件时间。有关设置日志对象键格式的更多信息，请参阅the section called “如何启用日志传送？”

```
{
  "LoggingEnabled": {
      "TargetBucket": "amzn-s3-demo-destination-bucket-logs",
      "TargetPrefix": "amzn-s3-demo-destination-bucket/",
      "TargetObjectKeyFormat": {
          "PartitionedPrefix": {
              "PartitionDateSource": "EventTime"
          }
       }
```

```
    }
}
```

5. 使用下列 bash 脚本之一为您账户中的所有存储桶添加访问日志记录。将 *amzn-s3-demo-destination-bucket-logs* 替换为目的地（目标）存储桶的名称，并将 *us-west-2* 替换为存储桶所在的区域的名称。

> **Note**
>
> 此脚本仅在所有存储桶均位于同一区域中时有用。如果您在多个区域中有存储桶，则必须调整该脚本。

Example — 使用存储桶策略授予访问权限并为账户中的存储桶添加日志记录

```
loggingBucket='amzn-s3-demo-destination-bucket-logs'
region='us-west-2'


# Create the logging bucket.
aws s3 mb s3://$loggingBucket --region $region

aws s3api put-bucket-policy --bucket $loggingBucket --policy file://policy.json

# List the buckets in this account.
buckets="$(aws s3 ls | awk '{print $3}')"

# Put a bucket logging configuration on each bucket.
for bucket in $buckets
    do
      # This if statement excludes the logging bucket.
      if [ "$bucket" != "$loggingBucket" ] ; then
          continue;
      fi
      printf '{
        "LoggingEnabled": {
          "TargetBucket": "%s",
          "TargetPrefix": "%s/"
      }
    }' "$loggingBucket" "$bucket"  > logging.json
```

```
      aws s3api put-bucket-logging --bucket $bucket --bucket-logging-status file://
logging.json
      echo "$bucket done"
  done

  rm logging.json

  echo "Complete"
```

Example — 使用存储桶 ACL 授予访问权限并为账户中的存储桶添加日志记录

```
  loggingBucket='amzn-s3-demo-destination-bucket-logs'
  region='us-west-2'


  # Create the logging bucket.
  aws s3 mb s3://$loggingBucket --region $region

  aws s3api put-bucket-acl --bucket $loggingBucket --grant-write URI=http://
acs.amazonaws.com/groups/s3/LogDelivery --grant-read-acp URI=http://
acs.amazonaws.com/groups/s3/LogDelivery

  # List the buckets in this account.
  buckets="$(aws s3 ls | awk '{print $3}')"

  # Put a bucket logging configuration on each bucket.
  for bucket in $buckets
      do
        # This if statement excludes the logging bucket.
        if [ "$bucket" != "$loggingBucket" ] ; then
            continue;
        fi
        printf '{
          "LoggingEnabled": {
            "TargetBucket": "%s",
            "TargetPrefix": "%s/"
        }
      }' "$loggingBucket" "$bucket"  > logging.json
      aws s3api put-bucket-logging --bucket $bucket --bucket-logging-status file://
logging.json
      echo "$bucket done"
  done
```

```
rm logging.json

echo "Complete"
```

### 验证服务器访问日志设置

启用服务器访问日志记录后，请完成以下步骤：

- 访问目标存储桶并验证是否正在传输日志文件。设置访问日志后，Amazon S3 会立即开始捕获请求并记录这些请求。但是，日志会在数小时后传输到目标存储桶。有关更多信息，请参阅the section called “存储桶日志记录状态更改将逐渐生效”和the section called “最大努力服务器日志传输”。

  还可以通过使用 Amazon S3 请求指标并为这些指标设置 Amazon CloudWatch 警报，来自动验证日志传输。有关更多信息，请参阅 使用 Amazon CloudWatch 监控指标。
- 验证您是否能够打开和读取日志文件的内容。

有关服务器访问日志记录故障排除信息，请参阅排查服务器访问日志记录问题。

## Amazon S3 服务器访问日志格式

服务器访问日志记录详细地记录对 Amazon S3 存储桶提出的各种请求。您可以将服务器访问日志用于以下目的：

- 进行安全和访问审计
- 了解您的客户群
- 了解您的 Amazon S3 账单

本节介绍了有关 Amazon S3 服务器访问日志文件的格式和其他详细信息。

服务器访问日志文件由一系列的换行分隔日志记录组成。每个日志记录表示一个请求并由空格分隔的字段组成。

以下是含有五份日志记录的示例日志。

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 amzn-s3-demo-bucket1 [06/Feb/2019:00:00:38 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be 3E57427F3EXAMPLE
```

```
 REST.GET.VERSIONING - "GET /amzn-s3-demo-bucket1?versioning HTTP/1.1" 200 - 113 - 7 -
 "-" "S3Console/0.4" - s9lzHYrFp76ZVxRcpX9+5cjAnEH2ROuNkd2BHfIa6UkFVdtjf5mKR3/eTPFvsiP/
XV/VLi31234= SigV4 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader amzn-s3-demo-bucket1.s3.us-
west-1.amazonaws.com TLSV1.2 arn:aws:s3:us-west-1:123456789012:accesspoint/example-AP
 Yes
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 amzn-s3-demo-bucket1 [06/Feb/2019:00:00:38 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be 891CE47D2EXAMPLE
 REST.GET.LOGGING_STATUS - "GET /amzn-s3-demo-bucket1?logging HTTP/1.1" 200 -
 242 - 11 - "-" "S3Console/0.4" - 9vKBE6vMhrNiWHZmb2L0mXOcqPGzQOI5XLnCtZNPxev+Hf
+7tpT6sxDwDty4LHBUOZJG96N1234= SigV4 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader amzn-s3-
demo-bucket1.s3.us-west-1.amazonaws.com TLSV1.2 - -
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 amzn-s3-demo-bucket1 [06/Feb/2019:00:00:38 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be A1206F460EXAMPLE
 REST.GET.BUCKETPOLICY - "GET /amzn-s3-demo-bucket1?policy HTTP/1.1" 404
 NoSuchBucketPolicy 297 - 38 - "-" "S3Console/0.4" - BNaBsXZQQDbssi6xMBdBU2sLt
+Yf5kZDmeBUP35sFoKa3sLLeMC78iwEIWxs99CRUrbS4n11234= SigV4 ECDHE-RSA-AES128-GCM-SHA256
 AuthHeader amzn-s3-demo-bucket1.s3.us-west-1.amazonaws.com TLSV1.2 - Yes
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 amzn-s3-demo-bucket1 [06/Feb/2019:00:01:00 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be 7B4A0FABBEXAMPLE
 REST.GET.VERSIONING - "GET /amzn-s3-demo-bucket1?versioning HTTP/1.1" 200 -
 113 - 33 - "-" "S3Console/0.4" - Ke1bUcazaN1jWuUlPJaxF64cQVpUEhoZKEG/hmy/gijN/
I1DeWqDfFvnpybfEseEME/u7ME1234= SigV4 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader amzn-s3-
demo-bucket1.s3.us-west-1.amazonaws.com TLSV1.2 - -
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 amzn-s3-demo-bucket1 [06/Feb/2019:00:01:57 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 DD6CC733AEXAMPLE REST.PUT.OBJECT s3-dg.pdf "PUT /amzn-s3-demo-bucket1/
s3-dg.pdf HTTP/1.1" 200 - - 4406583 41754 28 "-" "S3Console/0.4" -
 10S62Zv81kBW7BB6SX4XJ48o6kpcl6LPwEoizZQQxJd5qDSCTLX0TgS37kYUBKQW3+bPdrg1234= SigV4
 ECDHE-RSA-AES128-SHA AuthHeader amzn-s3-demo-bucket1.s3.us-west-1.amazonaws.com
 TLSV1.2 - Yes
```

> **Note**
>
> 任何字段都可以设置为 - 以指示数据未知或不可用，或者该字段不适用于此请求。

### 主题

- 日志记录字段

- 复制操作的其他日志记录
- 自定义访问日志信息
- 可扩展服务器访问日志格式的编程注意事项

## 日志记录字段

以下列表介绍了日志记录字段。

存储桶拥有者

源存储桶拥有者的规范用户 ID。规范用户 ID 是另一种形式的 Amazon Web Services 账户 ID。有关规范用户 ID 的更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon Web Services 账户 标识符。有关如何查找您的账户的规范用户 ID 的信息，请参阅查找 Amazon Web Services 账户 的规范用户 ID。

示例条目

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

存储桶

请求处理的存储桶的名称。如果系统收到格式错误的请求且无法确定存储桶，则请求不会显示在任何的服务器访问日志中。

示例条目

```
amzn-s3-demo-bucket1
```

Time

收到请求的时间；这些日期和时间采用协调世界时 (UTC)。使用 `strftime()` 术语的格式如下所示：`[%d/%b/%Y:%H:%M:%S %z]`

示例条目

```
[06/Feb/2019:00:00:38 +0000]
```

远程 IP

请求者的显式 IP 地址。中间代理和防火墙可能会隐藏发出请求的计算机的实际 IP 地址。

示例条目

```
192.0.2.3
```

请求者

请求者的规范用户 ID 或用于未经验证请求的 -。如果请求者是 IAM 用户，此字段会返回请求者的 IAM 用户名以及该 IAM 用户所属的 Amazon Web Services 账户。此标识符与用于访问控制目的的标识符是相同的。

示例条目

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

如果请求者使用代入的角色，则此字段返回代入的 IAM 角色。

示例条目

```
arn:aws:sts::123456789012:assumed-role/roleName/test-role
```

请求 ID

由 Amazon S3 生成的字符串，可用于唯一地标识每个请求。

示例条目

```
3E57427F33A59F07
```

操作

此处列出的操作将声明为 SOAP.*operation*、REST.*HTTP_method*.*resource_type*、WEBSITE.*HTTP_method*.*resource_t* 或 BATCH.DELETE.OBJECT，或者 S3 生命周期和日志记录 的 S3.action.resource_type。

示例条目

```
REST.PUT.OBJECT
```

键

请求的密钥（对象名称）部分。

示例条目

```
/photos/2019/08/puppy.jpg
```

Request-URI

HTTP 请求消息的 Request-URI 部分。

示例条目

```
"GET /amzn-s3-demo-bucket1/photos/2019/08/puppy.jpg?x-foo=bar HTTP/1.1"
```

HTTP 状态

响应的数字 HTTP 状态代码。

示例条目

```
200
```

错误代码

Amazon S3 Error responses 或 -（如果没有发生错误）。

示例条目

```
NoSuchBucket
```

发送的字节数

发送的响应字节数（不包括 HTTP 协议支出），或 -（如果为零)。

示例条目

```
2662992
```

对象大小

所涉及的对象的总大小。

示例条目

```
3462992
```

总时间

从服务器的角度传输请求的毫秒数。该值计算从收到请求到发送响应的最后一个字节的时间。由于网络延迟，从客户端计算出的时间可能会更长。

示例条目

```
70
```

周转时间

Amazon S3 处理您的请求所花费的毫秒数。该值计算从收到您的请求的最后一个字节到发出响应的第一个字节的时间。

示例条目

```
10
```

Referer

HTTP `Referer` 标头的值（如果存在）。发送请求时，HTTP 用户代理（例如，浏览器）通常会将此标头设置为链接的 URL 或嵌入页面。

示例条目

```
"http://www.example.com/webservices"
```

User-Agent

HTTP `User-Agent` 标头的值。

示例条目

```
"curl/7.15.1"
```

版本 ID

请求中的版本 ID；如果操作没有使用 versionId 参数，则为 -。

示例条目

```
3HL4kqtJvjVBH40Nrjfkd
```

主机 ID

x-amz-id-2 或 Amazon S3 扩展请求 ID。

示例条目

```
s9lzHYrFp76ZVxRcpX9+5cjAnEH2ROuNkd2BHfIa6UkFVdtjf5mKR3/eTPFvsiP/XV/VLi31234=
```

签名版本

签名版本，用于对请求进行身份验证的 SigV2 或 SigV4，或未经身份验证的请求的 -。

示例条目

```
SigV2
```

密码套件

协商用于处理 HTTPS 请求的传输层安全性协议（TLS）密码，或者，对于 HTTP 为 -。

示例条目

```
ECDHE-RSA-AES128-GCM-SHA256
```

身份验证类型

所使用的请求身份验证的类型：身份验证标头使用 AuthHeader，查询字符串（预签名 URL）使用 QueryString，未经身份验证的请求使用 -。

示例条目

```
AuthHeader
```

主机标头

用于连接到 Amazon S3 的端点。

示例条目

```
s3.us-west-2.amazonaws.com
```

某些较早的区域支持传统的端点。您可能会在服务器访问日志或 Amazon CloudTrail 日志中看到这些端点。有关更多信息，请参阅 传统终端节点。有关 Amazon S3 区域和端点的完整列表，请参阅《Amazon Web Services 一般参考》中的 Amazon S3 端点和限额。

TLS 版本

客户端协商的传输层安全性（TLS）版本。此值为以下值之一：TLSv1.1、TLSv1.2、TLSv1.3；如果不使用 TLS，则为 -。

示例条目

```
TLSv1.2
```

接入点 ARN

请求接入点的 Amazon Resource Name（ARN）。如果接入点的 ARN 格式不正确或未使用，则该字段将包含 -。有关接入点的更多信息，请参阅 使用通用存储桶的 Amazon S3 接入点。有关 ARN 的更多信息，请参阅《Amazon 参考指南》中的 Amazon 资源名称（ARN）。

示例条目

```
arn:aws:s3:us-east-1:123456789012:accesspoint/example-AP
```

aclRequired

一个字符串，用于指示请求是否需要访问控制列表（ACL）以进行授权。如果请求需要 ACL 进行授权，则字符串为 Yes。如果不需要 ACL，则字符串为 -。有关 ACL 的更多信息，请参阅 访问控制列表 (ACL) 概述。有关使用 aclRequired 字段禁用 ACL 的更多信息，请参阅为您的存储桶控制对象所有权和禁用 ACL。。

示例条目

```
Yes
```

## 复制操作的其他日志记录

复制操作包括 GET 和 PUT。出于该原因，我们会在执行复制操作时记录两份记录。前面的部分描述了与操作的 PUT 部分相关的字段。以下列表描述了记录中与复制操作的 GET 部分相关的字段。

存储桶拥有者

用于存储将复制的对象的存储桶的规范用户 ID。规范用户 ID 是另一种形式的 Amazon Web Services 账户 ID。有关规范用户 ID 的更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon Web Services 账户 标识符。有关如何查找您的账户的规范用户 ID 的信息，请参阅查找 Amazon Web Services 账户 的规范用户 ID。

示例条目

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

存储桶

用于存储被复制对象的存储桶的名称。

示例条目

```
amzn-s3-demo-bucket1
```

Time

收到请求的时间；这些日期和时间采用协调世界时 (UTC)。使用 `strftime()` 术语的格式如下所示：`[%d/%B/%Y:%H:%M:%S %z]`

示例条目

```
[06/Feb/2019:00:00:38 +0000]
```

远程 IP

请求者的显式 IP 地址。中间代理和防火墙可能会隐藏发出请求的计算机的实际 IP 地址。

示例条目

```
192.0.2.3
```

请求者

请求者的规范用户 ID 或用于未经验证请求的 -。如果请求者是 IAM 用户，此字段将返回请求者的 IAM 用户名以及该 IAM 用户所属的 Amazon Web Services 账户根用户。此标识符与用于访问控制目的的标识符是相同的。

示例条目

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

如果请求者使用代入的角色，则此字段返回代入的 IAM 角色。

示例条目

```
arn:aws:sts::123456789012:assumed-role/roleName/test-role
```

请求 ID

由 Amazon S3 生成的字符串，可用于唯一地标识每个请求。

示例条目

```
3E57427F33A59F07
```

操作

此处列出的操作将声明为 SOAP.*operation*、REST.*HTTP_method*.*resource_type*、WEBSITE.*HTTP_method*.*resource_t* 或 BATCH.DELETE.OBJECT。

示例条目

```
REST.COPY.OBJECT_GET
```

键

被复制对象的键（对象名称）；或者，如果操作没有使用键参数，则为 -。

示例条目

```
/photos/2019/08/puppy.jpg
```

### Request-URI

HTTP 请求消息的 Request-URI 部分。

示例条目

```
"GET /amzn-s3-demo-bucket1/photos/2019/08/puppy.jpg?x-foo=bar"
```

### HTTP 状态

复制操作的 GET 部分的数字 HTTP 状态代码。

示例条目

```
200
```

### 错误代码

复制操作的 GET 部分的 Amazon S3 Error responses 或 -（如果没有发生错误）。

示例条目

```
NoSuchBucket
```

### 发送的字节数

发送的响应字节数（不包括 HTTP 协议支出）；或者，如果为零，则为 -。

示例条目

```
2662992
```

### 对象大小

所涉及的对象的总大小。

示例条目

```
3462992
```

总时间

从服务器的角度传输请求的毫秒数。该值计算从收到请求到发送响应的最后一个字节的时间。由于网络延迟，从客户端计算出的时间可能会更长。

示例条目

```
70
```

周转时间

Amazon S3 处理您的请求所花费的毫秒数。该值计算从收到您的请求的最后一个字节到发出响应的第一个字节的时间。

示例条目

```
10
```

Referer

HTTP `Referer` 标头的值（如果存在）。发送请求时，HTTP 用户代理（例如，浏览器）通常会将此标头设置为链接的 URL 或嵌入页面。

示例条目

```
"http://www.example.com/webservices"
```

User-Agent

HTTP `User-Agent` 标头的值。

示例条目

```
"curl/7.15.1"
```

版本 ID

被复制对象的版本 ID，或者，如果 x-amz-copy-source 标头没有将 versionId 参数指定为复制源的一部分，则为 -。

示例条目

```
3HL4kqtJvjVBH40Nrjfkd
```

主机 ID

x-amz-id-2 或 Amazon S3 扩展请求 ID。

示例条目

```
s9lzHYrFp76ZVxRcpX9+5cjAnEH2ROuNkd2BHfIa6UkFVdtjf5mKR3/eTPFvsiP/XV/VLi31234=
```

签名版本

签名版本 SigV2 或 SigV4，用于对请求进行身份验证；或者，对于未经身份验证的请求，则为 -。

示例条目

```
SigV4
```

密码套件

协商用于处理 HTTPS 请求的传输层安全性协议（TLS）密码，或者，对于 HTTP 为 -。

示例条目

```
ECDHE-RSA-AES128-GCM-SHA256
```

身份验证类型

所使用的请求身份验证的类型：身份验证标头使用 AuthHeader，查询字符串（预签名 URL）使用 QueryString，未经身份验证的请求使用 -。

示例条目

```
AuthHeader
```

主机标头

用于连接到 Amazon S3 的端点。

示例条目

```
s3.us-west-2.amazonaws.com
```

某些较早的区域支持传统的端点。您可能会在服务器访问日志或 Amazon CloudTrail 日志中看到这些端点。有关更多信息，请参阅 传统终端节点。有关 Amazon S3 区域和端点的完整列表，请参阅《Amazon Web Services 一般参考》中的 Amazon S3 端点和限额。

TLS 版本

客户端协商的传输层安全性（TLS）版本。此值为以下值之一：TLSv1.1、TLSv1.2、TLSv1.3；如果不使用 TLS，则为 -。

示例条目

```
TLSv1.2
```

接入点 ARN

请求接入点的 Amazon Resource Name（ARN）。如果接入点的 ARN 格式不正确或未使用，则该字段将包含 -。有关接入点的更多信息，请参阅 使用通用存储桶的 Amazon S3 接入点。有关 ARN 的更多信息，请参阅《Amazon 参考指南》中的 Amazon 资源名称（ARN）。

示例条目

```
arn:aws:s3:us-east-1:123456789012:accesspoint/example-AP
```

aclRequired

一个字符串，用于指示请求是否需要访问控制列表（ACL）以进行授权。如果请求需要 ACL 进行授权，则字符串为 Yes。如果不需要 ACL，则字符串为 -。有关 ACL 的更多信息，请参阅 访问控制列表 (ACL) 概述。有关使用 aclRequired 字段禁用 ACL 的更多信息，请参阅为您的存储桶控制对象所有权和禁用 ACL。。

示例条目

```
Yes
```

### 自定义访问日志信息

您可以包含要存储在请求的访问日志记录中的自定义信息。为此，请将自定义查询字符串参数添加到请求的 URL 中。Amazon S3 忽略以 x- 开头的查询字符串参数，但是会将这些参数包含在请求的访问日志记录中，以作为日志记录的 Request-URI 字段的一部分。

例如，GET 的 "s3.amazonaws.com/amzn-s3-demo-bucket1/photos/2019/08/puppy.jpg?x-user=johndoe" 请求工作方式与 "s3.amazonaws.com/amzn-s3-demo-bucket1/photos/2019/08/puppy.jpg" 的请求的相同，只是 "x-user=johndoe" 字符串包含在关联日志记录的 Request-URI 字段中。此功能仅在 REST 界面中可用。

### 可扩展服务器访问日志格式的编程注意事项

有时，我们可能会通过向每一行的末尾添加新字段来扩展访问日志记录格式。因此，请确保用于解析服务器访问日志的任何代码都可以处理它后续可能不理解的字段。

## 删除 Amazon S3 日志文件

一个已启用服务器访问日志记录的 Amazon S3 存储桶可能会随时间推移积累许多服务器日志对象。您的应用程序可能在创建之后的特定时间段内需要这些访问日志，在此之后，您可能希望删除它们。您可以使用 Amazon S3 生命周期配置来设置规则，以便 Amazon S3 可自动对这些对象进行排队，从而在其生命周期结束时进行删除。

您可以使用共享前缀为 S3 存储桶中的对象子集定义生命周期配置。如果您在服务器访问日志记录配置中指定了前缀，则可以设置生命周期配置规则，以删除具有该前缀的日志对象。

例如，假定您的日志对象具有前缀 logs/。您可以设置生命周期配置规则，以便在指定的时间段后删除存储桶中具有 logs/ 前缀的所有对象。

有关生命周期配置的更多信息，请参阅 管理对象的生命周期。

有关服务器访问日志记录的一般信息，请参阅 使用服务器访问日志记录来记录请求。

## 使用 Amazon S3 服务器访问日志来确定请求

您可以使用 Amazon S3 服务器访问日志来确定 Amazon S3 请求。

> **Note**
>
> - 要确定 Amazon S3 请求，建议您使用 Amazon CloudTrail 数据事件而不是 Amazon S3 服务器访问日志。CloudTrail 数据事件更易于设置并包含更多信息。有关更多信息，请参阅 使用 CloudTrail 识别 Amazon S3 请求。
> - 根据您获得的访问请求数量，与使用 CloudTrail 数据事件相比，分析日志使用的资源或时间可能会更多。

主题


- 使用 Amazon Athena 查询访问日志中的请求
- 使用 Amazon S3 访问日志确定签名版本 2 请求
- 使用 Amazon S3 访问日志确定对象访问请求


## 使用 Amazon Athena 查询访问日志中的请求

您可以使用 Amazon Athena 查询 Amazon S3 访问日志以确定 Amazon S3 请求。

Amazon S3 将服务器访问日志作为对象存储在 S3 存储桶中。使用可以分析 Amazon S3 中的日志的工具通常会更轻松。Athena 支持分析 S3 对象，并且可用于查询 Amazon S3 访问日志。

Example

以下示例说明了如何在 Amazon Athena 中查询 Amazon S3 服务器访问日志。将以下示例中使用的 *user input placeholders* 替换为您自己的信息。

> **Note**
>
> 要在 Athena 查询中指定 Amazon S3 位置，您必须提供将日志传输到的存储桶的 S3 URI。此 URI 必须包含以下格式的存储桶名称和前缀：`s3://amzn-s3-demo-bucket1-logs/prefix/`

1. 从 https://console.aws.amazon.com/athena/ 打开 Athena 控制台。
2. 在查询编辑器中，运行类似如下的命令。将 *s3_access_logs_db* 替换为要为数据库指定的名称。

```
CREATE DATABASE s3_access_logs_db
```

> **Note**
>
> 最佳实践是在与 S3 存储桶所在相同的 Amazon Web Services 区域中创建数据库。

3. 在查询编辑器中，运行类似如下的命令以便在步骤 2 中创建的数据库中创建一个表架构。将 *s3_access_logs_db.mybucket_logs* 替换为要为表指定的名称。STRING 和 BIGINT 数据类型值是访问日志属性。您可以在 Athena 中查询这些属性。对于 LOCATION，输入之前记下的 S3 存储桶和前缀。

   Date-based paritioning

```
CREATE EXTERNAL TABLE s3_access_logs_db.mybucket_logs(
 `bucketowner` STRING,
 `bucket_name` STRING,
 `requestdatetime` STRING,
 `remoteip` STRING,
 `requester` STRING,
 `requestid` STRING,
 `operation` STRING,
 `key` STRING,
 `request_uri` STRING,
 `httpstatus` STRING,
 `errorcode` STRING,
 `bytessent` BIGINT,
 `objectsize` BIGINT,
 `totaltime` STRING,
 `turnaroundtime` STRING,
 `referrer` STRING,
 `useragent` STRING,
 `versionid` STRING,
 `hostid` STRING,
 `sigv` STRING,
 `ciphersuite` STRING,
 `authtype` STRING,
 `endpoint` STRING,
 `tlsversion` STRING,
 `accesspointarn` STRING,
 `aclrequired` STRING)
 PARTITIONED BY (
```

```
   `timestamp` string)
ROW FORMAT SERDE
 'org.apache.hadoop.hive.serde2.RegexSerDe'
WITH SERDEPROPERTIES (
 'input.regex'='([^ ]*) ([^ ]*) \\[(.*?)\\] ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*)
 ([^ ]*) (\"[^\"]*\"|-) (-|[0-9]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*)
 ([^ ]*) (\"[^\"]*\"|-) ([^ ]*)(?: ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*)
 ([^ ]*) ([^ ]*) ([^ ]*))?.*$')
STORED AS INPUTFORMAT
 'org.apache.hadoop.mapred.TextInputFormat'
OUTPUTFORMAT
 'org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat'
LOCATION
 's3://bucket-name/prefix-name/account-id/region/source-bucket-name/'
 TBLPROPERTIES (
  'projection.enabled'='true',
  'projection.timestamp.format'='yyyy/MM/dd',
  'projection.timestamp.interval'='1',
  'projection.timestamp.interval.unit'='DAYS',
  'projection.timestamp.range'='2024/01/01,NOW',
  'projection.timestamp.type'='date',
  'storage.location.template'='s3://bucket-name/prefix-name/account-id/region/
source-bucket-name/${timestamp}')
```

### Non-date-based partitioning

```
CREATE EXTERNAL TABLE `s3_access_logs_db.mybucket_logs`(
  `bucketowner` STRING,
  `bucket_name` STRING,
  `requestdatetime` STRING,
  `remoteip` STRING,
  `requester` STRING,
  `requestid` STRING,
  `operation` STRING,
  `key` STRING,
  `request_uri` STRING,
  `httpstatus` STRING,
  `errorcode` STRING,
  `bytessent` BIGINT,
  `objectsize` BIGINT,
  `totaltime` STRING,
  `turnaroundtime` STRING,
```

```
  `referrer` STRING,
  `useragent` STRING,
  `versionid` STRING,
  `hostid` STRING,
  `sigv` STRING,
  `ciphersuite` STRING,
  `authtype` STRING,
  `endpoint` STRING,
  `tlsversion` STRING,
  `accesspointarn` STRING,
  `aclrequired` STRING)
ROW FORMAT SERDE
  'org.apache.hadoop.hive.serde2.RegexSerDe'
WITH SERDEPROPERTIES (
  'input.regex'='([^ ]*) ([^ ]*) \\[(.*?)\\] ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*)
 ([^ ]*) (\"[^\"]*\"|-) (-|[0-9]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*)
 ([^ ]*) (\"[^\"]*\"|-) ([^ ]*)(?: ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*)
 ([^ ]*) ([^ ]*) ([^ ]*))?.*$')
STORED AS INPUTFORMAT
  'org.apache.hadoop.mapred.TextInputFormat'
OUTPUTFORMAT
  'org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat'
LOCATION
  's3://amzn-s3-demo-bucket1-logs/prefix/'
```

4. 在导航窗格中，在 Database (数据库) 下，请选择您的数据库。
5. 在 Tables (表) 下，请选择表名称旁边的 Preview table (预览表)。

   在 Results (结果) 窗格中，您应看到来自服务器访问日志中的数据，如 `bucketowner`、`bucket`、`requestdatetime` 等。这表示您成功创建了 Athena 表。您现在可以查询 Amazon S3 服务器访问日志。

Example — 显示已删除对象的人员和时间（时间戳、IP 地址和 IAM 用户）

```
SELECT requestdatetime, remoteip, requester, key
FROM s3_access_logs_db.mybucket_logs
WHERE key = 'images/picture.jpg' AND operation like '%DELETE%';
```

Example — 显示 IAM 用户执行的所有操作

```
SELECT *
FROM s3_access_logs_db.mybucket_logs
WHERE requester='arn:aws:iam::123456789123:user/user_name';
```

Example — 显示在特定时间段内对对象执行的所有操作

```
SELECT *
FROM s3_access_logs_db.mybucket_logs
WHERE Key='prefix/images/picture.jpg'
    AND parse_datetime(requestdatetime,'dd/MMM/yyyy:HH:mm:ss Z')
    BETWEEN parse_datetime('2017-02-18:07:00:00','yyyy-MM-dd:HH:mm:ss')
    AND parse_datetime('2017-02-18:08:00:00','yyyy-MM-dd:HH:mm:ss');
```

Example — 显示在特定时间段内传输到特定 IP 地址的数据量

```
SELECT coalesce(SUM(bytessent), 0) AS bytessenttotal
FROM s3_access_logs_db.mybucket_logs
WHERE remoteip='192.0.2.1'
AND parse_datetime(requestdatetime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2022-06-01','yyyy-MM-dd')
AND parse_datetime('2022-07-01','yyyy-MM-dd');
```

Example — 查找特定时间段内 HTTP 5xx 错误的请求 ID

```
SELECT requestdatetime, key, httpstatus, errorcode, requestid, hostid
FROM s3_access_logs_db.mybucket_logs
WHERE httpstatus like '5%'AND timestamp
BETWEEN '2024/01/29'
AND '2024/01/30'
```

> **Note**
>
> 要减少保留日志的时间，您可以为服务器访问日志存储桶创建 S3 生命周期配置。创建生命周期配置规则以定期删除日志文件。这样做可以减少 Athena 为每个查询分析的数据量。有关更多信息，请参阅 在存储桶上设置 S3 生命周期配置。

## 使用 Amazon S3 访问日志确定签名版本 2 请求

对 Signature Version 2 的 Amazon S3 支持将会关闭（弃用）。之后，Amazon S3 将不再接受使用 Signature Version 2 的请求，并且所有请求必须使用 Signature Version 4 进行签署。您可以使用 Amazon S3 访问日志确定签名版本 2 访问请求。

> **Note**
>
> 要确定签名版本 2 请求，建议您使用 Amazon CloudTrail 数据事件而不是 Amazon S3 服务器访问日志。CloudTrail 数据事件更易于设置，并且包含比服务器访问日志更多的信息。有关更多信息，请参阅 使用 CloudTrail 识别 Amazon S3 签名版本 2 请求。

Example — 显示发送签名版本 2 流量的所有请求者

```
SELECT requester, sigv, Count(sigv) as sigcount
FROM s3_access_logs_db.mybucket_logs
GROUP BY requester, sigv;
```

## 使用 Amazon S3 访问日志确定对象访问请求

对于诸如 GET、PUT 和 DELETE 等操作，您可以对 Amazon S3 服务访问日志使用查询以确定 Amazon S3 对象访问请求，并发现有关这些请求的进一步信息。

以下 Amazon Athena 查询示例说明如何从服务器访问日志中获取 Amazon S3 的所有 PUT 对象请求。

Example — 显示在特定时段内正在发送 **PUT** 对象请求的所有请求者

```
SELECT bucket_name, requester, remoteip, key, httpstatus, errorcode, requestdatetime
FROM s3_access_logs_db
WHERE operation='REST.PUT.OBJECT' AND
```

```
parse_datetime(requestdatetime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2019-07-01:00:42:42','yyyy-MM-dd:HH:mm:ss')
AND
parse_datetime('2019-07-02:00:42:42','yyyy-MM-dd:HH:mm:ss')
```

以下 Amazon Athena 查询示例说明了如何从服务器访问日志中获取 Amazon S3 的所有 GET 对象请求。

Example — 显示在特定时段内正在发送 **GET** 对象请求的所有请求者

```
SELECT bucket_name, requester, remoteip, key, httpstatus, errorcode, requestdatetime
FROM s3_access_logs_db
WHERE operation='REST.GET.OBJECT' AND
parse_datetime(requestdatetime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2019-07-01:00:42:42','yyyy-MM-dd:HH:mm:ss')
AND
parse_datetime('2019-07-02:00:42:42','yyyy-MM-dd:HH:mm:ss')
```

以下 Amazon Athena 查询示例说明了如何从服务器访问日志中获取向 S3 存储桶发出的所有匿名请求。

Example — 显示在特定时段内向存储桶发出请求的所有匿名请求者

```
SELECT bucket_name, requester, remoteip, key, httpstatus, errorcode, requestdatetime
FROM s3_access_logs_db.mybucket_logs
WHERE requester IS NULL AND
parse_datetime(requestdatetime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2019-07-01:00:42:42','yyyy-MM-dd:HH:mm:ss')
AND
parse_datetime('2019-07-02:00:42:42','yyyy-MM-dd:HH:mm:ss')
```

以下 Amazon Athena 查询说明如何识别向 S3 存储桶发出的所有请求，这些请求需要访问控制列表（ACL）进行授权。您可以使用此信息将这些 ACL 权限迁移到相应的存储桶策略并禁用 ACL。创建这些存储桶策略后，您可以对这些存储桶禁用 ACL。有关禁用 ACL 的更多信息，请参阅禁用 ACL 的先决条件。

Example — 识别所有需要 ACL 进行授权的请求

```
SELECT bucket_name, requester, key, operation, aclrequired, requestdatetime
```

```
FROM s3_access_logs_db
WHERE aclrequired = 'Yes' AND
parse_datetime(requestdatetime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2022-05-10:00:00:00','yyyy-MM-dd:HH:mm:ss')
AND parse_datetime('2022-08-10:00:00:00','yyyy-MM-dd:HH:mm:ss')
```

> **Note**
>
> - 您可以修改日期范围以满足您的需要。
> - 也可以使用这些查询示例进行安全监控。您可以查看意外或未经授权的 IP 地址或请求者发出的 PutObject 或 GetObject 调用的结果，以及确定向存储桶发出的任何匿名请求。
> - 此查询仅从启用了日志记录的时间检索信息。
> - 如果您使用 Amazon CloudTrail 日志，请参阅 使用 CloudTrail 识别对 S3 对象的访问权限。

## 排查服务器访问日志记录问题

以下主题可以帮助您排查在使用 Amazon S3 设置日志记录时可能遇到的问题。

主题

- 设置日志记录时的常见错误消息
- 排查传输失败问题

### 设置日志记录时的常见错误消息

当您通过 Amazon Command Line Interface（Amazon CLI）和 Amazon SDK 启用日志记录功能时，可能会出现以下常见错误消息：

错误：不允许进行跨 S3 位置日志记录

如果目的地存储桶（也称为目标存储桶）与源存储桶位于不同的区域，则会出现不允许跨 S3 位置日志记录错误。要解决此错误，请确保配置为接收访问日志的目标存储桶与源存储桶位于相同的 Amazon Web Services 区域和 Amazon Web Services 账户中。

错误：要记录的存储桶的拥有者与目标存储桶的拥有者必须相同

启用服务器访问日志记录时，如果指定的目标存储桶属于其他账户，则会出现此错误。要解决此错误，请确保目标存储桶与源存储桶位于相同 Amazon Web Services 账户中。

> **Note**
>
> 我们建议您选择不同于源存储桶的目的地存储桶。当源存储桶和目标存储桶相同时，将为写入存储桶的日志创建额外的日志，这会增加您的存储费用。这些关于日志的额外日志也可能使您难以找到您正在寻找的特定日志。为了更方便地管理日志，我们建议将访问日志保存在不同的存储桶中。有关更多信息，请参阅 the section called “如何启用日志传送？”。

错误：用于日志记录的目标存储桶不存在

在设置配置之前，目标存储桶必须已存在。此错误表示目标存储桶不存在或找不到目标存储桶。确保存储桶名称拼写正确，然后重试。

错误：不允许对强制存储桶拥有者的存储存储桶进行目标授权

此错误表明目标存储桶为 S3 对象所有权使用“强制存储桶拥有者”设置。“强制存储桶拥有者”设置不支持目的地（目标）存储桶。有关更多信息，请参阅 日志传输的权限。

## 排查传输失败问题

为避免出现服务器访问日志记录问题，请确保遵循以下最佳实践：

- S3 日志传输组具有对目的地存储桶的写入权限 – S3 日志传输组将服务器访问日志传输到目的地存储桶。存储桶策略或存储桶访问控制列表（ACL）可用于授予对目标存储桶的写入权限。但是，我们建议您使用存储桶策略，而不是 ACL。有关如何授予对目标存储桶的写入权限的更多信息，请参阅日志传输的权限。

  > **Note**
  >
  > 如果目标存储桶为对象所有权使用“强制存储桶拥有者”设置，请注意以下几点：
  >
  > - ACL 已禁用，不再影响权限。这意味着，您无法更新存储桶 ACL 以授予对 S3 日志传输组的访问权限。相反，要授予对日志记录服务主体的访问权限，您必须更新目标存储桶的存储桶策略。
  > - 您不能将目标授权包含在 `PutBucketLogging` 配置中。

- 目标存储桶的存储桶策略允许访问日志 – 检查目标存储桶的存储桶策略。在存储桶策略中搜索包含 `"Effect": "Deny"` 的所有语句。然后，验证 Deny 语句不会阻止将访问日志写入存储桶中。

- 未对目标存储桶启用 S3 对象锁定 – 检查目标存储桶是否启用了对象锁定。对象锁定阻止服务器访问日志传输。您必须选择未启用对象锁定的目标存储桶。
- 如果在目标存储桶上启用了默认加密，则选择 Amazon S3 托管密钥（SSE-S3）– 仅当使用具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）时，才能对目标存储桶使用默认存储桶加密。服务器访问日志记录目标存储桶不支持采用 Amazon Key Management Service（Amazon KMS）密钥的默认服务器端加密（SSE-KMS）。有关如何启用默认加密的更多信息，请参阅配置默认加密。
- 目标存储桶未启用申请方付款 – 不支持将申请方付款存储桶用作服务器访问日志记录的目标存储桶。要允许传输服务器访问日志，请对目标存储桶禁用申请方付款选项。
- 查看您的 Amazon Organizations 服务控制策略（SCP）和资源控制策略（RCP）- 当使用 Amazon Organizations 时，请检查服务控制策略和资源控制策略以确保允许 Amazon S3 访问。这些策略指定了受影响账户中的主体和资源的最大权限。在策略中搜索任何包含 `"Effect": "Deny"` 的语句，并验证 `Deny` 语句不会阻止将任何访问日志写入存储桶中。有关更多信息，请参阅《Amazon Organizations User Guide》中的 Authorization policies in Amazon Organizations。
- 等待一段时间让最近的日志记录配置更改生效 – 首次启用服务器访问日志记录或更改日志的目标存储桶时，需要一定的时间才能完全生效。要正确记录和传输所有请求，可能需要一个多小时的时间。

  要检查日志传输失败，请在 Amazon CloudWatch 中启用请求指标。如果日志在几个小时内未传输，请查找 `4xxErrors` 指标，该指标可能表明日志传输失败。有关启用请求指标的更多信息，请参阅the section called “为所有对象创建指标配置”。

# 使用 Amazon CloudWatch 监控指标

Amazon S3 的 Amazon CloudWatch 指标可帮助您了解和提高使用 Amazon S3 的应用程序的性能。您可以通过多种方法将 CloudWatch 与 Amazon S3 结合使用。

存储桶的每日存储指标

使用 CloudWatch 来监控存储桶存储，此工具将从 Amazon S3 收集存储数据，并将数据处理为便于读取的每日指标。Amazon S3 的这些存储指标每天报告一次并提供给所有客户，无需额外费用。

请求指标

监控 Amazon S3 请求，以快速识别运行问题并对其采取措施。这些指标在要处理的某些延迟后每隔 1 分钟提供一次。这些 CloudWatch 指标的计费费率与 Amazon CloudWatch 自定义指标相同。有关 CloudWatch 定价的信息，请参阅 Amazon CloudWatch 定价。要了解如何选择获取这些指标，请参阅 CloudWatch 指标配置。

启用后，将为所有对象操作报告请求指标。默认情况下，这些 1 分钟指标在 Amazon S3 存储桶级别提供。您还可以使用共享前缀或对象标签或接入点为指标定义筛选条件。

- 接入点 - 接入点是命名为连接到存储桶的网络端点，可简化对 S3 中的共享数据集的大规模数据访问管理。通过接入点筛选条件，您可以深入了解您的接入点使用情况。有关接入点的更多信息，请参阅 监控和记录通用存储桶的接入点。
- 前缀 – 尽管 Amazon S3 数据模型是一种扁平结构，但您仍可以使用前缀推断层次结构。前缀类似于允许您将存储桶中的类似对象组合在一起的目录名称。S3 控制台支持这些带有文件夹概念的前缀。如果您按前缀进行筛选，有相同前缀的对象将包含在指标配置中。有关前缀的更多信息，请参阅 使用前缀组织对象。
- 标签 – 标记是可以添加到对象的键值名称对。标签可让您轻松查找和整理对象。您还可以使用标签作为指标配置的筛选条件，以便仅包含具有这些标签的对象。有关对象标签的更多信息，请参阅 使用标签对存储进行分类。

要将这些指标与特定的业务应用程序、工作流或内部组织对齐，您可以在共享前缀、对象标记或接入点上进行筛选。

复制指标

监控待复制的 S3 API 操作的总数、待复制的对象的总大小、到目标 Amazon Web Services 区域的最长复制时间以及复制失败的操作总数。已启用 S3 Replication Time Control（S3 RTC）或 S3 复制指标的复制规则会发布复制指标。

有关更多信息，请参阅使用指标、事件通知和状态监控复制或使用 S3 Replication Time Control 满足合规性要求。

Amazon S3 Storage Lens 存储统计管理工具指标

您可以将 S3 Storage Lens 存储统计管理工具使用情况和活动指标发布到 Amazon CloudWatch，以便在 CloudWatch 控制面板中创建运营状况的统一视图。S3 Storage Lens 存储统计管理工具指标可以在 `AWS/S3/Storage-Lens` 命名空间中可用。CloudWatch 发布选项可用于让 S3 Storage Lens 存储统计管理工具升级到 advanced metrics and recommendations（高级指标和建议）。您可以在 S3 Storage Lens 存储统计管理工具中为新的或现有的仪表板配置启用 CloudWatch 发布选项。

有关更多信息，请参阅 在 CloudWatch 中监控 S3 Storage Lens 存储统计管理工具指标。

所有 CloudWatch 统计数据会保留 15 个月，从而使您能够访问历史信息，并能够更好地了解您的 Web 应用程序或服务的运行情况。有关 CloudWatch 的更多信息，请参阅 Amazon CloudWatch 用户指南中的什么是 Amazon CloudWatch？。根据您的用例，您可能需要对 CloudWatch 警报进行一些额外的配

置。例如，您可以使用指标数学表达式来创建警报。有关更多信息，请参阅《Amazon CloudWatch 用户指南》中的使用 CloudWatch 指标、使用指标数学、使用 Amazon CloudWatch 警报以及根据指标数学表达式创建 CloudWatch 警报。

最大努力 CloudWatch 指标传输

系统将以最大努力传输 CloudWatch 指标。大多数具有请求指标的针对 Amazon S3 对象的请求会导致将数据点发送到 CloudWatch。

无法保证指标的完整性和及时性。可能返回特定请求的数据点，其时间戳晚于实际处理请求的时间。1 分钟的数据点在通过 CloudWatch 提供之前可能会延迟，或者根本不会提供该数据点。您可以通过 CloudWatch 请求指标近乎实时地了解有关存储桶流量性质方面的信息。这并不意味着会完整记录所有请求。

根据此特征的最大努力性质，在账单和成本管理控制面板提供的报告中可能有一个或多个访问请求不会出现在存储桶指标中。

有关更多信息，请参阅以下主题。

主题

- 指标与维度
- 访问 CloudWatch 指标
- CloudWatch 指标配置

## 指标与维度

以下各表列出了 Amazon S3 发送到 Amazon CloudWatch 的存储指标和维度。

最大努力 CloudWatch 指标传输

系统将以最大努力传输 CloudWatch 指标。大多数具有请求指标的针对 Amazon S3 对象的请求会导致将数据点发送到 CloudWatch。

无法保证指标的完整性和及时性。可能返回特定请求的数据点，其时间戳晚于实际处理请求的时间。1 分钟的数据点在通过 CloudWatch 提供之前可能会延迟，或者根本不会提供该数据点。您可以通过 CloudWatch 请求指标近乎实时地了解有关存储桶流量性质方面的信息。这并不意味着会完整记录所有请求。

根据此特征的最大努力性质，在账单和成本管理控制面板提供的报告中可能有一个或多个访问请求不会出现在存储桶指标中。

主题


- 在 CloudWatch 中存储桶的 Amazon S3 每日存储指标
- CloudWatch 中的 Amazon S3 CloudWatch 请求指标
- CloudWatch 中的 S3 复制指标
- CloudWatch 中的 S3 Storage Lens 存储统计管理工具指标
- CloudWatch 中的 S3 对象 Lambda 请求指标
- CloudWatch 中的 Amazon S3 维度
- CloudWatch 中的 S3 复制维度
- CloudWatch 中的 S3 Storage Lens 存储统计管理工具维度
- CloudWatch 中的 S3 对象 Lambda 请求维度
- Amazon S3 用量指标


## 在 CloudWatch 中存储桶的 Amazon S3 每日存储指标

AWS/S3 命名空间包含存储桶的以下每日存储指标。

| 指标 | 描述 |
| --- | --- |
| BucketSizeBytes | 存储在以下存储类的存储桶中的数据量（以字节为单位）：<br>• 低冗余存储（RRS）（REDUCED_REDUNDANCY ）<br>• S3 Express One Zone（EXPRESS_ONEZONE ）<br>• S3 Glacier Deep Archive (DEEP_ARCHIVE )<br>• S3 Glacier Flexible Retrieval (GLACIER)<br>• S3 Glacier Instant Retrieval (GLACIER_IR )<br>• S3 Intelligent-Tiering (INTELLIGENT_TIERING )<br>• S3 One Zone-Infrequent Access（ONEZONE_IA ）<br>• S3 Standard (STANDARD)<br>• S3 Standard-Infrequent Access (STANDARD_IA )<br><br>此值通过汇总存储桶中所有对象（当前对象和非当前对象）和元数据（例如存储桶名称）的大小计算得出，包括所有向存储桶进行分段上传而未完成的所有部分的大小。 |

| 指标 | 描述 |
| --- | --- |
| | **Note**<br>S3 Express One Zone 存储类仅可用于目录存储桶。<br><br>有效的存储类型筛选条件（请参阅 StorageType 维度）<br>• 低冗余存储（RRS）：ReducedRedundancyStorage<br>• S3 Express One Zone：ExpressOneZoneStorage<br>• S3 Glacier Deep Archive：DeepArchiveObjectOverhead、DeepArchiveS3ObjectOverhead、DeepArchiveStagingStorage、DeepArchiveStorage<br>• S3 Glacier Flexible Retrieval：GlacierObjectOverhead、GlacierS3ObjectOverhead、GlacierStagingStorage、GlacierStorage<br>• S3 Glacier Instant Retrieval：GlacierInstantRetrievalStorage、GlacierIRSizeOverhead<br>• S3 Intelligent-Tiering：IntelligentTieringAAStorage、IntelligentTieringAIAStorage、IntelligentTieringDAAStorage、IntelligentTieringFAStorage、IntelligentTieringIAStorage<br>• S3 One Zone-Infrequent Access：OneZoneIASizeOverhead、OneZoneIAStorage<br>• S3 Standard：StandardStorage<br>• S3 Standard-Infrequent Access：StandardIAObjectOverhead、StandardIASizeOverhead、StandardIAStorage<br><br>单位：字节<br><br>有效统计数据：Average<br><br>有关 StorageType 维度的更多信息，请参阅 the section called “CloudWatch 中的 Amazon S3 维度”。 |

| 指标 | 描述 |
| --- | --- |
| NumberOfObjects | 通用存储桶中存储的所有存储类的对象的总数。此值通过对存储桶中的所有对象（包括当前对象和非当前对象）、删除标记以及所有向存储桶进行分段上传而未完成的所有分段的总数进行计数而计算得出。对于对象位于 S3 Express One Zone 存储类中的目录桶，此值通过对桶中所有对象进行计数来计算得出，但不包括向桶进行的多次未完成的上传次数。<br><br>有效的存储类型筛选条件：AllStorageTypes （请参阅 StorageType 维度）<br><br>单位：计数<br><br>有效统计数据：平均值 |

## CloudWatch 中的 Amazon S3 CloudWatch 请求指标

AWS/S3 命名空间包含以下请求指标。这些指标包括不可计费的请求（如果是来自 CopyObject 和复制的 GET 请求）。

> **Note**
>
> 目录桶不支持 CloudWatch 中的 Amazon S3 请求指标。

| 指标 | 描述 |
| --- | --- |
| AllRequests | 向 Amazon S3 存储桶提出的 HTTP 请求（不论类型如何）的总数。如果您要将某个指标配置用于某个筛选条件，则该指标将仅返回符合该筛选条件要求的 HTTP 请求。<br><br>单位：计数<br><br>有效统计数据：Sum |
| GetRequests | 向 Amazon S3 存储桶中的对象发出的 HTTP GET 请求的数量。这不包括列表操作。对于每个 CopyObject 请求的来源，此指标会递增。<br><br>单位：计数 |

| 指标 | 描述 |
| --- | --- |
| | 有效统计数据：Sum<br><br>Note<br>面向分页列表的请求（例如 ListMultipartUploads、ListParts、ListObjectVersions 和其它）不包含在此指标中。 |
| PutRequests | 向 Amazon S3 存储桶中的对象发出的 HTTP PUT 请求的数量。对于每个 CopyObject 请求的目标，此指标会递增。<br><br>单位：计数<br><br>有效统计数据：Sum |
| DeleteRequests | 向 Amazon S3 存储桶中的对象发出的 HTTP DELETE 请求的数量。此指标还包括 DeleteObjects 请求。此指标显示发出的请求数量，而不是删除的对象数量。<br><br>单位：计数<br><br>有效统计数据：Sum |
| HeadRequests | 向 Amazon S3 存储桶发出的 HTTP HEAD 请求的数量。<br><br>单位：计数<br><br>有效统计数据：Sum |
| PostRequests | 向 Amazon S3 存储桶发出的 HTTP POST 请求的数量。<br><br>单位：计数<br><br>有效统计数据：Sum<br><br>Note<br>此指标不包括 DeleteObjects 和 SelectObjectContent 请求。 |

| 指标 | 描述 |
| --- | --- |
| SelectRequests | 向 Amazon S3 存储桶中的对象发出的 Amazon S3 SelectObjectContent 请求的数量。<br><br>单位：计数<br><br>有效统计数据：Sum |
| SelectBytesScanned | 使用 Amazon S3 存储桶中的 Amazon S3 SelectObjectContent 请求扫描的数据字节数。<br><br>单位：字节<br><br>有效统计数据：Average（每个请求的字节数）、Sum（每个周期的字节数）、Sample Count、Min、Max（与 p100 相同）、任何在 p0.0 和 p99.9 之间的百分位数 |
| SelectBytesReturned | 使用 Amazon S3 存储桶中的 Amazon S3 SelectObjectContent 请求返回的数据字节数。<br><br>单位：字节<br><br>有效统计数据：Average (每个请求的字节数)、Sum (每个周期的字节数)、Sample Count、Min、Max（与 p100 相同）、任何在 p0.0 和 p99.9 之间的百分位数 |
| ListRequests | 列出存储桶内容的 HTTP 请求的数量。<br><br>单位：计数<br><br>有效统计数据：Sum |
| BytesDownloaded | 为向 Amazon S3 存储桶提出的请求下载的字节数（请求的响应包含正文）。<br><br>单位：字节<br><br>有效统计数据：Average（每个请求的字节数）、Sum（每个周期的字节数）、Sample Count、Min、Max（与 p100 相同）、任何在 p0.0 和 p99.9 之间的百分位数 |

| 指标 | 描述 |
| --- | --- |
| BytesUploaded | 为向 Amazon S3 存储桶发出的请求上传的字节数（请求包含正文）。<br><br>单位：字节<br><br>有效统计数据：Average (每个请求的字节数)、Sum (每个周期的字节数)、Sample Count、Min、Max（与 p100 相同）、任何在 p0.0 和 p99.9 之间的百分位数 |
| 4xxErrors | 向 Amazon S3 存储桶发出的值为 0 或 1 的 HTTP 4xx 客户端错误状态代码请求数。Average 统计数据显示了错误率，Sum 统计数据显示了每个周期内该类型的错误的计数。<br><br>单位：计数<br><br>有效统计数据：Average (每个请求的报告数)、Sum (每个周期的报告数)、Min、Max、Sample Count |
| 5xxErrors | 向 Amazon S3 存储桶发出的值为 0 或 1 的 HTTP 5xx 服务器错误状态代码请求数。Average 统计数据显示了错误率，Sum 统计数据显示了每个周期内该类型的错误的计数。<br><br>单位：计数<br><br>有效统计数据：Average（每个请求的报告数）、Sum（每个周期的报告数）、Min、Max、Sample Count |
| FirstByte Latency | 从 Amazon S3 存储桶收到完整请求到开始返回响应的每请求时间。<br><br>单位：毫秒<br><br>有效统计数据：Average、Sum、Min、Max（与 p100 相同）、Sample Count、任何在 p0.0 和 p100 之间的百分位数 |

| 指标 | 描述 |
| --- | --- |
| TotalRequestLatency | 从收到第一个字节到将最后一个字节发送到 Amazon S3 存储桶的已用每请求时间。此指标包括接收请求正文和发送响应正文所耗的时间（未包含在 FirstByteLatency 中）。<br><br>单位：毫秒<br><br>有效统计数据：Average、Sum、Min、Max（与 p100 相同）、Sample Count、任何在 p0.0 和 p100 之间的百分位数 |

## CloudWatch 中的 S3 复制指标

您可以使用 S3 复制指标，通过跟踪待处理的字节、待处理的操作和复制延迟，监控复制的进度。有关更多信息，请参阅使用复制指标监控进度。

> **Note**
>
> 您可以在 Amazon CloudWatch 中对复制指标启用告警。为复制指标设置警报时，请将 Missing data treatment (丢失数据处理) 字段设置为 Treat missing data as ignore (maintain the alarm state) [将丢失的数据视为忽略（保持警报状态）]。

| 指标 | 描述 |
| --- | --- |
| ReplicationLatency | 对于给定的复制规则，复制目标 Amazon Web Services 区域落后于源 Amazon Web Services 区域的最大秒数。<br><br>单位：秒<br><br>有效统计数据：Max |
| BytesPendingReplication | 给定复制规则的待复制对象的总字节数。<br><br>单位：字节<br><br>有效统计数据：Max |

| 指标 | 描述 |
| --- | --- |
| OperationsPendingReplication | 给定复制规则的待复制操作数。<br><br>单位：计数<br><br>有效统计数据：Max |
| OperationsFailedReplication | 给定复制规则的复制失败的操作数。<br><br>单位：计数<br><br>有效统计信息：总和（失败操作总数）、平均值（失败率）、样本数（复制操作总数） |

## CloudWatch 中的 S3 Storage Lens 存储统计管理工具指标

您可以将 S3 Storage Lens 存储统计管理工具使用情况和活动指标发布到 Amazon CloudWatch，以便在 CloudWatch 控制面板中创建运营状况的统一视图。S3 Storage Lens 存储统计管理工具指标已发布到 CloudWatch 中的 AWS/S3/Storage-Lens 命名空间。CloudWatch 发布选项可用于已升级为 advanced metrics and recommendations（高级指标和建议）的 S3 Storage Lens 存储统计管理工具控制面板。

有关发布到 CloudWatch 的 S3 Storage Lens 存储统计管理工具指标列表，请参阅 Amazon S3 Storage Lens 存储统计管理工具指标词汇表。有关维度的完整列表，请参阅 Dimensions。

## CloudWatch 中的 S3 对象 Lambda 请求指标

S3 对象 Lambda 包含以下请求指标。

| 指标 | 描述 |
| --- | --- |
| AllRequests | 使用对象 Lambda 接入点向 Amazon S3 存储桶发出的 HTTP 请求总数。<br><br>单位：计数<br><br>有效统计数据：Sum |
| GetRequests | 使用对象 Lambda 接入点对于对象发出的 HTTP GET 请求的数量。该指标不包括列出操作。 |

| 指标 | 描述 |
| --- | --- |
| | 单位：计数<br><br>有效统计数据：Sum |
| BytesUploaded | 使用对象 Lambda 接入点上传到 Amazon S3 存储桶的字节数（请求包含正文）。<br><br>单位：字节<br><br>有效统计数据：Average（每个请求的字节数）、Sum（每个周期的字节数）、Sample Count、Min、Max（与 p100 相同）、任何在 p0.0 和 p99.9 之间的百分位数 |
| PostRequests | 使用对象 Lambda 接入点向 Amazon S3 存储桶发出的 HTTP POST 请求的数量。<br><br>单位：计数<br><br>有效统计数据：Sum |
| PutRequests | 使用对象 Lambda 接入点对于 Amazon S3 存储桶中的对象发出的 HTTP PUT 请求的数量。<br><br>单位：计数<br><br>有效统计数据：Sum |
| DeleteRequests | 使用对象 Lambda 接入点对于 Amazon S3 存储桶中的对象发出的 HTTP DELETE 请求的数量。此指标包括 DeleteObjects 请求。此指标显示发出的请求数量，而不是删除的对象数量。<br><br>单位：计数<br><br>有效统计数据：Sum |

| 指标 | 描述 |
| --- | --- |
| BytesDownloaded | 为使用对象 Lambda 接入点向 Amazon S3 存储桶发出的请求下载的字节数（响应包括正文）。<br><br>单位：字节<br><br>有效统计数据：Average（每个请求的字节数）、Sum（每个周期的字节数）、Sample Count、Min、Max（与 p100 相同）、任何在 p0.0 和 p99.9 之间的百分位数 |
| FirstByteLatency | 从 Amazon S3 存储桶通过对象 Lambda 接入点收到完整请求到开始返回响应的每请求时间。此指标取决于在 Amazon Lambda 函数将字节返回给对象 Lambda 接入点之前，该函数对于对象进行转换的运行时间。<br><br>单位：毫秒<br><br>有效统计数据：Average、Sum、Min、Max（与 p100 相同）、Sample Count、任何在 p0.0 和 p100 之间的百分位数 |
| TotalRequestLatency | 从收到第一个字节到将最后一个字节发送到对象 Lambda 接入点的已用每请求时间。此指标包括接收请求正文和发送响应正文所耗的时间（未包含在 FirstByteLatency 中）。<br><br>单位：毫秒<br><br>有效统计数据：Average、Sum、Min、Max（与 p100 相同）、Sample Count、任何在 p0.0 和 p100 之间的百分位数 |
| HeadRequests | 使用对象 Lambda 接入点向 Amazon S3 存储桶发出的 HTTP HEAD 请求的数量。<br><br>单位：计数<br><br>有效统计数据：Sum |

| 指标 | 描述 |
| --- | --- |
| ListRequests | 列出 Amazon S3 存储桶内容的 HTTP GET 请求的数量。该指标同时包含 ListObjects 和 ListObjectsV2 操作。<br><br>单位：计数<br><br>有效统计数据：Sum |
| 4xxErrors | 使用对象 Lambda 接入点向 Amazon S3 存储桶发出的值为 0 或 1 的 HTTP 4xx 客户端错误状态代码请求数。Average 统计数据显示了错误率，Sum 统计数据显示了每个周期内该类型的错误的计数。<br><br>单位：计数<br><br>有效统计数据：Average（每个请求的报告数）、Sum（每个周期的报告数）、Min、Max、Sample Count |
| 5xxErrors | 使用对象 Lambda 接入点向 Amazon S3 存储桶发出的值为 0 或 1 的 HTTP 5xx 服务器错误状态代码请求数。Average 统计数据显示了错误率，Sum 统计数据显示了每个周期内该类型的错误的计数。<br><br>单位：计数<br><br>有效统计数据：Average（每个请求的报告数）、Sum（每个周期的报告数）、Min、Max、Sample Count |
| ProxiedRequests | 向返回标准 Amazon S3 API 响应的对象 Lambda 接入点发出的 HTTP 请求的数量。（此类请求没有配置 Lambda 函数。）<br><br>单位：计数<br><br>有效统计数据：Sum |
| InvokedLambda | 对在其中调用 Lambda 函数的 S3 对象的 HTTP 请求数。<br><br>单位：计数<br><br>有效统计数据：Sum |

| 指标 | 描述 |
| --- | --- |
| LambdaResponseRequests | Lambda 函数发出的 WriteGetObjectResponse 请求的数量。此指标仅适用于 GetObject 请求。 |
| LambdaResponse4xx | 从 Lambda 函数调用 WriteGetObjectResponse 时发生的 HTTP 4xx 客户端错误的数量。此指标提供的信息与 4xxErrors 相同，但仅适用于 WriteGetObjectResponse 调用。 |
| LambdaResponse5xx | 从 Lambda 函数调用 WriteGetObjectResponse 时发生的 HTTP 5xx 服务器错误的数量。此指标提供的信息与 5xxErrors 相同，但仅适用于 WriteGetObjectResponse 调用。 |

## CloudWatch 中的 Amazon S3 维度

下列维度用于筛选 Amazon S3 指标。

| 维度 | 描述 |
| --- | --- |
| BucketName | 此维度筛选您仅为已识别存储桶请求的数据。 |
| StorageType | 此维度按以下存储类型筛选您存储在存储桶中的数据：<br>• DeepArchiveObjectOverhead – 对于每个归档对象，S3 Glacier 为索引及相关元数据添加 32KB 存储。标识和还原对象需要此额外数据。按照 S3 Glacier Deep Archive 费率对此附加存储收费。<br>• DeepArchiveS3ObjectOverhead – 对于归档到 S3 Glacier Deep Archive 的每个对象，Amazon S3 将 8KB 存储用于对象和其他元数据的名称。将按照 S3 Standard 标准费率对此附加存储收费。<br>• DeepArchiveStagingStorage - 在 S3 Glacier Deep Archive 存储类中的对象上完成 CompleteMultipartUpload 请求之前，用于分段上传对象的各个分段的字节数。<br>• DeepArchiveStorage – 用于 S3 Glacier Deep Archive 存储类中的对象的字节数。 |

| 维度 | 描述 |
| --- | --- |
| | • `ExpressOneZoneStorage` – 用于 S3 Express One Zone 存储类中的对象的字节数。<br>• `GlacierInstantRetrievalStorage` – 用于 S3 Glacier 即时检索存储类中的对象的字节数。<br>• `GlacierIRSizeOverhead` – 用于 S3 Glacier Instant Retrieval 存储类中小于 128KB 的对象的字节数。<br>• `GlacierObjectOverhead` – 对于每个归档对象，S3 Glacier 为索引及相关元数据添加 32KB 存储。标识和还原对象需要此额外数据。按照 S3 Glacier Flexible Retrieval 费率对此附加存储收费。<br>• `GlacierS3ObjectOverhead` – 对于归档到 S3 Glacier Flexible Retrieval 的每个对象，Amazon S3 将 8KB 存储用于对象和其他元数据的名称。将按照 S3 Standard 标准费率对此附加存储收费。<br>• `GlacierStagingStorage` – 在 S3 Glacier Flexible Retrieval 存储类中的对象上完成 `CompleteMultipartUpload` 请求之前，用于分段上传对象的各个分段的字节数。<br>• `GlacierStorage` – 用于 S3 Glacier Flexible Retrieval 存储类中的对象的字节数。<br>• `IntAAObjectOverhead` – 对于归档访问层中 `INTELLIGENT_TIERING` 存储类的每个对象，S3 Glacier 为索引和相关元数据添加了 32KB 的存储空间。标识和还原对象需要此额外数据。按照 S3 Glacier Flexible Retrieval 费率对此附加存储收费。<br>• `IntAAS3ObjectOverhead` – 对于归档访问层中 `INTELLIGENT_TIERING` 存储类的每个对象，Amazon S3 使用 8KB 的存储空间作为对象和其他元数据的名称。将按照 S3 Standard 标准费率对此附加存储收费。<br>• `IntDAAObjectOverhead` – 对于深度归档访问层中 `INTELLIGENT_TIERING` 存储类的每个对象，S3 Glacier 为索引和相关元数据添加了 32KB 的存储空间。标识和还原对象需要此额外数据。按照 S3 Glacier Deep Archive 存储费率对此附加存储收费。 |

| 维度 | 描述 |
| --- | --- |
| | • IntDAAS3ObjectOverhead – 对于深度归档访问层中 INTELLIGENT_TIERING 存储类的每个对象，Amazon S3 为索引和相关元数据添加了 8KB 的存储空间。标识和还原对象需要此额外数据。将按照 S3 Standard 标准费率对此附加存储收费。<br>• IntelligentTieringAAStorage – 用于 INTELLIGENT_TIERING 存储类的归档访问层中的对象的字节数。<br>• IntelligentTieringAIAStorage – 用于 INTELLIGENT_TIERING 存储类的归档即时访问层中的对象的字节数。<br>• IntelligentTieringDAAStorage – 用于 INTELLIGENT_TIERING 存储类的深层归档访问层中的对象的字节数。<br>• IntelligentTieringFAStorage – 用于 INTELLIGENT_TIERING 存储类的频繁访问层中的对象的字节数。<br>• IntelligentTieringIAStorage – 用于 INTELLIGENT_TIERING 存储类的不频繁访问层中的对象的字节数。<br>• OneZoneIASizeOverhead – 用于 ONEZONE_IA 存储类中小于 128KB 的对象的字节数。<br>• OneZoneIAStorage – 用于“S3 单区 - 不频繁访问层（ONEZONE_IA ）”存储类中的对象的字节数。<br>• ReducedRedundancyStorage – 用于低冗余存储 (RRS) 类中的对象的字节数。<br>• StandardIASizeOverhead – 用于 STANDARD_IA 存储类中小于 128KB 的对象的字节数。<br>• StandardIAStorage – 用于 S3 Standard-Infrequent Access（STANDARD_IA ）存储类中的对象的字节数。<br>• StandardStorage – 用于 STANDARD 存储类中的对象的字节数。 |
| FilterId | 此维度将筛选您为存储桶上的请求指标指定的指标配置。创建指标配置时，需要指定筛选条件 ID（例如，前缀、标签或接入点）。有关更多信息，请参阅创建指标配置。 |

## CloudWatch 中的 S3 复制维度

下列维度用于筛选 S3 复制指标。

| 维度 | 描述 |
| --- | --- |
| SourceBucket | 从中进行复制的桶对象的名称。 |
| DestinationBucket | 要复制到的桶对象的名称。 |
| RuleId | 触发该复制指标进行更新的规则的唯一标识符。 |

## CloudWatch 中的 S3 Storage Lens 存储统计管理工具维度

有关用于在 CloudWatch 中筛选 S3 Storage Lens 存储统计管理工具指标的维度列表，请参阅Dimensions。

## CloudWatch 中的 S3 对象 Lambda 请求维度

以下维度用于筛选来自对象 Lambda 接入点的数据。

| 维度 | 描述 |
| --- | --- |
| AccessPointName | 正在向其发出请求的接入点的名称。 |
| DataSourceARN | 对象 Lambda 接入点正从中检索数据的来源。如果请求调用 Lambda 函数，则这指的是 Lambda Amazon 资源名称（ARN）。否则，这指接入点 ARN。 |

## Amazon S3 用量指标

您可以使用 CloudWatch 使用情况指标来提供账户资源使用情况的可见性。这些指标可在 CloudWatch 图表和控制面板上直观呈现当前的服务使用情况。

Amazon S3 用量指标与 Amazon 服务配额相对应。您可以配置警报，以在用量接近服务配额时向您发出警报。有关 CloudWatch 与 Service Quotas 集成的更多信息，请参阅《Amazon CloudWatch 用户指南》中的 Amazon 使用情况指标。

Amazon S3 在 AWS/Usage 命名空间中发布以下指标。

| 指标 | 描述 |
| --- | --- |
| ResourceCount | 您账户中运行的指定资源的数量。资源由与指标关联的维度定义。 |

以下维度用于优化由 Amazon S3 发布的用量指标。

| 维度 | 描述 |
| --- | --- |
| Service | 包含该资源的 Amazon 服务的名称。对于 Amazon S3 用量指标，此维度的值为 S3。 |
| Type | 正在报告的实体的类型。目前，Amazon S3 用量指标的唯一有效值为 Resource。 |
| Resource | 正在运行的资源的类型。目前，Amazon S3 用量指标的唯一有效值是 GeneralPurposeBuckets ，它返回 Amazon Web Services 账户中通用存储桶的数量。通用存储桶支持跨所有存储类（S3 Express One Zone 除外）存储的对象。 |

## 访问 CloudWatch 指标

您可以按照以下步骤查看 Amazon S3 的存储指标。要获取涉及的 Amazon S3 指标，您必须设置开始和结束时间戳。对于任意给定 24 小时内的指标，请将时间段设置为 86400 秒（一天的秒数）。另外，请记得设置 BucketName 和 StorageType 维度。

使用 Amazon CLI

例如，如果您想要使用 Amazon CLI 以字节为单位获取特定桶的大小平均值，则可以使用以下命令：

```
aws cloudwatch get-metric-statistics --metric-name BucketSizeBytes --namespace AWS/S3
 --start-time 2016-10-19T00:00:00Z --end-time 2016-10-20T00:00:00Z --statistics Average
 --unit Bytes --region us-west-2 --dimensions Name=BucketName,Value=amzn-s3-demo-bucket
 Name=StorageType,Value=StandardStorage --period 86400 --output json
```

此示例将生成以下输出。

```
{
```

```
    "Datapoints": [
        {
            "Timestamp": "2016-10-19T00:00:00Z",
            "Average": 1025328.0,
            "Unit": "Bytes"
        }
    ],
    "Label": "BucketSizeBytes"
}
```

使用 S3 控制台

使用 Amazon CloudWatch 控制台查看指标

1. 通过 https://console.aws.amazon.com/cloudwatch/ 打开 CloudWatch 控制台。
2. 在左侧导航窗格中，选择 Metrics。
3. 请选择 S3 命名空间。
4. （可选）要查看某个指标，请在搜索框中输入该指标的名称。
5. （可选）要按 StorageType 维度进行筛选，请在搜索框中输入该存储类的名称。

使用 Amazon CLI 查看为您的 Amazon Web Services 账户存储的有效指标列表

- 在命令提示符处，使用以下命令。

```
aws cloudwatch list-metrics --namespace "AWS/S3"
```

有关访问 CloudWatch 控制面板所需权限的更多信息，请参阅《Amazon CloudWatch 用户指南》中的 Amazon CloudWatch 控制面板权限。

## CloudWatch 指标配置

借助 Amazon S3 的 Amazon CloudWatch 请求指标，您可以接收 1 分钟 CloudWatch 指标、设置 CloudWatch 警报和访问 CloudWatch 控制面板，从而近乎实时地查看 Amazon S3 存储的运行和性能。对于依赖于云存储的应用程序而言，这些指标使您可以快速识别运行问题并采取措施。启用后，这些 1 分钟指标默认在 Amazon S3 存储桶级别提供。

如果您要获取某个存储桶中的对象的 CloudWatch 请求指标，则必须为该存储桶创建指标配置。有关更多信息，请参阅 为存储桶中的所有对象创建 CloudWatch 指标配置。

您还可以使用共享前缀，对象标签或接入点为收集的指标定义筛选条件。这种定义筛选条件的方法将使您能够使各个指标筛选条件满足特定业务应用程序、工作流或内部组织的要求。有关更多信息，请参阅创建按前缀，对象标签或接入点筛选的指标配置。有关可用 CloudWatch 指标的更多信息和存储指标与请求指标之间的区别，请参阅 使用 Amazon CloudWatch 监控指标。

在使用指标配置时，请记住以下几点：

- 每个存储桶最多可以配置 1,000 个指标。
- 您可以利用筛选条件选择存储桶中的哪些对象可纳入指标配置。您可以筛选共享前缀，对象标签或接入点使各个指标筛选条件满足特定业务应用程序、工作流或内部组织的需求。要请求整个存储桶的指标，请创建一种不带筛选条件的指标配置。
- 只有启用请求指标才需要指标配置。存储桶级每日存储指标始终保持开启状态，并且免费提供。目前不能为筛选过的对象子集获取日常存储指标。
- 每个指标配置均可启用全套可用请求指标。只有存在适用于您的存储桶或筛选条件请求类型，才会报告特定于操作的指标（例如 `PostRequests`）。
- 将为对象级别操作报告请求指标。还为列出存储桶内容的操作 GET Bucket（List Objects）、GET Bucket Object Versions 和 List Multipart Uploads 报告请求指标，但不会为存储桶上的其他操作进行报告。
- 请求指标支持按前缀，对象标签或接入点进行筛选，但存储指标不支持。

### 最大努力 CloudWatch 指标传输

系统将以最大努力传输 CloudWatch 指标。大多数具有请求指标的针对 Amazon S3 对象的请求会导致将数据点发送到 CloudWatch。

无法保证指标的完整性和及时性。可能返回特定请求的数据点，其时间戳晚于实际处理请求的时间。1 分钟的数据点在通过 CloudWatch 提供之前可能会延迟，或者根本不会提供该数据点。您可以通过 CloudWatch 请求指标近乎实时地了解有关存储桶流量性质方面的信息。这并不意味着会完整记录所有请求。

根据此特征的最大努力性质，在账单和成本管理控制面板提供的报告中可能有一个或多个访问请求不会出现在存储桶指标中。

有关在 Amazon S3 中使用 CloudWatch 指标的更多信息，请参阅以下主题。

主题

- 为存储桶中的所有对象创建 CloudWatch 指标配置
- 创建按前缀，对象标签或接入点筛选的指标配置

- 删除指标筛选条件

## 为存储桶中的所有对象创建 CloudWatch 指标配置

配置请求指标时，您可以为存储桶中的所有对象创建 CloudWatch 指标配置，也可以按前缀，对象标签或接入点进行筛选。本主题中的步骤向您介绍如何为存储桶中的所有对象创建配置。要创建按对象标签，前缀或接入点筛选的配置，请参阅 创建按前缀，对象标签或接入点筛选的指标配置。

Amazon S3 存在三种类型的 Amazon CloudWatch 指标：存储指标、请求指标和复制指标。存储指标每天报告一次并提供给所有客户，无需额外费用。请求指标在要处理的某些延迟后每隔一分钟提供一次。请求指标按标准 CloudWatch 费率计费。您必须通过在控制台中配置请求指标或使用 Amazon S3 API 来选择使用请求指标。S3 复制指标为复制配置中的复制规则提供了详细的指标。使用复制指标，您可以通过跟踪待复制的字节数、待复制的操作数、复制失败的操作数和复制延迟来逐分钟监控进度。

有关 Amazon S3 的 CloudWatch 指标的更多信息，请参阅 使用 Amazon CloudWatch 监控指标。

您可以使用 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）或 Amazon S3 REST API 向存储桶添加指标配置。

使用 S3 控制台

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在存储桶列表中，选择您要为其获取请求指标的对象所在的存储桶的名称。
4. 请选择 Metrics（指标）选项卡。
5. 在 Bucket metrics（存储桶指标）下，请选择 View additional charts（查看其他图表）。
6. 请选择 Request metrics（请求指标）选项卡。
7. 请选择 Create filter（创建筛选器）。
8. 在 Filter name（筛选器名称）框中，输入筛选器名称。

   名称可以包含字母、数字、句点、短划线和下划线。建议对应用于所有对象的筛选器使用 `EntireBucket` 作为名称。
9. 在选择筛选范围下，请选择此筛选条件应用于存储桶中的所有对象。

   您还可以定义筛选器，以便仅对此存储桶中的一部分对象收集和报告指标。有关更多信息，请参阅 创建按前缀，对象标签或接入点筛选的指标配置。

10. 选择 Save changes (保存更改)。
11. 在 Request metrics (请求指标) 选项卡的 Filters (筛选器) 下，请选择刚创建的筛选器。

    大约 15 分钟后，CloudWatch 开始跟踪这些请求指标。您可以在 Request metrics (请求指标) 选项卡上查看它们。您可以在 Amazon S3 或 CloudWatch 控制台上查看指标的图形。请求指标按标准 CloudWatch 费率计费。有关更多信息，请参阅 Amazon CloudWatch 定价。

使用 REST API

您还可以使用 Amazon S3 REST API 以编程方式添加指标配置。有关添加和使用指标配置的更多信息，请参阅 Amazon Simple Storage Service API 参考中的以下主题：

- PUT Bucket Metric 配置
- GET Bucket Metric 配置
- List Bucket Metric 配置
- DELETE Bucket Metric 配置

使用 Amazon CLI

1. 安装并设置 Amazon CLI。有关说明，请参阅 Amazon Command Line Interface 用户指南中的安装、更新和卸载 Amazon CLI。
2. 打开终端。
3. 运行以下命令以添加指标配置。

```
aws s3api put-bucket-metrics-configuration --endpoint https://s3.us-
west-2.amazonaws.com --bucket bucket-name --id metrics-config-id --metrics-
configuration '{"Id":"metrics-config-id"}'
```

## 创建按前缀，对象标签或接入点筛选的指标配置

Amazon S3 存在三种类型的 Amazon CloudWatch 指标：存储指标、请求指标和复制指标。存储指标每天报告一次并提供给所有客户，无需额外费用。请求指标在要处理的某些延迟后每隔一分钟提供一次。请求指标按标准 CloudWatch 费率计费。您必须通过在控制台中配置请求指标或使用 Amazon S3 API 来选择使用请求指标。S3 复制指标为复制配置中的复制规则提供了详细的指标。使用复制指标，您可以通过跟踪待复制的字节数、待复制的操作数、复制失败的操作数和复制延迟来逐分钟监控进度。

有关 Amazon S3 的 CloudWatch 指标的更多信息，请参阅 使用 Amazon CloudWatch 监控指标。

配置 CloudWatch 指标时，您可以为存储桶中的所有对象创建筛选条件，也可以将配置筛选到单个存储桶中的相关对象组中。您可以基于以下一个或多个筛选条件类型在存储桶中筛选包含在指标配置中的对象：

- 对象键名称前缀 – 尽管 Amazon S3 数据模型是一种扁平结构，但您仍可以使用前缀推断层次结构。Amazon S3 控制台支持这些带有文件夹概念的前缀。如果您按前缀进行筛选，有相同前缀的对象将包含在指标配置中。有关前缀的更多信息，请参阅 使用前缀组织对象。
- 标签 – 您可以为对象添加标签（键值名称对）。标签可让您轻松查找和整理对象。您还可以使用标签作为指标配置的筛选条件。有关对象标签的更多信息，请参阅 使用标签对存储进行分类。
- 接入点 - S3 接入点是命名为连接到存储桶的网络端点，可简化对 S3 中的共享数据集的大规模数据访问管理。创建接入点筛选条件时，Amazon S3 会包含对指标配置中指定的接入点请求。有关更多信息，请参阅 监控和记录通用存储桶的接入点。

> **Note**
>
> 创建按接入点筛选的指标配置时，必须使用接入点 Amazon Resource Name (ARN)，而不是接入点别名。请确保您将 ARN 用于接入点本身，而不是特定对象的 ARN。有关接入点 ARN 的更多信息，请参阅 使用通用存储桶的 Amazon S3 接入点。

如果您指定了一项筛选条件，则仅在单个对象运行的请求可以满足筛选条件，并包含在报告的指标中。与 DeleteObjects 和 `ListObjects` 请求类似的请求不会使用筛选条件为配置返回任何指标。

要请求更复杂的筛选，请选择两个或更多元素。只有拥有所有这些元素的对象才会包含在指标配置中。如果未设置筛选条件，则存储桶中的所有对象都会包含在指标配置中。

使用 S3 控制台

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶
3. 在存储桶列表中，选择您要为其获取请求指标的对象所在的存储桶的名称。
4. 请选择 Metrics (指标) 选项卡。
5. 在 Bucket metrics（存储桶指标）下，请选择 View additional charts（查看其他图表）。
6. 请选择 Request metrics（请求指标）选项卡。
7. 请选择 Create filter（创建筛选器）。

8. 在 Filter name（筛选器名称）框中，输入筛选器名称。

   名称可以包含字母、数字、句点、短划线和下划线。

9. 在筛选条件范围中，请选择使用前缀、对象标签和 S3 接入点（或三个全选）来限制此筛选条件的范围。

10. 在筛选条件类型中，请至少选择一个筛选条件类型：前缀、对象标签，或接入点。

11. 要定义前缀筛选条件并将筛选范围限制为单个路径，请在前缀框中输入前缀。

12. 要定义对象标签筛选条件，请在对象标签中，请选择添加标签，然后输入标签密钥和值。

13. 要定义接入点筛选条件，请在 S3 接入点字段中，输入接入点 ARN，或选择浏览 S3导航到接入点。

> **Important**
>
> 您无法输入接入点别名。必须输入接入点本身的 ARN，而不是特定对象的 ARN。

14. 选择 Save changes (保存更改)。

    Amazon S3 会用您指定的前缀，标签或接入点创建筛选条件。

15. 在 Request metrics（请求指标）选项卡的 Filters（筛选器）下，请选择刚创建的筛选器。

    您现在已创建一个筛选条件，该筛选条件通过前缀，标签或接入点限制请求指标范围。在 CloudWatch 开始跟踪这些请求指标后大约 15 分钟，您就可以看到 Amazon S3 和 CloudWatch 控制台中的指标的图表。请求指标按标准 CloudWatch 费率计费。有关更多信息，请参阅 Amazon CloudWatch 定价。

    还可以在存储桶级别配置请求指标。有关信息，请参阅为存储桶中的所有对象创建 CloudWatch 指标配置。

使用 Amazon CLI

1. 安装并设置 Amazon CLI。有关说明，请参阅 Amazon Command Line Interface 用户指南中的安装、更新和卸载 Amazon CLI。

2. 打开终端。

3. 要添加指标配置，运行以下命令。

Example ：按前缀筛选

```
aws s3api put-bucket-metrics-configuration --bucket amzn-s3-demo-bucket --
id metrics-config-id --metrics-configuration '{"Id":"metrics-config-id", "Filter":
{"Prefix":"prefix1"}} '
```

Example ：按标签筛选

```
aws s3api put-bucket-metrics-configuration --bucket amzn-s3-demo-bucket --
id metrics-config-id --metrics-configuration '{"Id":"metrics-config-id", "Filter":
{"Tag": {"Key": "string", "Value": "string"}} '
```

Example ：按接入点筛选

```
aws s3api put-bucket-metrics-configuration --bucket amzn-s3-demo-bucket --
id metrics-config-id --metrics-configuration '{"Id":"metrics-config-id", "Filter":
{"AccessPointArn":"arn:aws:s3:Region:account-id:accesspoint/access-point-name"}} '
```

Example ：按前缀、标签和接入点筛选

```
aws s3api put-bucket-metrics-configuration --endpoint https://
s3.Region.amazonaws.com --bucket amzn-s3-demo-bucket --id metrics-config-id --
metrics-configuration '
{
    "Id": "metrics-config-id",
    "Filter": {
        "And": {
            "Prefix": "string",
            "Tags": [
                {
                    "Key": "string",
                    "Value": "string"
                }
            ],
            "AccessPointArn": "arn:aws:s3:Region:account-id:accesspoint/access-
point-name"
        }
    }
}'
```

使用 REST API

您还可以使用 Amazon S3 REST API 以编程方式添加指标配置。有关添加和使用指标配置的更多信息，请参阅 Amazon Simple Storage Service API 参考中的以下主题：

- PUT Bucket Metric 配置
- GET Bucket Metric 配置
- List Bucket Metric 配置
- DELETE Bucket Metric 配置

## 删除指标筛选条件

如果您不再需要 Amazon CloudWatch 请求指标筛选器，可以删除它。删除筛选条件时，您不再需要为使用该特定筛选条件的请求指标付费。但是，您将继续为存在的任何其他筛选条件配置付费。

删除筛选条件时，您不再能够对请求指标使用筛选条件。删除筛选条件的操作无法撤消。

有关创建请求指标筛选条件的信息，请参阅以下主题：

- 为存储桶中的所有对象创建 CloudWatch 指标配置
- 创建按前缀，对象标签或接入点筛选的指标配置

使用 S3 控制台

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在存储桶列表中，选择要删除其请求指标筛选条件的存储桶的名称。
4. 请选择 Metrics（指标）选项卡。
5. 在 Bucket metrics（存储桶指标）下，请选择 View additional charts（查看其他图表）。
6. 请选择 Request metrics (请求指标) 选项卡。
7. 请选择 Manage filters (管理筛选条件)。
8. 请选择您的筛选条件。

> **Important**
>
> 删除筛选条件的操作无法撤消。

9. 请选择 Delete。

   Amazon S3 会删除您的筛选条件。

使用 REST API

您还可以使用 Amazon S3 REST API 以编程方式添加指标配置。有关添加和使用指标配置的更多信息，请参阅 Amazon Simple Storage Service API 参考中的以下主题：

- PUT Bucket Metric 配置
- GET Bucket Metric 配置
- List Bucket Metric 配置
- DELETE Bucket Metric 配置

# Amazon S3 事件通知

您可以使用 Amazon S3 事件通知特征在 S3 存储桶中发生某些事件时接收通知。要启用通知，请添加一个通知配置，该配置标识您希望 Amazon S3 发布的事件。确保它还标识您希望 Amazon S3 将通知发送到的目的地。您可以将此配置存储在与存储桶关联的通知子资源中。有关更多信息，请参阅 通用存储桶配置选项。Amazon S3 提供了一个 API，用于管理此子资源。

> **Important**
>
> Amazon S3 事件通知设计为至少传送一次。通常，事件通知在几秒内传输，不过有时可能需要一分钟或更长时间。

## Amazon S3 事件通知概述

目前，Amazon S3 可以发布用于以下事件的通知：

- 新的对象创建事件

- 对象移除事件
- 还原对象事件
- 低冗余存储 (RRS) 对象丢失事件
- 复制事件
- S3 生命周期到期事件
- S3 生命周期转换事件
- S3 Intelligent-Tiering 自动归档事件
- 对象标记事件
- 对象 ACL PUT 事件

有关受支持事件类型的完整描述，请参阅 SQS、SNS 和 Lambda 支持的事件类型。

Amazon S3 可以将事件通知消息发送到以下目标。您在通知配置中指定这些目标的 Amazon Resource Name (ARN) 值。

- Amazon Simple Notification Service (Amazon SNS) 主题
- Amazon Simple Queue Service (Amazon SQS) 队列
- Amazon Lambda 函数
- Amazon EventBridge

有关更多信息，请参阅 受支持的事件目标。

> **Note**
>
> 不支持将 Amazon Simple Queue Service FIFO（先进先出）队列作为 Amazon S3 事件通知目标。要向 Amazon SQS FIFO 队列发送 Amazon S3 事件的通知，您可以使用 Amazon EventBridge。有关更多信息，请参阅 启用 Amazon EventBridge。

> **Warning**
>
> 如果您的通知写入触发通知的同一存储桶，则可能会导致执行循环。例如，如果每当上传一个对象，存储桶就触发某个 Lambda 函数，而该函数又上传一个对象给存储桶，则该函数间接触发了自身。为避免这种情况，请使用两个存储桶，或将触发器配置为仅适用于传入对象所用的前缀。

有关将 Amazon S3 通知与 Amazon Lambda 结合使用的更多信息和示例，请参阅 Amazon Lambda 开发人员指南中的结合使用 Amazon Lambda 和 Amazon S3。

有关每个存储桶可以创建的事件通知配置数的更多信息，请参阅 Amazon 一般参考中的 Amazon S3 服务配额。

有关事件通知的更多信息，请参阅以下部分：

主题


- 事件通知类型和目标
- 使用 Amazon SQS、Amazon SNS 和 Lambda
- 使用 EventBridge


## 事件通知类型和目标

Amazon S3 支持多种可以发布通知的事件通知类型和目标。配置事件通知时，您可以指定事件类型和目标。只能为每个事件通知指定一个目标。Amazon S3 事件通知为每条通知消息发送一个事件条目。

主题


- 受支持的事件目标
- SQS、SNS 和 Lambda 支持的事件类型
- Amazon EventBridge 支持的事件类型
- 事件排序和重复事件


### 受支持的事件目标

Amazon S3 可以将事件通知消息发送到以下目标。

- Amazon Simple Notification Service（Amazon SNS）主题
- Amazon Simple Queue Service（Amazon SQS）队列
- Amazon Lambda
- Amazon EventBridge

但是，只能为每个事件通知指定一种目标类型。

> **Note**
>
> 您必须授予 Amazon S3 将消息发布到 Amazon SNS 主题或 Amazon SQS 队列的权限。您还必须授予 Amazon S3 代表您调用 Amazon Lambda 函数的权限。有关如何授予这些权限的说明，请参阅 授予将事件通知消息发布到目标的权限。

### Amazon SNS 主题

Amazon SNS 是一项灵活且完全托管的消息推送服务。使用此服务，您可以将消息推送到移动设备或分布式服务。通过 SNS，，您只需要发布一次消息，就能将其发送无数遍。目前，仅允许标准 SNS 作为 S3 事件通知目标，而不允许 SNS FIFO。

Amazon SNS 用于协调和管理向订阅端点或客户交付或发送消息的过程。您可以使用 Amazon SNS 控制台创建 Amazon SNS 主题以便向其发送通知。

该主题必须与您的 Amazon S3 存储桶位于同一 Amazon Web Services 区域。有关如何创建 Amazon SNS 主题的信息，请参阅 Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 入门和 Amazon SNS 常见问题。

您先需要以下内容，然后才能将创建的 Amazon SNS 主题用作事件通知目标：

- Amazon SNS 主题的 Amazon Resource Name (ARN)
- 有效的 Amazon SNS 主题订阅。当消息发布到您的 Amazon SNS 主题时，主题订阅者将得到通知。

### Amazon SQS 队列

Amazon SQS 提供了可靠且可扩展的托管队列，用于存储计算机之间传输的消息。您可以使用 Amazon SQS 来传输任何容量的数据，而不需要其他服务始终可用。您可以使用 Amazon SQS 控制台创建 Amazon SQS 队列以便向其发送通知。

Amazon SQS 队列必须与您的 Amazon S3 存储桶位于同一 Amazon Web Services 区域。有关如何创建 Amazon SQS 队列的说明，请参阅 Amazon Simple Queue Service 开发人员指南中的什么是 Amazon Simple Queue Service 和 Amazon SQS 入门。

您先需要以下内容，然后才能使用 Amazon SQS 队列作为事件通知目标：

- Amazon SQS 队列的 Amazon Resource Name (ARN)

> **Note**
>
> 不支持将 Amazon Simple Queue Service FIFO（先进先出）队列作为 Amazon S3 事件通知目标。要向 Amazon SQS FIFO 队列发送 Amazon S3 事件的通知，您可以使用 Amazon EventBridge。有关更多信息，请参阅 启用 Amazon EventBridge。

### Lambda 函数

您可以使用 Amazon Lambda 通过自定义逻辑扩展其他 Amazon 服务，或创建您自己的按 Amazon 规模、性能和安全性运行的后端。借助 Lambda，您可以创建仅在需要时运行的离散、事件驱动的应用程序。您还可以使用它自动将这些应用程序从每天的几个请求扩展到每秒数千个请求。

Lambda 可以运行自定义代码以响应 Amazon S3 存储桶事件。您将自定义代码上传到 Lambda，并创建所谓的 Lambda 函数。当 Amazon S3 检测到特定类型的事件时，它可以将该事件发布到 Amazon Lambda 并在 Lambda 中调用您的函数。作为回应，Lambda 将运行您的函数。例如，它可能检测到的一种事件类型是对象创建的事件。

您可以使用 Amazon Lambda 控制台创建使用 Amazon 基础设施代表您运行代码的 Lambda 函数。Lambda 函数必须与您的 S3 存储桶位于同一区域。您还必须具有 Lambda 函数的名称或 ARN 才能将 Lambda 函数设置为事件通知目标。

> **Warning**
>
> 如果您的通知写入触发通知的同一存储桶，则可能会导致执行循环。例如，如果每当上传一个对象，存储桶就触发某个 Lambda 函数，而该函数又上传一个对象给存储桶，则该函数间接触发了自身。为避免这种情况，请使用两个存储桶，或将触发器配置为仅适用于传入对象所用的前缀。
>
> 有关将 Amazon S3 通知与 Amazon Lambda 结合使用的更多信息和示例，请参阅 Amazon Lambda 开发人员指南中的结合使用 Amazon Lambda 和 Amazon S3。

### Amazon EventBridge

Amazon EventBridge 是一个无服务器事件总线，它接收来自 Amazon 服务的事件。您可以设置规则来匹配事件并将它们传输到目标，例如 Amazon 服务或 HTTP 端点。有关更多信息，请参阅 Amazon EventBridge 用户指南中的什么是 EventBridge。

与其他目的地不同，您可以启用或禁用为存储桶传送到 EventBridge 的事件。如果启用传输，所有事件都发送到 EventBridge。此外，您可以使用 EventBridge 规则将事件路由到其他目标。

## SQS、SNS 和 Lambda 支持的事件类型

Amazon S3 可以发布以下类型的事件。您在通知配置中指定这些事件类型。

| 事件类型 | 描述 |
| --- | --- |
| s3:TestEvent | 启用通知后，Amazon S3 将发布测试通知。这是为了确保主题存在，并且存储桶拥有者有权发布指定主题。<br><br>如果启用通知失败，则不会收到测试通知。 |
| s3:ObjectCreated:*<br><br>s3:ObjectCreated:Put<br><br>s3:ObjectCreated:Post<br><br>s3:ObjectCreated:Copy<br><br>s3:ObjectCreated:CompleteMultipartUpload | 诸如 PUT、POST 和 COPY 之类的 Amazon S3 API 操作可以创建对象。通过这些事件类型，您可以在使用特定 API 操作创建对象时启用通知。或者，您可以使用 s3:ObjectCreated:* 事件类型来请求通知，而不考虑用于创建对象的 API。<br><br>s3:ObjectCreated:CompleteMultipartUpload 包含使用 UploadPartCopy 进行复制操作所创建的对象。 |
| s3:ObjectRemoved:*<br><br>s3:ObjectRemoved:Delete<br><br>s3:ObjectRemoved:DeleteMarkerCreated | 通过使用 ObjectRemoved 事件类型，您可以在从存储桶中移除一个对象或一批对象时启用通知。<br><br>您可以使用 s3:ObjectRemoved:Delete 事件类型请求在删除对象或永久删除受版本控制的对象时收到通知。或者，也可以使用 s3:ObjectRemoved:DeleteMarkerCreated 请求在为受版本控制的对象创建删除标记时收到通知。有关如何删除版本控制对象的说明，请参阅 从启用了版本控制的存储桶中删除对象版本。您还可以使用通配符 s3:ObjectRemoved:* 来请求在每次删除对象时收到通知。<br><br>这些事件通知不会针对从生命周期配置中的自动删除或失败的操作向您发出提示。 |
| s3:ObjectRestore:*<br><br>s3:ObjectRestore:Post | 通过使用 ObjectRestore 事件类型，可在从 S3 Glacier Flexible Retrieval 存储类、S3 Glacier Deep Archive 存储类、S3 Intelligent-Tiering 归档访问层和 S3 Intelligent-Tierin |

| 事件类型 | 描述 |
| --- | --- |
| s3:ObjectRestore:Completed<br><br>s3:ObjectRestore:Delete | g 深度归档访问层还原对象时收到事件启动和完成的通知。您还可以接收对象的恢复副本何时过期的通知。<br><br>s3:ObjectRestore:Post 事件类型通知您对象还原启动。s3:ObjectRestore:Completed 事件类型会通知您还原完成。s3:ObjectRestore:Delete 事件类型会在恢复的对象的临时副本过期时通知您。 |
| s3:ReducedRedundancyLostObject | 当 Amazon S3 检测到 RRS 存储类的对象丢失时，您会收到此通知事件。 |
| s3:Replication:*<br><br>s3:Replication:OperationFailedReplication<br><br>s3:Replication:OperationMissedThreshold<br><br>s3:Replication:OperationReplicatedAfterThreshold<br><br>s3:Replication:OperationNotTracked | 通过使用 Replication 事件类型，可以对具有 S3 复制指标或启用 S3 Replication Time Control（S3 RTC）的复制配置接收通知。您可以通过跟踪待处理字节数、待处理的操作和复制延迟来逐分钟监控复制事件的进度。有关复制指标的信息，请参阅 使用指标、事件通知和状态监控复制。<br><br>• 当符合复制条件的对象复制失败时，s3:Replication:OperationFailedReplication 事件类型将通知您。<br>• 当符合复制（使用 S3 RTC）条件的对象超过 15 分钟的复制阈值时，s3:Replication:OperationMissedThreshold 事件类型将通知您。<br>• 当符合复制（使用 S3 RTC）条件的对象在 15 分钟阈值后复制时，s3:Replication:OperationReplicatedAfterThreshold 事件类型将通知您。<br>• 当符合实时复制（同区域复制 [SRR] 或跨区域复制 [CRR]）条件的对象不再受复制指标跟踪时，s3:Replication:OperationNotTracked 事件类型会通知您。 |

| 事件类型 | 描述 |
| --- | --- |
| s3:LifecycleExpiration:*<br><br>s3:LifecycleExpiration:Delete<br><br>s3:LifecycleExpiration:DeleteMarkerCreated | 通过使用 LifecycleExpiration 事件类型，当 Amazon S3 基于 S3 生命周期配置删除对象时，您可以收到通知。<br><br>s3:LifecycleExpiration:Delete 事件类型在删除未转换存储桶中的对象时通知您。当 S3 生命周期配置永久删除对象版本时，它也会通知您。版本控制的存储桶中对象的当前版本删除后，当 S3 生命周期创建删除标记时，s3:LifecycleExpiration:DeleteMarkerCreated 事件类型会通知您。 |
| s3:LifecycleTransition | 当一个对象通过 S3 Lifecycle 配置转移到另一个 Amazon S3 存储类时，您会收到这个通知事件。 |
| s3:IntelligentTiering | 当 S3 Intelligent-Tiering 存储类中的对象迁移到归档访问层或深层归档访问层时，会收到此通知事件。 |
| s3:ObjectTagging:*<br><br>s3:ObjectTagging:Put<br><br>s3:ObjectTagging:Delete | 通过使用 ObjectTagging 事件类型，您可以在从对象中添加或删除对象标签时启用通知。<br><br>s3:ObjectTagging:Put 事件类型会在对象上放置标签或现有标签更新时通知您。当从对象中移除标签时，s3:ObjectTagging:Delete 事件类型会通知您。 |
| s3:ObjectAcl:Put | 当 ACL 放在对象上或更改现有 ACL 时，您会收到此通知事件。当请求导致对象的 ACL 没有更改时，不会生成事件。 |

## Amazon EventBridge 支持的事件类型

有关 Amazon S3 将发送到 Amazon EventBridge 的事件类型的列表，请参阅使用 EventBridge。

## 事件排序和重复事件

Amazon S3 事件通知设计为至少发送一次通知，但不能保证它们以与事件发生相同的顺序到达。在极少数情况下，Amazon S3 的重试机制可能会导致同一对象事件出现重复的 S3 事件通知。有关处理重复或无序事件的更多信息，请参阅 Amazon 存储博客 上的 Manage event ordering and duplicate events with Amazon S3 Event Notifications。

# 使用 Amazon SQS、Amazon SNS 和 Lambda

启用通知是存储桶级操作。您可以在与该存储桶关联的通知子资源中存储通知配置信息。创建或更改存储桶通知配置后，通常必须等待 5 分钟才能使更改生效。首次启用通知时会发生 `s3:TestEvent`。您可以使用以下任意方法来管理通知配置：

- 使用 Amazon S3 控制台 – 控制台 UI 允许您在存储桶上设置通知配置，而无需编写任何代码。有关更多信息，请参阅 使用 Amazon S3 控制台启用和配置事件通知。
- 以编程方式使用 Amazon SDK – 在内部，控制台和 SDK 都调用 Amazon S3 REST API 来管理与存储桶关联的通知子资源。有关使用 Amazon SDK 的通知配置示例，请参阅 演练：为存储桶配置通知（SNS 主题或 SQS 队列）。

> **Note**
>
> 您也可以直接从代码中调用 Amazon S3 REST API。但是，这可能会比较繁琐，因为您必须编写代码对请求进行身份验证。

无论您使用哪种方法，Amazon S3 都将通知配置作为 XML 存储在与存储桶关联的通知子资源中。有关存储桶子资源的信息，请参阅 通用存储桶配置选项。

> **Note**
>
> 如果您由于已删除的目标而收到多个失败事件通知，则在尝试删除这些通知时，您可能会收到无法验证以下目标配置。您可以在 S3 控制台中通过同时删除所有失败的通知来解决此问题。

主题


- 授予将事件通知消息发布到目标的权限
- 使用 Amazon S3 控制台启用和配置事件通知
- 以编程方式配置事件通知
- 演练：为存储桶配置通知（SNS 主题或 SQS 队列）
- 使用对象键名筛选配置事件通知
- 事件消息结构

## 授予将事件通知消息发布到目标的权限

您必须向 Amazon S3 主体授予调用相关 API 的必要权限，以将消息发布到 SNS 主题、SQS 队列或 Lambda 函数。这是为了让 Amazon S3 能够将事件通知消息发布到目标。

要解决向目标发布事件通知消息的问题，请参阅将 Amazon S3 事件通知发布到 Amazon Simple Notification Service 主题的疑难解答。

主题

- 授予调用 Amazon Lambda 函数的权限
- 授予将消息发布到 SNS 主题或 SQS 队列的权限

### 授予调用 Amazon Lambda 函数的权限

Amazon S3 通过调用 Lambda 函数并提供事件消息作为参数来将事件消息发布到 Amazon Lambda。

使用 Amazon S3 控制台在 Amazon S3 存储桶上为 Lambda 函数配置事件通知时，控制台将在 Lambda 函数上设置必要的权限。这是为了让 Amazon S3 有权从存储桶调用函数。有关更多信息，请参阅 使用 Amazon S3 控制台启用和配置事件通知。

您还可以从 Amazon Lambda 向 Amazon S3 授予调用 Lambda 函数的权限。有关更多信息，请参阅 Amazon Lambda 开发人员指南中的教程：将 Amazon Lambda 与 Amazon S3 结合使用。

### 授予将消息发布到 SNS 主题或 SQS 队列的权限

要授予 Amazon S3 权限以将消息发布到 SNS 主题或 SQS 队列，请将 Amazon Identity and Access Management（IAM）策略附加到目标 SNS 主题或 SQS 队列。

有关如何将策略附加到 SNS 主题或 SQS 队列的示例，请参阅 演练：为存储桶配置通知（SNS 主题或 SQS 队列）。有关权限的更多信息，请参阅以下主题：

- Amazon Simple Notification Service 开发人员指南中的 Amazon SNS 访问控制示例案例
- Amazon Simple Queue Service 开发人员指南中的 Amazon SQS 中的 Identity and Access Management

#### 目标 SNS 主题的 IAM 策略

以下是您附加到目标 SNS 主题的 Amazon Identity and Access Management（IAM）策略示例。有关如何使用此策略为事件通知设置目标 Amazon SNS 主题的说明，请参阅 演练：为存储桶配置通知（SNS 主题或 SQS 队列）。

```
{
    "Version": "2012-10-17",
    "Id": "example-ID",
    "Statement": [
        {
            "Sid": "Example SNS topic policy",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "SNS:Publish"
            ],
            "Resource": "SNS-topic-ARN",
            "Condition": {
                "ArnEquals": {
                    "aws:SourceArn": "arn:aws:s3:::amzn-s3-demo-bucket"
                },
                "StringEquals": {
                    "aws:SourceAccount": "bucket-owner-account-id"
                }
            }
        }
    ]
}
```

目标 SQS 队列的 IAM 策略

以下是您附加到目标 SQS 队列的 IAM 策略示例。有关如何使用此策略为事件通知设置目标 Amazon SQS 队列的说明，请参阅 演练：为存储桶配置通知（SNS 主题或 SQS 队列）。

要使用此策略，您必须更新 Amazon SQS 队列 ARN、存储桶名称和存储桶拥有者的 Amazon Web Services 账户 ID。

```
{
    "Version": "2012-10-17",
    "Id": "example-ID",
    "Statement": [
        {
            "Sid": "example-statement-ID",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
```

```
            },
            "Action": [
                "SQS:SendMessage"
            ],
            "Resource": "arn:aws:sqs:Region:account-id:queue-name",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:*:*:awsexamplebucket1"
                },
                "StringEquals": {
                    "aws:SourceAccount": "bucket-owner-account-id"
                }
            }
        }
    ]
}
```

对于 Amazon SNS 和 Amazon SQS IAM 策略，您可以在策略中指定 `StringLike` 条件而不是 `ArnLike` 条件。

使用 `ArnLike` 时，ARN 的分区、服务、账户 ID、资源类型和部分资源 ID 等部分必须与请求上下文中的 ARN 完全匹配。只有区域和资源路径允许部分匹配。

当使用 `StringLike` 而不是 `ArnLike` 时，无论哪个部分使用通配符，匹配都会忽略 ARN 结构并允许部分匹配。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素。

```
"Condition": {
  "StringLike": { "aws:SourceArn": "arn:aws:s3:*:*:amzn-s3-demo-bucket" }
  }
```

Amazon KMS 密钥政策

如果 SQS 队列或 SNS 主题使用 Amazon Key Management Service（Amazon KMS）客户托管密钥进行加密，则必须向 Amazon S3 服务主体授予处理加密主题和/或队列的权限。要向 Amazon S3 服务主体授予权限，请将以下语句添加到客户托管密钥策略中。

```
{
    "Version": "2012-10-17",
    "Id": "example-ID",
    "Statement": [
        {
            "Sid": "example-statement-ID",
```

```
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "*"
        }
    ]
}
```

有关 Amazon KMS 密钥策略的更多信息，请参阅 Amazon Key Management Service 开发人员指南中的使用 Amazon KMS 中的密钥策略。

有关将服务器端加密与适用于 Amazon SQS 和 Amazon SNS 的 Amazon KMS 结合使用的更多信息，请参阅以下内容：

- mazon Simple Notification Service 开发人员指南中的密钥管理。
- Amazon Simple Queue Service 开发人员指南中的密钥管理。
- Amazon 计算博客中的利用 Amazon KMS 加密发布到 Amazon SNS 的消息。

## 使用 Amazon S3 控制台启用和配置事件通知

您可以启用特定的 Amazon S3 通用存储桶事件，以便在每次发生这些事件时向目标发送通知消息。本部分介绍了如何使用 Amazon S3 控制台启用事件通知。有关将事件通知与 Amazon SDK 和 Amazon S3 REST API 结合使用的信息，请参阅 以编程方式配置事件通知。

先决条件：您必须先设置其中一个目标类型并配置权限，然后才能为存储桶启用事件通知。有关更多信息，请参阅受支持的事件目标和授予将事件通知消息发布到目标的权限。

> **Note**
>
> 不支持将 Amazon Simple Queue Service FIFO（先进先出）队列作为 Amazon S3 事件通知目标。要向 Amazon SQS FIFO 队列发送 Amazon S3 事件的通知，您可以使用 Amazon EventBridge。有关更多信息，请参阅 启用 Amazon EventBridge。

主题

- 使用 Amazon S3 控制台启用 Amazon SNS、Amazon SQS 或 Lambda 通知

使用 Amazon S3 控制台启用 Amazon SNS、Amazon SQS 或 Lambda 通知

为 S3 存储桶启用和配置事件通知

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在存储桶列表中，选择要为其启用事件的存储桶的名称。
4. 选择 Properties (属性)。
5. 导航到 Event Notifications (事件通知) 部分，然后选择 Create event notification (创建事件通知)。
6. 在 General configuration (常规配置) 部分中，为事件通知指定描述性事件名称。您还可以选择指定前缀和后缀，以将通知限制为键以指定字符结尾的对象。

   a. 为 Event name (事件名称) 输入描述。

      如果未输入名称，则将生成一个全局唯一标识符 (GUID) 并用作名称。

   b. （可选）要选择按前缀筛选事件通知，请输入 Prefix (前缀)。

      例如，可以设置前缀筛选器，使得仅在文件添加到特定文件夹（例如 `images/`）时，您才会收到通知。

   c. （可选）要选择按后缀筛选事件通知，请输入 Suffix (后缀)。

      有关更多信息，请参阅 使用对象键名筛选配置事件通知。
7. 在 Event types (事件类型) 部分中，选择要接收其通知的一个或多个事件类型。

   有关不同事件类型的列表，请参阅 SQS、SNS 和 Lambda 支持的事件类型。
8. 在 Destination (目标) 部分中，请选择事件通知目标。

> **Note**
>
> 在发布事件通知之前，您必须向 Amazon S3 主体授予调用相关 API 的必要权限。这是为了使它可以将通知发布到 Lambda 函数、SNS 主题或 SQS 队列。

a. 选择目标类型：Lambda Function (Lambda 函数)、SNS Topic (SNS 主题) 或 SQS Queue (SQS 队列)。
b. 请选择目标类型后，从列表中选择函数、主题或队列。
c. 或者，如果您希望指定 Amazon Resource Name (ARN)，请选择输入 ARN 并输入 ARN。

有关更多信息，请参阅 受支持的事件目标。

9. 请选择 Save changes (保存更改)，Amazon S3 会向事件通知目标发送一条测试消息。

## 以编程方式配置事件通知

默认情况下，不为任何类型的事件启用通知。因此，通知子资源最初存储空配置。

```
<NotificationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
</NotificationConfiguration>
```

要为特定类型的事件启用通知，请将 XML 替换为适当的配置，该配置可标识您希望 Amazon S3 发布的事件类型和您希望将事件发布到的目标。对于每个目标，添加相应的 XML 配置。

将事件消息发布到 SQS 队列

要将 SQS 队列设置为一个或多个事件类型的通知目标，请添加 `QueueConfiguration`。

```
<NotificationConfiguration>
  <QueueConfiguration>
    <Id>optional-id-string</Id>
    <Queue>sqs-queue-arn</Queue>
    <Event>event-type</Event>
    <Event>event-type</Event>
     ...
  </QueueConfiguration>
   ...
</NotificationConfiguration>
```

将事件消息发布到 SNS 主题

要将 SNS 主题设置为特定事件类型的通知目标，请添加 `TopicConfiguration`。

```
<NotificationConfiguration>
```

```
  <TopicConfiguration>
     <Id>optional-id-string</Id>
     <Topic>sns-topic-arn</Topic>
     <Event>event-type</Event>
     <Event>event-type</Event>
      ...
  </TopicConfiguration>
   ...
</NotificationConfiguration>
```

调用 Amazon Lambda 函数并提供事件消息作为参数

要将 Lambda 函数设置为特定事件类型的通知目标，请添加CloudFunctionConfiguration。

```
<NotificationConfiguration>
  <CloudFunctionConfiguration>
     <Id>optional-id-string</Id>
     <CloudFunction>cloud-function-arn</CloudFunction>
     <Event>event-type</Event>
     <Event>event-type</Event>
      ...
  </CloudFunctionConfiguration>
   ...
</NotificationConfiguration>
```

删除存储桶上配置的所有通知

要删除存储桶上配置的所有通知，请在通知子资源中保存一个空 <NotificationConfiguration/> 元素。

当 Amazon S3 检测到特定类型的事件时，它会发布包含事件信息的消息。有关更多信息，请参阅 事件消息结构。

有关配置事件通知的详细信息，请参阅以下主题：

- 演练：为存储桶配置通知（SNS 主题或 SQS 队列）.
- 使用对象键名筛选配置事件通知

# 演练：为存储桶配置通知（SNS 主题或 SQS 队列）

您可以使用 Amazon Simple Notification Service (Amazon SNS) 或 Amazon Simple Queue Service (Amazon SQS) 接收 Amazon S3 通知。在此演练中，您将使用 Amazon SNS 主题和 Amazon SQS 队列向存储桶添加通知配置。

> **Note**
>
> 不支持将 Amazon Simple Queue Service FIFO（先进先出）队列作为 Amazon S3 事件通知目标。要向 Amazon SQS FIFO 队列发送 Amazon S3 事件的通知，您可以使用 Amazon EventBridge。有关更多信息，请参阅 启用 Amazon EventBridge。

主题


- 演练摘要
- 第 1 步：创建 Amazon SQS 队列
- 第 2 步：创建 Amazon SNS 主题
- 步骤 3：将通知配置添加到存储桶
- 步骤 4：测试设置


## 演练摘要

此演练可以帮助您执行以下操作：

- 将 `s3:ObjectCreated:*` 类型的事件发布到 Amazon SQS 队列。
- 将 `s3:ReducedRedundancyLostObject` 类型的事件发布到 Amazon SNS 主题。

有关通知配置的信息，请参阅 使用 Amazon SQS、Amazon SNS 和 Lambda。

您可以使用控制台执行这些步骤，无需编写任何代码。此外，还提供了使用适用于 Java 和 .NET 的 Amazon SDK 的代码示例，以帮助您通过编程方式添加通知配置。

该过程包括以下步骤：

1. 创建 Amazon SQS 队列。

   使用 Amazon SQS 控制台创建 SQS 队列。您可以通过编程方式访问 Amazon S3 发送到队列的所有消息。但对于此演练，您在控制台中验证通知消息。

您可将访问策略附加到队列以授予 Amazon S3 发布消息的权限。

2. 创建 Amazon SNS 主题。

   使用 Amazon SNS 控制台创建 SNS 主题并订阅该主题。这样，发布到此项目的所有事件都传送给您。指定电子邮件作为通信协议。创建主题后，Amazon SNS 会发送电子邮件。您可使用电子邮件中的链接确认订阅主题。

   您可将访问策略附加到主题以授予 Amazon S3 发布消息的权限。

3. 将通知配置添加到存储桶。

### 第 1 步：创建 Amazon SQS 队列

按照以下步骤创建并订阅 Amazon Simple Queue Service (Amazon SQS) 队列。

1. 使用 Amazon SQS 控制台创建队列。有关说明，请参阅 Amazon Simple Queue Service 开发人员指南中的 Amazon SQS 入门。
2. 使用以下策略替换附加到队列的访问策略。

   a. 在 Amazon SQS 控制台的 Queues (队列) 列表中，请选择队列名称。

   b. 在 Access policy (访问策略) 选项卡上，请选择 Edit (编辑)。

   c. 替换附加到队列的访问策略。在其中，提供您的 Amazon SQS ARN、源存储桶名称和存储桶拥有者账户 ID。

```
{
    "Version": "2012-10-17",
    "Id": "example-ID",
    "Statement": [
        {
            "Sid": "example-statement-ID",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "SQS:SendMessage"
            ],
            "Resource": "SQS-queue-ARN",
            "Condition": {
                "ArnLike": {
```

```
                    "aws:SourceArn": "arn:aws:s3:*:*:awsexamplebucket1"
                },
                "StringEquals": {
                    "aws:SourceAccount": "bucket-owner-account-id"
                }
            }
        }
    ]
}
```

d. 选择保存。

3. （可选）如果 Amazon SQS 队列或 Amazon SNS 主题已通过 Amazon Key Management Service (Amazon KMS) 启用服务器端加密，可将以下策略添加到关联的对称加密客户托管式密钥。

   必须将此策略添加到客户托管密钥中，因为您无法为 Amazon SQS 或 Amazon SNS 修改 Amazon 托管密钥。

```
{
    "Version": "2012-10-17",
    "Id": "example-ID",
    "Statement": [
        {
            "Sid": "example-statement-ID",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "*"
        }
    ]
}
```

   有关将适用于 Amazon SQS 和 Amazon SNS 的 SSE 与 Amazon KMS 结合使用的更多信息，请参阅以下内容：

   - mazon Simple Notification Service 开发人员指南中的密钥管理。
   - Amazon Simple Queue Service 开发人员指南中的密钥管理。

4. 记录队列 ARN。

   您创建的 SQS 队列是您的 Amazon Web Services 账户 中另一个资源。它有唯一的 Amazon Resource Name (ARN)。在下一步骤中，您需要用到此 ARN。ARN 的格式如下所示：

   ```
   arn:aws:sqs:aws-region:account-id:queue-name
   ```

第 2 步：创建 Amazon SNS 主题

按照以下步骤创建并订阅 Amazon SNS 主题。

1. 使用 Amazon SNS 控制台创建主题。有关说明，请参阅 Amazon Simple Notification Service 开发人员指南中的创建 Amazon SNS 主题。
2. 订阅至主题。对于此练习，请使用电子邮件作为通信协议。有关说明，请参阅 Amazon Simple Notification Service 开发人员指南中的订阅 Amazon SNS 主题。

   您将收到电子邮件要求您确认订阅该主题。确认订阅。
3. 使用以下策略替换附加到主题的访问策略。在其中，提供您的 SNS 主题 ARN、存储桶名称和存储桶拥有者账户 ID。

   ```
   {
       "Version": "2012-10-17",
       "Id": "example-ID",
       "Statement": [
           {
               "Sid": "Example SNS topic policy",
               "Effect": "Allow",
               "Principal": {
                   "Service": "s3.amazonaws.com"
               },
               "Action": [
                   "SNS:Publish"
               ],
               "Resource": "SNS-topic-ARN",
               "Condition": {
                   "ArnLike": {
                       "aws:SourceArn": "arn:aws:s3:*:*:amzn-s3-demo-bucket"
                   },
                   "StringEquals": {
                       "aws:SourceAccount": "bucket-owner-account-id"
   ```

```
                }
            }
        }
    ]
}
```

4. 记录主题 ARN。

   您创建的 SNS 主题是您的 Amazon Web Services 账户中的另一项资源，它有唯一的 ARN。在下一步骤中，您需要用到此 ARN。ARN 格式如下：

   ```
   arn:aws:sns:aws-region:account-id:topic-name
   ```

步骤 3：将通知配置添加到存储桶

您可以使用 Amazon S3 控制台或以编程方式使用 Amazon SDK 启用存储桶通知。请选择任何一个选项以配置存储桶通知。此部分提供使用适用于 Java 和 .NET 的 Amazon SDK 的代码示例。

选项 A：使用控制台在存储桶上启用通知

使用 Amazon S3 控制台，添加请求 Amazon S3 执行以下操作的通知配置：

- 将所有对象创建事件类型的事件发布到 Amazon SQS 队列。
- 将 RRS 中的对象丢失类型的事件发布到 Amazon SNS 主题。

在您保存通知配置后，Amazon S3 会发布测试消息，您将通过电子邮件收到该消息。

有关说明，请参阅 使用 Amazon S3 控制台启用和配置事件通知。

选项 B：使用 Amazon SDK 在存储桶上启用通知

.NET

下面的 C# 代码示例提供一个完整的代码列表，用于为存储桶添加通知配置。您必须更新该代码，提供您的存储桶名称和 SNS 主题 ARN。有关设置和运行代码示例的信息，请参阅《适用于 .NET 的 Amazon SDK 开发人员指南》中的适用于 .NET 的 Amazon SDK 入门。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
```

```
using System.Collections.Generic;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class EnableNotificationsTest
    {
        private const string bucketName = "*** bucket name ***";
        private const string snsTopic = "*** SNS topic ARN ***";
        private const string sqsQueue = "*** SQS topic ARN ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;

        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            EnableNotificationAsync().Wait();
        }

        static async Task EnableNotificationAsync()
        {
            try
            {
               PutBucketNotificationRequest request = new
 PutBucketNotificationRequest
                {
                    BucketName = bucketName
                };

                TopicConfiguration c = new TopicConfiguration
                {
                    Events = new List<EventType> { EventType.ObjectCreatedCopy },
                    Topic = snsTopic
                };
                request.TopicConfigurations = new List<TopicConfiguration>();
                request.TopicConfigurations.Add(c);
                request.QueueConfigurations = new List<QueueConfiguration>();
                request.QueueConfigurations.Add(new QueueConfiguration()
                {
                    Events = new List<EventType> { EventType.ObjectCreatedPut },
                    Queue = sqsQueue
                });
```

```
                PutBucketNotificationResponse response = await
 client.PutBucketNotificationAsync(request);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' ",
 e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown error encountered on server.
 Message:'{0}' ", e.Message);
            }
        }
    }
}
```

Java

以下示例说明如何将通知配置添加到存储桶。有关如何创建和测试有效示例的说明，请参阅《适用于 Java 的 Amazon SDK 开发人员指南》中的入门。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.io.IOException;
import java.util.EnumSet;

public class EnableNotificationOnABucket {

    public static void main(String[] args) throws IOException {
        String bucketName = "*** Bucket name ***";
        Regions clientRegion = Regions.DEFAULT_REGION;
        String snsTopicARN = "*** SNS Topic ARN ***";
        String sqsQueueARN = "*** SQS Queue ARN ***";
```

```
        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();
            BucketNotificationConfiguration notificationConfiguration = new
 BucketNotificationConfiguration();

            // Add an SNS topic notification.
            notificationConfiguration.addConfiguration("snsTopicConfig",
                    new TopicConfiguration(snsTopicARN,
 EnumSet.of(S3Event.ObjectCreated)));

            // Add an SQS queue notification.
            notificationConfiguration.addConfiguration("sqsQueueConfig",
                    new QueueConfiguration(sqsQueueARN,
 EnumSet.of(S3Event.ObjectCreated)));

            // Create the notification configuration request and set the bucket
 notification
            // configuration.
            SetBucketNotificationConfigurationRequest request = new
 SetBucketNotificationConfigurationRequest(
                    bucketName, notificationConfiguration);
            s3Client.setBucketNotificationConfiguration(request);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

### 步骤 4：测试设置

现在，您可以通过将对象上传到存储桶来测试设置，并在 Amazon SQS 控制台中验证事件通知。有关说明，请参阅 Amazon Simple Queue Service 开发人员指南“入门”部分中的接收消息。

# 使用对象键名筛选配置事件通知

配置 Amazon S3 事件通知时，您必须指定哪些受支持的 Amazon S3 事件类型会导致 Amazon S3 发送通知。如果 S3 存储桶中发生了您未指定的事件类型，Amazon S3 不会发送通知。

您可以将通知配置为按对象的键名的前缀和后缀进行筛选。例如，您可以设置一个配置，以便仅在带有 ".jpg" 文件扩展名的图像文件添加到存储桶时收到通知。或者，您也可以设置一个配置，该配置仅在将带有前缀“images/”的对象添加到存储桶时将通知发送到 Amazon SNS 主题，同时将同一存储桶中带有前缀“logs/”的对象的通知发送到 Amazon Lambda 函数。

> **Note**
>
> 通配符（"*"）不能在筛选条件中用作前缀或后缀。如果您的前缀或后缀包含空格，则必须将其替换为“+”字符。如果您在前缀或后缀的值中使用任何其他特殊字符，您必须以 URL 编码（百分比编码）格式输入它们。有关在事件通知的前缀或后缀中使用时必须转换为 URL 编码格式的特殊字符的完整列表，请参阅安全字符。

您可以在 Amazon S3 控制台中设置使用对象密钥名称过滤的通知配置。您可以直接通过 Amazon SDK 或 REST API 使用 Amazon S3 API 来实现该操作。有关使用控制台 UI 在存储桶上设置通知配置的信息，请参阅使用 Amazon S3 控制台启用和配置事件通知。

Amazon S3 在与存储桶关联的通知子资源中以 XML 形式存储通知配置，如 使用 Amazon SQS、Amazon SNS 和 Lambda 中所述。您使用 `Filter` XML 结构定义要按对象键名的前缀和后缀进行筛选的通知的规则。有关 `Filter` XML 结构的信息，请参阅 Amazon Simple Storage Service API 参考中的 PUT Bucket 通知。

使用 `Filter` 的通知配置无法定义采用重叠前缀、重叠后缀或前缀和后缀重叠的筛选规则。以下部分提供了使用对象键名称筛选的有效通知配置的示例。它们还包含由于前缀和后缀重叠而无效的通知配置的示例。

主题

- 采用对象键名筛选的有效通知配置的示例
- 采用无效前缀和后缀重叠的通知配置的示例

### 采用对象键名筛选的有效通知配置的示例

以下通知配置包含用于标识 Amazon S3 的 Amazon SQS 队列以发布 s3:ObjectCreated:Put 类型的事件的队列配置。每当具有前缀 images/ 和后缀 jpg 的对象被放置（PUT）到存储桶时，就会发布这些事件。

```
<NotificationConfiguration>
  <QueueConfiguration>
      <Id>1</Id>
      <Filter>
          <S3Key>
              <FilterRule>
                  <Name>prefix</Name>
                  <Value>images/</Value>
              </FilterRule>
              <FilterRule>
                  <Name>suffix</Name>
                  <Value>jpg</Value>
              </FilterRule>
          </S3Key>
      </Filter>
      <Queue>arn:aws:sqs:us-west-2:444455556666:s3notificationqueue</Queue>
      <Event>s3:ObjectCreated:Put</Event>
  </QueueConfiguration>
</NotificationConfiguration>
```

以下通知配置有多个非重叠前缀。该配置作出以下定义：images/ 文件夹中针对 PUT 请求的通知进入队列 A，logs/ 文件夹中针对 PUT 请求的通知进入队列 B。

```
<NotificationConfiguration>
  <QueueConfiguration>
      <Id>1</Id>
      <Filter>
            <S3Key>
                <FilterRule>
                    <Name>prefix</Name>
                    <Value>images/</Value>
                </FilterRule>
            </S3Key>
      </Filter>
      <Queue>arn:aws:sqs:us-west-2:444455556666:sqs-queue-A</Queue>
      <Event>s3:ObjectCreated:Put</Event>
  </QueueConfiguration>
```

```
  <QueueConfiguration>
     <Id>2</Id>
     <Filter>
            <S3Key>
                <FilterRule>
                    <Name>prefix</Name>
                    <Value>logs/</Value>
                </FilterRule>
            </S3Key>
     </Filter>
     <Queue>arn:aws:sqs:us-west-2:444455556666:sqs-queue-B</Queue>
     <Event>s3:ObjectCreated:Put</Event>
  </QueueConfiguration>
</NotificationConfiguration>
```

以下通知配置有多个非重叠后缀。该配置作出以下定义：所有新添加到存储桶的 .jpg 映像都由 Lambda cloud-function-A 处理，所有新添加的 .png 映像都由云函数 B 处理。.png 和 .jpg 后缀不重叠，即使它们有相同的最后一个字母也是如此。如果某个给定的字符串能够以这两个后缀结尾，则将它们视为重叠。一个字符串无法同时以 .png 和 .jpg 结尾，因此示例配置中的后缀不是重叠后缀。

```
<NotificationConfiguration>
  <CloudFunctionConfiguration>
     <Id>1</Id>
     <Filter>
            <S3Key>
                <FilterRule>
                    <Name>suffix</Name>
                    <Value>.jpg</Value>
                </FilterRule>
            </S3Key>
     </Filter>
     <CloudFunction>arn:aws:lambda:us-west-2:444455556666:cloud-function-A</
CloudFunction>
     <Event>s3:ObjectCreated:Put</Event>
  </CloudFunctionConfiguration>
  <CloudFunctionConfiguration>
     <Id>2</Id>
     <Filter>
            <S3Key>
                <FilterRule>
                    <Name>suffix</Name>
                    <Value>.png</Value>
                </FilterRule>
```

```
            </S3Key>
     </Filter>
     <CloudFunction>arn:aws:lambda:us-west-2:444455556666:cloud-function-B</
CloudFunction>
     <Event>s3:ObjectCreated:Put</Event>
  </CloudFunctionConfiguration>
</NotificationConfiguration>
```

使用 Filter 的通知配置不能使用重叠前缀为相同的事件类型定义筛选规则。只有在与后缀不重叠一起使用的重叠前缀时，他们才能这样做。以下示例配置显示了如何将使用通用前缀和非重叠后缀创建的对象传递到其他目标。

```
<NotificationConfiguration>
  <CloudFunctionConfiguration>
     <Id>1</Id>
     <Filter>
            <S3Key>
                <FilterRule>
                    <Name>prefix</Name>
                    <Value>images</Value>
                </FilterRule>
                <FilterRule>
                    <Name>suffix</Name>
                    <Value>.jpg</Value>
                </FilterRule>
            </S3Key>
     </Filter>
     <CloudFunction>arn:aws:lambda:us-west-2:444455556666:cloud-function-A</
CloudFunction>
     <Event>s3:ObjectCreated:Put</Event>
  </CloudFunctionConfiguration>
  <CloudFunctionConfiguration>
     <Id>2</Id>
     <Filter>
            <S3Key>
                <FilterRule>
                    <Name>prefix</Name>
                    <Value>images</Value>
                </FilterRule>
                <FilterRule>
                    <Name>suffix</Name>
                    <Value>.png</Value>
                </FilterRule>
```

```
            </S3Key>
     </Filter>
     <CloudFunction>arn:aws:lambda:us-west-2:444455556666:cloud-function-B</
CloudFunction>
     <Event>s3:ObjectCreated:Put</Event>
  </CloudFunctionConfiguration>
</NotificationConfiguration>
```

采用无效前缀和后缀重叠的通知配置的示例

大多数情况下，使用 Filter 的通知配置无法使用重叠前缀、重叠后缀或前缀和后缀的重叠组合为相同的事件类型定义筛选规则。只要后缀不重叠，您就可以采用重叠前缀。有关示例，请参阅 使用对象键名筛选配置事件通知。

您可以将重叠对象键名筛选用于不同的事件类型。例如，您可以创建一个通知配置，该配置将前缀 image/ 用于 ObjectCreated:Put 事件类型并将前缀 image/ 用于 ObjectRemoved:* 事件类型。

在使用 Amazon S3 控制台或 API 时，如果您尝试保存具有对相同的活动类型无效的重叠名称筛选的通知配置，则会出现错误。此部分显示了因重叠名称筛选而无效的通知配置的示例。

任何现有通知配置规则都被假定为具有与任何其他前缀和后缀分别匹配的默认前缀和后缀。由于具有重叠前缀，以下通知配置无效。具体来说，根前缀与任何其他前缀重叠。（如果在此示例中使用后缀而不是前缀，则会发生同样的情况。根后缀与任何其他后缀重叠。）

```
<NotificationConfiguration>
     <TopicConfiguration>
         <Topic>arn:aws:sns:us-west-2:444455556666:sns-notification-one</Topic>
         <Event>s3:ObjectCreated:*</Event>
    </TopicConfiguration>
    <TopicConfiguration>
         <Topic>arn:aws:sns:us-west-2:444455556666:sns-notification-two</Topic>
         <Event>s3:ObjectCreated:*</Event>
         <Filter>
             <S3Key>
                 <FilterRule>
                     <Name>prefix</Name>
                     <Value>images</Value>
                 </FilterRule>
            </S3Key>
        </Filter>
    </TopicConfiguration>
```

```
</NotificationConfiguration>
```

由于具有重叠后缀，以下通知配置无效。如果某个给定的字符串能够以这两个后缀结尾，则将它们视为重叠。字符串可以用 jpg 和 pg 结尾。因此，后缀会重叠。（前缀也是如此。如果给定字符串能够以两个前缀开头，则认为这两个前缀是重叠的。

```
 <NotificationConfiguration>
     <TopicConfiguration>
         <Topic>arn:aws:sns:us-west-2:444455556666:sns-topic-one</Topic>
         <Event>s3:ObjectCreated:*</Event>
         <Filter>
             <S3Key>
                 <FilterRule>
                     <Name>suffix</Name>
                     <Value>jpg</Value>
                 </FilterRule>
            </S3Key>
        </Filter>
    </TopicConfiguration>
    <TopicConfiguration>
         <Topic>arn:aws:sns:us-west-2:444455556666:sns-topic-two</Topic>
         <Event>s3:ObjectCreated:Put</Event>
         <Filter>
             <S3Key>
                 <FilterRule>
                     <Name>suffix</Name>
                     <Value>pg</Value>
                 </FilterRule>
            </S3Key>
        </Filter>
    </TopicConfiguration>
</NotificationConfiguration
```

由于具有重叠前缀和后缀，以下通知配置无效。

```
<NotificationConfiguration>
     <TopicConfiguration>
         <Topic>arn:aws:sns:us-west-2:444455556666:sns-topic-one</Topic>
         <Event>s3:ObjectCreated:*</Event>
         <Filter>
             <S3Key>
                 <FilterRule>
```

```
                    <Name>prefix</Name>
                    <Value>images</Value>
                </FilterRule>
                <FilterRule>
                    <Name>suffix</Name>
                    <Value>jpg</Value>
                </FilterRule>
            </S3Key>
        </Filter>
    </TopicConfiguration>
    <TopicConfiguration>
         <Topic>arn:aws:sns:us-west-2:444455556666:sns-topic-two</Topic>
         <Event>s3:ObjectCreated:Put</Event>
         <Filter>
             <S3Key>
                 <FilterRule>
                     <Name>suffix</Name>
                     <Value>jpg</Value>
                 </FilterRule>
             </S3Key>
         </Filter>
    </TopicConfiguration>
</NotificationConfiguration>
```

## 事件消息结构

Amazon S3 为发布事件而发送的通知消息采用 JSON 格式。

有关配置事件通知的一般概述和说明，请参阅 Amazon S3 事件通知。

此示例说明了事件通知 JSON 结构的版本 2.2。Amazon S3 使用了这个事件结构的版本 2.1、2.2 和 2.3。Amazon S3 使用版本 2.2 进行跨区域复制事件通知。它将 2.3 版本用于 S3 生命周期、S3 Intelligent-Tiering、对象 ACL、对象标记和对象恢复删除事件。这些版本包含特定于这些操作的额外信息。版本 2.2 和版本 2.3 与版本 2.1 兼容，Amazon S3 当前将该版本用于所有其他事件类型。

```
{
   "Records":[
      {
         "eventVersion":"2.2",
         "eventSource":"aws:s3",
         "awsRegion":"us-west-2",
         "eventTime":"The time, in ISO-8601 format, for example,
 1970-01-01T00:00:00.000Z, when Amazon S3 finished processing the request",
```

```
         "eventName":"event-type",
         "userIdentity":{
            "principalId":"Amazon-customer-ID-of-the-user-who-caused-the-event"
         },
         "requestParameters":{
            "sourceIPAddress":"ip-address-where-request-came-from"
         },
         "responseElements":{
            "x-amz-request-id":"Amazon S3 generated request ID",
            "x-amz-id-2":"Amazon S3 host that processed the request"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"ID found in the bucket notification configuration",
            "bucket":{
               "name":"amzn-s3-demo-bucket",
               "ownerIdentity":{
                  "principalId":"Amazon-customer-ID-of-the-bucket-owner"
               },
               "arn":"bucket-ARN"
            },
            "object":{
               "key":"object-key",
               "size":"object-size in bytes",
               "eTag":"object eTag",
               "versionId":"object version if bucket is versioning-enabled, otherwise
 null",
               "sequencer": "a string representation of a hexadecimal value used to
 determine event sequence, only used with PUTs and DELETEs"
            }
         },
         "glacierEventData": {
            "restoreEventData": {
               "lifecycleRestorationExpiryTime": "The time, in ISO-8601 format, for
 example, 1970-01-01T00:00:00.000Z, of Restore Expiry",
               "lifecycleRestoreStorageClass": "Source storage class for restore"
            }
         }
      }
   ]
}
```

注意，以下是关于事件消息结构：

- `eventVersion` 键值包含 `<major>.<minor>` 格式的主要版本和次要版本。

  如果 Amazon S3 对不向后兼容的事件结构进行更改，则主要版本将递增。这包括删除已存在的 JSON 字段或更改字段内容的表示方式（例如，日期格式）。

  如果 Amazon S3 向事件结构添加新字段，则次要版本将递增。如果为某些或所有现有事件提供了新信息，则可能会发生这种情况 如果仅提供有关新引入的事件类型的新信息，则可能会发生这种情况。应用程序应忽略新字段，以保持与事件结构的新次要版本的前向兼容。

  如果引入了新的事件类型但事件的结构未经修改，则事件版本不会更改。

  为确保您的应用程序可以正确解析事件结构，我们建议您对主要版本号进行相等比较。为了确保您的应用程序所期望的字段存在，我们还建议对次要版本进行大于或等于比较。
- `eventName` 引用事件通知类型列表，但不包含 `s3:` 前缀。
- 如果您希望通过联系 Amazon Web Services 支持 来跟踪请求，则 `responseElements` 键值很有用。`x-amz-request-id` 和 `x-amz-id-2` 都可帮助 Amazon S3 跟踪单个请求。这些值与 Amazon S3 为响应您启动事件的请求而返回的值相同。这是因为它们可以用于将事件与请求匹配。
- `s3` 键提供事件中涉及的存储桶和对象的相关信息。对象键名称值进行了 URL 编码。例如，“red flower.jpg”变成了“red+flower.jpg”（Amazon S3 返回“`application/x-www-form-urlencoded`”作为响应中的内容类型）。
- `sequencer` 键提供了确定事件顺序的方法。无法保证事件通知按事件发生的顺序到达。然而，来自创建对象 (PUTs) 和删除对象事件的通知将包含 `sequencer`。它可用于确定给定对象密钥的事件的顺序。

  如果将来自同一对象键上的两个事件通知的 `sequencer` 字符串进行比较，就会发现 `sequencer` 十六进制值较大的事件通知是后发生的事件。如果您正在使用事件通知来维护 Amazon S3 对象的单独数据库或索引，我们建议您在处理每个事件通知时比较和存储 `sequencer` 值。

  请注意以下几点：

  - 您不能使用 `sequencer` 确定不同对象键上的事件的顺序。
  - 排序器可以有不同的长度。因此，要比较这些值，您必须先使用零填补较短的值的右侧，然后进行字母表顺序比较。
- `glacierEventData` 键只对 `s3:ObjectRestore:Completed` 事件可见。
- `restoreEventData` 键包含与您的还原请求相关的属性。
- `replicationEventData` 键只对复制事件可见。
- `intelligentTieringEventData` 密钥只对 S3 Intelligent-Tiering 可见。

- `lifecycleEventData` 密钥只对 S3 生命周期转换事件可见。

### 示例消息

以下是 Amazon S3 事件通知消息的示例。

#### Amazon S3 测试消息

当您在存储桶上配置事件通知时，Amazon S3 会发送以下测试消息。

```
{
   "Service":"Amazon S3",
   "Event":"s3:TestEvent",
   "Time":"2014-10-13T15:57:02.089Z",
   "Bucket":"amzn-s3-demo-bucket",
   "RequestId":"5582815E1AEA5ADF",
   "HostId":"8cLeGAmw098X5cv4Zkwcmo8vvZa3eH3eKxsPzbB9wrR+YstdA6Knx4Ip8EXAMPLE"
}
```

#### 使用 PUT 请求创建对象时的示例消息

以下消息是 Amazon S3 发送以发布 `s3:ObjectCreated:Put` 事件的消息示例。

```
{
   "Records":[
      {
         "eventVersion":"2.1",
         "eventSource":"aws:s3",
         "awsRegion":"us-west-2",
         "eventTime":"1970-01-01T00:00:00.000Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"AIDAJDPLRKLG7UEXAMPLE"
         },
         "requestParameters":{
            "sourceIPAddress":"127.0.0.1"
         },
         "responseElements":{
            "x-amz-request-id":"C3D13FE58DE4C810",
            "x-amz-id-2":"FMyUVURIY8/IgAtTv8xRjskZQpcIZ9KG4V5Wp6S7S/
JRWeUWerMUE5JgHvANOjpD"
         },
```

```
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"testConfigRule",
            "bucket":{
               "name":"amzn-s3-demo-bucket",
               "ownerIdentity":{
                  "principalId":"A3NL1KOZZKExample"
               },
               "arn":"arn:aws:s3:::amzn-s3-demo-bucket"
            },
            "object":{
               "key":"HappyFace.jpg",
               "size":1024,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "versionId":"096fKKXTRTtl3on89fVO.nfljtsv6qko",
               "sequencer":"0055AED6DCD90281E5"
            }
         }
      }
   ]
}
```

有关每个 IAM 标识前缀（如 AIDA、AROA、AGPA 等）的定义，请参阅 IAM 用户指南中的 IAM 标识符。

## 使用 EventBridge

无论何时在存储桶中发生某些事件，Amazon S3 都可以将事件发送到 Amazon EventBridge。与其他目的地不同，您无需选择要提供的活动类型。启用 EventBridge 后，以下所有事件都将发送到 EventBridge。您可以使用 EventBridge 规则将事件路由到其他目标。以下列出了 Amazon S3 发送给 EventBridge 的事件。

| 事件类型 | 说明 |
| --- | --- |
| Object Created（已创建对象） | 创建了一个对象。<br><br>事件消息结构中的原因字段表示使用哪个 S3 API 创建对象：PutObject、POST 对象、CopyObject 还是 CompleteMultipartUpload。 |
| 已删除对象 (DeleteObject) | 已删除对象。 |

| 事件类型 | 说明 |
| --- | --- |
| 已删除对象（生命周期过期） | 使用 S3 API 调用 DeleteObject 时，原因字段将设置为 deleteObject。当 S3 生命周期过期规则删除对象时，原因字段将设置为生命周期过期。有关更多信息，请参阅 即将过期的对象。<br><br>当删除未受版本控制的对象或永久删除受版本控制的对象时，删除类型字段将设置为永久删除。为受版本控制的对象创建删除标记时，删除类型字段将设置为删除标记已创建。有关更多信息，请参阅 从启用了版本控制的存储桶中删除对象版本。 |
| Object Restore Initiated（已启动对象还原） | 从 S3 Glacier 或 S3 Glacier Deep Archive 存储类或 S3 Intelligent-Tiering 归档访问层或深度归档访问层启动对象还原。有关更多信息，请参阅 使用归档的对象。 |
| Object Restore Completed（已完成对象还原） | 对象还原已完成。 |
| Object Restore Expired（对象还原已过期） | 从 S3 Glacier 或 S3 Glacier Deep Archive 还原的对象的临时副本过去并被删除。 |
| Object Storage Class Changed（对象存储类已更改） | 对象已过渡到不同的存储类。有关更多信息，请参阅 使用 Amazon S3 生命周期转换对象。 |
| Object Access Tier Changed（对象访问层已更改） | 对象已转换为 S3 Intelligent-Tiering 归档访问层或深度归档访问层。有关更多信息，请参阅 使用 Amazon S3 Intelligent-Tiering 管理存储成本。 |
| Object ACL Updated（已更新对象 ACL） | 对象的访问控制列表 (ACL) 是使用 putObjecTACL 设置的。当请求导致对象的 ACL 没有更改时，不会生成事件。有关更多信息，请参阅 访问控制列表 (ACL) 概述。 |
| Object Tags Added（已添加对象标签） | 使用 PutObjectTagging 向对象添加了一组标签。有关更多信息，请参阅 使用标签对存储进行分类。 |
| Object Tags Deleted（已删除对象标签） | 使用 DeleteObjectTagging 从对象中移除了所有标签。有关更多信息，请参阅 使用标签对存储进行分类。 |

> **Note**
>
> 有关 Amazon S3 事件类型如何映射到 EventBridge 事件类型的更多信息，请参阅 Amazon EventBridge 映射和故障排除。

您可以将 Amazon S3 事件通知与 EventBridge 结合使用，编写规则，以便在存储桶中发生事件时采取行动。例如，可获得向您发送的电子邮件通知。有关更多信息，请参阅 Amazon EventBridge 用户指南中的什么是 EventBridge。

有关可以使用 EventBridge API 进行交互的操作和数据类型的更多信息，请参阅《Amazon EventBridge API 参考》中的 Amazon EventBridge API Reference。

有关定价的更多信息，请参阅 Amazon EventBridge pricing（Amazon EventBridge 定价）。

主题


- Amazon EventBridge 权限
- 启用 Amazon EventBridge
- EventBridge 事件消息结构
- Amazon EventBridge 映射和故障排除


## Amazon EventBridge 权限

Amazon S3 不需要任何其他权限即可向 Amazon EventBridge 传输事件。

## 启用 Amazon EventBridge

您可以通过 S3 控制台、Amazon Command Line Interface (Amazon CLI) 或 Amazon S3 REST API 启用 Amazon EventBridge。

> **Note**
>
> 在启用 EventBridge 后，所做的更改需要大约五分钟才能生效。

使用 S3 控制台

在 S3 控制台中启用 EventBridge 事件传输。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在存储桶列表中，选择要为其启用事件的存储桶的名称。
4. 选择属性。
5. 导航到 Event Notifications（事件通知）章节，然后找到 Amazon EventBridge 小节。请选择编辑。
6. 在 Send notifications to Amazon EventBridge for all events in this bucket（为此存储桶中的所有事件向 Amazon EventBridge 发送通知）下方，请选择 On（打开）。

使用 Amazon CLI

以下示例为启用了 Amazon EventBridge 的存储桶 `amzn-s3-demo-bucket1` 创建了一个存储桶通知配置。

```
aws s3api put-bucket-notification-configuration --bucket amzn-s3-demo-bucket1 --
notification-configuration='{ "EventBridgeConfiguration": {} }'
```

使用 REST API

您可以通过调用 Amazon S3 REST API 以编程方式在存储桶上启用 Amazon EventBridge。有关更多信息，请参阅 Amazon Simple Storage Service API Reference 中的 PutBucketNotificationConfiguration。

下面的例子展示了在启用 Amazon EventBridge 的情况下，用来创建存储桶通知配置的 XML。

```
<NotificationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <EventBridgeConfiguration>
  </EventBridgeConfiguration>
</NotificationConfiguration>
```

创建 EventBridge 规则

启用后，您可以为某些任务创建 Amazon EventBridge 规则。例如，您可以在创建对象时发送电子邮件通知。有关完整的教程，请参阅 Amazon EventBridge User Guide（Amazon EventBridge 用户指南）

中的 Tutorial: Send a notification when an Amazon S3 object is created（教程：创建 Amazon S3 对象时发送通知）。

## EventBridge 事件消息结构

Amazon S3 为发布事件而发送的通知消息采用 JSON 格式。当 Amazon S3 将事件发送到 Amazon EventBridge 时，会显示以下字段。

- version（版本）— 目前所有活动均为 0（零）。
- id：为每个事件生成的 UUID。
- detail-type— 正在发送的事件类型。有关事件类型的列表，请参阅 使用 EventBridge。
- source（源）— 识别生成事件的服务。
- account（账户）- 存储桶拥有者的 12 位 Amazon Web Services 账户 ID。
- time（时间）- 事件发生的时间。
- region（区域）—识别存储桶的 Amazon Web Services 区域。
- resource（资源）- 包含存储桶的 Amazon 资源名称（ARN）的 JSON 数组。
- detail（详细信息）—包含关于事件信息的 JSON 对象。有关此字段中可包含的内容的更多信息，请参阅事件消息详细信息。

### 事件消息结构示例

以下是一些可以发送到 Amazon EventBridge 的 Amazon S3 事件通知消息的示例。

#### 已创建对象

```
{
  "version": "0",
  "id": "17793124-05d4-b198-2fde-7ededc63b103",
  "detail-type": "Object Created",
  "source": "aws.s3",
  "account": "111122223333",
  "time": "2021-11-12T00:00:00Z",
  "region": "ca-central-1",
  "resources": [
    "arn:aws:s3:::amzn-s3-demo-bucket1"
  ],
  "detail": {
    "version": "0",
    "bucket": {
```

```
      "name": "amzn-s3-demo-bucket1"
    },
    "object": {
      "key": "example-key",
      "size": 5,
      "etag": "b1946ac92492d2347c6235b4d2611184",
      "version-id": "IYV3p45BT0ac8hjHg1houSdS1a.Mro8e",
      "sequencer": "617f08299329d189"
    },
    "request-id": "N4N7GDK58NMKJ12R",
    "requester": "123456789012",
    "source-ip-address": "1.2.3.4",
    "reason": "PutObject"
  }
}
```

### 已删除对象（使用 DeleteObject）

```
{
  "version": "0",
  "id": "2ee9cc15-d022-99ea-1fb8-1b1bac4850f9",
  "detail-type": "Object Deleted",
  "source": "aws.s3",
  "account": "111122223333",
  "time": "2021-11-12T00:00:00Z",
  "region": "ca-central-1",
  "resources": [
    "arn:aws:s3:::amzn-s3-demo-bucket1"
  ],
  "detail": {
    "version": "0",
    "bucket": {
      "name": "amzn-s3-demo-bucket1"
    },
    "object": {
      "key": "example-key",
      "etag": "d41d8cd98f00b204e9800998ecf8427e",
      "version-id": "1QW9g1Z99LUNbvaaYVpW9xDlOLU.qxgF",
      "sequencer": "617f0837b476e463"
    },
    "request-id": "0BH729840619AG5K",
    "requester": "123456789012",
```

```
    "source-ip-address": "1.2.3.4",
    "reason": "DeleteObject",
    "deletion-type": "Delete Marker Created"
  }
}
```

### 已删除对象（使用生命周期过期）

```
{
  "version": "0",
  "id": "ad1de317-e409-eba2-9552-30113f8d88e3",
  "detail-type": "Object Deleted",
  "source": "aws.s3",
  "account": "111122223333",
  "time": "2021-11-12T00:00:00Z",
  "region": "ca-central-1",
  "resources": [
    "arn:aws:s3:::amzn-s3-demo-bucket1"
  ],
  "detail": {
    "version": "0",
    "bucket": {
      "name": "amzn-s3-demo-bucket1"
    },
    "object": {
      "key": "example-key",
      "etag": "d41d8cd98f00b204e9800998ecf8427e",
      "version-id": "mtB0cV.jejK63XkRNceanNMC.qXPWLeK",
      "sequencer": "617b398000000000"
    },
    "request-id": "20EB74C14654DC47",
    "requester": "s3.amazonaws.com",
    "reason": "Lifecycle Expiration",
    "deletion-type": "Delete Marker Created"
  }
}
```

### 已完成对象还原

```
{
  "version": "0",
```

```
  "id": "6924de0d-13e2-6bbf-c0c1-b903b753565e",
  "detail-type": "Object Restore Completed",
  "source": "aws.s3",
  "account": "111122223333",
  "time": "2021-11-12T00:00:00Z",
  "region": "ca-central-1",
  "resources": [
    "arn:aws:s3:::amzn-s3-demo-bucket1"
  ],
  "detail": {
    "version": "0",
    "bucket": {
      "name": "amzn-s3-demo-bucket1"
    },
    "object": {
      "key": "example-key",
      "size": 5,
      "etag": "b1946ac92492d2347c6235b4d2611184",
      "version-id": "KKsjUC1.6gIjqtvhfg5AdMI0eCePIiT3"
    },
    "request-id": "189F19CB7FB1B6A4",
    "requester": "s3.amazonaws.com",
    "restore-expiry-time": "2021-11-13T00:00:00Z",
    "source-storage-class": "GLACIER"
  }
}
```

事件消息详细信息

详细信息字段包含一个 JSON 对象，其中包含事件相关信息。详细信息字段中可能存在以下字段。

- version（版本）— 目前所有活动均为 0（零）。
- bucket（存储桶）— 有关事件中涉及的 Amazon S3 存储桶的相关信息。
- object（对象）— 有关事件中涉及的 Amazon S3 对象的相关信息。
- request-id — S3 响应中的请求 ID。
- requester（请求者）—请求者的 Amazon Web Services 账户 ID 或 Amazon 服务主体。
- source-ip-address — S3 请求的源 IP 地址。仅用于 S3 请求触发的事件。
- 原因 — 对于 Object Created（已创建对象）事件，S3 API 用来创建对象：PutObject、POST 对象、CopyObject 或 CompleteMultipartUpload。对于 Object Deleted（已删除对象），当对象由 S3

API 调用删除时，这将设为 DeleteObject，或者当对象由 S3 生命周期过期规则删除时，这将设为 Lifecycle Expiration。有关更多信息，请参阅 即将过期的对象。

- deletion-type — 对于 Object Deleted（已删除对象），当删除未受版本控制的对象或永久删除受版本控制的对象时，删除类型字段将设置为永久删除。为受版本控制的对象创建删除标记时，此将设为 Delete Marker Created（已创建删除标记）。有关更多信息，请参阅 从启用了版本控制的存储桶中删除对象版本。

  > **Note**
  >
  > 某些对象属性（例如 `etag` 和 `size`）仅在创建删除标记时才会出现。

- restore-expiry-time — 对于 Object Restore Completed（已完成对象还原）事件，该对象的临时副本将从 S3 中删除的时间。有关更多信息，请参阅 使用归档的对象。
- source-storage-class — 对于 Object Restore Initiated（已启动对象还原）和 Object Restore Completed（已完成对象还原）事件，即正在恢复的对象的存储类。有关更多信息，请参阅 使用归档的对象。
- destination-storage-class — 对于 Object Storage Class Changed（已更改对象存储类）事件，对象的新存储类。有关更多信息，请参阅 使用 Amazon S3 生命周期转换对象。
- destination-access-tier — 对于 Object Access Tier Changed（已更改对象访问层）事件，对象的新访问层。有关更多信息，请参阅 使用 Amazon S3 Intelligent-Tiering 管理存储成本。

## Amazon EventBridge 映射和故障排除

下表介绍了 Amazon S3 事件类型如何映射到 Amazon EventBridge 事件类型。

| S3 事件类型 | Amazon EventBridge 详细信息类型 |
| --- | --- |
| ObjectCreated:Put<br>ObjectCreated:Post<br>ObjectCreated:Copy<br>ObjectCreated:CompleteMultipartUpload | 已创建对象 |
| ObjectRemoved：删除 | 已删除对象 |

| S3 事件类型 | Amazon EventBridge 详细信息类型 |
| --- | --- |
| ObjectRemoved:DeleteMarkerCreated<br><br>LifecycleExpiration：删除<br><br>LifecycleExpiration:DeleteMarkerCreated | |
| ObjectRestore:Post | 已启动对象还原 |
| ObjectRestore:Completed | 已完成对象还原 |
| ObjectRestore：删除 | 对象还原已过期 |
| LifecycleTransition | 已更改对象存储类 |
| IntelligentTiering | 已更改对象访问层 |
| ObjectTagging:Put | 已添加对象标签 |
| ObjectTagging:Delete | 已删除对象标签 |
| ObjectAcl:Put | 已更新对象 ACL |

Amazon EventBridge 故障排除

有关 EventBridge 故障排除的信息，请参阅 Amazon EventBridge User Guide（Amazon EventBridge 用户指南）中的 Troubleshooting Amazon EventBridge（对 Amazon EventBridge 进行故障排除）。

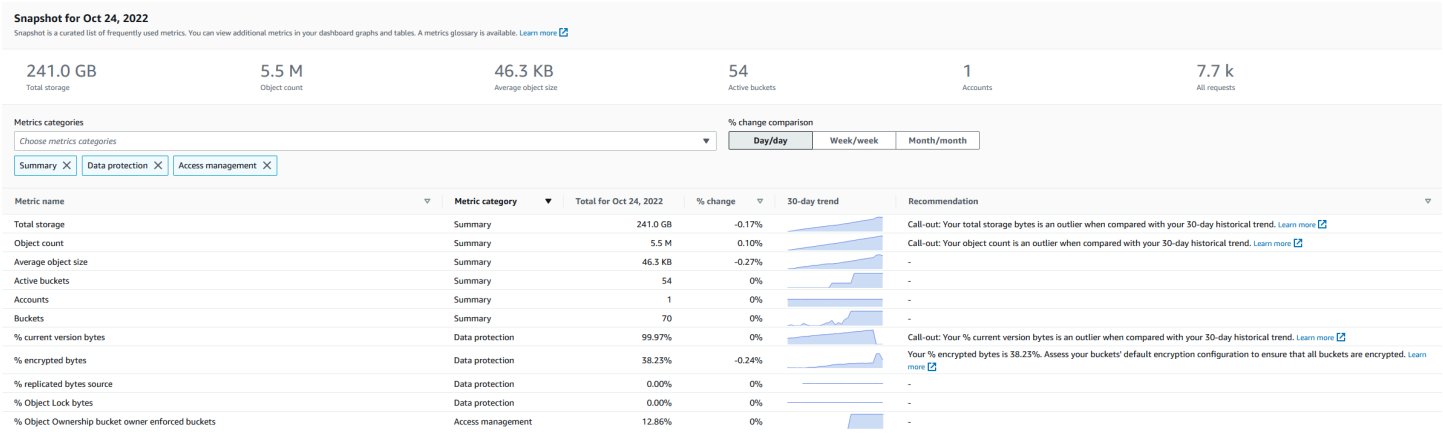
# 使用 Amazon S3 Storage Lens 存储统计管理工具评估您的存储活动和使用情况

Amazon S3 Storage Lens 存储统计管理工具是一项云存储分析功能，您可以使用它在整个组织范围内了解对象存储和活动。S3 Storage Lens 存储统计管理工具还分析指标以提供上下文建议，您可以使用这些建议来优化存储成本并应用最佳实践来保护数据。

您可以使用 S3 Storage Lens 存储统计管理工具指标生成汇总见解。例如，您可以了解整个组织中有多少存储空间，或增长最快的桶和前缀是哪些。您还可以使用 S3 Storage Lens 存储统计管理工具指标来

识别成本优化机会，实施数据保护和访问管理最佳实践，并提高应用程序工作负载的性能。例如，您可以识别尚未设置 S3 生命周期规则的存储桶，而这些生命周期规则使超过 7 天的未完成分段上传过期。您还可以识别未遵循数据保护最佳实践（例如使用 S3 复制或 S3 版本控制）的存储桶。

S3 Storage Lens 存储统计管理工具聚合您的指标，并在 Amazon S3 控制台的 Buckets（桶）页上的 Account snapshot（账户快照）部分中显示此信息。S3 Storage Lens 存储统计管理工具还提供了一个交互式控制面板，您可以使用它来可视化见解和趋势，标记异常值，并接收有关优化存储成本和应用数据保护最佳实践的建议。控制面板提供深入分析选项，用于在组织、账户、Amazon Web Services 区域、存储类、存储桶、前缀或 Storage Lens 组级别生成和可视化见解。您还可以将采用 CSV 或 Parquet 格式的每日指标导出发送到 S3 存储桶。




## S3 Storage Lens 存储统计管理工具指标和功能

S3 Storage Lens 存储统计管理工具提供每日更新的交互式原定设置控制面板。S3 Storage Lens 存储统计管理工具预配置此控制面板，以直观显示整个账户的见解和趋势，并在 S3 控制台中每天更新这些信息。此控制面板中的指标也会在 Buckets（桶）页面上的账户快照进行汇总。有关更多信息，请参阅默认控制面板。

要创建其他控制面板并按 Amazon Web Services 区域、S3 桶或账户（对于 Amazon Organizations）限定其范围，您可以创建 S3 Storage Lens 存储统计管理工具控制面板配置。您可以使用 Amazon S3 控制台、Amazon Command Line Interface (Amazon CLI)、Amazon SDK 或 Amazon S3 REST API 创建和管理 S3 Storage Lens 存储统计管理工具控制面板配置。创建或编辑 S3 Storage Lens 存储统计管理工具控制面板时，定义控制面板范围和指标选择。

S3 Storage Lens 存储统计管理工具提供免费指标、高级指标和建议，您可以支付额外费用升级到高级指标和建议。借助高级指标和建议，您可以访问其他指标和功能，以深入了解您的存储。这些功能包括高级指标类别、前缀聚合、上下文建议和 Amazon CloudWatch 发布。前缀聚合和上下文建议仅在 Amazon S3 控制台中提供。有关 S3 Storage Lens 存储统计管理工具定价的信息，请参阅 Amazon S3 定价。

指标类别

在免费和高级套餐中，指标划分为与关键使用案例一致的类别，例如成本优化和数据保护。免费指标包括摘要、成本优化、数据保护、访问管理、性能和事件指标。升级到高级指标和建议时，可以启用高级成本优化和数据保护指标。您可以使用这些高级指标进一步降低您的 S3 存储成本并改善您的数据保护态势。您还可以启用活动指标和详细的状态代码指标，以提高访问您的 S3 桶的应用程序工作负载的性能。有关免费和高级指标类别的更多信息，请参阅指标选择。

您可以根据 S3 最佳实践来评估存储，例如分析启用了加密或 S3 对象锁定或 S3 版本控制的桶的百分比。您还可以确定潜在的成本节约机会。例如，您可以使用 S3 生命周期规则计数指标来识别缺少生命周期过期或转换规则的桶。此外，您还可以分析每个桶的请求活动，以查找可以将对象转换为较低成本存储类的桶。有关更多信息，请参阅 Amazon S3 Storage Lens 存储统计管理工具使用案例。

指标导出

除了查看 S3 控制台中的控制面板之外，您还可以将指标以 CSV 或 Parquet 格式导出至 S3 桶中，以使用您选择的分析工具进行进一步分析。有关更多信息，请参阅 使用数据导出查看 Amazon S3 Storage Lens 存储统计管理工具指标。

Amazon CloudWatch 发布

您可以将 S3 Storage Lens 存储统计管理工具使用情况和活动指标发布到 Amazon CloudWatch，以便在 CloudWatch dashboards（控制面板）中创建运营状况的统一视图。您还可以使用 CloudWatch 功能（如告警和触发操作、指标数学和异常检测）来监控 S3 Storage Lens 存储统计管理工具指标并采取措施。此外，CloudWatch API 操作使应用程序（包括第三方提供商）能够访问 S3 Storage Lens 存储统计管理工具指标。CloudWatch 发布选项可用于升级到 S3 Storage Lens 存储统计管理工具高级指标和建议。有关在 CloudWatch 中 S3 Storage Lens 存储统计管理工具支持的更多信息，请参阅 在 CloudWatch 中监控 S3 Storage Lens 存储统计管理工具指标。

有关使用 S3 Storage Lens 存储统计管理工具的更多信息，请参阅以下主题。

主题

- 了解 Amazon S3 Storage Lens 存储统计管理工具
- Amazon S3 Storage Lens 存储统计管理工具指标词汇表
- 设置 Amazon S3 Storage Lens 存储统计管理工具权限
- 通过控制台和 API 使用 Amazon S3 Storage Lens 存储统计管理工具
- 使用 Amazon S3 Storage Lens 存储统计管理工具查看指标
- 将 Amazon S3 Storage Lens 存储统计管理工具与 Amazon Organizations 结合使用
- 使用 S3 Storage Lens 组筛选和汇总指标

# 了解 Amazon S3 Storage Lens 存储统计管理工具

> **Important**
>
> Amazon S3 现在将具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）作为 Amazon S3 中每个存储桶的基本加密级别。从 2023 年 1 月 5 日起，上传到 Amazon S3 的所有新对象都将自动加密，不会产生额外费用，也不会影响性能。S3 存储桶默认加密配置和上传的新对象的自动加密状态可在 Amazon CloudTrail 日志、S3 清单、S3 Storage Lens 存储统计管理工具、Amazon S3 控制台中获得，并可用作 Amazon Command Line Interface 和 Amazon SDK 中的附加 Amazon S3 API 响应标头。有关更多信息，请参阅默认加密常见问题解答。

Amazon S3 Storage Lens 存储统计管理工具是一项云存储分析功能，您可以使用它在整个组织范围内了解对象存储的使用情况和活动。您可以使用 S3 Storage Lens 存储统计管理工具指标生成摘要见解，例如，了解整个组织中有多少存储空间，或增长最快的桶和前缀是哪些。您还可以使用 S3 Storage Lens 存储统计管理工具指标来识别成本优化机会，实施数据保护和安全最佳实践，并提高应用程序工作负载的性能。例如，您可以识别没有 S3 生命周期规则的桶，使超过 7 天的未完成分段上传过期。您还可以识别未遵循数据保护最佳实践（例如使用 S3 复制或 S3 版本控制）的桶。S3 Storage Lens 存储统计管理工具还分析指标以提供上下文建议，您可以使用这些建议来优化存储成本并应用最佳实践来保护数据。

S3 Storage Lens 存储统计管理工具聚合您的指标，并在 Amazon S3 控制台的 Buckets（桶）页上的 Account snapshot（账户快照）部分中显示此信息。S3 Storage Lens 存储统计管理工具还提供了一个交互式控制面板，您可以使用它来可视化见解和趋势，标记异常值，并接收有关优化存储成本和应用数据保护最佳实践的建议。控制面板提供深入分析选项，用于在组织、账户、Amazon Web Services 区域、存储类、存储桶、前缀或 Storage Lens 组级别生成和可视化见解。您还可以将采用 CSV 或 Parquet 格式的每日指标导出发送到 S3 存储桶。您可以使用 Amazon S3 控制台、Amazon Command Line Interface (Amazon CLI)、Amazon SDK 或 Amazon S3 REST API 创建和管理 S3 Storage Lens 存储统计管理工具控制面板。

## S3 Storage Lens 存储统计管理工具的概念和术语

本部分包含成功了解和使用 Amazon S3 Storage Lens 存储统计管理工具所必需的术语和概念。

主题


- 控制面板配置
- 默认控制面板

- 控制面板
- 账户快照
- 指标导出
- 主区域
- 保留期
- 指标类别
- 建议
- 指标选择
- S3 Storage Lens 存储统计管理工具和 Amazon Organizations

### 控制面板配置

S3 Storage Lens 存储统计管理工具需要控制面板配置，其中包含代表您聚合指标所需的属性，以供单个控制面板或导出使用。创建配置时，您可以选择控制面板名称和主区域，创建控制面板后无法对其进行更改。您可以选择添加标签并配置以 CSV 或 Parquet 格式导出指标。

在控制面板配置中，您还可以定义控制面板范围和指标选择。范围可以包括您的组织账户或按区域、桶和账户筛选的分区的所有存储。配置指标选择时，您可以在免费指标与高级指标和建议之间进行选择，您可以额外付费升级到高级指标和建议。借助高级指标和建议，您可以访问其他指标和功能。这些功能包括高级指标类别、前缀级聚合、上下文建议和 Amazon CloudWatch 发布。有关 S3 Storage Lens 存储统计管理工具定价的信息，请参阅 Amazon S3 定价。

### 默认控制面板

控制台上的 S3 Storage Lens 存储统计管理工具默认控制面板命名为 default-account-dashboard。S3 预配置此控制面板，以直观显示整个账户的见解和趋势，并在 S3 控制台中每天更新这些信息。您无法修改原定设置控制面板的配置范围，但可以将指标选择从免费指标升级到高级指标和建议。您可以配置可选指标导出，甚至可以禁用控制面板。但是，您无法删除默认控制面板。

> **Note**
>
> 如果您禁用原定设置控制面板，则它将不再更新。您将不会再在 S3 Storage Lens 存储统计管理工具控制面板、指标导出或 S3 桶页面上的账户快照中收到任何新的每日指标。如果控制面板使用高级指标和建议，则不再向您收费。在数据查询的 14 天期限到期之前，您仍然可以在控制面板中查看历史数据。如果您启用了高级指标和建议，则此期限为 15 个月。要访问历史数据，您可以在到期期限内重新启用控制面板。

### 控制面板

您可以创建其他 S3 Storage Lens 存储统计管理工具控制面板，并按 Amazon Web Services 区域、S3 桶或账户（对于 Amazon Organizations）限定其范围。创建或编辑 S3 Storage Lens 存储统计管理工具控制面板时，定义控制面板范围和指标选择。S3 Storage Lens 存储统计管理工具提供免费指标、高级指标和建议，您可以支付额外费用升级到高级指标和建议。借助高级指标和建议，您可以访问其他指标和功能，以深入了解您的存储。这些功能包括高级指标类别、前缀级聚合、上下文建议和 Amazon CloudWatch 发布。有关 S3 Storage Lens 存储统计管理工具定价的信息，请参阅 Amazon S3 定价。

您还可以禁用或删除控制面板。如果禁用控制面板，它将不再更新，并且您将不再收到任何新的每日指标。在 14 天到期之前，您仍然可以查看历史数据。如果您为该控制面板启用了高级指标和建议，则此期限为 15 个月。要访问历史数据，您可以在到期期限内重新启用控制面板。

如果删除控制面板，将丢失所有控制面板的配置设置。您将不再收到任何新的每日指标，而且您也无法访问与该控制面板关联的历史数据。如果要访问已删除控制面板的历史数据，则必须在同一主区域中创建另一个具有相同名称的控制面板。

> **Note**
>
> - 您可以使用 S3 Storage Lens 存储统计管理工具为每个主区域创建多达 50 个控制面板。
> - 组织级控制面板只能限于区域范围。

### 账户快照

S3 Storage Lens 存储统计管理工具的 Account snapshot（账户快照）汇总了原定设置控制面板中的指标，并在 S3 控制台的 Buckets（桶）页面上显示总存储空间、对象计数和平均对象大小。账户快照让您可以快速获取有关存储的见解，而不必离开 Buckets（桶）页面。账户快照还允许您一键访问您的交互式 S3 Storage Lens 存储统计管理工具控制面板。

您可以使用控制面板可视化见解和趋势，标记异常值，并接收有关优化存储成本和应用数据保护最佳实践的建议。控制面板提供深入分析选项，用于在组织、账户、桶、对象或前缀级别生成见解。您还可以按 CSV 或 Parquet 格式将每天一次的指标导出发送到 S3 桶。

因为 default-account dashboard（原定设置账户控制面板）已链接到 Account snapshot（账户快照），所以您无法修改其控制面板范围。但是，在 default-account-dashboard（原定设置账户控制面板）中，您可以将指标选择从免费指标升级到付费的高级指标和建议。升级后，您可以在 S3 Storage Lens 存储统计管理工具 Account snapshot（账户快照）中显示所有请求、上载的字节数和下载的字节数。

> **Note**
>
> 如果禁用原定设置控制面板，将不再更新您的 Account snapshot（账户快照）。要在 Account snapshot（账户快照）中继续显示指标，您可以重新启用 default-account-dashboard（原定设置账户控制面板）。

### 指标导出

S3 Storage Lens 存储统计管理工具指标导出是一个包含 S3 Storage Lens 存储统计管理工具配置中标识的所有指标的文件。此信息每天以 CSV 或 Parquet 格式生成，并发送到 S3 桶。您可以通过所选的指标工具使用指标导出进行进一步分析。用于指标导出的 S3 桶必须与 S3 Storage Lens 存储统计管理工具配置位于同一区域。您可以通过编辑控制面板配置，从 S3 控制台生成 S3 Storage Lens 存储统计管理工具指标导出。您也可以使用 Amazon CLI 和 Amazon SDK 配置指标导出。

### 主区域

主区域是在其中存储给定控制面板配置的所有 Amazon S3 Storage Lens 存储统计管理工具指标的 Amazon Web Services 区域。创建 S3 Storage Lens 存储统计管理工具控制面板配置时，必须选择主区域。选择主区域后，无法对其进行更改。此外，如果您要创建 Storage Lens 组，我们建议您选择与 Storage Lens 存储统计管理工具控制面板相同的主区域。

> **Note**
>
> 您可以选择以下一个区域作为主区域：
>
> - 美国东部（弗吉尼亚州北部）– us-east-1
> - 美国东部（俄亥俄州）– us-east-2
> - 美国西部（加利福尼亚北部）– us-west-1
> - 美国西部（俄勒冈州）– us-west-2
> - 亚太地区（孟买）–(ap-south-1)
> - 亚太地区（首尔）–(ap-northeast-2)
> - 亚太地区（新加坡）–(ap-southeast-1)
> - 亚太地区（悉尼）– ap-southeast-2
> - 亚太地区（东京）–(ap-northeast-1)
> - 加拿大（中部）– ca-central-1
> - 中国（北京）– cn-north-1

- 中国（宁夏）– cn-northwest-1
- 欧洲地区（法兰克福）– eu-central-1
- 欧洲地区（爱尔兰）– eu-west-1
- 欧洲地区（伦敦）– eu-west-2
- 欧洲地区（巴黎）– eu-west-3
- 欧洲地区（斯德哥尔摩）– eu-north-1
- 南美洲（圣保罗）– (sa-east-1)

保留期

S3 Storage Lens 存储统计管理工具指标将保留，以便您可以查看历史趋势并比较存储和活动随时间推移的差异。您可以使用 Amazon S3 Storage Lens 存储统计管理工具指标以进行查询，因此您可以查看历史趋势并比较存储使用情况和活动随时间推移的差异。

所有 S3 Storage Lens 存储统计管理工具指标将保留 15 个月。但是，指标仅适用于特定持续时间的查询，这取决于您的指标选择。无法修改此持续时间。免费指标可用于 14 天的查询，高级指标可用于 15 个月的查询。

指标类别

在免费和高级套餐中，S3 Storage Lens 存储统计管理工具指标划分为与关键使用案例一致的类别，例如成本优化和数据保护。免费指标包括摘要、成本优化、数据保护、访问管理、性能和事件指标。升级到高级指标和建议时，您可以启用额外的成本优化和数据保护指标，这些指标可用于进一步降低 S3 存储成本和确保数据受到保护。您还可以启用活动指标和详细的状态代码指标，这些指标可用于提高应用程序工作流的性能。

以下列表显示了所有免费和高级指标类别。有关每个类别中包含的各个指标的完整列表，请参阅指标词汇表。

汇总指标

摘要指标提供有关您的 S3 存储的一般见解，包括您的总存储字节数和对象计数。

成本优化指标

成本优化指标提供见解，您可以使用这些见解来管理和优化存储成本。例如，您可以识别具有超过 7 天的未完成分段上传的桶。

借助高级指标和建议，您可以启用高级成本优化指标。这些指标包括 S3 生命周期规则计数指标，您可以使用这些指标来获取每个桶的到期时间和转换 S3 生命周期规则计数。

数据保护指标

数据保护指标提供对于加密和 S3 版本控制等数据保护功能的见解。您可以使用这些指标来识别未遵循数据保护最佳实践的桶。例如，您可以识别未使用具有 Amazon Key Management Service 密钥的原定设置加密（SSE-KMS）或 S3 版本控制的桶。

借助高级指标和建议，您可以启用高级数据保护指标。这些指标包括每个桶的复制规则计数指标。

访问管理指标

访问管理指标提供 S3 对象所有权的见解。您可以使用这些指标来查看您的桶使用了哪些对象所有权设置。

事件指标

事件指标提供 S3 事件通知的见解。通过事件指标，您可以查看哪些桶配置了 S3 事件通知。

性能指标

性能指标提供 S3 Transfer Acceleration 的见解。通过性能指标，您可以查看哪些桶启用了 Transfer Acceleration。

活动指标（高级）

如果您将控制面板升级到高级指标和建议，则可以启用活动指标。活动指标提供有关如何请求存储（例如，All 请求、Get 请求、Put 请求）、上传或下载的字节数以及错误的详细信息。

前缀级别的活动指标可用于帮助您确定哪些前缀不经常使用，以便您可以使用 S3 生命周期过渡到更适合的存储类。

详细状态代码指标（高级）

如果您将控制面板升级到高级指标和建议，则可以启用详细状态代码指标。详细状态代码指标提供有关 HTTP 状态代码的见解，例如“403 禁止”和“503 服务不可用”，您可以使用这些信息来排查访问或性能问题。例如，您可以查看 403 Forbidden error count（403 禁止错误计数）指标，以确定在未应用正确权限的情况下访问桶的工作负载。

前缀级别的详细状态代码指标可用于更好地了解按前缀划分的 HTTP 状态代码出现次数。例如，“503 错误计数”指标使您能够识别在数据摄取期间收到节流请求的前缀。

建议

S3 Storage Lens 存储统计管理工具提供自动建议来帮助您优化存储。在 S3 Storage Lens 存储统计管理工具控制面板中，建议与相关指标一起放置在上下文中。历史数据不符合建议的条件，因为建议与最近一段时期的情况相关。仅在建议相关时才会显示它们。

S3 Storage Lens 存储统计管理工具建议有以下形式：

- 建议

  建议会提醒您注意存储和活动中的趋势，这些趋势可能表明存储成本优化机会或可采用某种数据保护最佳实践。您可以使用《Amazon S3 用户指南》和 S3 Storage Lens 存储统计管理工具控制面板中的建议主题，深入了解有关特定区域、桶或前缀的更多详细信息。

- 标注

  标注是一些建议，可提醒您注意在一段时间内存储和活动中存在的值得留意的异常，您可能需要进一步关注或监控这些异常。

  - 异常标注

    S3 Storage Lens 存储统计管理工具根据您最近 30 天的趋势，为异常的指标提供了标注。异常是使用标准分数（也称为 z 得分）计算的。在这个分数中，将从该指标过去 30 天的平均值中减去当天的指标。然后用当天的指标除以该指标在过去 30 天内的标准差。得出的分数通常在 -3 到 +3 之间。此数字代表当天的指标与平均值相比的标准差。

    S3 Storage Lens 存储统计管理工具将分数 > 2 或 <-2 的指标视为异常，因为它们高于或低于正态分布数据的 95%。

  - 重大更改标注

    重大更改标注适用于预计更改频率较低的指标。因此，重大更改标注的灵敏度设置为高于异常值计算（异常值计算的浮动相对于前一天、前一周或前个月通常介于 +/-20% 的范围内）。

    解决存储和活动中的标注问题 – 如果您收到重大更改标注，这不一定意味着出现问题。该标注可能是由于您的存储中发生预期变化所致。例如，您最近可能添加了大量新对象、删除了大量对象或进行了类似的计划更改。

    如果您在控制面板上看到重大更改标注，请记下它并确定是否可以根据最近的情况来解释。如果没有，请使用 S3 Storage Lens 存储统计管理工具控制面板深入了解更多详细信息，以了解导致波动的特定区域、桶或前缀。

- 提醒

提醒可以深入了解 Amazon S3 的工作原理。它们可以帮助您详细了解如何使用 S3 功能来降低存储成本或应用数据保护最佳实践。

### 指标选择

S3 Storage Lens 存储统计管理工具提供了两个指标选择，您可以为控制面板和导出进行选择：免费指标和高级指标和建议。

- 免费指标

  S3 Storage Lens 存储统计管理工具为所有控制面板和配置提供免费指标。免费指标包含与存储相关的指标，例如桶数量和账户中的对象数。免费指标还包括基于使用案例的指标（例如，成本优化和数据保护指标），您可以使用这些指标来调查您的存储配置是否符合 S3 最佳实践。所有免费指标每天收集。数据可用于查询达 14 天。有关免费指标可提供哪些指标的更多信息，请参阅Amazon S3 Storage Lens 存储统计管理工具指标词汇表。

- 高级指标和建议

  S3 Storage Lens 存储统计管理工具为所有控制面板和配置提供免费指标以及升级到高级指标和建议选项的选择。将收取额外费用。有关更多信息，请参阅 Amazon S3 定价。

  高级指标和建议包括免费指标中的所有指标以及其他指标，例如高级数据保护和成本优化指标、活动指标和详细的状态代码指标。高级指标和建议还提供了帮助您优化存储的建议。建议与控制面板中的相关指标一起放置在上下文中。

  高级指标和建议包括以下功能：

  - 高级指标 - 生成其他指标。有关高级指标类别的完整列表，请参阅指标类别。要获得指标的完整列表，请参阅Amazon S3 Storage Lens 存储统计管理工具指标词汇表。
  - Amazon CloudWatch 发布 – 将 S3 Storage Lens 存储统计管理工具指标发布到 CloudWatch，以便在 CloudWatch 控制面板中创建运营状况的统一视图。您还可以使用 CloudWatch 操作和功能（如告警和触发操作、指标数学和异常检测）来监控 S3 Storage Lens 存储统计管理工具指标并采取措施。有关更多信息，请参阅 在 CloudWatch 中监控 S3 Storage Lens 存储统计管理工具指标。
  - 前缀聚合 – 收集前缀级别的指标。启用前缀聚合可在前缀级别扩展控制面板配置中包含的所有指标。仅为满足所配置阈值的前缀生成指标。请注意，适用于前缀级别的指标可用于前缀聚合，但桶级别的设置和规则计数指标除外。前缀级别的指标不会发布到 CloudWatch。
  - Storage Lens 组聚合 – 收集 Storage Lens 组级别的指标。启用高级指标和建议以及 Storage Lens 组聚合后，您可以指定要在 Storage Lens 控制面板中包括或排除哪些 Storage Lens 组。必须至

少指定一个 Storage Lens 组。指定的 Storage Lens 组还必须位于控制面板账户中指定的主区域内。Storage Lens 组级别的指标不会发布到 CloudWatch。

所有高级指标每天收集。数据最长在 15 个月内可供查询。有关 S3 Storage Lens 存储统计管理工具聚合的存储指标的更多信息，请参阅Amazon S3 Storage Lens 存储统计管理工具指标词汇表。

> **Note**
>
> 仅当在 Amazon S3 控制台上使用 S3 Storage Lens 存储统计管理工具控制面板时建议才可用。

S3 Storage Lens 存储统计管理工具和 Amazon Organizations

Amazon Organizations 是一项 Amazon Web Services 服务，可帮助您将所有 Amazon Web Services 账户聚合在一个组织层次结构下。Amazon S3 Storage Lens 存储统计管理工具与 Amazon Organizations 配合使用，可提供整个 Amazon S3 存储范围内对象存储和活动的单一视图。

有关更多信息，请参阅 将 Amazon S3 Storage Lens 存储统计管理工具与 Amazon Organizations 结合使用。

- 可信访问权限

  使用组织的管理账户，您必须为 S3 Storage Lens 存储统计管理工具启用可信访问权限，以聚合组织中所有成员账户的存储指标和使用情况数据。然后，您可以使用管理账户或向组织中其他账户授予委托管理员访问权限，为组织创建控制面板或导出。

  您可以随时为 S3 Storage Lens 存储统计管理工具禁用可信访问权限，这将阻止 S3 Storage Lens 存储统计管理工具聚合组织的指标。

- 委托管理员

  您可以使用 Amazon Organizations 管理账户或向组织中其他账户授予委托管理员访问权限，为您的组织创建 S3 Storage Lens 存储统计管理工具的控制面板和指标。您可以随时取消注册委托管理员。取消注册委托管理员还会自动阻止该委托管理员创建的所有组织级控制面板聚合新的存储指标。

有关更多信息，请参阅《Amazon Organizations 用户指南》中的 Amazon S3 Storage Lens 存储统计管理工具和 Amazon Organizations。

### Amazon S3 Storage Lens 存储统计管理工具服务相关角色

除了 Amazon Organizations 可信访问权限外，Amazon S3 Storage Lens 存储统计管理工具还使用 Amazon Identity and Access Management（IAM）服务相关角色。服务相关角色是一种与 S3 Storage Lens 存储统计管理工具直接关联的独特类型的 IAM 角色。S3 Storage Lens 存储统计管理工具预定义了服务相关角色，并包括从组织中的成员账户收集每日存储和活动指标所需的所有权限。

有关更多信息，请参阅使用面向 Amazon S3 Storage Lens 存储统计管理工具的服务相关角色。

## Amazon S3 Storage Lens 存储统计管理工具指标词汇表

Amazon S3 Storage Lens 存储统计管理工具指标词汇表提供了 S3 Storage Lens 存储统计管理工具的免费和高级指标的完整列表。

S3 Storage Lens 存储统计管理工具为所有控制面板和配置提供免费指标以及升级到高级指标的选项。

- 免费指标包含与存储使用情况相关的指标，例如账户中的桶数量和对象数量。免费指标还包括基于应用场景的指标，例如成本优化和数据保护指标。每天都会收集所有免费指标，数据在最多 14 天内可供查询。
- 高级指标和建议包括免费指标中的所有指标以及其它指标，例如高级数据保护和成本优化指标。高级指标还包括其它指标类别，例如活动指标和详细状态代码指标。高级指标数据可供查询 15 个月。

  如果您使用 S3 Storage Lens 存储统计管理工具和高级指标和建议，则需要支付额外费用。有关更多信息，请参阅 Amazon S3 定价。有关高级指标和建议功能的更多信息，请参阅指标选择。

> **Note**
>
> 对于 Storage Lens 组，只有免费存储指标可用。高级指标在 Storage Lens 组级别不可用。

#### 指标名称

下表中的 Metric name（指标名称）列提供了 S3 控制台中每个 S3 Storage Lens 存储统计管理工具的名称。CloudWatch and export（CloudWatch 和导出）列提供了 Amazon CloudWatch 中每个指标的名称以及您可以在 S3 Storage Lens 存储统计管理工具控制面板中配置的指标导出文件。

#### 派生指标公式

派生指标不适用于指标导出和 CloudWatch 发布选项。但是，您可以使用 Derived metrics formula（派生指标公式）列中所示的指标公式来计算它们。

解释 Amazon S3 Storage Lens 存储统计管理工具的指标单位倍数的前缀符号（K、M、G 等）

S3 Storage Lens 存储统计管理工具指标单位倍数用前缀符号编写。这些前缀符号与由国际计量局（BIPM）标准化的国际单位制（SI）符号相符。这些符号还用于统一计量单位代码（UCUM)中。有关更多信息，请参阅 SI 前缀符号列表。

> **Note**
>
> - S3 存储字节的计量单位是二进制千兆字节（GB），其中 1GB 是 $2^{30}$ 字节，1TB 是 $2^{40}$ 字节，1PB 是 $2^{50}$ 字节。根据国际电工委员会（IEC）的定义，该计量单位也称为吉比字节（GiB）。
> - 在对象根据其生命周期配置的生存期结束后，Amazon S3 会将该对象加入移除队列并异步移除它。因此，过期日期和 Amazon S3 删除对象的日期之间可能会有一段延迟。S3 Storage Lens 存储统计管理工具不包含已过期但尚未移除的对象的指标。有关 S3 生命周期中的过期操作的更多信息，请参阅即将过期的对象。

下表显示了 S3 Storage Lens 存储统计管理工具指标词汇表。

| 指标名称 | CloudWatch 和导出 | 描述 | 级别[1] | 类别[2] | 派生 | 派生指标公式 |
|---|---|---|---|---|---|---|
| 总存储空间 | StorageBytes | 总存储空间，包括未完成的分段上传、对象元数据和删除标记 | 免费 | 摘要 | 否 | - |
| 对象计数 | ObjectCount | 对象总数 | 免费 | 摘要 | N | - |
| 平均对象大小 | - | 对象平均大小 | 免费 | 摘要 | Y | sum(StorageBytes)/ |

| 指标名称 | CloudWatch 和导出 | 描述 | 级别[1] | 类别[2] | 派生 | 派生指标公式 |
|---|---|---|---|---|---|---|
| | | | | | | sum(ObjectCount) |
| 处于活动状态的桶数 | - | 存储大于 0 字节的存储桶总数 | 免费 | 摘要 | Y | - |
| 桶 | - | 桶的总数 | 免费 | 摘要 | Y | - |
| 账户 | - | 其存储在范围内的账户数量 | 免费 | 摘要 | Y | - |
| 当前版本字节数 | CurrentVersionStorageBytes | 属于对象的当前版本的字节数 | 免费 | 成本优化 | N | - |
| 当前版本字节百分比 | - | 范围内属于对象的当前版本的字节百分比 | 免费 | 成本优化 | Y | sum(CurrentVersionStorageBytes)/sum(StorageBytes) |
| 当前版本对象计数 | CurrentVersionObjectCount | 当前版本对象的计数 | 免费 | 数据保护 | N | - |

| 指标名称 | CloudWatch 和导出 | 描述 | 级别[1] | 类别[2] | 派生 | 派生指标公式 |
|---|---|---|---|---|---|---|
| 当前版本对象百分比 | - | 范围内属当前版本的对象的百分比 | 免费 | 成本优化 | Y | sum(CurrentVersionObjectCount)/sum(ObjectCount) |
| 非当前版本字节数 | NonCurrentVersionStorageBytes | 非当前版本的字节数 | 免费 | 成本优化 | N | - |
| 非当前版本字节百分比 | - | 范围内非当前版本字节百分比 | 免费 | 成本优化 | Y | sum(NonCurrentVersionStorageBytes)/sum(StorageBytes) |
| 非当前版本对象计数 | NonCurrentVersionObjectCount | 非当前版本对象的计数 | 免费 | 成本优化 | N | - |

| 指标名称 | CloudWatch 和导出 | 描述 | 级别[1] | 类别[2] | 派生 | 派生指标公式 |
|---|---|---|---|---|---|---|
| 非当前版本对象百分比 | - | 范围内非当前版本对象百分比 | 免费 | 成本优化 | Y | sum(NonCurrentVersionObjectCount)/sum(ObjectCount) |
| 删除标记字节 | DeleteMarkerStorageBytes | 范围内作为删除标记的字节数 | 免费 | 成本优化 | N | - |
| 删除标记字节百分比 | - | 范围内作为删除标记的字节百分比 | 免费 | 成本优化 | Y | sum(DeleteMarkerStorageBytes)/sum(StorageBytes) |
| 删除标记对象计数 | DeleteMarkerObjectCount | 带有删除标记的对象总数 | 免费 | 成本优化 | N | - |

| 指标名称 | CloudWatch 和导出 | 描述 | 级别[1] | 类别[2] | 派生 | 派生指标公式 |
|---|---|---|---|---|---|---|
| 删除标记对象百分比 | - | 范围内带有删除标记的对象百分比 | 免费 | 成本优化 | Y | sum(DeleteMarkerObjectCount)/sum(ObjectCount) |
| 未完成分段上传字节 | IncompleteMultipartUploadStorageBytes | 范围内未完成分段上传的总字节数 | 免费 | 成本优化 | N | - |
| 未完成分段上传字节百分比 | - | 范围内由于未完成分段上传导致的字节百分比 | 免费 | 成本优化 | Y | sum(IncompleteMultipartUploadStorageBytes)/sum(StorageBytes) |
| 未完成分段上传对象计数 | IncompleteMultipartUploadObjectCount | 范围内未完成分段上传的对象数量 | 免费 | 成本优化 | N | - |

| 指标名称 | CloudWatch 和导出 | 描述 | 级别[1] | 类别[2] | 派生 | 派生指标公式 |
|---|---|---|---|---|---|---|
| 未完成分段上传对象百分比 | - | 范围内未完成分段上传的对象百分比 | 免费 | 成本优化 | Y | sum(IncompleteMultipartUploadObjectCount)/sum(ObjectCount) |
| 超过 7 天的未完成分段上传存储字节 | IncompleteMPUStorageBytesOlderThan7Days | 范围内超过 7 天的未完成分段上传的总字节数 | 免费 | 成本优化 | N | - |
| 超过 7 天的未完成分段上传存储字节百分比 | - | 超过 7 天的未完成分段上传字节的百分比 | 免费 | 成本优化 | Y | sum(IncompleteMPUStorageBytesOlderThan7Days)/sum(StorageBytes) |
| 超过 7 天的未完成分段上传对象计数 | IncompleteMPUObjectCountOlderThan7Days | 超过 7 天的未完成分段上传的对象数量 | 免费 | 成本优化 | N | - |

| 指标名称 | CloudWatch 和导出 | 描述 | 级别[1] | 类别[2] | 派生 | 派生指标公式 |
|---|---|---|---|---|---|---|
| 超过 7 天的未完成分段上传对象计数百分比 | - | 超过 7 天的未完成分段上传对象的百分比 | 免费 | 成本优化 | Y | sum(IncompleteMPUObjectCountOlderThan7Days)/sum(ObjectCount) |
| 转换生命周期规则计数 | TransitionLifecycleRuleCount | 将对象转换为另一个存储类的生命周期规则计数 | 高级 | 成本优化 | N | - |
| 每个桶的平均转换生命周期规则数 | - | 将对象转换为另一个存储类的生命周期规则的平均数量 | 高级 | 成本优化 | Y | sum(TransitionLifecycleRuleCount)/sum(DistinctNumberOfBuckets) |
| 过期生命周期规则计数 | ExpirationLifecycleRuleCount | 使对象过期的生命周期规则计数 | 高级 | 成本优化 | N | - |

| 指标名称 | CloudWatch 和导出 | 描述 | 级别[1] | 类别[2] | 派生 | 派生指标公式 |
|---|---|---|---|---|---|---|
| 每个桶的平均过期生命周期规则数 | - | 使对象过期的生命周期规则的平均数量 | 高级 | 成本优化 | Y | sum(ExpirationLifecycleRuleCount)/sum(DistinctNumberOfBuckets) |
| 非当前版本转换生命周期规则计数 | NoncurrentVersionTransitionLifecycleRuleCount | 将非当前对象版本转换为其他存储类的生命周期规则计数 | 高级 | 成本优化 | N | |
| 每个桶的平均非当前版本转换生命周期规则数 | - | 将非当前对象版本转换到另一个存储类的生命周期规则的平均数量 | 高级 | 成本优化 | Y | sum(NoncurrentVersionTransitionLifecycleRuleCount)/sum(DistinctNumberOfBuckets) |

| 指标名称 | CloudWatch 和导出 | 描述 | 级别[1] | 类别[2] | 派生 | 派生指标公式 |
|---|---|---|---|---|---|---|
| 非当前版本过期生命周期规则计数 | NoncurrentVersionExpirationLifecycleRuleCount | 使非当前对象版本过期的生命周期规则计数 | 高级 | 成本优化 | N | - |
| 每个桶的平均非当前版本过期生命周期规则数 | - | 使非当前对象版本过期的生命周期规则的平均数量 | 高级 | 成本优化 | Y | sum(NoncurrentVersionExpirationLifecycleRuleCount)/sum(DistinctNumberOfBuckets) |
| 中止未完成的分段上传生命周期规则计数 | AbortIncompleteMPULifecycleRuleCount | 删除未完成分段上传的生命周期规则计数 | 高级 | 成本优化 | N | - |

| 指标名称 | CloudWatch 和导出 | 描述 | 级别[1] | 类别[2] | 派生 | 派生指标公式 |
|---|---|---|---|---|---|---|
| 每个桶的中止未完成分段上传生命周期规则的平均数量 | - | 删除未完成分段上传的生命周期规则的平均数量 | 高级 | 成本优化 | Y | sum(AbortIncompleteMPULifecycleRuleCount)/sum(DistinctNumberOfBuckets) |
| 过期对象删除标记生命周期规则计数 | ExpiredObjectDeleteMarkerLifecycleRuleCount | 移除过期对象删除标记的生命周期计数 | 高级 | 成本优化 | N | - |
| 每个桶的过期对象删除标记生命周期规则的平均数量 | - | 移除过期对象删除标记的生命周期的平均数量 | 高级 | 成本优化 | Y | sum(ExpiredObjectDeleteMarkerLifecycleRuleCount)/sum(DistinctNumberOfBuckets) |

| 指标名称 | CloudWatch 和导出 | 描述 | 级别[1] | 类别[2] | 派生 | 派生指标公式 |
|---|---|---|---|---|---|---|
| 生命周期规则总计数 | TotalLifecycleRuleCount | 生命周期规则的总计数 | 高级 | 成本优化 | N | - |
| 每个桶的生命周期规则平均计数 | - | 生命周期规则平均数量 | 高级 | 成本优化 | Y | sum(TotalLifecycleRuleCount)/sum(DistinctNumberOfBuckets) |
| 加密字节数 | EncryptedStorageBytes | 加密字节总数 | 免费 | 数据保护 | 否 | - |
| 加密字节百分比 | - | 已加密总字节数的百分比 | 免费 | 数据保护 | Y | sum(EncryptedObjectCount)/sum(StorageBytes) |
| 加密对象计数 | EncryptedObjectCount | 加密对象的总计数 | 免费 | 数据保护 | 否 | - |

| 指标名称 | CloudWatch 和导出 | 描述 | 级别[1] | 类别[2] | 派生 | 派生指标公式 |
|---|---|---|---|---|---|---|
| 加密对象百分比 | - | 加密对象的百分比 | 免费 | 数据保护 | Y | sum(EncryptedStorageBytes)/sum(ObjectCount) |
| 未加密字节数 | UnencryptedStorageBytes | 未加密的字节数 | 免费 | 数据保护 | Y | sum(StorageBytes) - sum(EncryptedStorageBytes) |
| 未加密字节百分比 | - | 未加密字节的百分比 | 免费 | 数据保护 | Y | sum(UnencryptedStorageBytes)/sum(StorageBytes) |
| 未加密对象计数 | UnencryptedObjectCount | 未加密对象的总计数 | 免费 | 数据保护 | Y | sum(ObjectCount) - sum(EncryptedObjectCount) |

| 指标名称 | CloudWatch 和导出 | 描述 | 级别[1] | 类别[2] | 派生 | 派生指标公式 |
|---|---|---|---|---|---|---|
| 未加密对象百分比 | - | 未加密对象的百分比 | 免费 | 数据保护 | Y | sum(UnencryptedStorageBytes)/ sum(ObjectCount) |
| 复制的存储字节源 | ReplicatedStorageBytesSource | 从源桶复制的总字节数 | 免费 | 数据保护 | N | - |
| 复制字节源百分比 | - | 从源桶复制的总字节数的百分比 | 免费 | 数据保护 | Y | sum(ReplicatedStorageBytesSource)/ sum(StorageBytes) |
| 复制对象计数源 | ReplicatedObjectCountSource | 从源桶中复制的对象的计数 | 免费 | 数据保护 | N | - |

| 指标名称 | CloudWatch 和导出 | 描述 | 级别[1] | 类别[2] | 派生 | 派生指标公式 |
|---|---|---|---|---|---|---|
| 复制对象源百分比 | - | 从源桶复制的总对象数的百分比 | 免费 | 数据保护 | Y | sum(ReplicatedStorageObjectCount)/sum(ObjectCount) |
| 复制的存储字节目标 | ReplicatedStorageBytes | 复制到目标桶的总字节数 | 免费 | 数据保护 | N | - |
| 复制字节目标百分比 | - | 复制到目标桶的总字节数的百分比 | 免费 | 数据保护 | Y | sum(ReplicatedStorageBytes)/sum(StorageBytes) |
| 复制对象计数目标 | ReplicatedObjectCount | 复制到目标桶的对象计数 | 免费 | 数据保护 | N | - |
| 复制对象目标百分比 | - | 复制到目标桶的总对象数的百分比 | 免费 | 数据保护 | Y | sum(ReplicatedObjectCount)/sum(ObjectCount) |

| 指标名称 | CloudWatch 和导出 | 描述 | 级别[1] | 类别[2] | 派生 | 派生指标公式 |
|---|---|---|---|---|---|---|
| 对象锁定字节 | ObjectLockEnabledStorageBytes | 启用对象锁定的存储字节总计数 | 免费 | 数据保护 | N | sum(UnencryptedStorageBytes)/ sum(ObjectLockEnabledStorageCount) - sum(ObjectLockEnabledStorageBytes) |
| 对象锁定字节百分比 | - | 启用对象锁定的存储字节的百分比 | 免费 | 数据保护 | Y | sum(ObjectLockEnabledStorageBytes)/ sum(StorageBytes) |
| 对象锁定对象计数 | ObjectLockEnabledObjectCount | 对象锁定对象的总计数 | 免费 | 数据保护 | 否 | - |

| 指标名称 | CloudWatch 和导出 | 描述 | 级别[1] | 类别[2] | 派生 | 派生指标公式 |
| --- | --- | --- | --- | --- | --- | --- |
| 对象锁定对象百分比 | - | 启用了对象锁定的总对象百分比 | 免费 | 数据保护 | Y | sum(ObjectLockEnabledObjectCount)/sum(ObjectCount) |
| 启用版本控制的桶计数 | VersioningEnabledBucketCount | 启用 S3 版本控制的桶的计数 | 免费 | 数据保护 | N | - |
| 启用版本控制的桶百分比 | - | 启用 S3 版本控制的桶的百分比 | 免费 | 数据保护 | Y | sum(VersioningEnabledBucketCount)/sum(DistinctNumberOfBuckets) |
| 启用 MFA 删除的桶计数 | MFADeleteEnabledBucketCount | 启用 MFA（多重验证）删除的桶计数 | 免费 | 数据保护 | N | - |

| 指标名称 | CloudWatch 和导出 | 描述 | 级别[1] | 类别[2] | 派生 | 派生指标公式 |
|---|---|---|---|---|---|---|
| 启用 MFA 删除的桶百分比 | - | 启用 MFA（多重验证）删除的桶百分比 | 免费 | 数据保护 | Y | sum(MFADeleteEnabledBucketCount)/ sum (Distinct NumberOfBuckets) |
| 启用 SSE-KMS 的桶计数 | SSEKMSEnabledBucketCount | 使用具有 Amazon Key Management Service 密钥的服务器端加密（SSE-KMS）进行原定设置桶加密的桶计数 | 免费 | 数据保护 | N | - |
| 启用 SSE-KMS 的桶百分比 | - | 使用 SSE-KMS 进行原定设置桶加密的桶百分比 | 免费 | 数据保护 | Y | sum(SSEKMSEnabledBucketCount)/ sum(DistinctNumberOfBuckets) |
| 所有不支持的签名请求 | AllUnsupportedSignatureRequests | 使用不支持的 Amazon 签名版本的请求总数 | 高级 | 数据保护 | N | - |

| 指标名称 | CloudWatch 和导出 | 描述 | 级别[1] | 类别[2] | 派生 | 派生指标公式 |
|---|---|---|---|---|---|---|
| 所有不支持的签名请求百分比 | - | 使用不支持的 Amazon 签名版本的请求的百分比 | 高级 | 数据保护 | Y | sum(AllUnsupportedSignatureRequests) / sum(AllRequests) |
| 所有不支持的 TLS 请求 | AllUnsupportedTLSRequests | 使用不支持的传输层安全性协议（TLS）版本的请求数量 | 高级 | 数据保护 | N | - |
| 所有不支持的 TLS 请求百分比 | - | 使用不支持的 TLS 版本的请求的百分比 | 高级 | 数据保护 | Y | sum(AllUnsupportedTLSRequests)/ sum(AllRequests) |
| 所有 SSE-KMS 请求 | AllSSEKMSRequests | 指定 SSE-KMS 的请求总数 | 高级 | 数据保护 | N | - |

| 指标名称 | CloudWatch 和导出 | 描述 | 级别[1] | 类别[2] | 派生 | 派生指标公式 |
|---|---|---|---|---|---|---|
| 所有 SSE-KMS 请求的百分比 | - | 指定 SSE-KMS 的请求百分比 | 高级 | 数据保护 | Y | sum(AllSSEKMSRequests)/sum(AllRequests) |
| 同区域复制规则计数 | SameRegionReplicationRuleCount | 同区域复制（SRR）的复制规则计数 | 高级 | 数据保护 | N | - |
| 每个桶的平均同区域复制规则数 | - | SRR 的复制规则的平均数量 | 高级 | 数据保护 | Y | sum(SameRegionReplicationRuleCount)/sum(DistinctNumberOfBuckets) |
| 跨区域复制规则计数 | CrossRegionReplicationRuleCount | 跨区域复制（CRR）的复制规则计数 | 高级 | 数据保护 | N | - |

| 指标名称 | CloudWatch 和导出 | 描述 | 级别[1] | 类别[2] | 派生 | 派生指标公式 |
|---|---|---|---|---|---|---|
| 每个桶的平均跨区域复制规则数 | - | CRR 的复制规则的平均数量 | 高级 | 数据保护 | Y | sum(CrossRegionReplicationRuleCount) / sum(DistinctNumberOfBuckets) |
| 同账户复制规则计数 | SameAccountReplicationRuleCount | 同一账户内用于复制的复制规则计数 | 高级 | 数据保护 | N | - |
| 每个桶的平均同账户复制规则数 | - | 同一账户内用于复制的复制规则平均数量 | 高级 | 数据保护 | Y | sum(SameAccountReplicationRuleCount) / sum(DistinctNumberOfBuckets) |
| 跨账户复制规则计数 | CrossAccountReplicationRuleCount | 跨账户复制的复制规则计数 | 高级 | 数据保护 | N | - |

| 指标名称 | CloudWatch 和导出 | 描述 | 级别[1] | 类别[2] | 派生 | 派生指标公式 |
|---|---|---|---|---|---|---|
| 每个桶的跨账户复制规则平均数量 | - | 跨账户复制的复制规则的平均数量 | 高级 | 数据保护 | Y | sum(CrossAccountReplicationRuleCount)/ sum(DistinctNumberOfBuckets) |
| 目标复制规则计数无效 | InvalidDestinationReplicationRuleCount | 具有无效复制目标的复制规则计数 | 高级 | 数据保护 | N | - |
| 每个桶的无效目标复制规则的平均数量 | - | 具有无效复制目标的复制规则的平均数量 | 高级 | 数据保护 | Y | sum(InvalidReplicationRuleCount)/ sum (DistinctNumberOfBuckets) |
| 复制规则总计数 | - | 复制规则总计数 | 高级 | 数据保护 | Y | - |

| 指标名称 | CloudWatch 和导出 | 描述 | 级别[1] | 类别[2] | 派生 | 派生指标公式 |
| --- | --- | --- | --- | --- | --- | --- |
| 每个桶的复制规则平均计数 | - | 复制规则总计数的平均值 | 高级 | 数据保护 | Y | sum(all replication rule count metrics)/ sum(DistinctNumberOfBuckets) |
| 对象所有权强制桶所有者计数 | ObjectOwnershipBucketOwnerEnforcedBucketCount | 通过为对象所有权使用“强制桶所有者”设置禁用了访问控制列表（ACL）的桶总计数 | 免费 | 访问权限管理 | N | - |
| 对象所有权“强制桶所有者”的桶的百分比 | - | 通过为对象所有权使用“强制桶所有者”设置禁用了 ACL 的桶的百分比 | 免费 | 访问权限管理 | Y | sum(ObjectOwnershipBucketOwnerEnforcedBucketCount)/ sum (DistinctNumberOfBuckets) |

| 指标名称 | CloudWatch 和导出 | 描述 | 级别[1] | 类别[2] | 派生 | 派生指标公式 |
|---|---|---|---|---|---|---|
| 对象所有权“首选桶所有者”的桶的计数 | ObjectOwnershipBucketOwnerPreferredBucketCount | 为对象所有权使用“首选桶所有者”设置的桶的总计数 | 免费 | 访问权限管理 | N | - |
| 对象所有权“首选桶所有者”的桶的百分比 | - | 为对象所有权使用“首选桶所有者”设置的桶的百分比 | 免费 | 访问权限管理 | Y | sum(ObjectOwnershipBucketOwnerPreferredBucketCount)/sum(DistinctNumberOfBuckets) |
| 对象所有权“对象写入器”桶计数 | ObjectOwnershipObjectWriterBucketCount | 为对象所有权使用“对象写入器”设置的桶的总计数 | 免费 | 访问权限管理 | N | - |

| 指标名称 | CloudWatch 和导出 | 描述 | 级别[1] | 类别[2] | 派生 | 派生指标公式 |
|---|---|---|---|---|---|---|
| 对象所有权“对象写入器”桶的百分比 | - | 为对象所有权使用“对象写入器”设置的桶的百分比 | 免费 | 访问权限管理 | Y | sum(ObjectOwnershipObjectWriterBucketCount)/sum(DistinctNumberOfBuckets) |
| 启用 Transfer Acceleration 的桶计数 | TransferAccelerationEnabledBucketCount | 启用 Transfer Acceleration 的桶的总计数 | 免费 | 性能 | N | - |
| 启用 Transfer Acceleration 的桶的百分比 | - | 已启用 Transfer Acceleration 的桶的百分比 | 免费 | 性能 | Y | sum(TransferAccelerationEnabledBucketCount)/sum(DistinctNumberOfBuckets) |
| 启用事件通知的桶计数 | EventNotificationEnabledBucketCount | 启用了事件通知的桶的总计数 | 免费 | 事件 | N | |

| 指标名称 | CloudWatch 和导出 | 描述 | 级别[1] | 类别[2] | 派生 | 派生指标公式 |
|---|---|---|---|---|---|---|
| 启用事件通知的桶的百分比 | - | 启用了事件通知的桶的百分比 | 免费 | 事件 | Y | sum(EventNotificationEnabledBucketCount)/sum(DistinctNumberOfBuckets) |
| 所有请求 | AllRequests | 发出的 请求总数 | 高级 | 活动 | N | - |
| Get 请求 | GetRequests | 发出的 GET 请求总数 | 高级 | 活动 | 否 | - |
| Put 请求 | PutRequests | 发出的 PUT 请求总数 | 高级 | 活动 | 否 | - |
| Head 请求 | HeadRequests | 发出的 HEAD 请求总数 | 高级 | 活动 | 否 | - |
| Delete 请求 | DeleteRequests | 发出的 DELETE 请求总数 | 高级 | 活动 | 否 | - |
| List 请求 | ListRequests | 发出的 LIST 请求总数 | 高级 | 活动 | 否 | - |
| Post 请求 | PostRequests | 发出的 POST 请求总数 | 高级 | 活动 | 否 | - |

| 指标名称 | CloudWatch 和导出 | 描述 | 级别[1] | 类别[2] | 派生 | 派生指标公式 |
|---|---|---|---|---|---|---|
| Select 请求 | SelectRequests | S3 Select 请求的总数 | 高级 | 活动 | 否 | - |
| Select 扫描的字节 | SelectScannedBytes | 扫描的 S3 Select 字节数 | 高级 | 活动 | 否 | - |
| Select 返回的字节 | SelectReturnedBytes | 返回的 S3 Select 字节数 | 高级 | 活动 | 否 | - |
| 已下载字节 | BytesDownloaded | 下载的字节数 | 高级 | 活动 | 否 | - |
| 检索率百分比 | - | 下载的字节的百分比 | 高级 | 活动 | Y | sum(BytesDownloaded)/ sum(StorageBytes) |
| 已上传字节 | BytesUploaded | 上传的字节数 | 高级 | 活动 | 否 | - |
| 摄取率百分比 | - | 上载的字节的百分比 | 高级 | 活动 | Y | sum(BytesUploaded) / sum(StorageBytes) |
| 4xx 错误 | 4xxErrors | HTTP 4xx 状态代码的总数 | 高级 | 活动 | 否 | - |

| 指标名称 | CloudWatch 和导出 | 描述 | 级别[1] | 类别[2] | 派生 | 派生指标公式 |
|---|---|---|---|---|---|---|
| 5xx 错误 | 5xxErrors | HTTP 5xx 状态代码的总数 | 高级 | 活动 | 否 | - |
| 总错误数 | - | 所有 4xx 和 5xx 错误的总和 | 高级 | 活动 | Y | sum(4xxErrors) + sum(5xxErrors) |
| 错误率百分比 | - | 4xx 和 5xx 错误总数占总请求数的百分比 | 高级 | 活动 | Y | sum(TotalErrors)/ sum(TotalRequests) |
| 200 OK 状态计数 | 200OKStatusCount | 200 OK 状态代码的总计数 | 高级 | 详细状态代码 | N | - |
| % 200 OK 状态百分比 | - | 200 OK 状态代码总数占总请求数的百分比 | 高级 | 详细状态代码 | Y | sum(200OKStatusCount)/ sum(AllRequests) |

| 指标名称 | CloudWatch 和导出 | 描述 | 级别[1] | 类别[2] | 派生 | 派生指标公式 |
|---|---|---|---|---|---|---|
| 206 部分内容状态计数 | 206PartialContentStatusCount | 206 部分内容状态代码的总计数 | 高级 | 详细状态代码 | N | - |
| 206 部分内容状态百分比 | - | 206 部分内容状态代码总数占总请求数的百分比 | 高级 | 详细状态代码 | Y | sum(206PartialContentStatusCount)/sum(AllRequests) |
| 400 错误请求错误计数 | 400BadRequestErrorCount | 400 错误请求状态代码的总计数 | 高级 | 详细状态代码 | N | - |
| 400 错误请求错误百分比 | - | 400 错误请求状态代码总数占总请求数的百分比 | 高级 | 详细状态代码 | Y | sum(400BadRequestErrorCount)/sum(AllRequests) |

| 指标名称 | CloudWatch 和导出 | 描述 | 级别[1] | 类别[2] | 派生 | 派生指标公式 |
|---|---|---|---|---|---|---|
| 403 禁止错误计数 | 403ForbiddenErrorCount | 403 禁止状态代码的总计数 | 高级 | 详细状态代码 | N | - |
| 403 禁止错误百分比 | - | 403 禁止状态代码总数占总请求数的百分比 | 高级 | 详细状态代码 | Y | sum(403ForbiddenErrorCount) / sum(AllRequests) |
| 404 找不到错误计数 | 404NotFoundErrorCount | 404 找不到状态代码的总计数 | 高级 | 详细状态代码 | N | - |
| 404 找不到错误百分比 | - | 404 找不到状态代码总数占总请求数的百分比 | 高级 | 详细状态代码 | Y | sum(404NotFoundErrorCount)/ sum(AllRequests) |

| 指标名称 | CloudWatch 和导出 | 描述 | 级别[1] | 类别[2] | 派生 | 派生指标公式 |
|---|---|---|---|---|---|---|
| 500 内部服务器错误计数 | 500InternalServerErrorCount | 500 内部服务器错误状态代码总计数 | 高级 | 详细状态代码 | N | - |
| 500 内部服务器错误百分比 | - | 500 内部服务器错误状态代码总数占总请求数的百分比 | 高级 | 详细状态代码 | Y | sum(500InternalServerErrorCount)/sum(AllRequests) |
| 503 服务不可用错误计数 | 503ServiceUnavailableErrorCount | 503 服务不可用状态代码的总计数 | 高级 | 详细状态代码 | N | - |
| 503 服务不可用错误百分比 | - | 503 服务不可用状态代码总数占总请求数的百分比 | 高级 | 详细状态代码 | Y | sum(503ServiceUnavailableErrorCount)/sum(AllRequests) |

[1] 所有免费存储指标均在 Storage Lens 组级别可用。高级指标在 Storage Lens 组级别不可用。

[2] 规则计数指标和桶设置指标在前缀级别不可用。

## 设置 Amazon S3 Storage Lens 存储统计管理工具权限

Amazon S3 Storage Lens 存储统计管理工具需要 Amazon Identity and Access Management（IAM）中的新权限才能授权访问 S3 Storage Lens 存储统计管理工具操作。要授予这些权限，您可以使用基于身份的 IAM policy。您可以将此策略附加到 IAM 用户、组或角色，以授予其权限。此类权限可能包括启用或禁用 S3 Storage Lens 存储统计管理工具或访问任何 S3 Storage Lens 存储统计管理工具控制面板或配置。

除非同时满足以下两个条件，否则 IAM 用户或角色必须属于创建或拥有控制面板或配置的账户：

- 您的账户是 Amazon Organizations 的成员。
- 您获得了相关访问权限，可以使用您的管理账户作为委托管理员，创建组织级别的控制面板。

> **Note**
>
> - 您不能使用账户的根用户凭证查看 Amazon S3 Storage Lens 存储统计管理工具控制面板。要访问 S3 Storage Lens 存储统计管理工具控制面板，您必须向新的或现有的 IAM 用户授予所需的 IAM 权限。然后，使用这些用户凭证登录以访问 S3 Storage Lens 存储统计管理工具控制面板。有关更多信息，请参阅《IAM 用户指南》中的 IAM 安全最佳实践。
> - 在 Amazon S3 控制台上使用 S3 Storage Lens 存储统计管理工具可能需要多个权限。例如，要在控制台上编辑控制面板，您需要以下权限：
>   - `s3:ListStorageLensConfigurations`
>   - `s3:GetStorageLensConfiguration`
>   - `s3:PutStorageLensConfiguration`

主题


- 设置账户权限以使用 S3 Storage Lens 存储统计管理工具
- 设置账户权限以使用 S3 Storage Lens 组
- 设置将 S3 Storage Lens 存储统计管理工具与 Amazon Organizations 结合使用的权限

## 设置账户权限以使用 S3 Storage Lens 存储统计管理工具

要创建和管理 S3 Storage Lens 存储统计管理工具控制面板和 Storage Lens 存储统计管理工具控制面板配置，您必须拥有以下权限，具体取决于您要执行的操作：

下表显示 Amazon S3 Storage Lens 存储统计管理工具相关的 IAM 权限。

| 操作 | IAM 权限 |
| --- | --- |
| 在 Amazon S3 控制台中创建或更新 S3 Storage Lens 存储统计管理工具控制面板。 | `s3:ListStorageLensConfigurations`<br>`s3:GetStorageLensConfiguration`<br>`s3:GetStorageLensConfigurationTagging`<br>`s3:PutStorageLensConfiguration`<br>`s3:PutStorageLensConfigurationTagging` |
| 在 Amazon S3 控制台上获取 S3 Storage Lens 存储统计管理工具控制面板的标签。 | `s3:ListStorageLensConfigurations`<br>`s3:GetStorageLensConfigurationTagging` |
| 在 Amazon S3 控制台上查看 S3 Storage Lens 存储统计管理工具控制面板。 | `s3:ListStorageLensConfigurations`<br>`s3:GetStorageLensConfiguration`<br>`s3:GetStorageLensDashboard` |
| 在 Amazon S3 控制台上删除 S3 Storage Lens 存储统计管理工具控制面板。 | `s3:ListStorageLensConfigurations`<br>`s3:GetStorageLensConfiguration`<br>`s3:DeleteStorageLensConfiguration` |
| 在 Amazon CLI 或 Amazon SDK 中创建或更新 S3 Storage Lens 存储统计管理工具配置。 | `s3:PutStorageLensConfiguration` |

| 操作 | IAM 权限 |
| --- | --- |
| | `s3:PutStorageLensConfigurationTagging` |
| 使用 Amazon CLI 或 Amazon SDK 获取 S3 Storage Lens 存储统计管理工具配置的标签。 | `s3:GetStorageLensConfigurationTagging` |
| 使用 Amazon CLI 或 Amazon SDK 查看 S3 Storage Lens 存储统计管理工具配置。 | `s3:GetStorageLensConfiguration` |
| 使用 Amazon CLI 或 Amazon SDK 删除 S3 Storage Lens 存储统计管理工具配置。 | `s3:DeleteStorageLensConfiguration` |

Note

- 您可以使用 IAM policy 中的资源标签来管理权限。
- 具有这些权限的 IAM 用户或角色可以查看他们可能不具备从中读取或列出对象的直接权限的桶和前缀中的指标。
- 对于启用了前缀级别指标的 S3 Storage Lens 存储统计管理工具控制面板，如果选定的前缀路径与某个对象键相匹配，则控制面板可能会将该对象键显示为另一个前缀。
- 对于存储在账户的桶中的指标导出，使用 IAM policy 中的现有 `s3:GetObject` 权限进行权限授权。同样，对于 Amazon Organizations 实体，组织的管理账户或委托管理员账户可以使用 IAM policy 来管理组织级控制面板和配置的访问权限。

## 设置账户权限以使用 S3 Storage Lens 组

您可以使用 S3 Storage Lens 组，根据前缀、后缀、对象标签、对象大小或对象期龄来了解桶内的存储分布。您可以将 Storage Lens 组附加到控制面板以查看其聚合指标。

要使用 Storage Lens 组，你需要具备某些权限。有关更多信息，请参阅 the section called “Storage Lens 组权限”。

### 设置将 S3 Storage Lens 存储统计管理工具与 Amazon Organizations 结合使用的权限

您可以使用 Amazon S3 Storage Lens 存储统计管理工具收集属于 Amazon Organizations 层次结构的所有账户的存储指标和使用情况数据。下表显示了与在组织中使用 S3 Storage Lens 存储统计管理工具相关的操作和权限。

| 操作 | IAM 权限 |
| --- | --- |
| 为您的组织启用 S3 Storage Lens 存储统计管理工具的可信访问权限。 | `organizations:EnableAWSServiceAccess` |
| 为您的组织禁用 S3 Storage Lens 存储统计管理工具的可信访问权限。 | `organizations:DisableAWSServiceAccess` |
| 注册委托管理员，为您的组织创建 S3 Storage Lens 存储统计管理工具控制面板或配置。 | `organizations:RegisterDelegatedAdministrator` |
| 取消注册委托管理员，这样他们就无法再为您的组织创建 S3 Storage Lens 存储统计管理工具控制面板或配置。 | `organizations:DeregisterDelegatedAdministrator` |
| 创建 S3 Storage Lens 存储统计管理工具组织范围配置的其他权限。 | `organizations:DescribeOrganization`<br>`organizations:ListAccounts`<br>`organizations:ListAWSServiceAccessForOrganization`<br>`organizations:ListDelegatedAdministrators`<br>`iam:CreateServiceLinkedRole` |

## 通过控制台和 API 使用 Amazon S3 Storage Lens 存储统计管理工具

Amazon S3 Storage Lens 存储统计管理工具是一项云存储分析功能，您可以使用它在整个组织范围内了解对象存储的使用情况和活动。您可以使用 S3 Storage Lens 存储统计管理工具指标生成摘要见解，例如，了解整个组织中有多少存储空间，或增长最快的桶和前缀是哪些。您还可以使用 S3 Storage

Lens 存储统计管理工具指标来识别成本优化机会，实施数据保护和安全最佳实践，并提高应用程序工作负载的性能。例如，您可以识别没有 S3 生命周期规则的桶，使超过 7 天的未完成分段上传过期。您还可以识别未遵循数据保护最佳实践（例如使用 S3 复制或 S3 版本控制）的桶。S3 Storage Lens 存储统计管理工具还分析指标以提供上下文建议，您可以使用这些建议来优化存储成本并应用最佳实践来保护数据。

S3 Storage Lens 存储统计管理工具聚合您的指标，并在 Amazon S3 控制台的 Buckets（桶）页上的 Account snapshot（账户快照）部分中显示此信息。S3 Storage Lens 存储统计管理工具还提供了一个交互式控制面板，您可以使用它来可视化见解和趋势，标记异常值，并接收有关优化存储成本和应用数据保护最佳实践的建议。控制面板提供深入分析选项，用于在组织、账户、Amazon Web Services 区域、存储类、存储桶、前缀或 Storage Lens 组级别生成和可视化见解。您还可以将采用 CSV 或 Parquet 格式的每日指标导出发送到 S3 存储桶。

以下部分包含创建、更新和查看 S3 Storage Lens 存储统计管理工具配置以及执行与该功能相关的操作的示例。如果您在 Amazon Organizations 中使用 S3 Storage Lens 存储统计管理工具，这些示例还涵盖了这些使用案例。在这些示例中，将任何变量值替换为符合您要求的变量值。

主题


- 创建 Amazon S3 Storage Lens 存储统计管理工具控制面板
- 更新 Amazon S3 Storage Lens 存储统计管理工具控制面板
- 禁用 Amazon S3 Storage Lens 存储统计管理工具控制面板
- 删除 Amazon S3 Storage Lens 存储统计管理工具控制面板
- 列出 Amazon S3 Storage Lens 存储统计管理工具控制面板
- 查看 Amazon S3 Storage Lens 存储统计管理工具控制面板配置详细信息
- 使用 S3 Storage Lens 存储统计管理工具管理 Amazon 资源标签
- 使用 Amazon S3 Storage Lens 存储统计管理工具的帮助程序文件


## 创建 Amazon S3 Storage Lens 存储统计管理工具控制面板

可以创建其它 S3 Storage Lens 存储统计管理工具自定义控制面板，其范围可以限定为涵盖 Amazon Organizations 中您的组织，或者账户中的特定 Amazon Web Services 区域或存储桶。

> **Note**
>
> 对控制面板配置所做的任何更新最长可能需要 48 小时才能准确显示或可视化。

使用 S3 控制台

使用以下步骤在 Amazon S3 控制台中创建 Amazon S3 Storage Lens 存储统计管理工具控制面板。

步骤 1：定义控制面板范围

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在页面顶部的导航栏中，选择当前所显示 Amazon 区域的名称。接下来，选择要切换到的区域。
3. 在导航窗格中，在 S3 Storage Lens 存储统计管理工具下选择控制面板。
4. 选择创建控制面板。
5. 在控制面板页面的常规部分中，执行以下操作：

   a. 查看控制面板的主区域。主区域是在其中存储此 Storage Lens 存储分析功能控制面板的配置和指标的 Amazon Web Services 区域。

   b. 输入控制面板名称。

      控制面板名称必须少于 65 个字符，且不得包含特殊字符或空格。

      > **Note**
      > 创建控制面板后，您无法更改此控制面板名称。

   c. 您可以选择将标签添加到控制面板。您可以使用标签管理控制面板的权限并跟踪 S3 Storage Lens 存储统计管理工具的成本。

      有关更多信息，请参阅《IAM 用户指南》中的使用资源标签控制访问以及 Amazon Billing 用户指南中的 Amazon 生成的成本分配标签。

      > **Note**
      > 您最多可以在控制面板配置中添加 50 个标签。

6. 在控制面板范围部分中，执行以下操作：

   a. 选择希望 S3 Storage Lens 存储统计管理工具在控制面板中包括或排除的区域和桶。

   b. 在所选区域中选择希望 S3 Storage Lens 存储统计管理工具包括或排除的桶。您可以包括或排除桶，但不能同时包括和排除桶。创建组织级控制面板时，此选项不可用。

> **Note**
>
> - 您可以包括或排除区域和桶。在组织中跨成员账户创建组织级控制面板时，此选项仅限于“区域”。
> - 您最多可以选择 50 个桶来包括或排除。

步骤 2：配置指标选择

1. 在指标选择部分，选择要为此控制面板聚合的指标类型。

   - 要包括在桶级别聚合且可用于 14 天查询的免费指标，请选择 Free Metrics（免费指标）。
   - 要启用高级指标和其他高级选项，请选择 Advanced metrics and recommendations（高级指标和建议）。这些选项包括高级前缀聚合、Amazon CloudWatch 发布和上下文建议。数据可查询 15 个月。高级指标和建议需要额外付费。有关更多信息，请参阅 Amazon S3 定价。

     有关高级指标和免费指标的更多信息，请参阅指标选择。

2. 在 Advanced metrics and recommendations features（高级指标和建议功能）下方，选择您要启用的选项：

   - Advanced metrics（高级指标）
   - CloudWatch publishing（CloudWatch 发布）
   - Prefix aggregation（前缀聚合）

> **Important**
>
> 如果您为 S3 Storage Lens 存储统计管理工具配置启用了前缀聚合，那么前缀级别的指标将不会发布到 CloudWatch。只有桶、账户和企业级 S3 Storage Lens 存储统计管理工具指标才会发布到 CloudWatch。

3. 如果您启用了 Advanced metrics（高级指标），请选择要在 S3 Storage Lens 存储统计管理工具控制面板中显示的 Advanced metrics categories（高级指标类别）：

   - 活动指标
   - Detailed status code metrics（详细的状态代码指标）

- Advanced cost optimization metrics（高级成本优化指标）
- Advanced data protection metrics（高级数据保护指标）

有关指标类别的更多信息，请参阅指标类别。要获得指标的完整列表，请参阅 Amazon S3 Storage Lens 存储统计管理工具指标词汇表。

4. 如果选择启用前缀聚合，请配置以下内容：

   a. 选择此控制面板的最小前缀阈值大小。

      例如，5% 的前缀阈值表示将聚合构成占桶的总存储大小 5% 或更大的前缀。

   b. 选择前缀名称。

      此设置指示评估前缀的最大级别数。前缀深度必须小于 10。

   c. 输入前缀分隔符字符。

      此值用来标识每个前缀级别。Amazon S3 中的原定设置值为 / 个字符，但是您的存储结构可能会使用其他分隔符字符。

（可选）步骤 3：导出控制面板的指标

1. 在 Metrics export（指标导出）部分中，要创建将每天放置在您选择的目标桶中的指标导出，请选择 Enable（启用）。

   指标导出为 CSV 或 Apache Parquet 格式。它代表的数据范围与 S3 Storage Lens 存储统计管理工具控制面板数据相同，但不包含建议。

2. 如果启用了指标导出，请选择每日指标导出的输出格式：CSV 或 Apache Parquet。

   Parquet 是 Hadoop 的开源文件格式，它以平面列格式存储嵌套数据。

3. 为您的指标导出选择目标 S3 桶。

   您可以在 S3 Storage Lens 存储统计管理工具控制面板的当前账户中选择桶。或者，如果您拥有目标桶权限和目标桶拥有者的账户 ID，则可以选择另一个 Amazon Web Services 账户。

4. 选择目标 S3 桶（格式：`s3://bucket-name/prefix`）。

   桶必须在 S3 Storage Lens 存储统计管理工具控制面板的主区域中。S3 控制台向您显示 Amazon S3 将添加到目标桶策略的 Destination bucket permission（目标桶权限）。Amazon S3 将更新目标桶上的桶策略，以允许 S3 在该桶中放置数据。

5. （可选）要对指标导出启用服务器端加密，请选择 Specify an encryption key（指定加密密钥）。然后，选择加密类型：Amazon S3 托式管密钥（SSE-S3）或 Amazon Key Management Service 密钥（SSE-KMS）。

   您可以在 Amazon S3 托管式密钥（SSE-S3）和 Amazon Key Management Service（Amazon KMS）密钥（SSE-KMS）之间进行选择。
6. （可选）要指定 Amazon KMS 密钥，必须选择 KMS 密钥或输入密钥 Amazon 资源名称（ARN）。

   如果您选择客户托管式密钥，则必须在 Amazon KMS 密钥策略中向 Amazon S3 Storage Lens 存储统计管理工具授予加密权限。有关更多信息，请参阅 使用 Amazon KMS key 加密您的指标导出。
7. 请选择创建控制面板。

使用 Amazon CLI

Example

以下示例命令创建带标签的 Amazon S3 Storage Lens 存储统计管理工具配置。要使用这些示例，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control put-storage-lens-configuration --account-id=111122223333 --
config-id=example-dashboard-configuration-id --region=us-east-1 --storage-lens-
configuration=file://./config.json --tags=file://./tags.json
```

Example

以下示例命令创建不带标签的 Amazon S3 Storage Lens 存储统计管理工具配置。要使用这些示例，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control put-storage-lens-configuration --account-id=222222222222 --config-
id=your-configuration-id --region=us-east-1 --storage-lens-configuration=file://./
config.json
```

使用适用于 Java 的 Amazon SDK

Example – 创建和更新 Amazon S3 Storage Lens 存储统计管理工具配置

以下示例在适用于 Java 的 SDK 中创建和更新 Amazon S3 Storage Lens 存储统计管理工具配置：

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.AccountLevel;
import com.amazonaws.services.s3control.model.ActivityMetrics;
import com.amazonaws.services.s3control.model.BucketLevel;
import com.amazonaws.services.s3control.model.CloudWatchMetrics;
import com.amazonaws.services.s3control.model.Format;
import com.amazonaws.services.s3control.model.Include;
import com.amazonaws.services.s3control.model.OutputSchemaVersion;
import com.amazonaws.services.s3control.model.PrefixLevel;
import com.amazonaws.services.s3control.model.PrefixLevelStorageMetrics;
import com.amazonaws.services.s3control.model.PutStorageLensConfigurationRequest;
import com.amazonaws.services.s3control.model.S3BucketDestination;
import com.amazonaws.services.s3control.model.SSES3;
import com.amazonaws.services.s3control.model.SelectionCriteria;
import com.amazonaws.services.s3control.model.StorageLensAwsOrg;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;
import com.amazonaws.services.s3control.model.StorageLensDataExport;
import com.amazonaws.services.s3control.model.StorageLensDataExportEncryption;
import com.amazonaws.services.s3control.model.StorageLensTag;

import java.util.Arrays;
import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class CreateAndUpdateDashboard {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "111122223333";
        String exportAccountId = "Destination Account ID";
        String exportBucketArn = "arn:aws:s3:::destBucketName"; // The destination
 bucket for your metrics export must be in the same Region as your S3 Storage Lens
 configuration.
        String awsOrgARN = "arn:aws:organizations::123456789012:organization/o-
abcdefgh";
        Format exportFormat = Format.CSV;
```

```
        try {
            SelectionCriteria selectionCriteria = new SelectionCriteria()
                    .withDelimiter("/")
                    .withMaxDepth(5)
                    .withMinStorageBytesPercentage(10.0);
            PrefixLevelStorageMetrics prefixStorageMetrics = new
PrefixLevelStorageMetrics()
                    .withIsEnabled(true)
                    .withSelectionCriteria(selectionCriteria);
            BucketLevel bucketLevel = new BucketLevel()
                    .withActivityMetrics(new ActivityMetrics().withIsEnabled(true))
                    .withAdvancedCostOptimizationMetrics(new
AdvancedCostOptimizationMetrics().withIsEnabled(true))
                    .withAdvancedDataProtectionMetrics(new
AdvancedDataProtectionMetrics().withIsEnabled(true))
                    .withDetailedStatusCodesMetrics(new
DetailedStatusCodesMetrics().withIsEnabled(true))
                    .withPrefixLevel(new
PrefixLevel().withStorageMetrics(prefixStorageMetrics));
            AccountLevel accountLevel = new AccountLevel()
                    .withActivityMetrics(new ActivityMetrics().withIsEnabled(true))
                    .withAdvancedCostOptimizationMetrics(new
AdvancedCostOptimizationMetrics().withIsEnabled(true))
                    .withAdvancedDataProtectionMetrics(new
AdvancedDataProtectionMetrics().withIsEnabled(true))
                    .withDetailedStatusCodesMetrics(new
DetailedStatusCodesMetrics().withIsEnabled(true))
                    .withBucketLevel(bucketLevel);

            Include include = new Include()
                    .withBuckets(Arrays.asList("arn:aws:s3:::bucketName"))
                    .withRegions(Arrays.asList("us-west-2"));

            StorageLensDataExportEncryption exportEncryption = new
StorageLensDataExportEncryption()
                    .withSSES3(new SSES3());
            S3BucketDestination s3BucketDestination = new S3BucketDestination()
                    .withAccountId(exportAccountId)
                    .withArn(exportBucketArn)
                    .withEncryption(exportEncryption)
                    .withFormat(exportFormat)
                    .withOutputSchemaVersion(OutputSchemaVersion.V_1)
                    .withPrefix("Prefix");
```

```
            CloudWatchMetrics cloudWatchMetrics = new CloudWatchMetrics()
                    .withIsEnabled(true);
            StorageLensDataExport dataExport = new StorageLensDataExport()
                    .withCloudWatchMetrics(cloudWatchMetrics)
                    .withS3BucketDestination(s3BucketDestination);

            StorageLensAwsOrg awsOrg = new StorageLensAwsOrg()
                    .withArn(awsOrgARN);

            StorageLensConfiguration configuration = new StorageLensConfiguration()
                    .withId(configurationId)
                    .withAccountLevel(accountLevel)
                    .withInclude(include)
                    .withDataExport(dataExport)
                    .withAwsOrg(awsOrg)
                    .withIsEnabled(true);

            List<StorageLensTag> tags = Arrays.asList(
                    new StorageLensTag().withKey("key-1").withValue("value-1"),
                    new StorageLensTag().withKey("key-2").withValue("value-2")
            );

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.putStorageLensConfiguration(new
PutStorageLensConfigurationRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
                    .withStorageLensConfiguration(configuration)
                    .withTags(tags)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
```

```
}
```

要进一步了解您的存储，您可以创建一个或多个 S3 Storage Lens 组并将它们附加到您的控制面板。S3 Storage Lens 组是基于前缀、后缀、对象标签、对象大小、对象龄期或这些筛选条件的组合的自定义对象筛选条件。

您可以使用 S3 Storage Lens 组获得对大型共享桶（例如数据湖）的精细可见性，从而做出更明智的业务决策。例如，您可以将存储使用情况细分到一个或多个桶中各个项目和成本中心的特定对象组，从而简化存储分配并优化成本报告。

要使用 S3 Storage Lens 组，您必须升级控制面板以使用高级指标和建议。有关 S3 Storage Lens 组的更多信息，请参阅 the section called “使用 Storage Lens 组”。

## 更新 Amazon S3 Storage Lens 存储统计管理工具控制面板

Amazon S3 Storage Lens 存储统计管理工具默认控制面板是 `default-account-dashboard`。此控制面板由 Amazon S3 预配置，可帮助您在控制台上直观显示整个账户的聚合费用和高级指标的汇总见解和趋势。您无法修改原定设置控制面板的配置范围，但是您可以将指标选择从免费指标升级到付费的高级指标和建议，配置可选指标导出，甚至可以禁用原定设置控制面板。无法删除默认控制面板，而只能禁用它。有关更多信息，请参阅 使用 S3 控制台。

使用 S3 控制台

使用以下步骤在 Amazon S3 控制台中更新 Amazon S3 Storage Lens 存储统计管理工具控制面板。

步骤 1：更新控制面板范围

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Storage Lens（Storage Lens 存储统计管理工具）和 Dashboards（控制面板）。
3. 请选择要编辑的控制面板，然后选择 Edit（编辑）。

   此时将打开 Edit dashboard（编辑控制面板）页。

> **Note**
>
> 不能更改以下内容：

- 控制面板名称
- 主区域
- 原定设置控制面板的控制面板范围，其范围限于整个账户的存储

4. （可选）在控制面板配置页面上的 General（常规）部分中，更新标签并向控制面板添加标签。

   您可以使用标签来管理控制面板的权限和跟踪 S3 Storage Lens 存储统计管理工具的成本。有关更多信息，请参阅《IAM 用户指南》中的使用资源标签控制访问以及 Amazon Billing 用户指南中的 Amazon 生成的成本分配标签。

   > **Note**
   >
   > 您最多可以在控制面板配置中添加 50 个标签。

5. 在控制面板范围部分中，执行以下操作：

   a. 更新希望 S3 Storage Lens 存储统计管理工具在控制面板中包含或排除的区域和桶。

   > **Note**
   >
   > - 您可以包括或排除区域和桶。在组织中跨成员账户创建组织级控制面板时，此选项仅限于“区域”。
   > - 您最多可以选择 50 个桶来包括或排除。

   b. 更新您希望 S3 Storage Lens 存储统计管理工具包含或排除的选定区域中的桶。您可以包括或排除桶，但不能同时包括和排除桶。创建组织级控制面板时，此选项不存在。

步骤 2：更新指标选择

1. 在指标选择部分，选择要为此控制面板聚合的指标类型。

   - 要包括在桶级别聚合且可用于 14 天查询的免费指标，请选择 Free Metrics（免费指标）。
   - 要启用高级指标和其他高级选项，请选择 Advanced metrics and recommendations（高级指标和建议）。这些选项包括高级前缀聚合、Amazon CloudWatch 发布和上下文建议。数据可查询 15 个月。高级指标和建议需要额外付费。有关更多信息，请参阅 Amazon S3 定价。

     有关高级指标和免费指标的更多信息，请参阅指标选择。

2. 在 Advanced metrics and recommendations features（高级指标和建议功能）下方，选择您要启用的选项：

   - Advanced metrics（高级指标）
   - CloudWatch publishing（CloudWatch 发布）
   - Prefix aggregation（前缀聚合）

   > **Important**
   >
   > 如果您为 S3 Storage Lens 存储统计管理工具配置启用了前缀聚合，那么前缀级别的指标将不会发布到 CloudWatch。只有桶、账户和企业级 S3 Storage Lens 存储统计管理工具指标才会发布到 CloudWatch。

3. 如果您启用了 Advanced metrics（高级指标），请选择要在 S3 Storage Lens 存储统计管理工具控制面板中显示的 Advanced metrics categories（高级指标类别）：

   - 活动指标
   - Detailed status code metrics（详细的状态代码指标）
   - Advanced cost optimization metrics（高级成本优化指标）
   - Advanced data protection metrics（高级数据保护指标）

   有关指标类别的更多信息，请参阅指标类别。要获得指标的完整列表，请参阅 Amazon S3 Storage Lens 存储统计管理工具指标词汇表。

4. 如果选择启用前缀聚合，请配置以下内容：

   a. 选择此控制面板的最小前缀阈值大小。

      例如，5% 的前缀阈值表示将聚合构成占桶的总存储大小 5% 或更大的前缀。

   b. 选择前缀名称。

      此设置指示评估前缀的最大级别数。前缀深度必须小于 10。

   c. 输入前缀分隔符字符。

      这是用来标识每个前缀级别的值。Amazon S3 中的原定设置值为 / 个字符，但是您的存储结构可能会使用其他分隔符字符。

（可选）步骤 3：导出控制面板的指标

1. 在 Metrics export（指标导出）部分中，要创建将每天放置在您选择的目标桶中的指标导出，请选择 Enable（启用）。要禁用指标导出，请选择 Disable（禁用）。

   指标导出为 CSV 或 Apache Parquet 格式。它代表的数据范围与 S3 Storage Lens 存储统计管理工具控制面板数据相同，但不包含建议。

2. 如果启用，请选择每日指标导出的输出格式：CSV 或 Apache Parquet。

   Parquet 是 Hadoop 的开源文件格式，它以平面列格式存储嵌套数据。

3. 为您的指标导出选择目标 S3 桶。

   您可以在 S3 Storage Lens 存储统计管理工具控制面板的当前账户中选择桶。或者，如果您拥有目标桶权限和目标桶拥有者的账户 ID，则可以选择另一个 Amazon Web Services 账户。

4. 选择目标 S3 桶（格式：`s3://bucket-name/prefix`）。

   桶必须在 S3 Storage Lens 存储统计管理工具控制面板的主区域中。S3 控制台向您显示 Amazon S3 将添加到目标桶策略的 Destination bucket permission（目标桶权限）。Amazon S3 将更新目标桶上的桶策略，以允许 S3 在该桶中放置数据。

5. （可选）要对指标导出启用服务器端加密，请选择 Specify an encryption key（指定加密密钥）。然后，选择加密类型：Amazon S3 托式管密钥（SSE-S3）或 Amazon Key Management Service 密钥（SSE-KMS）。

   您可以在 Amazon S3 托管式密钥（SSE-S3）和 Amazon Key Management Service（Amazon KMS）密钥（SSE-KMS）之间进行选择。

6. （可选）要指定 Amazon KMS 密钥，必须选择 KMS 密钥或输入密钥 Amazon 资源名称（ARN）。在 Amazon KMS 密钥下，通过以下方式之一指定您的 KMS 密钥：

   - 要从可用的 KMS 密钥列表中进行选择，请选择从您的 Amazon KMS keys 密钥中进行选择，并从可用密钥的列表中选择您的 KMS 密钥。

     Amazon 托管式密钥 (aws/s3) 和您的客户自主管理型密钥都显示在此列表中。有关客户自主管理型密钥的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的客户密钥和 Amazon 密钥。

> **Note**
>
> 使用 S3 Storage Lens 存储统计管理工具进行的 SSE-KMS 加密不支持 Amazon 托管式密钥（aws/S3）。

- 要输入 KMS 密钥 ARN，请选择输入 Amazon KMS key ARN，然后在显示的字段中输入您的 KMS 密钥 ARN。
- 要在 Amazon KMS 控制台中创建新的客户自主管理型密钥，请选择创建 KMS 密钥。

  如果您选择客户托管式密钥，则必须在 Amazon KMS 密钥策略中向 Amazon S3 Storage Lens 存储统计管理工具授予加密权限。有关更多信息，请参阅 使用 Amazon KMS key 加密您的指标导出。

  有关创建 Amazon KMS key 的更多信息，请参阅 Amazon Key Management Service 开发人员指南中的创建密钥。

7. 选择保存更改。

要进一步了解您的存储，您可以创建一个或多个 S3 Storage Lens 组并将它们附加到您的控制面板。S3 Storage Lens 组是基于前缀、后缀、对象标签、对象大小、对象龄期或这些筛选条件的组合的自定义对象筛选条件。

您可以使用 S3 Storage Lens 组获得对大型共享桶（例如数据湖）的精细可见性，从而做出更明智的业务决策。例如，您可以将存储使用情况细分到一个或多个桶中各个项目和成本中心的特定对象组，从而简化存储分配并优化成本报告。

要使用 S3 Storage Lens 组，您必须升级控制面板以使用高级指标和建议。有关 S3 Storage Lens 组的更多信息，请参阅 the section called “使用 Storage Lens 组”。

使用 Amazon CLI

Example

以下示例命令更新 Amazon S3 Storage Lens 存储统计管理工具控制面板配置。要使用这些示例，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control put-storage-lens-configuration --account-id=111122223333 --
config-id=example-dashboard-configuration-id --region=us-east-1 --storage-lens-
configuration=file://./config.json --tags=file://./tags.json
```

使用适用于 Java 的 Amazon SDK

Example – 使用高级指标和建议更新默认 Amazon S3 Storage Lens 存储统计管理工具配置

以下示例显示了如何在适用于 Java 的 SDK 中使用高级指标和建议来更新默认 S3 Storage Lens 存储统计管理工具配置。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.AccountLevel;
import com.amazonaws.services.s3control.model.ActivityMetrics;
import com.amazonaws.services.s3control.model.BucketLevel;
import com.amazonaws.services.s3control.model.Format;
import com.amazonaws.services.s3control.model.Include;
import com.amazonaws.services.s3control.model.OutputSchemaVersion;
import com.amazonaws.services.s3control.model.PrefixLevel;
import com.amazonaws.services.s3control.model.PrefixLevelStorageMetrics;
import com.amazonaws.services.s3control.model.PutStorageLensConfigurationRequest;
import com.amazonaws.services.s3control.model.S3BucketDestination;
import com.amazonaws.services.s3control.model.SSES3;
import com.amazonaws.services.s3control.model.SelectionCriteria;
import com.amazonaws.services.s3control.model.StorageLensAwsOrg;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;
import com.amazonaws.services.s3control.model.StorageLensDataExport;
import com.amazonaws.services.s3control.model.StorageLensDataExportEncryption;
import com.amazonaws.services.s3control.model.StorageLensTag;

import java.util.Arrays;
import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class UpdateDefaultConfigWithPaidFeatures {

    public static void main(String[] args) {
        String configurationId = "default-account-dashboard"; // This configuration ID
 cannot be modified.
        String sourceAccountId = "111122223333";
```

```
        try {
            SelectionCriteria selectionCriteria = new SelectionCriteria()
                    .withDelimiter("/")
                    .withMaxDepth(5)
                    .withMinStorageBytesPercentage(10.0);
            PrefixLevelStorageMetrics prefixStorageMetrics = new
PrefixLevelStorageMetrics()
                    .withIsEnabled(true)
                    .withSelectionCriteria(selectionCriteria);
            BucketLevel bucketLevel = new BucketLevel()
                    .withActivityMetrics(new ActivityMetrics().withIsEnabled(true))
                    .withPrefixLevel(new
PrefixLevel().withStorageMetrics(prefixStorageMetrics));
            AccountLevel accountLevel = new AccountLevel()
                    .withActivityMetrics(new ActivityMetrics().withIsEnabled(true))
                    .withBucketLevel(bucketLevel);

            StorageLensConfiguration configuration = new StorageLensConfiguration()
                    .withId(configurationId)
                    .withAccountLevel(accountLevel)
                    .withIsEnabled(true);

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.putStorageLensConfiguration(new
PutStorageLensConfigurationRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
                    .withStorageLensConfiguration(configuration)
            );

        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
```

```
}
```

> **Note**
>
> 高级指标和建议需支付额外费用。有关详细信息，请参阅高级指标和建议。

## 禁用 Amazon S3 Storage Lens 存储统计管理工具控制面板

可以从 Amazon S3 控制台中禁用 Amazon S3 Storage Lens 存储统计管理工具控制面板。禁用控制面板会阻止其将来生成指标。禁用的控制面板仍会保留其配置信息，以便重新启用后可以轻松恢复。禁用的控制面板将保留其历史数据，直到其不再可用于查询。

使用 S3 控制台

使用以下步骤在 Amazon S3 控制台中禁用 Amazon S3 Storage Lens 存储统计管理工具控制面板。

禁用 Amazon S3 Storage Lens 存储统计管理工具控制面板

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Storage Lens 和 Dashboards（控制面板）。
3. 在控制面板列表中，选择要禁用的控制面板，然后选择列表顶部的禁用。
4. 在确认页面上，通过在文本字段中输入控制面板名称来确认要禁用控制面板，然后选择确认。

## 删除 Amazon S3 Storage Lens 存储统计管理工具控制面板

您无法删除原定设置控制面板。但是，您可以将其禁用。删除您创建的控制面板之前，请考虑以下事项：

- 作为删除控制面板的替代方法，您可以禁用控制面板，以便将来可以重新启用该控制面板。有关更多信息，请参阅 使用 S3 控制台。
- 删除控制面板将删除与其关联的所有配置设置。
- 删除控制面板将使所有历史指标数据不可用。这些历史数据仍会保留 15 个月。如果您想再次访问此数据，请在与删除控制面板相同的主区域中以相同名称创建一个控制面板。

使用 S3 控制台

可以从 Amazon S3 控制台中删除 Amazon S3 Storage Lens 存储统计管理工具控制面板。但是，删除控制面板会阻止其将来生成指标。

删除 Amazon S3 Storage Lens 存储统计管理工具控制面板

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Storage Lens 和 Dashboards（控制面板）。
3. 在控制面板列表中，选择要删除的控制面板，然后选择列表顶部的删除。
4. 在删除控制面板页面上，通过在文本字段中输入控制面板名称来确认要删除控制面板。然后，选择 Confirm（确认）。

使用 Amazon CLI

Example

以下示例删除 S3 Storage Lens 存储统计管理工具配置。要使用这些示例，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control delete-storage-lens-configuration --account-id=222222222222 --region=us-east-1 --config-id=your-configuration-id
```

使用适用于 Java 的 Amazon SDK

Example – 删除 Amazon S3 Storage Lens 存储统计管理工具控制面板配置

以下示例显示了如何使用适用于 Java 的 SDK 来删除 S3 Storage Lens 存储统计管理工具配置：

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.DeleteStorageLensConfigurationRequest;
```

```
import static com.amazonaws.regions.Regions.US_WEST_2;

public class DeleteDashboard {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "111122223333";
        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.deleteStorageLensConfiguration(new
 DeleteStorageLensConfigurationRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

## 列出 Amazon S3 Storage Lens 存储统计管理工具控制面板

### 使用 S3 控制台

列出 S3 Storage Lens 存储统计管理工具控制面板

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，导航到 Storage Lens 存储统计管理工具。
3. 选择控制面板。现在，您可以在 Amazon Web Services 账户中查看控制面板。

使用 Amazon CLI

Example

以下示例命令列出了 Amazon Web Services 账户中的 S3 Storage Lens 存储统计管理工具控制面板。要使用这些示例，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control list-storage-lens-configurations --account-id=222222222222 --region=us-east-1 --next-token=abcdefghij1234
```

Example

以下示例列出了没有下一个令牌的 S3 Storage Lens 存储统计管理工具配置。要使用这些示例，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control list-storage-lens-configurations --account-id=222222222222 --region=us-east-1
```

使用适用于 Java 的 Amazon SDK

Example – 列出 S3 Storage Lens 存储统计管理工具控制面板配置

以下示例显示了如何在适用于 Java 的 SDK 中列出 S3 Storage Lens 存储统计管理工具配置。要使用此示例，请将每个示例描述中的 *user input placeholders* 替换为 您自己的信息。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.ListStorageLensConfigurationEntry;
import com.amazonaws.services.s3control.model.ListStorageLensConfigurationsRequest;

import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class ListDashboard {

    public static void main(String[] args) {
```

```
        String sourceAccountId = "111122223333";
        String nextToken = "nextToken";

        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            final List<ListStorageLensConfigurationEntry> configurations =
                    s3ControlClient.listStorageLensConfigurations(new
 ListStorageLensConfigurationsRequest()
                            .withAccountId(sourceAccountId)
                            .withNextToken(nextToken)
                    ).getStorageLensConfigurationList();

            System.out.println(configurations.toString());
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

## 查看 Amazon S3 Storage Lens 存储统计管理工具控制面板配置详细信息

可以从 Amazon S3 控制台、Amazon CLI 和适用于 Java 的 SDK 中查看 Amazon S3 Storage Lens 存储统计管理工具控制面板。

使用 S3 控制台

查看 S3 Storage Lens 存储统计管理工具控制面板配置详细信息

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，导航到 Storage Lens 存储统计管理工具。
3. 选择控制面板。

4. 从控制面板列表中，单击您要查看的控制面板。现在，您可以查看 Storage Lens 存储统计管理工具控制面板的详细信息。

使用 Amazon CLI

Example

以下示例检索 S3 Storage Lens 存储统计管理工具配置，以便您可以查看配置详细信息。要使用这些示例，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control get-storage-lens-configuration --account-id=222222222222 --config-
id=your-configuration-id --region=us-east-1
```

使用适用于 Java 的 Amazon SDK

Example – 检索和查看 S3 Storage Lens 存储统计管理工具配置

以下示例显示了如何在适用于 Java 的 SDK 中检索 S3 Storage Lens 存储统计管理工具配置，以便您可以查看配置详细信息。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.GetStorageLensConfigurationRequest;
import com.amazonaws.services.s3control.model.GetStorageLensConfigurationResult;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class GetDashboard {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "111122223333";

        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
```

```
                    .withRegion(US_WEST_2)
                    .build();

            final StorageLensConfiguration configuration =
                    s3ControlClient.getStorageLensConfiguration(new
 GetStorageLensConfigurationRequest()
                            .withAccountId(sourceAccountId)
                            .withConfigId(configurationId)
                    ).getStorageLensConfiguration();

            System.out.println(configuration.toString());
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

## 使用 S3 Storage Lens 存储统计管理工具管理 Amazon 资源标签

每个 Amazon S3 Storage Lens 存储统计管理工具控制面板都计为一项 Amazon 资源，具有其自己的 Amazon 资源名称（ARN）。因此，在配置 Storage Lens 存储统计管理工具控制面板时，可以选择向控制面板添加 Amazon 资源标签。最多可以为每个 Storage Lens 存储统计管理工具控制面板添加 50 个标签。要创建带标签的 Storage Lens 存储统计管理工具控制面板，您必须拥有以下 S3 Storage Lens 存储统计管理工具权限：

- `s3:ListStorageLensConfigurations`
- `s3:GetStorageLensConfiguration`
- `s3:GetStorageLensConfigurationTagging`
- `s3:PutStorageLensConfiguration`
- `s3:PutStorageLensConfigurationTagging`

您可以使用 Amazon 资源标签根据部门、业务线或项目对资源进行分类。这在您有许多相同类型的资源时会非常有用。通过应用标签，可以根据分配给特定 S3 Storage Lens 存储统计管理工具控制面板的标签，来快速识别该控制面板。您还可以使用标签对成本进行跟踪和分配。

此外，当您向 Storage Lens 存储统计管理工具控制面板添加 Amazon 资源标签时，将激活基于属性的访问权限控制（ABAC）。ABAC 是一种基于属性（如标签）定义权限的授权策略。您还可以在 IAM policy 中使用指定资源标签的条件，从而控制对 Amazon 资源的访问。

您可以修改标签的键和值，还可以随时删除资源的标签。此外，请注意以下限制：

- 标签键和标签值区分大小写。
- 如果您添加的标签的值与该实例上现有标签的值相同，新的值就会覆盖旧值。
- 如果删除资源，资源的所有标签也会被删除。
- 不要在 Amazon 资源标签中包含隐私或敏感数据。
- 不支持系统标签（标签键以 `aws:` 开头）。
- 每个标签键的长度不能超过 128 个字符。每个标签值的长度不能超过 256 个字符。

以下示例演示如何将 Amazon 资源标签与 Storage Lens 存储统计管理工具控制面板结合使用。

主题

- 将 Amazon 资源标签添加到 Storage Lens 存储统计管理工具控制面板
- 检索 Storage Lens 存储统计管理工具控制面板的 Amazon 资源标签
- 更新 Storage Lens 存储统计管理工具控制面板标签
- 从 S3 Storage Lens 存储统计管理工具控制面板中删除 Amazon 资源标签

### 将 Amazon 资源标签添加到 Storage Lens 存储统计管理工具控制面板

以下示例演示如何将 Amazon 资源标签添加到 S3 Storage Lens 存储统计管理工具控制面板。您可以使用 Amazon S3 控制台、Amazon Command Line Interface (Amazon CLI) 和 适用于 Java 的 Amazon SDK 添加资源标签。

#### 使用 S3 控制台

将 Amazon 资源标签添加到 Storage Lens 存储统计管理工具控制面板

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，导航到 Storage Lens 存储统计管理工具。
3. 选择控制面板。
4. 选择您要更新的 Storage Lens 存储统计管理工具控制面板的单选按钮。然后选择 Edit（编辑）。

5. 在常规下，选择添加标签。
6. 在添加标签页面上，添加新的键值对。

> **Note**
>
> 如果添加的新标签与现有标签具有相同的键，则将覆盖之前的标签值。

7. （可选）要添加多个新标签，请再次选择添加标签以继续添加新条目。最多可以将 50 个 Amazon 资源标签添加到 Storage Lens 存储统计管理工具控制面板。
8. （可选）如果要移除新添加的条目，请选择要移除的标签旁的移除。
9. 选择保存更改。

使用 Amazon CLI

Example

以下示例命令将标签添加到 S3 Storage Lens 存储统计管理工具控制面板配置。要使用这些示例，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control put-storage-lens-configuration-tagging --account-id=222222222222 --
region=us-east-1 --config-id=your-configuration-id --tags=file://./tags.json
```

使用适用于 Java 的 Amazon SDK

以下示例命令在适用于 Java 的 SDK 中将标签添加到 Amazon S3 Storage Lens 存储统计管理工具配置。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

Example – 将标签添加到 S3 Storage Lens 存储统计管理工具配置

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import
 com.amazonaws.services.s3control.model.PutStorageLensConfigurationTaggingRequest;
import com.amazonaws.services.s3control.model.StorageLensTag;
```

```
import java.util.Arrays;
import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class PutDashboardTagging {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "111122223333";

        try {
            List<StorageLensTag> tags = Arrays.asList(
                    new StorageLensTag().withKey("key-1").withValue("value-1"),
                    new StorageLensTag().withKey("key-2").withValue("value-2")
            );

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.putStorageLensConfigurationTagging(new
 PutStorageLensConfigurationTaggingRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
                    .withTags(tags)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

检索 Storage Lens 存储统计管理工具控制面板的 Amazon 资源标签

以下示例演示如何检索 S3 Storage Lens 存储统计管理工具控制面板的 Amazon 资源标签。可以使用 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）和适用于 Java 的 Amazon SDK 来获取资源标签。

使用 S3 控制台

检索 Storage Lens 存储统计管理工具控制面板的 Amazon 资源标签

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，导航到 Storage Lens 存储统计管理工具。
3. 选择控制面板。
4. 选择您要查看的 Storage Lens 存储统计管理工具控制面板配置的单选按钮。然后，选择查看控制面板配置。
5. 在标签下，查看与控制面板关联的标签。
6. （可选）如果要添加新标签，请选择编辑。然后选择添加标签。在添加标签页面上，添加新的键值对。

   > **Note**
   >
   > 如果添加的新标签与现有标签具有相同的键，则将覆盖之前的标签值。

7. （可选）如果要移除新添加的条目，请选择要移除的标签旁的移除。
8. 选择保存更改。

使用 Amazon CLI

Example

以下示例命令检索 S3 Storage Lens 存储统计管理工具控制面板配置的标签。要使用这些示例，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control get-storage-lens-configuration-tagging --account-id=222222222222 --
region=us-east-1 --config-id=your-configuration-id --tags=file://./tags.json
```

使用适用于 Java 的 Amazon SDK

Example – 获取 S3 Storage Lens 存储统计管理工具控制面板配置的标签

以下示例显示了如何在适用于 Java 的 SDK 中检索 S3 Storage Lens 存储统计管理工具控制面板配置的标签。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.DeleteStorageLensConfigurationRequest;
import
 com.amazonaws.services.s3control.model.GetStorageLensConfigurationTaggingRequest;
import com.amazonaws.services.s3control.model.StorageLensTag;

import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class GetDashboardTagging {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "111122223333";
        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            final List<StorageLensTag> s3Tags = s3ControlClient
                    .getStorageLensConfigurationTagging(new
 GetStorageLensConfigurationTaggingRequest()
                            .withAccountId(sourceAccountId)
                            .withConfigId(configurationId)
                    ).getTags();

            System.out.println(s3Tags.toString());
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
```

```
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

更新 Storage Lens 存储统计管理工具控制面板标签

以下示例演示如何使用 Amazon S3 控制台、Amazon Command Line Interface（Amazon CLI）和适用于 Java 的 Amazon SDK 更新 Storage Lens 存储统计管理工具控制面板标签。

使用 S3 控制台

更新 Storage Lens 存储统计管理工具控制面板的 Amazon 资源标签

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，导航到 Storage Lens 存储统计管理工具。
3. 选择控制面板。
4. 选择您要查看的 Storage Lens 存储统计管理工具控制面板配置的单选按钮。然后，选择查看控制面板配置。
5. 在标签下，查看与控制面板关联的标签。
6. （可选）如果要添加新标签，请选择编辑。然后选择添加标签。在添加标签页面上，添加新的键值对。

   > **Note**
   >
   > 如果添加的新标签与现有标签具有相同的键，则将覆盖之前的标签值。

7. （可选）如果要移除新添加的条目，请选择要移除的标签旁的移除。
8. 选择保存更改。

使用 Amazon CLI

Example

以下示例命令添加或替换现有 Amazon S3 Storage Lens 存储统计管理工具控制面板配置上的标签。要使用这些示例，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control put-storage-lens-configuration-tagging --account-id=111122223333 --
config-id=example-dashboard-configuration-id --region=us-east-1 --config-id=your-
configuration-id
```

使用适用于 Java 的 Amazon SDK

以下适用于 Java 的 Amazon SDK 示例更新现有 Storage Lens 存储统计管理工具控制面板上的 Amazon 资源标签。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

Example – 更新现有 Storage Lens 存储统计管理工具控制面板配置上的标签

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import
 com.amazonaws.services.s3control.model.PutStorageLensConfigurationTaggingRequest;
import com.amazonaws.services.s3control.model.StorageLensTag;

import java.util.Arrays;
import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class PutDashboardTagging {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "111122223333";

        try {
            List<StorageLensTag> tags = Arrays.asList(
                    new StorageLensTag().withKey("key-1").withValue("value-1"),
```

```
                    new StorageLensTag().withKey("key-2").withValue("value-2")
            );

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.putStorageLensConfigurationTagging(new
 PutStorageLensConfigurationTaggingRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
                    .withTags(tags)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

从 S3 Storage Lens 存储统计管理工具控制面板中删除 Amazon 资源标签

以下示例演示如何从现有 Storage Lens 存储统计管理工具控制面板中删除 Amazon 资源标签。您可以使用 Amazon S3 控制台、Amazon Command Line Interface (Amazon CLI) 和 适用于 Java 的 Amazon SDK 删除标签。

使用 S3 控制台

从现有 Storage Lens 存储统计管理工具控制面板中删除 Amazon 资源标签

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，导航到 Storage Lens 存储统计管理工具。
3. 选择控制面板。
4. 选择您要查看的 Storage Lens 存储统计管理工具控制面板配置的单选按钮。然后，选择查看控制面板配置。

5. 在标签下，查看与控制面板关联的标签。
6. 选择要移除的标签旁边的移除。
7. 选择保存更改。

### 使用 Amazon CLI

以下 Amazon CLI 命令从现有的 Storage Lens 存储统计管理工具控制面板中删除 Amazon 资源标签。要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

Example

```
aws s3control delete-storage-lens-configuration-tagging --account-id=222222222222 --
config-id=your-configuration-id --region=us-east-1
```

### 使用适用于 Java 的 Amazon SDK

以下适用于 Java 的 Amazon SDK 示例使用您在账户 *111122223333* 中指定的 Amazon 资源名称（ARN），从 Storage Lens 存储统计管理工具控制面板中删除 Amazon 资源标签。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

Example – 删除 S3 Storage Lens 存储统计管理工具控制面板配置的标签

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import
 com.amazonaws.services.s3control.model.DeleteStorageLensConfigurationTaggingRequest;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class DeleteDashboardTagging {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "111122223333";
        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
```

```
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.deleteStorageLensConfigurationTagging(new
 DeleteStorageLensConfigurationTaggingRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

## 使用 Amazon S3 Storage Lens 存储统计管理工具的帮助程序文件

为您的示例使用以下 JSON 文件及其关键输入。

JSON 格式的 S3 Storage Lens 存储统计管理工具示例配置

Example **`config.json`**

`config.json` 文件包含 S3 Storage Lens 存储统计管理工具组织级高级指标和建议配置的详细信息。要使用以下示例，请将 *`user input placeholders`* 替换为您自己的信息。

> **Note**
>
> 高级指标和建议需支付额外费用。有关详细信息，请参阅高级指标和建议。

```
{
  "Id": "SampleS3StorageLensConfiguration", //Use this property to identify your S3
 Storage Lens configuration.
  "AwsOrg": { //Use this property when enabling S3 Storage Lens for Amazon
 Organizations.
    "Arn": "arn:aws:organizations::123456789012:organization/o-abcdefgh"
```

```
  },
  "AccountLevel": {
    "ActivityMetrics": {
      "IsEnabled":true
    },
    "AdvancedCostOptimizationMetrics": {
      "IsEnabled":true
    },
    "AdvancedDataProtectionMetrics": {
      "IsEnabled":true
    },
    "DetailedStatusCodesMetrics": {
      "IsEnabled":true
    },
    "BucketLevel": {
      "ActivityMetrics": {
        "IsEnabled":true
      },
      "AdvancedDataProtectionMetrics": {
      "IsEnabled":true
      },
      "AdvancedCostOptimizationMetrics": {
        "IsEnabled":true
      },
      "DetailedStatusCodesMetrics": {
        "IsEnabled":true
      },
      "PrefixLevel":{
        "StorageMetrics":{
          "IsEnabled":true,
          "SelectionCriteria":{
            "MaxDepth":5,
            "MinStorageBytesPercentage":1.25,
            "Delimiter":"/"
          }
        }
      }
    }
  },
  "Exclude": { //Replace with "Include" if you prefer to include Regions.
    "Regions": [
      "eu-west-1"
    ],
```

```
    "Buckets": [ //This attribute is not supported for Amazon Organizations-level
 configurations.
      "arn:aws:s3:::amzn-s3-demo-source-bucket"
    ]
  },
  "IsEnabled": true, //Whether the configuration is enabled
  "DataExport": { //Details about the metrics export
    "S3BucketDestination": {
      "OutputSchemaVersion": "V_1",
      "Format": "CSV", //You can add "Parquet" if you prefer.
      "AccountId": "111122223333",
      "Arn": "arn:aws:s3:::
amzn-s3-demo-destination-bucket", // The destination bucket for your metrics export
 must be in the same Region as your S3 Storage Lens configuration.
      "Prefix": "prefix-for-your-export-destination",
      "Encryption": {
        "SSES3": {}
      }
    },
    "CloudWatchMetrics": {
      "IsEnabled": true
    }
  }
}
```

JSON 格式的 S3 Storage Lens 存储统计管理工具示例配置（带 Storage Lens 组）

Example **config.json**

config.json 文件包含在使用 Storage Lens 组时，要应用于 Storage Lens 存储统计管理工具配置的详细信息。要使用该示例，请将 *user input placeholders* 替换为您自己的信息。

要将所有 Storage Lens 组附加到您的控制面板，请使用以下语法更新 Storage Lens 存储统计管理工具配置：

```
{
  "Id": "ExampleS3StorageLensConfiguration",
  "AccountLevel": {
    "ActivityMetrics": {
      "IsEnabled":true
    },
    "AdvancedCostOptimizationMetrics": {
      "IsEnabled":true
```

```
    },
    "AdvancedDataProtectionMetrics": {
      "IsEnabled":true
    },
    "BucketLevel": {
      "ActivityMetrics": {
      "IsEnabled":true
      },
    "StorageLensGroupLevel": {},
  "IsEnabled": true
}
```

要在 Storage Lens 存储统计管理工具控制面板配置中仅包含两个 Storage Lens 组（*slg-1* 和 *slg-2*），请使用以下语法：

```
{
  "Id": "ExampleS3StorageLensConfiguration",
  "AccountLevel": {
    "ActivityMetrics": {
      "IsEnabled":true
    },
    "AdvancedCostOptimizationMetrics": {
      "IsEnabled":true
    },
    "AdvancedDataProtectionMetrics": {
      "IsEnabled":true
    },
    "BucketLevel": {
      "ActivityMetrics": {
      "IsEnabled":true
      },
   "StorageLensGroupLevel": {
        "SelectionCriteria": {
            "Include": [
                "arn:aws:s3:us-east-1:111122223333:storage-lens-group/slg-1",
                "arn:aws:s3:us-east-1:444455556666:storage-lens-group/slg-2"
            ]
    },
  "IsEnabled": true
}
```

要仅将某些 Storage Lens 组排除在您的控制面板配置之外，请使用以下语法：

```
{
  "Id": "ExampleS3StorageLensConfiguration",
  "AccountLevel": {
    "ActivityMetrics": {
      "IsEnabled":true
    },
    "AdvancedCostOptimizationMetrics": {
      "IsEnabled":true
    },
    "AdvancedDataProtectionMetrics": {
      "IsEnabled":true
    },
    "BucketLevel": {
      "ActivityMetrics": {
      "IsEnabled":true
      },
   "StorageLensGroupLevel": {
        "SelectionCriteria": {
            "Exclude": [
                "arn:aws:s3:us-east-1:111122223333:storage-lens-group/slg-1",
                "arn:aws:s3:us-east-1:444455556666:storage-lens-group/slg-2"
            ]
    },
  "IsEnabled": true
}
```

JSON 格式的 S3 Storage Lens 存储统计管理工具示例标签配置

Example **tags.json**

tags.json 文件包含要应用于 S3 Storage Lens 存储统计管理工具配置的标签。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
[
    {
        "Key": "key1",
        "Value": "value1"
    },
    {
        "Key": "key2",
        "Value": "value2"
    }
```

```
]
```

S3 Storage Lens 存储统计管理工具示例配置 IAM 权限

Example **permissions.json** – 特定控制面板名称

此示例策略显示具有指定的特定控制面板名称的 S3 Storage Lens 存储统计管理工具 IAM permissions.json 文件。将 *value1*、*us-east-1*、*your-dashboard-name* 和 *example-account-id* 替换为您自己的值。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetStorageLensConfiguration",
                "s3:DeleteStorageLensConfiguration",
                "s3:PutStorageLensConfiguration"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/key1": "value1"
                }
            },
            "Resource": "arn:aws:s3:us-east-1:example-account-id:storage-lens/your-dashboard-name"
        }
    ]
}
```

Example **permissions.json** – 没有特定的控制面板名称

此示例策略显示了未指定特定控制面板名称的 S3 Storage Lens 存储统计管理工具 IAM permissions.json 文件。将 *value1*、*us-east-1* 和 *example-account-id* 替换为您自己的值。

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetStorageLensConfiguration",
                "s3:DeleteStorageLensConfiguration",
                "s3:PutStorageLensConfiguration"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/key1": "value1"
                }
            },
            "Resource": "arn:aws:s3:us-east-1:example-account-id:storage-lens/*"
        }
    ]
}
```

## 使用 Amazon S3 Storage Lens 存储统计管理工具查看指标

S3 Storage Lens 存储统计管理工具聚合您的指标，并在 Amazon S3 控制台的 Buckets（桶）页上的 Account snapshot（账户快照）部分中显示此信息。S3 Storage Lens 存储统计管理工具还提供了一个交互式控制面板，您可以使用它来可视化见解和趋势，标记异常值，并接收有关优化存储成本和应用数据保护最佳实践的建议。控制面板提供深入分析选项，用于在组织、账户、Amazon Web Services 区域、存储类、存储桶、前缀或 Storage Lens 组级别生成和可视化见解。您还可以将采用 CSV 或 Parquet 格式的每日指标导出发送到 S3 存储桶。

原定设置情况下，所有控制面板都配置了免费指标，其中包括可用于了解 S3 存储中的使用情况和活动、优化存储成本以及实施数据保护和访问管理最佳实践的指标。免费指标向下聚合到桶级别。使用免费指标，数据最多在 14 天内可供查询。

高级指标和建议包括以下附加功能，您可以使用这些功能进一步了解跨存储的使用情况和活动以及优化存储的最佳实践：

- 上下文建议（仅在控制台中提供）
- 高级指标（包括按桶聚合的活动指标）
- Prefix aggregation（前缀聚合）
- Storage Lens 组聚合
- Storage Lens 组聚合
- Amazon CloudWatch 发布

高级指标数据可供查询 15 个月。使用包含高级指标的 S3 Storage Lens 存储统计管理工具需要额外收费。有关更多信息，请参阅 Amazon S3 定价。有关免费和高级指标的更多信息，请参阅指标选择。

主题

- 在控制面板上查看 S3 Storage Lens 存储统计管理工具指标
- 使用数据导出查看 Amazon S3 Storage Lens 存储统计管理工具指标
- 在 CloudWatch 中监控 S3 Storage Lens 存储统计管理工具指标
- Amazon S3 Storage Lens 存储统计管理工具使用案例

## 在控制面板上查看 S3 Storage Lens 存储统计管理工具指标

在 Amazon S3 控制台中，S3 Storage Lens 存储统计管理工具提供了一个交互式默认控制面板，可用于可视化数据中的见解和趋势。您还可以使用此控制面板标记异常值，并接收有关优化存储成本和应用数据保护最佳实践的建议。控制面板提供深入分析选项，用于在账户、桶、Amazon Web Services 区域、前缀或 Storage Lens 组级别生成见解。如果您启用了 S3 Storage Lens 存储统计管理工具以与 Amazon Organizations 配合使用，您还可以生成组织级别的见解（例如 Amazon Organizations 层次结构中所有账户的数据）。控制面板始终加载指标可用的最新日期。

控制台上的 S3 Storage Lens 存储统计管理工具默认控制面板命名为 default-account-dashboard。Amazon S3 会预配置此控制面板，以可视化整个账户的汇总见解和趋势，并在 S3 控制台中每天更新这些信息。您无法修改默认控制面板的配置范围，但可以将指标选择从免费指标升级到付费的高级指标和建议。借助高级指标和建议，您可以访问其他指标和功能。这些功能包括高级指标类别、前缀级聚合、上下文建议和 Amazon CloudWatch 发布。

您可以禁用原定设置控制面板，但不能删除它。如果您禁用原定设置控制面板，则它将不再更新。您也将不会再在 S3 Storage Lens 存储统计管理工具或存续桶页面上的账户快照部分收到任何新的每日指标。在数据查询的 14 天期限到期之前，您仍然可以在原定设置控制面板中查看历史数据。如果您启用了高级指标和建议，则此期限为 15 个月。要访问此数据，您可以在有效期内重新启用原定设置控制面板。

您可以创建其它 S3 Storage Lens 存储统计管理工具控制面板，并按 Amazon Web Services 区域、S3 桶或账户限定其范围。如果您启用了 Storage Lens 存储统计管理工具以与 Amazon Organizations 配合使用，则还可以按组织限定控制面板的范围。创建或编辑 S3 Storage Lens 存储统计管理工具控制面板时，定义控制面板范围和指标选择。

您可以禁用或删除您创建的任何其他控制面板。

- 如果禁用控制面板，它将不再更新，并且您将不再收到任何新的每日指标。在 14 天有效期内，您仍然可以查看免费指标的历史数据。如果您为该控制面板启用了高级指标和建议，则此期限为 15 个月。要访问此数据，您可以在有效期内重新启用控制面板。
- 如果删除控制面板，将丢失所有控制面板的配置设置。您将不再收到任何新的每日指标，而且您也无法访问与该控制面板关联的历史数据。如果要访问已删除控制面板的历史数据，则必须在同一主区域中创建另一个具有相同名称的控制面板。

主题


- 查看 Amazon S3 Storage Lens 存储统计管理工具控制面板
- 了解 S3 Storage Lens 存储统计管理工具控制面板


## 查看 Amazon S3 Storage Lens 存储统计管理工具控制面板

以下过程显示如何在 S3 控制台中查看 S3 Storage Lens 存储统计管理工具控制面板。请参阅 Amazon S3 Storage Lens 存储统计管理工具使用案例 中基于应用场景的介绍，了解如何使用控制面板优化成本、实施最佳实践以及提高访问 S3 桶的应用程序的性能。

> **Note**
>
> 您不能使用账户的根用户凭证查看 Amazon S3 Storage Lens 存储统计管理工具控制面板。要访问 S3 Storage Lens 存储统计管理工具控制面板，您必须向新的或现有的 IAM 用户授予所需的 Amazon Identity and Access Management（IAM）权限。然后，使用这些用户凭证登录以访问 S3 Storage Lens 存储统计管理工具控制面板。有关更多信息，请参阅《IAM 用户指南》中的 设置 Amazon S3 Storage Lens 存储统计管理工具权限 和 IAM 中的安全最佳实践。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Storage Lens 和 Dashboards（控制面板）。
3. 在控制面板列表中，选择要查看的控制面板。

   控制面板在 S3 Storage Lens 存储统计管理工具中打开。Snapshot for date（日期的快照）部分显示 S3 Storage Lens 存储统计管理工具收集指标的最新日期。您的控制面板始终加载指标可用的最新日期。
4. （可选）要更改 S3 Storage Lens 存储统计管理工具控制面板的日期，请在右上角的日期选择器中选择一个新日期。

5. （可选）要应用临时筛选条件以进一步限制控制面板数据的范围，请执行以下操作：

   a. 展开筛选条件部分。

   b. 要按特定账户、Amazon Web Services 区域、存储类、桶、前缀或 Storage Lens 组进行筛选，请选择相应的筛选依据选项。

   > **Note**
   >
   > 不能同时应用前缀筛选条件和 Storage Lens 组筛选条件。

   c. 要更新筛选条件，请选择 Apply（应用）。

   d. 要移除筛选条件，请单击筛选条件旁的 X。

6. 在 S3 Storage Lens 存储统计管理工具控制面板的任何部分中，要查看特定指标的数据，请为 Metric（指标）选择指标名称。

7. 在 S3 Storage Lens 存储统计管理工具控制面板中的任何图表或可视化效果中，您都可以使用账户、Amazon Web Services 区域、存储类、存储桶、前缀或 Storage Lens 组选项卡，深入到更深层次的聚合。有关示例，请参阅发现冷的 Amazon S3 桶。

### 了解 S3 Storage Lens 存储统计管理工具控制面板

S3 Storage Lens 存储统计管理工具控制面板具有一个主要的 Overview（概览）选项卡，以及表示每个聚合级别的最多五个附加选项卡：

- 账户
- Amazon Web Services 区域
- 存储类
- 存储桶
- 前缀
- Storage Lens 组

在 Overview（概览）选项卡上，您的控制面板数据聚合为三个不同的部分：Snapshot for date（日期的快照）、Trends and distributions（趋势和分布）以及 Top N overview（前 N 个概览）。

有关 S3 Storage Lens 存储统计管理工具控制面板的更多信息，请参阅以下各节。

### 快照

Snapshot for date（日期的快照）部分显示 S3 Storage Lens 存储统计管理工具在选定日期聚合的摘要指标。这些摘要指标包括以下指标：

- 总存储 – 使用的存储总量（以字节为单位）。
- 对象计数 – Amazon Web Services 账户 中的对象总数。
- 平均对象大小 – 对象的平均大小。
- 活动存储桶 – 账户中存储大于 0 字节，处于活动使用状态的活动桶总数。
- 账户 – 其存储在范围内的账户数量。除非您使用的是 Amazon Organizations，且您的 S3 Storage Lens 存储统计管理工具具有有效的服务相关角色的可信访问权限，否则此值为 1。有关更多信息，请参阅 将服务相关角色用于 Amazon S3 Storage Lens 存储统计管理工具。
- 存储桶 – 账户中的桶总数。

### 指标数据

对于快照中显示的每个指标，您可以看到以下数据：

- 指标名称 – 指标的名称。
- 指标类别 – 将指标组织到的类别。
- 日期 的总计 – 所选日期的总计数。
- 变化百分比 – 与上次快照日期相比的变化百分比。
- 30 天趋势 – 显示指标在 30 天期间内变化的趋势线。
- 建议 – 基于快照中提供的数据的上下文建议。建议与高级指标和建议一起提供。有关更多信息，请参阅 建议。

### 指标类别

您可以选择更新控制面板 Snapshot for date（日期的快照）部分，以显示其他类别的指标。如果您想查看其他指标的快照数据，可以从以下 Metrics categories（指标类别）中进行选择：

- 成本优化
- 数据保护
- 活动（适用于高级指标）
- 访问管理

- 性能
- 事件

Snapshot for date（日期的快照）部分仅显示每个类别的指标选择。要查看特定类别的所有指标，请在 Trends and distributions（趋势和分布）或 Top N overview（前 N 个概览）部分中选择该指标。有关指标类别的更多信息，请参阅指标类别。要获得 S3 Storage Lens 存储统计管理工具指标的完整列表，请参阅Amazon S3 Storage Lens 存储统计管理工具指标词汇表。

趋势和分布

Overview（概览）选项卡的第二部分是 Trends and distributions（趋势和分布）。在 Trends and distributions（趋势和分布）部分中，您可以选择两个指标以在您定义的日期范围内进行比较。Trends and distributions（趋势和分布）部分显示两个指标在一段时间内的关系。使用此部分显示的图表，您可以查看正在跟踪的两个趋势之间的 Storage class（存储类）和 Region（区域）分布。您可以选择向下钻取其中一个图表中的数据点以进行更深入的分析。

有关使用 Trends and distributions（趋势和分布）部分的演练，请参阅识别不使用具有 Amazon KMS 的服务器端加密（SSE-KMS）进行原定设置加密的桶。

前 N 个概述

S3 Storage Lens 存储统计管理工具控制面板的第三部分是前 N 个概述（按升序或降序排序）。此部分将跨最大数量的账户、Amazon Web Services 区域、桶、前缀或 Storage Lens 组，显示您选择的指标。如果您启用了 S3 Storage Lens 存储统计管理工具以与 Amazon Organizations 配合使用，您还可以跨组织查看您选择的指标。

有关使用 Top N overview（前 N 个概览）部分的演练，请参阅识别您最大的 S3 桶。

按选项深入探究和分析

为了提供流畅的分析体验，S3 Storage Lens 存储统计管理工具控制面板提供了一个操作菜单，当您选择任何图表值时将显示该菜单。要使用该菜单，请选择任意图表值以查看关联的指标值，然后在出现的框中从两个选项中进行选择：

- Drill down（深入了解）操作将所选值作为筛选条件应用于控制面板的所有选项卡。然后，您可以深入查看该值以进行更深入的分析。
- 分析依据操作可将您带到您选择的维度选项卡，并将该选项卡值作为筛选条件应用。这些选项卡包括账户、Amazon Web Services 区域、存储类、存储桶、前缀（适用于启用了高级指标和前缀聚合的控制面板）和 Storage Lens 组（适用于启用了高级指标和 Storage Lens 组聚合的控制面板）。使用分析依据，您可以在新维度的上下文中查看数据以进行更深入的分析。

如果会产生不合逻辑或没有任何价值的结果，则向下钻取和分析依据操作可能会被禁用。向下钻取和分析依据操作都会在控制面板所有选项卡中的任何现有筛选条件之上应用筛选条件。您还可以根据需要移除筛选条件。

选项卡

维度级别选项卡提供了特定维度中所有值的详细视图。例如，Amazon Web Services 区域选项卡显示所有 Amazon Web Services 区域的指标，存储桶选项卡显示所有桶的指标。每个维度选项卡包含由四个部分组成的相同布局：

- 趋势图表显示在过去 30 天内所选指标在维度中的前 N 个项目。默认情况下，此图表显示前 10 个项目，但您可以将其减少到至少 3 个项目或将其增加到最多 50 个项目。
- 直方图显示所选日期和指标的垂直条形图。如果您要在此图中显示的项目数量非常大，则可能需要水平滚动。
- 气泡分析图根据维度内的所有项目绘制。此图表用 x 轴表示第一个指标，用 y 轴表示第二个指标，用气泡大小表示第三个指标。
- 指标网格视图包含维度中的每个项目，以行列出。这些列代表每个可用的指标，在指标类别选项卡中排列，以便于导航。

## 使用数据导出查看 Amazon S3 Storage Lens 存储统计管理工具指标

Amazon S3 Storage Lens 存储统计管理工具指标每天以 CSV 或 Apache Parquet 格式的指标导出文件生成，并放置在您账户的 S3 桶中。您可以将导出的指标从 S3 桶引入自己选择的分析工具中，例如 Amazon QuickSight 和 Amazon Athena，在这里您可以分析存储使用情况和活动趋势。

主题

- 使用 Amazon KMS key 加密您的指标导出
- 什么是 S3 Storage Lens 存储统计管理工具导出清单？
- 了解 Amazon S3 Storage Lens 存储统计管理工具导出架构

使用 Amazon KMS key 加密您的指标导出

要向 Amazon S3 Storage Lens 存储统计管理工具授予使用客户托管式密钥加密指标导出的权限，必须使用密钥策略。要更新密钥策略，以便您可以使用 KMS 密钥加密 S3 Storage Lens 存储统计管理工具指标导出，请按照以下步骤操作。

授予 S3 Storage Lens 存储统计管理工具使用您的 KMS 密钥加密数据的权限

1. 使用拥有客户托管式密钥的 Amazon Web Services 账户登录 Amazon Web Services Management Console。
2. 从 https://console.aws.amazon.com/kms 打开 Amazon KMS 控制台。
3. 要更改 Amazon Web Services 区域，请使用页面右上角的 Region selector (区域选择器)。
4. 在左侧导航窗格中，选择 Customer managed keys (客户托管密钥)。
5. 在客户托管密钥下，选择要用于加密指标导出的密钥。Amazon KMS keys 是特定于区域的，必须与指标导出目标 S3 桶位于同一区域中。
6. 在 Key policy (密钥策略) 下，选择 Switch to policy view (切换到策略视图)。
7. 要更新密钥策略，选择 Edit (编辑)。
8. 在 Edit key policy (编辑密钥策略) 下，将以下密钥策略添加到现有密钥策略。要使用这一策略，请将 *user input placeholders* 替换为您的信息。

```
{
    "Sid": "Allow Amazon S3 Storage Lens use of the KMS key",
     "Effect": "Allow",
    "Principal": {
        "Service": "storage-lens.s3.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey"
    ],
    "Resource": "*",
    "Condition": {
       "StringEquals": {
           "aws:SourceArn": "arn:aws:s3:us-east-1:source-account-id:storage-
lens/your-dashboard-name",
           "aws:SourceAccount": "source-account-id"
        }
     }
}
```

9. 选择保存更改。

有关创建客户托管和使用密钥策略的更多信息，请参阅 Amazon Key Management Service 开发人员指南中的以下主题：

- 入门

- 使用 Amazon KMS 中的密钥策略

您还可以使用 Amazon KMS PUT 密钥策略 API 操作（PutKeyPolicy）将密钥策略复制到客户托管式密钥，用于通过 REST API、Amazon CLI 和开发工具包对指标导出进行加密。

什么是 S3 Storage Lens 存储统计管理工具导出清单？

鉴于聚合的数据量大，S3 Storage Lens 存储统计管理工具每日指标导出可以拆分为多个文件。清单文件 manifest.json 描述了当天的指标导出文件的位置。无论何时交付新的导出，都会附有新的清单。manifest.json 文件中包含的每个清单均提供了有关导出的元数据和其他基本信息。

清单信息包括以下属性：

- sourceAccountId – 配置拥有者的账户 ID。
- configId – 控制面板的唯一标识符。
- destinationBucket – 放置指标导出的目标桶 Amazon Resource Name（ARN）。
- reportVersion – 导出的版本。
- reportDate – 报告的日期。
- reportFormat – 报告的格式。
- reportSchema – 报告的架构。
- reportFiles – 目标桶中的导出报告文件的实际列表。

下面是 CSV 格式导出的 manifest.json 文件中的清单示例。

```
{
   "sourceAccountId":"123456789012",
   "configId":"my-dashboard-configuration-id",
   "destinationBucket":"arn:aws:s3:::amzn-s3-demo-destination-bucket",
   "reportVersion":"V_1",
   "reportDate":"2020-11-03",
   "reportFormat":"CSV",

 "reportSchema":"version_number,configuration_id,report_date,aws_account_number,aws_region,stor
   "reportFiles":[
        {
            "key":"DestinationPrefix/StorageLens/123456789012/my-dashboard-
configuration-id/V_1/reports/dt=2020-11-03/a38f6bc4-2e3d-4355-ac8a-e2fdcf3de158.csv",
            "size":1603959,
```

```
            "md5Checksum":"2177e775870def72b8d84febe1ad3574"
        }
      ]
}
```

下面是 Parquet 格式导出的 `manifest.json` 文件中的清单示例。

```
{
   "sourceAccountId":"123456789012",
   "configId":"my-dashboard-configuration-id",
   "destinationBucket":"arn:aws:s3:::amzn-s3-demo-destination-bucket",
   "reportVersion":"V_1",
   "reportDate":"2020-11-03",
   "reportFormat":"Parquet",
   "reportSchema":"message s3.storage.lens { required string version_number;
 required string configuration_id; required string report_date; required string
 aws_account_number; required string aws_region; required string storage_class;
 required string record_type; required string record_value; required string
 bucket_name; required string metric_name; required long metric_value; }",
   "reportFiles":[
      {
         "key":"DestinationPrefix/StorageLens/123456789012/my-dashboard-configuration-
id/V_1/reports/dt=2020-11-03/bd23de7c-b46a-4cf4-bcc5-b21aac5be0f5.par",
         "size":14714,
         "md5Checksum":"b5c741ee0251cd99b90b3e8eff50b944"
      }
}
```

您可以将指标导出配置为作为控制面板配置的一部分在 Amazon S3 控制台中生成，也可以使用 Amazon S3 REST API、Amazon CLI 和开发工具包进行生成。

了解 Amazon S3 Storage Lens 存储统计管理工具导出架构

下表包含 S3 Storage Lens 存储统计管理工具指标导出架构。

| 属性名称 | 数据类型 | 列名称 | 说明 |
| --- | --- | --- | --- |
| `VersionNumber` | 字符串 | `version_number` | 正在使用的 S3 Storage Lens 存储统计管理工具指标的版本。 |

| 属性名称 | 数据类型 | 列名称 | 说明 |
| --- | --- | --- | --- |
| ConfigurationId | 字符串 | configuration_id | S3 Storage Lens 存储统计管理工具配置的 configuration_id 。 |
| ReportDate | 字符串 | report_date | 跟踪指标的日期。 |
| AwsAccountNumber | 字符串 | aws_account_number | 您的 Amazon Web Services 账户 数字。 |
| AwsRegion | 字符串 | aws_region | 正在跟踪指标的 Amazon Web Services 区域。 |
| StorageClass | 字符串 | storage_class | 有问题的桶的存储类别。 |
| RecordType | ENUM | record_type | 正在报告的构件类型（账户、桶或前缀）。 |
| RecordValue | 字符串 | record_value | RecordType 构件的值。<br><br>**Note**<br>record_value 采用 URL 编码。 |
| BucketName | 字符串 | bucket_name | 正在报告的桶的名称。 |
| MetricName | 字符串 | metric_name | 正在报告的指标的名称。 |

| 属性名称 | 数据类型 | 列名称 | 说明 |
| --- | --- | --- | --- |
| MetricValue | 长整型 | metric_value | 正在报告的指标的值。 |

S3 Storage Lens 存储统计管理工具指标导出示例

以下是基于此架构导出的 S3 Storage Lens 存储统计管理工具指标的示例。

> **Note**
>
> 您可以通过在 record_type 列查找 STORAGE_LENS_GROUP_BUCKET 或 STORAGE_LENS_GROUP_ACCOUNT 值来识别 Storage Lens 组的指标。record_value 列将显示 Storage Lens 组的 Amazon 资源名称 (ARN)，例如，arn:aws:s3:us-east-1:123456789012:storage-lens-group/slg-1。

| version_r | configuration_id | report_date | aws_account_number | aws_region | storage_class | record_type | record_value | bucket_name | metric_name | metric_value |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| V_1 | sample-cmh-exclude | 11/3/2020 | 546264889236 | eu-west-1 | STANDARD | ACCOUNT | | | StorageBytes | 2478830621 |
| V_1 | sample-cmh-exclude | 11/3/2020 | 546264889236 | eu-west-1 | STANDARD | ACCOUNT | | | ObjectCount | 1598962 |
| V_1 | sample-cmh-exclude | 11/3/2020 | 546264889236 | eu-west-1 | STANDARD | ACCOUNT | | | ReplicatedStorageBytes | 20000 |
| V_1 | sample-cmh-exclude | 11/3/2020 | 546264889236 | eu-west-1 | STANDARD | ACCOUNT | | | ReplicatedObjectCount | 20 |
| V_1 | sample-cmh-exclude | 11/3/2020 | 546264889236 | eu-west-1 | STANDARD | ACCOUNT | | | EncryptedStorageBytes | 2478828742 |
| V_1 | sample-cmh-exclude | 11/3/2020 | 546264889236 | eu-west-1 | STANDARD | ACCOUNT | | | EncryptedObjectCount | 1598961 |
| V_1 | sample-cmh-exclude | 11/3/2020 | 546264889236 | eu-west-1 | STANDARD | ACCOUNT | | | DeleteMarkerObjectCount | 1500 |
| V_1 | sample-cmh-exclude | 11/3/2020 | 546264889236 | eu-west-1 | STANDARD | ACCOUNT | | | ObjectLockEnabledStorageBytes | 0 |
| V_1 | sample-cmh-exclude | 11/3/2020 | 546264889236 | eu-west-1 | STANDARD | ACCOUNT | | | ObjectLockEnabledObjectCount | 0 |
| V_1 | sample-cmh-exclude | 11/3/2020 | 546264889236 | eu-west-1 | STANDARD | ACCOUNT | | | CurrentVersionStorageBytes | 2478830621 |
| V_1 | sample-cmh-exclude | 11/3/2020 | 546264889236 | eu-west-1 | STANDARD | ACCOUNT | | | CurrentVersionObjectCount | 1598962 |
| V_1 | sample-cmh-exclude | 11/3/2020 | 546264889236 | eu-west-1 | STANDARD | ACCOUNT | | | NonCurrentVersionStorageBytes | 0 |
| V_1 | sample-cmh-exclude | 11/3/2020 | 546264889236 | eu-west-1 | STANDARD | ACCOUNT | | | NonCurrentVersionObjectCount | 0 |
| V_1 | sample-cmh-exclude | 11/3/2020 | 546264889236 | eu-west-1 | STANDARD | ACCOUNT | | | IncompleteMultipartUploadStorageBytes | 0 |
| V_1 | sample-cmh-exclude | 11/3/2020 | 546264889236 | eu-west-1 | STANDARD | ACCOUNT | | | IncompleteMultipartUploadObjectCount | 0 |
| V_1 | sample-cmh-exclude | 11/3/2020 | 546264889236 | us-west-1 | STANDARD | PREFIX | AWSLogs%2F546264889236%2FCloudTrail%2Fus | cloudtrail-log-sf | StorageBytes | 29996800 |
| V_1 | sample-cmh-exclude | 11/3/2020 | 546264889236 | us-west-1 | STANDARD | PREFIX | AWSLogs%2F546264889236%2FCloudTrail%2Fus | cloudtrail-log-sf | ObjectCount | 12264 |
| V_1 | sample-cmh-exclude | 11/3/2020 | 546264889236 | us-west-1 | STANDARD | PREFIX | AWSLogs%2F546264889236%2FCloudTrail%2Fus | cloudtrail-log-sf | ReplicatedStorageBytes | 0 |
| V_1 | sample-cmh-exclude | 11/3/2020 | 546264889236 | us-west-1 | STANDARD | PREFIX | AWSLogs%2F546264889236%2FCloudTrail%2Fus | cloudtrail-log-sf | ReplicatedObjectCount | 0 |
| V_1 | sample-cmh-exclude | 11/3/2020 | 546264889236 | us-west-1 | STANDARD | PREFIX | AWSLogs%2F546264889236%2FCloudTrail%2Fus | cloudtrail-log-sf | EncryptedStorageBytes | 29996800 |
| V_1 | sample-cmh-exclude | 11/3/2020 | 546264889236 | us-west-1 | STANDARD | PREFIX | AWSLogs%2F546264889236%2FCloudTrail%2Fus | cloudtrail-log-sf | EncryptedObjectCount | 12264 |
| V_1 | sample-cmh-exclude | 11/3/2020 | 546264889236 | us-west-1 | STANDARD | PREFIX | AWSLogs%2F546264889236%2FCloudTrail%2Fus | cloudtrail-log-sf | DeleteMarkerObjectCount | 0 |
| V_1 | sample-cmh-exclude | 11/3/2020 | 546264889236 | us-west-1 | STANDARD | PREFIX | AWSLogs%2F546264889236%2FCloudTrail%2Fus | cloudtrail-log-sf | ObjectLockEnabledStorageBytes | 0 |
| V_1 | sample-cmh-exclude | 11/3/2020 | 546264889236 | us-west-1 | STANDARD | PREFIX | AWSLogs%2F546264889236%2FCloudTrail%2Fus | cloudtrail-log-sf | ObjectLockEnabledObjectCount | 0 |
| V_1 | sample-cmh-exclude | 11/3/2020 | 546264889236 | us-west-1 | STANDARD | PREFIX | AWSLogs%2F546264889236%2FCloudTrail%2Fus | cloudtrail-log-sf | CurrentVersionStorageBytes | 29996800 |
| V_1 | sample-cmh-exclude | 11/3/2020 | 546264889236 | us-west-1 | STANDARD | PREFIX | AWSLogs%2F546264889236%2FCloudTrail%2Fus | cloudtrail-log-sf | CurrentVersionObjectCount | 12264 |
| V_1 | sample-cmh-exclude | 11/3/2020 | 546264889236 | us-west-1 | STANDARD | PREFIX | AWSLogs%2F546264889236%2FCloudTrail%2Fus | cloudtrail-log-sf | NonCurrentVersionStorageBytes | 0 |
| V_1 | sample-cmh-exclude | 11/3/2020 | 546264889236 | us-west-1 | STANDARD | PREFIX | AWSLogs%2F546264889236%2FCloudTrail%2Fus | cloudtrail-log-sf | NonCurrentVersionObjectCount | 0 |
| V_1 | sample-cmh-exclude | 11/3/2020 | 546264889236 | us-west-1 | STANDARD | PREFIX | AWSLogs%2F546264889236%2FCloudTrail%2Fus | cloudtrail-log-sf | IncompleteMultipartUploadStorageBytes | 0 |
| V_1 | sample-cmh-exclude | 11/3/2020 | 546264889236 | us-west-1 | STANDARD | PREFIX | AWSLogs%2F546264889236%2FCloudTrail%2Fus | cloudtrail-log-sf | IncompleteMultipartUploadObjectCount | 0 |

以下是 S3 Storage Lens 存储统计管理工具指标导出示例，其中包含 Storage Lens 组数据。

| version_numbe | configuration_id | report_date | aws_account_num | aws_region | storage_class | record_type | record_value | bucket_name | metric_name | metric_value |
|---|---|---|---|---|---|---|---|---|---|---|
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_ACCOUNT | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | | StorageBytes | 3128548856 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_ACCOUNT | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | | ObjectCount | 4440 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_ACCOUNT | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | | ReplicatedStorageBytes | 0 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_ACCOUNT | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | | ReplicatedObjectCount | 0 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_ACCOUNT | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | | EncryptedStorageBytes | 3128548856 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_ACCOUNT | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | | EncryptedObjectCount | 4440 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_ACCOUNT | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | | DeleteMarkerObjectCount | 0 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_ACCOUNT | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | | ObjectLockEnabledStorageBytes | 0 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_ACCOUNT | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | | ObjectLockEnabledObjectCount | 0 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_ACCOUNT | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | | CurrentVersionStorageBytes | 3128548856 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_ACCOUNT | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | | CurrentVersionObjectCount | 4440 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_ACCOUNT | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | | NonCurrentVersionStorageBytes | 0 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_ACCOUNT | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | | NonCurrentVersionObjectCount | 0 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_ACCOUNT | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | | IncompleteMultipartUploadStorageBytes | 0 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_ACCOUNT | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | | IncompleteMultipartUploadObjectCount | 0 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_ACCOUNT | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | | DeleteMarkerStorageBytes | 0 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_ACCOUNT | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | | ReplicatedStorageBytesSource | 0 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_ACCOUNT | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | | ReplicatedObjectCountSource | 0 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_ACCOUNT | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | | IncompleteMPUStorageBytesOlderThan7Days | 0 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_ACCOUNT | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | | IncompleteMPUObjectCountOlderThan7Days | 0 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_BUCKET | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | cloud-trail-log-sfo | StorageBytes | 676863200 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_BUCKET | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | cloud-trail-log-sfo | ObjectCount | 3000 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_BUCKET | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | cloud-trail-log-sfo | ReplicatedStorageBytes | 0 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_BUCKET | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | cloud-trail-log-sfo | ReplicatedObjectCount | 0 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_BUCKET | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | cloud-trail-log-sfo | EncryptedStorageBytes | 676863200 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_BUCKET | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | cloud-trail-log-sfo | EncryptedObjectCount | 3000 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_BUCKET | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | cloud-trail-log-sfo | DeleteMarkerObjectCount | 0 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_BUCKET | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | cloud-trail-log-sfo | ObjectLockEnabledStorageBytes | 0 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_BUCKET | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | cloud-trail-log-sfo | ObjectLockEnabledObjectCount | 0 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_BUCKET | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | cloud-trail-log-sfo | CurrentVersionStorageBytes | 676863200 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_BUCKET | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | cloud-trail-log-sfo | CurrentVersionObjectCount | 3000 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_BUCKET | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | cloud-trail-log-sfo | NonCurrentVersionStorageBytes | 0 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_BUCKET | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | cloud-trail-log-sfo | NonCurrentVersionObjectCount | 0 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_BUCKET | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | cloud-trail-log-sfo | IncompleteMultipartUploadStorageBytes | 0 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_BUCKET | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | cloud-trail-log-sfo | IncompleteMultipartUploadObjectCount | 0 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_BUCKET | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | cloud-trail-log-sfo | DeleteMarkerStorageBytes | 0 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_BUCKET | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | cloud-trail-log-sfo | ReplicatedStorageBytesSource | 0 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_BUCKET | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | cloud-trail-log-sfo | ReplicatedObjectCountSource | 0 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_BUCKET | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | cloud-trail-log-sfo | IncompleteMPUStorageBytesOlderThan7Days | 0 |
| V_1 | sample-sfo-exclude | 11/15/23 | 546264889236 | us-west-1 | STANDARD | STORAGE_LENS_GROUP_BUCKET | arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180 | cloud-trail-log-sfo | IncompleteMPUObjectCountOlderThan7Days | 0 |

## 在 CloudWatch 中监控 S3 Storage Lens 存储统计管理工具指标

您可以将 S3 Storage Lens 存储统计管理工具指标发布到 Amazon CloudWatch，以便在 CloudWatch 控制面板中创建运营状况的统一视图。您还可以使用 CloudWatch 功能（如告警和触发操作、指标数学和异常检测）来监控 S3 Storage Lens 存储统计管理工具指标并采取措施。此外，CloudWatch API 操作使应用程序（包括第三方提供商）能够访问 S3 Storage Lens 存储统计管理工具指标。有关 CloudWatch 功能的更多信息，请参阅 Amazon CloudWatch 用户指南。

您可以使用 Amazon S3 控制台、Amazon S3 REST API、Amazon CLI 和 Amazon SDK 针对新的或当前控制面板配置启用 CloudWatch 发布选项。升级到 S3 Storage Lens 存储统计管理工具 advanced metrics and recommendations（高级指标和建议）的控制面板可以使用 CloudWatch 发布选项。有关 S3 Storage Lens 存储统计管理工具高级指标和建议定价，请参阅 Amazon S3 定价。不会收取其他 CloudWatch 指标发布费用；但是，其他 CloudWatch 费用（例如控制面板、告警和 API 调用）确实适用。有关更多信息，请参阅 Amazon CloudWatch 定价。

S3 Storage Lens 存储统计管理工具指标在拥有 S3 Storage Lens 存储统计管理工具配置的账户中发布到 CloudWatch。在高级指标和建议中启用 CloudWatch 发布选项后，您可以在 CloudWatch 中访问组织、账户和桶级指标。前缀级别的指标在 CloudWatch 中不可用。

> **Note**
>
> S3 Storage Lens 存储统计管理工具指标是每日指标，每天发布到 CloudWatch 一次。当您在 CloudWatch 中查询 S3 Storage Lens 存储统计管理工具指标时，查询的期限必须为 1 天（86400 秒）。在您的每日 S3 Storage Lens 指标显示在 Amazon S3 控制台的 S3 Storage

Lens 存储统计管理工具控制面板中后，这些指标可能需要几个小时才能显示在 CloudWatch 中。当您首次为 S3 Storage Lens 存储统计管理工具指标启用 CloudWatch 发布选项时，您的指标最多可能需要 24 小时才能将指标发布到 CloudWatch。

启用 CloudWatch 发布选项后，您可以使用以下 CloudWatch 功能监控和分析 S3 Storage lens 存储统计管理工具数据：

- Dashboards（控制面板）— 使用 CloudWatch 控制面板创建定制 S3 Storage Lens 存储统计管理工具控制面板。将您的 CloudWatch 控制面板与团队间无法直接访问您的 Amazon Web Services 账户的人员、利益攸关方和组织外部的人员共享。
- Alarms and triggered actions（告警和触发操作）— 配置监视指标的警报，并在超出阈值时采取行动。例如，您可以配置告警，当 Incomplete Multipart Upload Bytes（未完成分段上传字节）指标连续三天超过 1GB 时发送 Amazon SNS 通知。
- Anomaly detection（异常检测）— 启用异常检测以持续分析指标、确定正常基线和表面异常。您可以根据指标的预期值创建异常检测告警。例如，您可以监视 Object Lock Enabled Bytes（启用对象锁定的字节）指标的异常情况，以检测未经授权移除对象锁定设置的情况。
- Metric math（指标数学）– 您还可以使用指标数学查询多个 S3 Storage Lens 存储统计管理工具指标，并使用数学表达式基于这些度量创建新的时间序列。例如，您可以通过将 `StorageBytes` 除以 `ObjectCount` 创建一个新指标来获得平均对象大小。

有关 S3 Storage Lens 存储统计管理工具指标的 CloudWatch 发布选项的更多信息，请参阅以下主题。

主题

- S3 Storage Lens 存储统计管理工具指标和维度
- 为 S3 Storage Lens 存储统计管理工具启用 CloudWatch 发布
- 在 CloudWatch 中结合使用 S3 Storage Lens 存储统计管理工具指标

S3 Storage Lens 存储统计管理工具指标和维度

要将 S3 Storage Lens 存储统计管理工具指标发送到 CloudWatch，您必须在 S3 Storage Lens 存储统计管理工具高级指标和建议中启用 CloudWatch 发布选项。启用高级指标后，您可以使用 CloudWatch 控制面板与其他应用程序指标一起监控 S3 Storage Lens 存储统计管理工具指标，并创建运营状况的统一视图。您可以使用维度在 CloudWatch 中按企业、账户、桶、存储类别、区域和指标配置 ID 筛选 CloudWatch 中的 S3 Storage Lens 存储统计管理工具指标。

S3 Storage Lens 存储统计管理工具指标在拥有 S3 Storage Lens 存储统计管理工具配置的账户中发布到 CloudWatch。在高级指标和建议中启用 CloudWatch 发布选项后，您可以在 CloudWatch 中访问组织、账户和桶级指标。前缀级别的指标在 CloudWatch 中不可用。

> **Note**
>
> S3 Storage Lens 存储统计管理工具指标是每日指标，每天发布到 CloudWatch 一次。当您在 CloudWatch 中查询 S3 Storage Lens 存储统计管理工具指标时，查询的期限必须为 1 天（86400 秒）。在您的每日 S3 Storage Lens 指标显示在 Amazon S3 控制台的 S3 Storage Lens 存储统计管理工具控制面板中后，这些指标可能需要几个小时才能显示在 CloudWatch 中。当您首次为 S3 Storage Lens 存储统计管理工具指标启用 CloudWatch 发布选项时，您的指标最多可能需要 24 小时才能将指标发布到 CloudWatch。

有关 CloudWatch 中 S3 Storage Lens 存储统计管理工具指标和维度的更多信息，请参阅以下主题。

主题

- Metrics
- Dimensions

Metrics

S3 Storage Lens 存储统计管理工具指标在 CloudWatch 中作为指标提供。S3 Storage Lens 存储统计管理工具指标已发布到 `AWS/S3/Storage-Lens` 命名空间。此命名空间仅适用于 S3 Storage Lens 存储统计管理工具指标。Amazon S3 桶、请求和复制指标已发布到 `AWS/S3` 命名空间。

S3 Storage Lens 存储统计管理工具指标在拥有 S3 Storage Lens 存储统计管理工具配置的账户中发布到 CloudWatch。在高级指标和建议中启用 CloudWatch 发布选项后，您可以在 CloudWatch 中访问组织、账户和桶级指标。前缀级别的指标在 CloudWatch 中不可用。

在 S3 Storage Lens 存储统计管理工具中，指标会聚合并仅存储在指定的主区域中。S3 Storage Lens 存储统计管理工具指标也发布到您在 S3 Storage Lens 存储统计管理工具配置中指定的主页区域中的 CloudWatch。

有关 S3 Storage Lens 存储统计管理工具指标的完整列表，包括 CloudWatch 中可用的指标列表，请参阅 Amazon S3 Storage Lens 存储统计管理工具指标词汇表。

> **Note**
>
> CloudWatch 中 S3 Storage Lens 存储统计管理工具指标的有效统计数据是平均值。有关 CloudWatch 中统计信息的更多信息，请参阅 Amazon CloudWatch 用户指南中的 CloudWatch 统计数据定义。

### CloudWatch 中 S3 Storage Lens 存储统计管理工具指标的粒度

S3 Storage Lens 存储统计管理工具提供企业、账户、桶和前缀粒度的指标。S3 Storage Lens 存储统计管理工具将企业、账户和桶级 S3 Storage Lens 存储统计管理工具指标发布到 CloudWatch。前缀级别的 S3 Storage Lens 存储统计管理工具指标在 CloudWatch 中不可用。

有关 CloudWatch 中可用 S3 Storage Lens 存储统计管理工具指标的粒度的更多信息，请参阅以下列表：

- Organization（企业）— 在企业中的成员账户中聚合的指标。S3 Storage Lens 存储统计管理工具将成员账户的指标发布到管理账户中的 CloudWatch。
  - Organization and account（企业和账户）— 在企业中的成员账户指标。
  - Organization and bucket（企业和桶）— 在企业的成员账户中的 Amazon S3 桶指标。
- 账户（非企业级别）— 您账户中桶之间汇总的指标。
- 桶（非企业级别）— 特定桶的指标。在 CloudWatch 中，S3 Storage Lens 存储统计管理工具将这些指标发布至创建 S3 Storage Lens 存储统计管理工具配置的 Amazon Web Services 账户。S3 Storage Lens 存储统计管理工具仅针对非企业配置发布这些指标。

### Dimensions

当 S3 Storage Lens 存储统计管理工具向 CloudWatch 发送数据时，维度附加到每个指标。维度是描述指标特征的类别。您可使用维度筛选 CloudWatch 返回的结果。

例如，CloudWatch 中的所有 S3 Storage Lens 存储统计管理工具指标都具有 `configuration_id` 维度。您可以使用此维度来区分与特定 S3 Storage Lens 存储统计管理工具配置关联的指标。`organization_id` 识别企业级指标。有关维度的更多信息，请参阅 CloudWatch User Guide（CloudWatch 用户指南）中的 Dimensions（维度）。

S3 Storage Lens 存储统计管理工具指标有不同的维度，具体取决于指标的粒度。例如，您可以使用 `organization_id` 维度按照 Amazon Organizations ID 筛选企业级的指标。但是，您不能将此维度用于桶和账户级指标。有关更多信息，请参阅 使用维度筛选指标。

要查看哪些维度可用于 S3 Storage Lens 存储统计管理工具配置，请参阅下表。

| 维度 | 描述 | 桶 | Organization（组织） | 组织和桶 | 组织和账户 |
|---|---|---|---|---|---|
| configuration_id | 指标中报告的 S3 Storage Lens 存储统计管理工具配置的控制面板名称 | . | . | . | . | . |
| metrics_version | S3 Storage Lens 存储统计管理工具指标的版本。指标版本的固定值为 1.0。 | . | . | . | . | . |
| organization_id | 指标的 Amazon Organizations ID | . | . | . | . | . |
| aws_account_number | 与指标关联的 Amazon Web Services 账户 | . | . | . | . | . |
| aws_region | 指标的 Amazon Web Services 区域 | . | . | . | . | . |
| bucket_name | 指标中报告的 S3 桶的名称 | . | . | . | . | . |
| storage_class | 指标中报告的桶的存储类 | . | . | . | . | . |
| record_type | 指标的粒度：组织、账户、桶 | 桶 | 账户 | 桶 | 账户 | 企业 |

为 S3 Storage Lens 存储统计管理工具启用 CloudWatch 发布

您可以将 S3 Storage Lens 存储统计管理工具指标发布到 Amazon CloudWatch，以便在 CloudWatch 控制面板中创建运营状况的统一视图。您还可以使用 CloudWatch 功能（如告警和触发操作、指标

数学和异常检测）来监控 S3 Storage Lens 存储统计管理工具指标并采取措施。此外，CloudWatch API 操作使应用程序（包括第三方提供商）能够访问 S3 Storage Lens 存储统计管理工具指标。有关 CloudWatch 功能的更多信息，请参阅 Amazon CloudWatch 用户指南。

S3 Storage Lens 存储统计管理工具指标在拥有 S3 Storage Lens 存储统计管理工具配置的账户中发布到 CloudWatch。在高级指标和建议中启用 CloudWatch 发布选项后，您可以在 CloudWatch 中访问组织、账户和桶级指标。前缀级别的指标在 CloudWatch 中不可用。

您可以使用 Amazon S3 控制台、REST API、Amazon CLI 和 Amazon SDK 针对新的或当前控制面板配置启用 CloudWatch 支持。CloudWatch 发布选项可用于升级到 S3 Storage Lens 存储统计管理工具高级指标和建议。有关 S3 Storage Lens 存储统计管理工具高级指标和建议定价，请参阅 Amazon S3 定价。不会收取其他 CloudWatch 指标发布费用；但是，其他 CloudWatch 费用（例如控制面板、告警和 API 调用）确实适用。

要启用 S3 Storage Lens 存储统计管理工具指标的 CloudWatch 发布选项，请参阅以下主题。

> **Note**
>
> S3 Storage Lens 存储统计管理工具指标是每日指标，每天发布到 CloudWatch 一次。当您在 CloudWatch 中查询 S3 Storage Lens 存储统计管理工具指标时，查询的期限必须为 1 天（86400 秒）。在您的每日 S3 Storage Lens 指标显示在 Amazon S3 控制台的 S3 Storage Lens 存储统计管理工具控制面板中后，这些指标可能需要几个小时才能显示在 CloudWatch 中。当您首次为 S3 Storage Lens 存储统计管理工具指标启用 CloudWatch 发布选项时，您的指标最多可能需要 24 小时才能将指标发布到 CloudWatch。
> 目前，S3 Storage Lens 存储统计管理工具指标无法通过 CloudWatch 流使用。

使用 S3 控制台

更新 S3 Storage Lens 存储统计管理工具控制面板时，无法更改控制面板名称或主区域。您也不能更改原定设置控制面板的范围，其范围限于整个账户的存储。

更新 S3 Storage Lens 存储统计管理工具控制面板以启用 CloudWatch 发布

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在导航窗格中，依次选择 S3 Storage Lens 和 Dashboards（控制面板）。
3. 请选择要编辑的控制面板，然后选择 Edit（编辑）。

4. 在 Metrics selection（指标选择）下方，请选择 Advanced metrics and recommendations（高级指标和建议）。

   高级指标和建议可额外收费。高级指标和建议包括 15 个月的数据查询期、在前缀级别聚合的使用情况指标、按桶聚合的活动指标、CloudWatch 发布选项，以及帮助您优化存储成本和应用数据保护最佳做法的上下文建议。有关更多信息，请参阅 Amazon S3 定价。

5. 在 Select Advanced metrics and recommendations features（选择高级指标和推荐功能）下方，选择 CloudWatch publishing（CloudWatch 发布）。

   > **Important**
   >
   > 如果您的配置启用了使用情况指标的前缀聚合，则前缀级指标将不会发布到 CloudWatch。只有桶、账户和企业级 S3 Storage Lens 存储统计管理工具指标才会发布到 CloudWatch。

6. 选择保存更改。

要创建启用 CloudWatch 支持的新 S3 Storage Lens 存储统计管理工具控制面板

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，依次选择 Storage Lens 和 Dashboards（控制面板）。
3. 请选择创建控制面板。
4. 在 General（常规）下，定义以下配置选项：

   a. 对于 Dashboard name（控制面板名称），输入您的控制面板名称。

      控制面板名称必须少于 65 个字符，且不得包含特殊字符或空格。创建控制面板后，您无法更改此控制面板名称。

   b. 为控制面板选择 Home Region（主区域）。

      此控制面板范围内所有包含的所有区域的指标，都集中存储在此指定的主区域中。在 CloudWatch 中，S3 Storage Lens 存储统计管理工具指标也可在主区域提供。创建控制面板后，您无法更改主区域。

5. （可选）要添加标签，请选择 Add tag （添加标签），然后输入标签 Key（密钥）和 Value（值）。

> **Note**
>
> 您最多可以在控制面板配置中添加 50 个标签。

6. 定义配置的范围：

   a. 如果您正在创建组织级配置，请选择要包含在配置中的账户：Include all accounts in your configuration（在配置中包括所有账户）或者 Limit the scope to your signed-in account（将范围限制为您的登录账户）。

   > **Note**
   >
   > 当您创建包含所有账户的组织级配置时，您只能包括或排除区域，而不能包括或排除桶。

   b. 通过执行以下操作，选择您希望 S3 Storage Lens 存储统计管理工具在控制面板配置中包括的区域和桶：

   - 要包含所有区域，请选择 Include Regions and buckets（包含区域和桶）。
   - 要包含特定的区域，请清除 Include all Regions（包含所有区域）。在 Choose Regions to include（选择要包含的区域）下方，请选择想要 S3 Storage Lens 存储统计管理工具包含在控制面板中的区域。
   - 要包含特定桶，请清除 Include all buckets（包含所有桶）。在 Choose buckets to include（选择要包含的桶）下方，请选择想要 S3 Storage Lens 存储统计管理工具包含在控制面板中的桶。

   > **Note**
   >
   > 您最多可以选择 50 个桶。

7. 对于 Metrics selection（指标选择），请选择 Advanced metrics and recommendations（高级指标和建议）。

   有关高级指标和建议定价的资讯，请参阅 Amazon S3 pricing（Amazon S3 定价）。

8. 在 Advanced metrics and recommendations features（高级指标和建议功能）下方，选择您要启用的选项：

   - Advanced metrics（高级指标）

- CloudWatch publishing（CloudWatch 发布）

> **Important**
>
> 如果您为 S3 Storage Lens 存储统计管理工具配置启用了前缀聚合，那么前缀级别的指标将不会发布到 CloudWatch。只有桶、账户和企业级 S3 Storage Lens 存储统计管理工具指标才会发布到 CloudWatch。

- Prefix aggregation（前缀聚合）

> **Note**
>
> 有关高级指标和建议功能的更多信息，请参阅指标选择。

9. 如果您启用了 Advanced metrics（高级指标），请选择要在 S3 Storage Lens 存储统计管理工具控制面板中显示的 Advanced metrics categories（高级指标类别）：

   - 活动指标
   - Detailed status code metrics（详细的状态代码指标）
   - Advanced cost optimization metrics（高级成本优化指标）
   - Advanced data protection metrics（高级数据保护指标）

   有关指标类别的更多信息，请参阅指标类别。要获得指标的完整列表，请参阅 Amazon S3 Storage Lens 存储统计管理工具指标词汇表。

10. （可选）配置您的指标导出。

    有关如何配置指标导出的更多信息，请参阅步骤 使用 S3 控制台。

11. 请选择创建控制面板。

使用 Amazon CLI

以下 Amazon CLI 示例将通过使用 S3 Storage Lens 存储统计管理工具组织级高级指标和建议配置启用 CloudWatch 发布选项。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control put-storage-lens-configuration --account-id=555555555555 --config-
id=your-configuration-id --region=us-east-1 --storage-lens-configuration=file://./
config.json

config.json
{
  "Id": "SampleS3StorageLensConfiguration", //Use this property to identify your S3
 Storage Lens configuration.
  "AwsOrg": { //Use this property when enabling S3 Storage Lens for Amazon
 Organizations.
    "Arn": "arn:aws:organizations::123456789012:organization/o-abcdefgh"
  },
  "AccountLevel": {
    "ActivityMetrics": {
      "IsEnabled":true
    },
    "AdvancedCostOptimizationMetrics": {
      "IsEnabled":true
    },
    "AdvancedDataProtectionMetrics": {
      "IsEnabled":true
    },
    "DetailedStatusCodesMetrics": {
      "IsEnabled":true
    },
    "BucketLevel": {
      "ActivityMetrics": {
        "IsEnabled":true //Mark this as false if you want only free metrics.
      },
      "ActivityMetrics": {
        "IsEnabled":true //Mark this as false if you want only free metrics.
      },
      "AdvancedCostOptimizationMetrics": {
        "IsEnabled":true //Mark this as false if you want only free metrics.
      },
      "DetailedStatusCodesMetrics": {
        "IsEnabled":true //Mark this as false if you want only free metrics.
      },
      "PrefixLevel":{
        "StorageMetrics":{
          "IsEnabled":true, //Mark this as false if you want only free metrics.
          "SelectionCriteria":{
            "MaxDepth":5,
```

```
            "MinStorageBytesPercentage":1.25,
            "Delimiter":"/"
          }
        }
      }
    }
  },
  "Exclude": { //Replace with "Include" if you prefer to include Regions.
    "Regions": [
      "eu-west-1"
    ],
    "Buckets": [ //This attribute is not supported for Amazon Organizations-level
 configurations.
      "arn:aws:s3:::amzn-s3-demo-source-bucket "
    ]
  },
  "IsEnabled": true, //Whether the configuration is enabled
  "DataExport": { //Details about the metrics export
    "S3BucketDestination": {
      "OutputSchemaVersion": "V_1",
      "Format": "CSV", //You can add "Parquet" if you prefer.
      "AccountId": "111122223333",
      "Arn": "arn:aws:s3:::amzn-s3-demo-destination-bucket", // The destination
 bucket for your metrics export must be in the same Region as your S3 Storage Lens
 configuration.
      "Prefix": "prefix-for-your-export-destination",
      "Encryption": {
        "SSES3": {}
      }
    },
    "CloudWatchMetrics": {
      "IsEnabled": true //Mark this as false if you want to export only free metrics.
    }
  }
}
```

### 使用适用于 Java 的 Amazon 开发工具包

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
```

```
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.AccountLevel;
import com.amazonaws.services.s3control.model.ActivityMetrics;
import com.amazonaws.services.s3control.model.BucketLevel;
import com.amazonaws.services.s3control.model.CloudWatchMetrics;
import com.amazonaws.services.s3control.model.Format;
import com.amazonaws.services.s3control.model.Include;
import com.amazonaws.services.s3control.model.OutputSchemaVersion;
import com.amazonaws.services.s3control.model.PrefixLevel;
import com.amazonaws.services.s3control.model.PrefixLevelStorageMetrics;
import com.amazonaws.services.s3control.model.PutStorageLensConfigurationRequest;
import com.amazonaws.services.s3control.model.S3BucketDestination;
import com.amazonaws.services.s3control.model.SSES3;
import com.amazonaws.services.s3control.model.SelectionCriteria;
import com.amazonaws.services.s3control.model.StorageLensAwsOrg;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;
import com.amazonaws.services.s3control.model.StorageLensDataExport;
import com.amazonaws.services.s3control.model.StorageLensDataExportEncryption;
import com.amazonaws.services.s3control.model.StorageLensTag;

import java.util.Arrays;
import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class CreateAndUpdateDashboard {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "Source Account ID";
        String exportAccountId = "Destination Account ID";
        String exportBucketArn = "arn:aws:s3:::amzn-s3-demo-destination-bucket"; //
 The destination bucket for your metrics export must be in the same Region as your S3
 Storage Lens configuration.
        String awsOrgARN = "arn:aws:organizations::123456789012:organization/o-
abcdefgh";
        Format exportFormat = Format.CSV;

        try {
            SelectionCriteria selectionCriteria = new SelectionCriteria()
                    .withDelimiter("/")
                    .withMaxDepth(5)
                    .withMinStorageBytesPercentage(10.0);
```

```
            PrefixLevelStorageMetrics prefixStorageMetrics = new
PrefixLevelStorageMetrics()
                    .withIsEnabled(true)
                    .withSelectionCriteria(selectionCriteria);
            BucketLevel bucketLevel = new BucketLevel()
                    .withActivityMetrics(new ActivityMetrics().withIsEnabled(true))
                    .withAdvancedCostOptimizationMetrics(new
AdvancedCostOptimizationMetrics().withIsEnabled(true))
                    .withAdvancedDataProtectionMetrics(new
AdvancedDataProtectionMetrics().withIsEnabled(true))
                    .withDetailedStatusCodesMetrics(new
DetailedStatusCodesMetrics().withIsEnabled(true))
                    .withPrefixLevel(new
PrefixLevel().withStorageMetrics(prefixStorageMetrics));
            AccountLevel accountLevel = new AccountLevel()
                    .withActivityMetrics(new ActivityMetrics().withIsEnabled(true))
                    .withAdvancedCostOptimizationMetrics(new
AdvancedCostOptimizationMetrics().withIsEnabled(true))
                    .withAdvancedDataProtectionMetrics(new
AdvancedDataProtectionMetrics().withIsEnabled(true))
                    .withDetailedStatusCodesMetrics(new
DetailedStatusCodesMetrics().withIsEnabled(true))
                    .withBucketLevel(bucketLevel);

            Include include = new Include()
                    .withBuckets(Arrays.asList("arn:aws:s3:::amzn-s3-demo-bucket"))
                    .withRegions(Arrays.asList("us-west-2"));

            StorageLensDataExportEncryption exportEncryption = new
StorageLensDataExportEncryption()
                    .withSSES3(new SSES3());
            S3BucketDestination s3BucketDestination = new S3BucketDestination()
                    .withAccountId(exportAccountId)
                    .withArn(exportBucketArn)
                    .withEncryption(exportEncryption)
                    .withFormat(exportFormat)
                    .withOutputSchemaVersion(OutputSchemaVersion.V_1)
                    .withPrefix("Prefix");
            CloudWatchMetrics cloudWatchMetrics = new CloudWatchMetrics()
                    .withIsEnabled(true);
            StorageLensDataExport dataExport = new StorageLensDataExport()
                    .withCloudWatchMetrics(cloudWatchMetrics)
                    .withS3BucketDestination(s3BucketDestination);
```

```
            StorageLensAwsOrg awsOrg = new StorageLensAwsOrg()
                    .withArn(awsOrgARN);

            StorageLensConfiguration configuration = new StorageLensConfiguration()
                    .withId(configurationId)
                    .withAccountLevel(accountLevel)
                    .withInclude(include)
                    .withDataExport(dataExport)
                    .withAwsOrg(awsOrg)
                    .withIsEnabled(true);

            List<StorageLensTag> tags = Arrays.asList(
                    new StorageLensTag().withKey("key-1").withValue("value-1"),
                    new StorageLensTag().withKey("key-2").withValue("value-2")
            );

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.putStorageLensConfiguration(new
 PutStorageLensConfigurationRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
                    .withStorageLensConfiguration(configuration)
                    .withTags(tags)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

使用 REST API

要使用 Amazon S3 REST API 启用 CloudWatch 发布选项，您可以使用 PutStorageLensConfiguration。

后续步骤

启用 CloudWatch 发布选项后，您可以在 CloudWatch 中访问 S3 Storage Lens 存储统计管理工具指标。您还可以利用 CloudWatch 功能在 CloudWatch 中监控和分析 S3 Storage Lens 存储统计管理工具数据。有关更多信息，请参阅以下主题：

- S3 Storage Lens 存储统计管理工具指标和维度
- 在 CloudWatch 中结合使用 S3 Storage Lens 存储统计管理工具指标

在 CloudWatch 中结合使用 S3 Storage Lens 存储统计管理工具指标

您可以将 S3 Storage Lens 存储统计管理工具指标发布到 Amazon CloudWatch，以便在 CloudWatch 控制面板中创建运营状况的统一视图。您还可以使用 CloudWatch 功能（如告警和触发操作、指标数学和异常检测）来监控 S3 Storage Lens 存储统计管理工具指标并采取措施。此外，CloudWatch API 操作使应用程序（包括第三方提供商）能够访问 S3 Storage Lens 存储统计管理工具指标。有关 CloudWatch 功能的更多信息，请参阅 Amazon CloudWatch 用户指南。

您可以使用 Amazon S3 控制台、Amazon S3 REST API、Amazon CLI 和 Amazon SDK 针对新的或当前控制面板配置启用 CloudWatch 发布选项。CloudWatch 发布选项可用于升级到 S3 Storage Lens 存储统计管理工具高级指标和建议。有关 S3 Storage Lens 存储统计管理工具高级指标和建议定价，请参阅 Amazon S3 定价。不会收取其他 CloudWatch 指标发布费用；但是，其他 CloudWatch 费用（例如控制面板、告警和 API 调用）确实适用。有关更多信息，请参阅 Amazon CloudWatch 定价。

S3 Storage Lens 存储统计管理工具指标在拥有 S3 Storage Lens 存储统计管理工具配置的账户中发布到 CloudWatch。在高级指标和建议中启用 CloudWatch 发布选项后，您可以在 CloudWatch 中访问组织、账户和桶级指标。前缀级别的指标在 CloudWatch 中不可用。

> **Note**
>
> S3 Storage Lens 存储统计管理工具指标是每日指标，每天发布到 CloudWatch 一次。当您在 CloudWatch 中查询 S3 Storage Lens 存储统计管理工具指标时，查询的期限必须为 1 天（86400 秒）。在您的每日 S3 Storage Lens 指标显示在 Amazon S3 控制台的 S3 Storage Lens 存储统计管理工具控制面板中后，这些指标可能需要几个小时才能显示在 CloudWatch 中。当您首次为 S3 Storage Lens 存储统计管理工具指标启用 CloudWatch 发布选项时，您的指标最多可能需要 24 小时才能将指标发布到 CloudWatch。

目前，S3 Storage Lens 存储统计管理工具指标无法通过 CloudWatch 流使用。

有关在 CloudWatch 中使用 S3 Storage Lens 存储统计管理工具指标的更多信息，请参阅以下主题。

主题


- 结合使用 CloudWatch 控制面板
- 设置警报、触发操作和使用异常检测
- 使用维度筛选指标
- 使用指标数学计算新指标
- 在图表中使用搜索表达式


## 结合使用 CloudWatch 控制面板

您可以使用 CloudWatch dashboards（控制面板）与其他应用程序指标一起监控 S3 Storage Lens 存储统计管理工具指标，并创建运营状况的统一视图。控制面板是 CloudWatch 控制台中的一种自定义主页，可用于在单一视图中监视资源。

CloudWatch 具有广泛的权限控制，不支持限制对一组特定指标或维度的访问。您的账户或企业中有权访问 CloudWatch 的用户将有权访问启用了 CloudWatch 支持选项的所有 S3 Storage Lens 存储统计管理工具配置的指标。您无法像在 S3 Storage Lens 存储统计管理工具中那样管理特定控制面板的权限。有关 CloudWatch 权限的更多信息，请参阅 Amazon CloudWatch User Guide（Amazon CloudWatch 用户指南）中的 Managing access permissions to your CloudWatch resources（管理对您的 CloudWatch 资源的访问权限）。

有关使用 CloudWatch 控制面板和配置权限的更多信息，请参阅 Amazon CloudWatch User Guide（Amazon CloudWatch 用户指南）中的 Using Amazon CloudWatch dashboards（使用 Amazon CloudWatch 控制面板）和 Sharing CloudWatch dashboards（共享 CloudWatch 控制面板）。

## 设置警报、触发操作和使用异常检测

您可以配置 CloudWatch 警报来监视 CloudWatch 中的 S3 Storage Lens 存储统计管理工具指标，并在超出阈值时采取行动。例如，您可以配置告警，当 Incomplete Multipart Upload Bytes（未完成分段上传字节）指标连续三天超过 1GB 时发送 Amazon SNS 通知。

您还可以启用异常检测以持续分析 S3 Storage Lens 存储统计管理工具指标、确定正常基线和表面异常。您可以根据指标的预期值创建异常检测告警。例如，您可以监视 Object Lock Enabled Bytes（启用对象锁定的字节）指标的异常情况，以检测未经授权移除对象锁定设置的情况。

有关更多信息以及示例，请参阅 Amazon CloudWatch User Guide（Amazon CloudWatch 用户指南）中的 Using Amazon CloudWatch alarms（使用 Using Amazon CloudWatch 告警）和 Creating an alarm from a metric on a graph（从图表上的指标创建告警）。

使用维度筛选指标

您可以在 CloudWatch 控制台中使用维度筛选 S3 Storage Lens 存储统计管理工具指标。例如，您可以按照 `configuration_id`、`aws_account_number`、`aws_region`、`bucket_name` 等方式进行筛选。

S3 Storage Lens 存储统计管理工具支持每个账户多个控制面板配置。这意味着不同的配置可以包含同一个桶。当这些指标发布到 CloudWatch 时，桶将在 CloudWatch 中具有重复的指标。要是只需查看 CloudWatch 中特定 S3 Storage Lens 存储统计管理工具配置的指标，您可以使用 `configuration_id` 维度。当您按照 `configuration_id` 筛选时，您只能看到与您标识的配置相关联的指标。

有关按配置 ID 进行筛选的更多信息，请参阅《Amazon CloudWatch 用户指南》中的搜索可用指标。

使用指标数学计算新指标

您可以使用指标数学查询多个 S3 Storage Lens 存储统计管理工具指标，并使用数学表达式基于这些度量创建新的时间序列。例如，您可以通过从对象计数中减去加密对象来为未加密对象创建一个新的指标。您还可以创建一个指标来获得平均对象大小，方法是将 `StorageBytes` 除以 `ObjectCount`，或者通过将 `BytesDownloaded` 除以 `StorageBytes` 来获得一天访问的字节数。

有关更多信息，请参阅 Amazon CloudWatch User Guide（Amazon CloudWatch 用户指南）中的 Using metric math（使用指标数学）。

在图表中使用搜索表达式

借助 S3 Storage Lens 存储统计管理工具指标，您可以创建搜索表达式。例如，您可以为所有名为 IncompleteMultipartUploadStorageBytes 的指标创建搜索表达式，并将 SUM 添加至表达式。使用此搜索表达式，您可以在单个指标中跨存储的所有维度查看未完成分段上传总字节数。

这个例子展示了用来为所有名为 IncompleteMultipartUploadStorageBytes 的指标创建搜索表达式的语法。

```
SUM(SEARCH('{AWS/S3/Storage-
Lens,aws_account_number,aws_region,configuration_id,metrics_version,record_type,storage_class}
 MetricName="IncompleteMultipartUploadStorageBytes"', 'Average',86400))
```

有关此语法的更多信息，请参阅 Amazon CloudWatch User Guide（Amazon CloudWatch 用户指南）中的 CloudWatch search expression syntax（CloudWatch 搜索表达式语法）。要使用搜索表达式创建 CloudWatch 图表，请参阅 Amazon CloudWatch User Guide（Amazon CloudWatch 用户指南）中的 Creating a CloudWatch graph with a search expression（使用搜索表达式创建 CloudWatch 图表）。

## Amazon S3 Storage Lens 存储统计管理工具使用案例

您可以使用 Amazon S3 Storage Lens 存储统计管理工具控制面板直观显示见解和趋势，标记异常值，并接收建议。S3 Storage Lens 存储统计管理工具指标分为与关键使用案例一致的类别。您可以使用这些指标来进行以下操作：

- 识别成本优化机会
- 应用数据保护最佳实践
- 应用访问管理最佳实践
- 提高应用程序工作负载的性能

例如，使用成本优化指标，您可以识别可降低您的 Amazon S3 存储成本的机会。您可以识别分段上传时间超过 7 天的桶，也可以识别正在累积非当前版本的桶。

同样，您可以使用数据保护指标来识别组织内未遵循数据保护最佳实践的桶。例如，您可以识别未使用 Amazon Key Management Service 密钥（SSE-KMS）进行原定设置加密或未启用 S3 版本控制的桶。

使用 S3 Storage Lens 存储统计管理工具访问管理指标，您可以识别 S3 对象所有权的桶设置，这样您就可以将访问控制列表（ACL）权限迁移到桶策略并禁用 ACL。

如果启用了 S3 Storage Lens 存储统计管理工具高级指标，您可以使用详细的状态代码指标了解成功或失败的请求的计数，这些计数可用于解决访问或性能问题。

借助高级指标，您还可以访问更多的成本优化和数据保护指标，这些指标可用于发现进一步降低整体 S3 存储成本的机会，并更好地遵循保护数据的最佳实践。例如，高级成本优化指标包括生命周期规则计数，您可以使用生命周期规则计数来识别没有生命周期规则的桶，从而使超过 7 天的未完成分段上传过期。高级数据保护指标包括复制规则计数。

有关指标类别的更多信息，请参阅指标类别。要获得 S3 Storage Lens 存储统计管理工具指标的完整列表，请参阅Amazon S3 Storage Lens 存储统计管理工具指标词汇表。

主题


- 使用 Amazon S3 Storage Lens 存储统计管理工具优化您的存储成本
- 使用 S3 Storage Lens 存储统计管理工具保护您的数据
- 使用 S3 Storage Lens 存储统计管理工具审计对象所有权设置
- 使用 S3 Storage Lens 存储统计管理工具指标提高性能


## 使用 Amazon S3 Storage Lens 存储统计管理工具优化您的存储成本

您可以使用 S3 Storage Lens 存储统计管理工具成本优化指标来降低 S3 存储的总体成本。成本优化指标可以帮助您确认您已根据最佳实践经济高效地配置 Amazon S3。例如，您可以确定以下成本优化机会：

- 具有超过 7 天的未完成分段上传的桶
- 累积了许多非当前版本的桶
- 不具有生命周期规则来中止未完成分段上传的桶
- 不具有使非当前版本对象过期的生命周期规则的桶
- 不具有将对象转换为其他存储类的生命周期规则的桶

然后，您可以使用这些数据向桶添加额外的生命周期规则。

以下示例说明如何使用 S3 Storage Lens 存储统计管理工具控制面板中的成本优化指标来优化存储成本。

主题


- 识别您最大的 S3 桶
- 发现冷的 Amazon S3 桶
- 查找未完成的分段上传
- 减少保留的非当前版本的数量
- 识别没有生命周期规则的桶并查看生命周期规则计数


### 识别您最大的 S3 桶

您要为在 S3 桶中存储对象付费。您需付费的费率取决于对象的大小、对象的存储时长及其存储类。利用 S3 Storage Lens 存储统计管理工具，您可以集中查看账户中的所有桶。要查看组织的所有账户中的

所有桶，您可以配置 Amazon Organizations 级 S3 Storage Lens 存储统计管理工具控制面板。在此控制面板视图中，您可以识别最大的桶。

步骤 1：识别最大的 S3 桶

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Storage Lens 和 Dashboards（控制面板）。
3. 在控制面板列表中，选择要查看的控制面板。

   控制面板打开后，您可以看到 S3 Storage Lens 存储统计管理工具收集指标的最新日期。您的控制面板始终加载指标可用的最新日期。
4. 要查看所选日期范围内按 Total storage（总存储）指标排列的最大桶的排名，请向下滚动到 Top N overview for date（日期的前 N 个概览）部分。

   您可以切换排序顺序以显示最小的桶。您还可以调整 Metric（指标）选择，以根据任何可用指标对桶进行排名。Top N overview for date（日期的前 N 个概览）部分还显示与前一天或前一周相比的百分比变化以及用于可视化趋势的火花线。该趋势对于免费指标为 14 天趋势，对于高级指标和建议为 30 天趋势。

   > **Note**
   >
   > 使用 S3 Storage Lens 存储统计管理工具高级指标和建议，指标可用于 15 个月的查询。有关更多信息，请参阅 指标选择。
5. 要了解有关您的桶的更详细的见解，请向上滚动到页面顶部，然后选择 Bucket（桶）选项卡。

   在 Bucket（桶）选项卡上，您可以看到诸如近期增长率、平均对象大小、最大前缀和对象数等详细信息。

步骤 2：导航到您的桶并进行调查

在确定最大的 S3 桶之后，您可以导航到 S3 控制台中的每个桶，以查看桶中的对象，了解其关联的工作负载，或识别桶的内部拥有者。您可以与桶拥有者联系，以了解此增长是否符合预期，或者此增长是否需要进一步监控和控制。

### 发现冷的 Amazon S3 桶

如果启用了 S3 Storage Lens 存储统计管理工具高级指标，您可以使用活动指标了解 S3 桶的活跃度。“冷”桶是指不再访问（或极少访问）其存储的桶。这种活跃程度缺乏通常表示桶的对象不经常访问。

活动指标，例如 GET Requests（Get 请求）和 Download Bytes（下载字节数），指明每天访问桶的频率。要了解访问模式的一致性并发现根本不再访问的桶，您可以对这些数据进行几个月的趋势分析。Retrieval rate（检索率）指标（计算方法为下载字节数/总存储），表示桶中每天访问的存储比例。

> **Note**
>
> 如果同一对象在一天中多次下载，则下载字节数会加倍。

#### 先决条件

要在 S3 Storage Lens 存储统计管理工具控制面板中查看活动指标，您必须启用 S3 Storage Lens 存储统计管理工具 Advanced metrics and recommendations（高级指标和建议），然后选择 Activity metrics（活动指标）。有关更多信息，请参阅 使用 S3 控制台。

#### 步骤 1：识别活动的桶

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Storage Lens 和 Dashboards（控制面板）。
3. 在控制面板列表中，选择要查看的控制面板。
4. 选择 Bucket（桶）选项卡，然后向下滚动到 Bubble analysis by buckets for date（按日期的桶划分的气泡分析）图表。

   在 Bubble analysis by buckets for date（按日期的桶划分的气泡分析）部分中，您可以使用任意三个指标在多个维度上绘制桶，以表示气泡的 X-axis（X 轴）、Y-axis（Y 轴）和 Size（大小）。
5. 要查找变冷的桶，请为 X-axis（X 轴）、Y-axis（Y 轴）和 Size（大小）选择 Total storage（总存储空间）、% retrieval rate（检索率百分比）和 Average object size（平均对象大小）指标。
6. 在 Bubble analysis by buckets for date（按日期的桶划分的气泡分析）部分中，查找检索率为零（或接近零）且相对存储大小较大的任何桶，然后选择代表桶的气泡。

   此时将出现一个方框，其中包含可提供更精细见解的选项。请执行以下操作之一：

a. 要更新 Bucket（桶）选项卡以仅显示选定桶的指标，请选择 Drill down（深入分析），然后选择 Apply（应用）。
b. 要按账户、Amazon Web Services 区域、存储类或桶聚合桶级别数据，请选择 Analyze by（分析依据），然后选择 Dimension（维度）。例如，要按存储类进行聚合，请为 Dimension（维度）选择 Storage class（存储类）。

要查找已经冷的桶，请使用 Total storage（总存储）、% retrieval rate（检索率百分比）和 Average object size（平均对象大小）指标执行气泡分析。查找检索率为零（或接近零）且相对存储大小较大的任何桶。

控制面板的 Bucket（桶）选项卡将更新，以显示所选聚合或筛选条件的数据。如果您按存储类或其他维度进行汇总，则该新选项卡将在您的控制面板中打开 [例如，Storage class（存储类）选项卡]。

步骤 2：调查冷桶

在此处，您可以识别您账户或组织中冷桶的拥有者，并了解是否仍然需要该存储。然后，您可以通过为这些桶配置生命周期过期配置或将数据存档到其中一个 Amazon S3 Glacier 存储类来优化成本。

为了避免冷桶继续发展的问题，您可以使用 S3 生命周期配置为桶自动转换数据，也可以启用使用 S3 Intelligent-Tiering 自动存档。

您也可以使用步骤 1 来识别热桶。然后，您可以确保这些桶使用正确的 S3 存储类，以确保它们在性能和成本方面最有效地处理请求。

查找未完成的分段上传

您可以使用分段上传将非常大的对象（最大 5TB）分成多个分段上载，以提高吞吐量并更快地从网络问题中恢复。如果分段上传过程未完成，则未完成的分段将保留在桶中（处于不可用状态）。这些未完成的分段将产生存储成本，直到上载过程完成或删除未完成的分段。有关更多信息，请参阅 在 Amazon S3 中使用分段上传来上传和复制对象。

借助 S3 Storage Lens 存储统计管理工具，您可以确定账户中或整个组织中未完成的分段上传字节数，包括超过 7 天的未完成多段上传。有关未完成分段上传指标的完整列表，请参阅Amazon S3 Storage Lens 存储统计管理工具指标词汇表。

作为最佳实践，我们建议配置生命周期规则，使超过特定天数的未完成分段上传过期。当您创建生命周期规则以使未完成分段上传过期时，我们建议以 7 天作为一个良好的起点。

步骤 1：查看未完成分段上传的总体趋势

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Storage Lens 和 Dashboards（控制面板）。
3. 在控制面板列表中，选择要查看的控制面板。
4. 在 Snapshot for date（日期的快照）部分中的 Metrics categories（指标类别）下，选择 Cost optimization（成本优化）。

   Snapshot for date（日期的快照）部分将更新，以显示 Cost optimization（成本优化）指标，其中包括 Incomplete multipart upload bytes greater than 7 days old（超过 7 天的未完成分段上传字节数）。

   在 S3 Storage Lens 存储统计管理工具控制面板的任何图表中，您都可以看到未完成分段上传的指标。您可以使用这些指标进一步评估未完成分段上传字节对存储的影响，包括对总体增长趋势的贡献。您还可以使用 Account（账户）、Amazon Web Services 区域、Bucket（桶）或 Storage class（存储类）选项卡深入到更深层次的聚合，对数据进行更深入的分析。有关示例，请参阅发现冷的 Amazon S3 桶。

步骤 2：识别具有最多不完整分段上传字节但没有生命周期规则来中止不完整分段上传的桶

先决条件

要在 S3 Storage Lens 存储统计管理工具控制面板中查看 Abort incomplete multipart upload lifecycle rule count（中止未完成分段上传生命周期规则计数）指标，您必须启用 S3 Storage Lens 存储统计管理工具 Advanced metrics and recommendations（高级指标和建议），然后选择 Advanced cost optimization metrics（高级成本优化指标）。有关更多信息，请参阅 使用 S3 控制台。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Storage Lens 和 Dashboards（控制面板）。
3. 在控制面板列表中，选择要查看的控制面板。
4. 要确定累积了超过 7 天的未完成分段上传的特定桶，请转到 Top N overview for date（日期的前 N 个概览）部分。

   原定设置情况下，Top N overview for date（日期的前 N 个概览）部分显示前 3 个桶的指标。您可以增加或减少 Top N（前 N 个）字段中的桶数量。Top N overview for date（日期的前 N 个概

览）部分还显示与前一天或前一周相比的百分比变化以及用于可视化趋势的火花线。（该趋势对于免费指标为 14 天趋势，对于高级指标和建议为 30 天趋势。）

> **Note**
>
> 使用 S3 Storage Lens 存储统计管理工具高级指标和建议，指标可用于 15 个月的查询。有关更多信息，请参阅 指标选择。

5. 对于 Metric（指标），在 Cost optimization（成本优化）类别中选择 Incomplete multipart upload bytes greater than 7 days old（超过 7 天的未完成分段上传字节数）。

   在 Top number buckets（前 number 个桶）下，您可以看到具有最多的超过 7 天的不完整分段上传存储字节的桶。

6. 要查看未完成分段上传的更详细的桶级指标，请滚动到页面顶部，然后选择 Bucket（桶）选项卡。

7. 向下滚动到 Bucket（桶）部分。对于 Metrics categories（指标类别），选择 Cost optimization（成本优化）。然后清除 Summary（摘要）。

   Buckets（桶）列表将更新，以显示所显示的桶的所有可用 Cost optimization（成本优化）指标。

8. 要筛选 Buckets（桶）列表以仅显示特定的成本优化指标，请选择首选项图标（ ）。

9. 清除所有成本优化指标的切换开关，直到只有 Incomplete multipart upload bytes greater than 7 days old（超过 7 天的未完成分段上传字节）和 Abort incomplete multipart upload lifecycle rule count（中止未完成的分段上传生命周期规则计数）保持选中状态。

10. （可选）在 Page size（页面大小）下，选择要在列表中显示的桶数。

11. 选择确认。

    Buckets（桶）列表会更新，以显示未完成分段上传和生命周期规则计数的桶级指标。您可以使用这些数据来识别具有最多的超过 7 天的不完整分段上传字节且缺少生命周期规则来中止未完成分段上传的桶。然后，您可以在 S3 控制台中导航到这些桶，并添加生命周期规则以删除已丢弃的未完成分段上传。

### 步骤 3：添加生命周期规则以在 7 天后删除未完成分段上传

要自动管理未完成的分段上传，您可以使用 S3 控制台创建生命周期配置，以使桶中的未完成分段上传字节在指定天数后过期。有关更多信息，请参阅 配置存储桶生命周期配置以删除未完成的分段上传。

### 减少保留的非当前版本的数量

启用后，S3 版本控制会保留同一对象的多个不同版本，当对象被意外删除或覆盖时，可以使用这些版本快速恢复数据。如果您在未配置生命周期规则以使非当前版本转换或过期的情况下启用了 S3 版本控制，则会累积大量以前的非当前版本，这可能会对存储成本产生影响。有关更多信息，请参阅 使用 S3 版本控制保留对象的多个版本。

步骤 1：识别具有最多非当前对象版本的桶

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Storage Lens 和 Dashboards（控制面板）。
3. 在控制面板列表中，选择要查看的控制面板。
4. 在 Snapshot for date（日期的快照）部分中的 Metric categories（指标类别）下，选择 Cost optimization（成本优化）。

   在 Snapshot for date（日期的快照）部分将更新，以显示 Cost optimization（成本优化）指标，其中包括 % noncurrent version bytes（非当前版本字节百分比）的指标。% noncurrent version bytes（非当前版本字节百分比）指标表示控制面板范围中在所选日期内归属于非当前版本的总存储字节的比例。

   > **Note**
   >
   > 如果 % noncurrent version bytes（非当前版本字节百分比）大于账户级存储的 10%，则可能表明您所存储的对象版本太多。

5. 要确定积累了大量非当前版本的特定桶，请执行以下操作：

   a. 向下滚动到 Top N overview for date（日期的前 N 个概览）部分。对于 Top N（前 N 个），输入您想要查看其数据的桶数。

   b. 对于 Metric（指标），选择 % noncurrent version bytes（非当前版本字节百分比）。

      在 Top number buckets（前 number 个桶）下，您可以看到 % noncurrent version bytes（非当前版本字节百分比）最高的桶（针对您指定的数字）。Top N overview for date（日期的前 N 个概览）部分还显示与前一天或前一周相比的百分比变化以及用于可视化趋势的火花线。该趋势对于免费指标为 14 天趋势，对于高级指标和建议为 30 天趋势。

> **Note**
>
> 使用 S3 Storage Lens 存储统计管理工具高级指标和建议，指标可用于 15 个月的查询。有关更多信息，请参阅 指标选择。

c. 要查看非当前对象版本的更详细的桶级指标，请滚动到页面顶部，然后选择 Bucket（桶）选项卡。

   在 S3 Storage Lens 存储统计管理工具控制面板中的任何图表或可视化效果中，您都可以使用 Account（账户）、Amazon Web Services 区域、Storage class（存储类）或 Bucket（桶）选项卡深入到更深层次的聚合。有关示例，请参阅发现冷的 Amazon S3 桶。

d. 在 Buckets（桶）部分中，对于 Metric categories（指标类别），选择 Cost optimization（成本优化）。然后，清除 Summary（摘要）。

   现在，您可以看到 % noncurrent version bytes（非当前版本字节百分比）指标，以及与非当前版本相关的其他指标。

步骤 2：确定缺少用于管理非当前版本的转换和过期生命周期规则的桶

先决条件

要在 S3 Storage Lens 存储统计管理工具控制面板中查看 Noncurrent version transition lifecycle rule count（非当前版本转换生命周期规则计数）和 Noncurrent version expiration lifecycle rule count（非当前版本过期生命周期规则计数）指标，必须启用 S3 Storage Lens 存储统计管理工具 Advanced metrics and recommendations（高级指标和建议），然后选择 Advanced cost optimization metrics（高级成本优化指标）。有关更多信息，请参阅 使用 S3 控制台。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Storage Lens 和 Dashboards（控制面板）。
3. 在控制面板列表中，选择要查看的控制面板。
4. 在 Storage Lens 存储统计管理工具控制面板中，选择 Bucket（桶）选项卡。
5. 向下滚动到 Bucket（桶）部分。对于 Metrics categories（指标类别），选择 Cost optimization（成本优化）。然后清除 Summary（摘要）。

   Buckets（桶）列表将更新，以显示所显示的桶的所有可用 Cost optimization（成本优化）指标。

6. 要筛选 Buckets（桶）列表以仅显示特定的成本优化指标，请选择首选项图标（ ）。
7. 清除所有成本优化指标的切换开关，直到只有以下指标保持选中状态：
   - % noncurrent version bytes（非当前版本字节百分比）
   - Noncurrent version transition lifecycle rule count（非当前版本转换生命周期规则计数）
   - Noncurrent version expiration lifecycle rule count（非当前版本过期生命周期规则计数）
8. （可选）在 Page size（页面大小）下，选择要在列表中显示的桶数。
9. 选择确认。

   Buckets（桶）列表将更新，以显示非当前版本字节和非当前版本生命周期规则计数的指标。您可以使用这些数据来识别非当前版本字节百分比高但缺少转换和过期生命周期规则的桶。然后，您可以在 S3 控制台中导航到这些桶，并将生命周期规则添加到这些桶。

步骤 3：添加转换非当前对象版本或使其过期的生命周期规则

确定哪些桶需要进一步调查后，您可以导航到 S3 控制台中的桶，并添加生命周期规则以使非当前版本在指定天数后过期。或者，为了降低成本，同时仍然保留非当前版本，您可以配置生命周期规则将非当前版本转换到 Amazon S3 Glacier 存储类之一。有关更多信息，请参阅 为启用了版本控制的存储桶指定生命周期规则。

识别没有生命周期规则的桶并查看生命周期规则计数

S3 Storage Lens 存储统计管理工具提供 S3 生命周期规则计数指标，您可以使用这些指标来识别缺少生命周期规则的桶。要查找没有生命周期规则的桶，您可以使用 Total buckets without lifecycle rules（无生命周期规则的桶总数）指标。没有 S3 生命周期配置的桶可能有您不再需要的存储，或者可以迁移到成本较低的存储类。您还可以使用生命周期规则计数指标来识别缺少特定类型的生命周期规则（例如过期或转换规则）的桶。

先决条件

要在 S3 Storage Lens 存储统计管理工具控制面板中查看生命规则计数指标和 Total buckets without lifecycle rules（无生命周期规则的桶总数）指标，您必须启用 S3 Storage Lens 存储统计管理工具 Advanced metrics and recommendations（高级指标和建议），然后选择 Advanced cost optimization metrics（高级成本优化指标）。有关更多信息，请参阅 使用 S3 控制台。

步骤 1：识别没有生命周期规则的桶

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Storage Lens 和 Dashboards（控制面板）。
3. 在控制面板列表中，选择要查看的控制面板。
4. 要识别没有生命周期规则的特定桶，请向下滚动到 Top N overview for date（日期的前 N 个概览）部分。

   原定设置情况下，Top N overview for date（日期的前 N 个概览）部分显示前 3 个桶的指标。在 Top N（前 N 个）字段中，您可以增加桶的数量。Top N overview for date（日期的前 N 个概览）部分还显示与前一天或前一周相比的百分比变化以及用于可视化趋势的火花线。该趋势对于免费指标为 14 天趋势，对于高级指标和建议为 30 天趋势。

   > **Note**
   >
   > 使用 S3 Storage Lens 存储统计管理工具高级指标和建议，指标可用于 15 个月的查询。有关更多信息，请参阅 指标选择。

5. 对于 Metric（指标），从 Cost optimization（成本优化）类别中选择 Total buckets without lifecycle rules（没有生命周期规则的桶总数）。
6. 查看 Total buckets without lifecycle rules（没有生命周期规则的桶总数）的以下数据：

   - Top number accounts（前 number 个账户）- 查看哪些账户拥有最多的没有生命周期规则的桶。
   - Top number Regions（前 number 个区域）- 按区域查看没有生命周期规则的桶的明细。
   - Top number buckets（前 number 个桶）- 查看哪些桶没有生命周期规则。

   在 S3 Storage Lens 存储统计管理工具控制面板中的任何图表或可视化效果中，您都可以使用 Account（账户）、Amazon Web Services 区域、Storage class（存储类）或 Bucket（桶）选项卡深入到更深层次的聚合。有关示例，请参阅发现冷的 Amazon S3 桶。

   在识别哪些桶没有生命周期规则后，您还可以查看桶的特定生命周期规则计数。

步骤 2：查看桶的生命周期规则计数

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Storage Lens 和 Dashboards（控制面板）。
3. 在控制面板列表中，选择要查看的控制面板。
4. 在 S3 Storage Lens 存储统计管理工具控制面板中，选择 Bucket（桶）选项卡。
5. 向下滚动到 Bucket（桶）部分。在 Metrics categories（指标类别）下，选择 Cost optimization（成本优化）。然后清除 Summary（摘要）。

   Buckets（桶）列表将更新，以显示所显示的桶的所有可用 Cost optimization（成本优化）指标。
6. 要筛选 Buckets（桶）列表以仅显示特定的成本优化指标，请选择首选项图标（  ）。
7. 清除所有成本优化指标的切换开关，直到只有以下指标保持选中状态：

   - Transition lifecycle rule count（转换生命周期规则计数）
   - Expiration lifecycle rule count（过期生命周期规则计数）
   - Noncurrent version transition lifecycle rule count（非当前版本转换生命周期规则计数）
   - Noncurrent version expiration lifecycle rule count（非当前版本过期生命周期规则计数）
   - Abort incomplete multipart upload lifecycle rule count（中止未完成分段上传生命周期规则计数）
   - Total lifecycle rule count（生命周期规则总计数）
8. （可选）在 Page size（页面大小）下，选择要在列表中显示的桶数。
9. 选择确认。

   Buckets（桶）列表会更新，以显示您的桶的生命周期规则计数指标。您可以使用这些数据来识别没有生命周期规则的桶或缺少特定类型的生命周期规则（例如过期或转换规则）的桶。然后，您可以在 S3 控制台中导航到这些桶，并将生命周期规则添加到这些桶。

步骤 3：添加生命周期规则

识别没有生命周期规则的桶后，您可以添加生命周期规则。有关更多信息，请参阅在存储桶上设置 S3 生命周期配置和S3 生命周期配置的示例。

使用 S3 Storage Lens 存储统计管理工具保护您的数据

您可以使用 Amazon S3 Storage Lens 存储统计管理工具数据保护指标来识别尚未应用数据保护最佳实践的桶。您可以使用这些指标来采取措施并应用符合最佳实践的标准设置，以保护您的账户或组织的桶中的数据。例如，您可以使用数据保护指标来识别不使用 Amazon Key Management Service（Amazon KMS）密钥（SSE-KMS）进行原定设置加密的桶或使用 Amazon 签名版本 2（SigV2）的请求。

以下使用案例提供使用 S3 Storage Lens 存储统计管理工具控制面板识别异常值并跨 S3 桶应用数据保护最佳实践的策略。

主题


- 识别不使用具有 Amazon KMS 的服务器端加密（SSE-KMS）进行原定设置加密的桶
- 识别已启用 S3 版本控制的桶
- 识别使用 Amazon 签名版本 2（SigV2）的请求
- 计算每个桶的复制规则总计数
- 确定对象锁定字节的百分比


识别不使用具有 Amazon KMS 的服务器端加密（SSE-KMS）进行原定设置加密的桶

借助 Amazon S3 原定设置加密，您可以设置 S3 桶的原定设置加密行为。有关更多信息，请参阅 the section called “设置默认存储桶加密”。

您可以使用 SSE-KMS enabled bucket count（启用 SSE-KMS 的桶计数）和 % SSE-KMS enabled buckets（启用 SSE-KMS 的桶的百分比）指标来识别使用具有 Amazon KMS 密钥的服务器端加密（SSE-KMS）进行原定设置加密的桶。S3 Storage Lens 存储统计管理工具还提供关于未加密字节、未加密对象、加密字节和加密对象的指标。要获得指标的完整列表，请参阅 Amazon S3 Storage Lens 存储统计管理工具指标词汇表。

您可以在常规加密指标的上下文中分析 SSE-KMS 加密指标，以识别不使用 SSE-KMS 的桶。如果您想对账户或组织中的所有桶使用 SSE-KMS，则可以将这些桶的原定设置加密设置更新为使用 SSE-KMS。除了 SSE-KMS 之外，您还可以将服务器端加密与 Amazon S3 托管式密钥（SSE-S3）或与客户托管式密钥（SSE-C）结合使用。有关更多信息，请参阅 利用加密来保护数据。

步骤 1：确定哪些桶使用 SSE-KMS 进行原定设置加密

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。

2. 在左侧导航窗格中，选择 Storage Lens 和 Dashboards（控制面板）。
3. 在 Dashboards（控制面板）列表中，选择您要查看的控制面板的名称。
4. 在 Trends and distributions（趋势和分布）部分中，为主要指标选择 % SSE-KMS enabled bucket count（启用 SSE-KMS 的桶计数百分比），为辅助指标选择 % encrypted bytes（加密字节百分比）。

   Trend for date（日期的趋势）图更新，以显示 SSE-KMS 和加密字节的趋势。
5. 要查看 SSE-KMS 的更精细桶级见解，请执行以下操作：

   a. 在图上选择一个点。此时将出现一个方框，其中包含可提供更精细见解的选项。

   b. 选择 Buckets（桶）维度。然后选择 Apply（应用）。
6. 在 Distribution by buckets for date（按日期的桶划分的分布）图中，选择 SSE-KMS enabled bucket count（启用 SSE-KMS 的桶计数）指标。
7. 现在，您可以查看哪些桶启用了 SSE-KMS，哪些桶未启用。

步骤 2：更新桶原定设置加密设置

现在，您已经确定了哪些桶在 % encrypted bytes（加密字节百分比）的上下文中使用 SSE-KMS，您可以识别不使用 SSE-KMS 的桶。然后，您可以选择在 S3 控制台中导航到这些桶，并更新其原定设置加密设置以使用 SSE-KMS 或 SSE-S3。有关更多信息，请参阅 配置默认加密。

识别已启用 S3 版本控制的桶

启用后，S3 版本控制功能会保留同一对象的多个版本，当对象被意外删除或覆盖时，可以使用这些版本快速恢复数据。您可以使用 Versioning-enabled bucket count（启用版本控制的桶计数）指标来查看哪些桶使用 S3 版本控制。然后，您可以在 S3 控制台中执行操作，从而为其他桶启用 S3 版本控制。

步骤 1：识别已启用 S3 版本控制的桶

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在导航窗格中，选择 Storage Lens 和 Dashboards（控制面板）。
3. 在 Dashboards（控制面板）列表中，选择您要查看的控制面板的名称。
4. 在 Trends and distributions（趋势和分布）部分中，为主要指标选择 Versioning-enabled bucket count（启用版本控制的桶计数），为辅助指标选择 Buckets（桶）。

Trend for date（日期的趋势）图更新，以显示启用 S3 版本控制的桶的趋势。在趋势线的正下方，您可以看到 Storage class distribution（存储类分布）和 Region distribution（区域分布）子部分。

5. 要查看您在 Trend for date（日期的趋势）图中看到的任何桶的更精细见解，以便进行更深入的分析，请执行以下操作：

   a. 在图上选择一个点。此时将出现一个方框，其中包含可提供更精细见解的选项。

   b. 选择一个维度应用于您的数据以进行更深入的分析：Account（账户）、Amazon Web Services 区域、Storage class（存储类）或 Bucket（桶）。然后选择 Apply（应用）。

6. 在 Bubble analysis by buckets for date（按日期的桶划分的气泡分析）部分中，选择 Versioning-enabled bucket count（启用版本控制的桶计数）、Buckets（桶）和 Active buckets（活动的桶）指标。

   Bubble analysis by buckets for date（按日期的桶划分的气泡分析）部分将更新，以显示所选指标的数据。您可以使用这些数据在桶总计数的上下文中查看哪些桶启用了 S3 版本控制。在 Bubble analysis by buckets for date（按日期的桶划分的气泡分析）部分中，您可以使用任意三个指标在多个维度上绘制桶，以表示气泡的 X-axis（X 轴）、Y-axis（Y 轴）和 Size（大小）。

步骤 2：启用 S3 版本控制

识别启用了 S3 版本控制的桶后，您可以识别从未启用 S3 版本控制或暂停版本控制的桶。然后，您可以选择在 S3 控制台中为这些桶启用版本控制。有关更多信息，请参阅 在存储桶上启用版本控制。

识别使用 Amazon 签名版本 2（SigV2）的请求

您可以使用 All unsupported signature requests（所有不支持的签名请求）指标来识别使用 Amazon 签名版本 2（SigV2）的请求。这些数据可以帮助您识别使用 SigV2 的特定应用程序。然后，您可以将这些应用程序迁移到 Amazon 签名版本 4（SigV4）。

SigV4 是所有新 S3 应用程序的推荐签名方法。SigV4 可提供更高的安全性，并且在所有 Amazon Web Services 区域中得到支持。有关更多信息，请参阅 Amazon S3 更新 - SigV2 弃用期延长并修改。

先决条件

要在 S3 Storage Lens 存储统计管理工具控制面板中查看 All unsupported signature requests（所有不支持的签名请求），您必须启用 S3 Storage Lens 存储统计管理工具 Advanced metrics and recommendations（高级指标和建议），然后选择 Advanced data protection metrics（高级数据保护指标）。有关更多信息，请参阅 使用 S3 控制台。

步骤 1：按 Amazon Web Services 账户、区域和桶检查 SigV2 签名趋势

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Storage Lens 和 Dashboards（控制面板）。
3. 在 Dashboards（控制面板）列表中，选择您要查看的控制面板的名称。
4. 要识别具有使用 SigV2 的请求的特定桶、账户和区域，请执行以下操作：

   a. 在 Top N overview for date（日期的前 N 个概览）下的 Top N（前 N 个）中，输入您想要查看其数据的桶数。

   b. 对于 Metric（指标），从 Data protection（数据保护）类别中选择 All unsupported signature requests（所有不支持的签名请求）。

   Top N overview for date（日期的前 N 个概览）将更新，以按账户、Amazon Web Services 区域和桶显示 SigV2 请求的数据。Top N overview for date（日期的前 N 个概览）部分还显示与前一天或前一周相比的百分比变化以及用于可视化趋势的火花线。该趋势对于免费指标为 14 天趋势，对于高级指标和建议为 30 天趋势。

   > **Note**
   >
   > 使用 S3 Storage Lens 存储统计管理工具高级指标和建议，指标可用于 15 个月的查询。有关更多信息，请参阅 指标选择。

步骤 2：识别应用程序通过 SigV2 请求访问的桶

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Storage Lens 和 Dashboards（控制面板）。
3. 在 Dashboards（控制面板）列表中，选择您要查看的控制面板的名称。
4. 在 Storage Lens 存储统计管理工具控制面板中，选择 Bucket（桶）选项卡。
5. 向下滚动到 Bucket（桶）部分。在 Metrics categories（指标类别）下，选择 Data protection（数据保护）。然后清除 Summary（摘要）。

   Buckets（桶）列表将更新，以显示所显示的桶的所有可用 Data protection（数据保护）指标。

6. 要筛选 Buckets（桶）列表以仅显示特定的数据保护指标，请选择首选项图标（  ）。
7. 清除所有数据保护指标的切换开关，直到只有以下指标保持选中状态：
   - All unsupported signature requests（所有不支持的签名请求）
   - % all unsupported signature requests（所有不支持的签名请求百分比）
8. （可选）在 Page size（页面大小）下，选择要在列表中显示的桶数。
9. 选择确认。

   Buckets（桶）列表将更新以显示 SigV2 请求的桶级指标。您可以使用这些数据来识别具有 SigV2 请求的特定桶。然后，您可以使用此信息将应用程序迁移到 SigV4。有关更多信息，请参阅《Amazon Simple Storage Service API》参考中的验证请求 (Amazon Signature Version 4)。

### 计算每个桶的复制规则总计数

S3 复制支持跨 Amazon S3 桶自动以异步方式复制对象。为对象复制配置的桶可由相同 Amazon Web Services 账户 或不同账户拥有。有关更多信息，请参阅 在区域内和跨区域复制对象。

您可以使用 S3 Storage Lens 存储统计管理工具复制规则计数指标来获取有关配置为进行复制的桶的每个桶的详细信息。此信息包括桶和区域内部以及跨桶和区域的复制规则。

#### 先决条件

要在 S3 Storage Lens 存储统计管理工具控制面板中查看复制规则计数指标，您必须启用 S3 Storage Lens 存储统计管理工具 Advanced metrics and recommendations（高级指标和建议），然后选择 Advanced data protection metrics（高级数据保护指标）。有关更多信息，请参阅 使用 S3 控制台。

#### 步骤 1：计算每个桶的复制规则总计数

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Storage Lens 和 Dashboards（控制面板）。
3. 在 Dashboards（控制面板）列表中，选择您要查看的控制面板的名称。
4. 在 Storage Lens 存储统计管理工具控制面板中，选择 Bucket（桶）选项卡。
5. 向下滚动到 Bucket（桶）部分。在 Metrics categories（指标类别）下，选择 Data protection（数据保护）。然后清除 Summary（摘要）。

6. 要筛选 Buckets（桶）列表以仅显示复制规则计数指标，请选择首选项图标（ ）。
7. 清除所有数据保护指标的切换开关，直到只有复制规则计数指标保持选中状态：
   - Same-Region Replication rule count（同区域复制规则计数）
   - Cross-Region Replication rule count（跨区域复制规则计数）
   - Same-account replication rule count（同账户复制规则计数）
   - Cross-account replication rule count（跨账户复制规则计数）
   - Total replication rule count（复制规则总计数）
8. （可选）在 Page size（页面大小）下，选择要在列表中显示的桶数。
9. 选择确认。

步骤 2：添加复制规则

获得每个桶的复制规则计数后，您可以选择创建其他复制规则。有关更多信息，请参阅 配置实时复制的示例。

确定对象锁定字节的百分比

借助 S3 对象锁定，您可以使用一次写入，多次读取（WORM）模式存储对象。您可以使用对象锁定帮助您防止在固定的时间段内或无限期地删除或覆盖对象。您只能在创建桶时启用对象锁定，也可以启用 S3 版本控制。但是，您可以编辑各个对象版本的保留期，也可以对启用了对象锁定的桶应用依法保留。有关更多信息，请参阅 使用对象锁定以锁定对象。

您可以使用 S3 Storage Lens 存储统计管理工具中的对象锁定指标来查看您的账户或组织的 % Object Lock bytes（对象锁定字节百分比）指标。您可以使用这些信息来识别您的账户或组织中未遵循数据保护最佳实践的桶。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Storage Lens 和 Dashboards（控制面板）。
3. 在 Dashboards（控制面板）列表中，选择您要查看的控制面板的名称。
4. 在 Snapshot（快照）部分的 Metrics categories（指标类别）下，选择 Data protection（数据保护）。

   Snapshot（快照）部分更新以显示数据保护指标，包括 % Object Lock bytes（对象锁定字节百分比）指标。您可以查看您的账户或组织的对象锁定字节的总体百分比。

5. 要查看每个桶的 % Object Lock bytes（对象锁定字节百分比），请向下滚动到 Top N overview（前 N 个概览）部分。

   要获取对象锁定的对象级数据，您还可以使用 Object Lock object count（对象锁定对象计数）和 % Object Lock objects（对象锁定对象百分比）指标。

6. 对于 Metric（指标），从 Data protection（数据保护）类别中选择 % Object Lock bytes（对象锁定字节百分比）。

   原定设置情况下，Top N overview for date（日期的前 N 个概览）部分显示前 3 个桶的指标。在 Top N（前 N 个）字段中，您可以增加桶的数量。Top N overview for date（日期的前 N 个概览）部分还显示与前一天或前一周相比的百分比变化以及用于可视化趋势的火花线。该趋势对于免费指标为 14 天趋势，对于高级指标和建议为 30 天趋势。

   > **Note**
   >
   > 使用 S3 Storage Lens 存储统计管理工具高级指标和建议，指标可用于 15 个月的查询。有关更多信息，请参阅 指标选择。

7. 查看 % Object Lock bytes（对象锁定字节百分比）的以下数据：

   - Top number accounts（前 number 个账户）- 查看哪些账户具有最高和最低的 % Object Lock bytes（对象锁定字节百分比）。
   - Top number Regions（前 number 个区域）- 查看按区域划分的 % Object Lock bytes（对象锁定字节百分比）明细。
   - Top number buckets（前 number 个桶）-查看哪些桶具有最高和最低的 % Object Lock bytes（对象锁定字节百分比）。

使用 S3 Storage Lens 存储统计管理工具审计对象所有权设置

Amazon S3 对象所有权是 S3 桶级别的设置，您可以使用它来禁用访问控制列表（ACL）并控制桶中对象的所有权。如果将对象所有权设置为“强制桶拥有者”，则可以禁用访问控制列表（ACL）并获取桶中每个对象的所有权。这种方法简化了对存储在 Amazon S3 中的数据的访问管理。

预设情况下，当另一个 Amazon Web Services 账户 将对象上载到您的 S3 桶，该账户（对象写入器）拥有该对象，拥有对象的访问权限，并可以授予其他用户通过 ACL 访问该数据元的权限。您可以使用对象所有权来更改此原定设置行为。

Amazon S3 中的大多数现代使用案例不再需要使用 ACL。因此，我们建议您禁用 ACL，除非出现必须单独控制每个对象的访问权限的异常情况。通过将对象所有权设置为“强制桶拥有者”，您可以禁用 ACL 并依赖策略进行访问控制。有关更多信息，请参阅 为您的存储桶控制对象所有权和禁用 ACL。。

使用 S3 Storage Lens 存储统计管理工具访问管理指标，您可以识别未禁用 ACL 的桶。识别这些桶后，您可以将 ACL 权限迁移到策略并对这些桶禁用 ACL。

主题


- 步骤 1：确定对象所有权设置的一般趋势
- 步骤 2：确定对象所有权设置的桶级趋势
- 步骤 3：将您的对象所有权设置更新为“强制桶拥有者”以禁用 ACL


### 步骤 1：确定对象所有权设置的一般趋势

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Storage Lens 和 Dashboards（控制面板）。
3. 在 Dashboards（控制面板）列表中，选择您要查看的控制面板的名称。
4. 在 Snapshot for date（日期的快照）部分中的 Metrics categories（指标类别）下，选择 Access management（访问管理）。

   Snapshot for date（日期的快照）部分将更新，以显示 % Object Ownership bucket owner enforced（对象所有权强制桶拥有者的百分比）指标。您可以看到账户或组织中为对象所有权使用“强制桶拥有者”设置以禁用 ACL 的桶的总体百分比。

### 步骤 2：确定对象所有权设置的桶级趋势

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Storage Lens 和 Dashboards（控制面板）。
3. 在 Dashboards（控制面板）列表中，选择您要查看的控制面板的名称。
4. 要查看更详细的桶级指标，请选择 Bucket（桶）选项卡。
5. 在 Distribution by buckets for date（按日期的桶划分的分布）部分中，选择 % Object Ownership bucket owner enforced（对象所有权强制桶拥有者的百分比）指标。

图表将更新以显示 % Object Ownership bucket owner enforced（对象所有权强制桶拥有者的百分比）的每个桶明细。您可以看到哪些桶对于对象所有权使用“强制桶拥有者”设置来禁用 ACL。

6. 要在上下文中查看“强制桶拥有者”设置，请向下滚动到 Buckets（桶）部分。对于 Metrics categories（指标类别），选择 Access management（访问管理）。然后清除 Summary（摘要）。

   Buckets（桶）列表显示所有三种对象所有权设置的数据：强制桶拥有者、首选桶拥有者以及对象写入器。

7. 要筛选 Buckets（桶）列表以仅显示特定对象所有权设置的指标，请选择首选项图标（  ）。
8. 清除您不想看到的指标。
9. （可选）在 Page size（页面大小）下，选择要在列表中显示的桶数。
10. 选择确认。

步骤 3：将您的对象所有权设置更新为“强制桶拥有者”以禁用 ACL

在确定对于对象所有权使用对象写入器和首选桶拥有者设置后，您可以将 ACL 权限迁移到桶策略。完成 ACL 权限迁移后，您可以将对象所有权设置更新为“强制桶拥有者”以禁用 ACL。有关更多信息，请参阅 禁用 ACL 的先决条件。

使用 S3 Storage Lens 存储统计管理工具指标提高性能

如果启用了 S3 Storage Lens 存储统计管理工具高级指标，您可以使用详细的状态代码指标来了解成功或失败的请求的计数。您可以使用此信息来排查访问或性能问题。详细的状态代码指标显示 HTTP 状态代码的计数，例如 403 Forbidden（403 禁止）和 503 Service Unavailable（503 服务不可用）。您可以查看跨 S3 桶、账户和组织的详细状态代码指标的总体趋势。然后，您可以深入了解桶级别的指标，以识别当前正在访问这些桶并导致错误的工作负载。

例如，您可以查看 403 Forbidden error count（403 禁止错误计数）指标，以确定在未应用正确权限的情况下访问桶的工作负载。识别这些工作负载后，您可以在 S3 Storage Lens 存储统计管理工具之外进行深入探索，以对 403 Forbidden（403 禁止）错误进行故障排除。

此示例向您展示如何使用 403 Forbidden error count（403 禁止错误计数）和 % 403 Forbidden errors（403 禁止错误百分比）指标对 403 Forbidden（403 禁止）错误进行趋势分析。您可以使用这些指标来识别在未应用正确权限的情况下访问桶的工作负载。您可以对任何其他 Detailed status code metrics（详细状态代码指标）进行类似的趋势分析。有关更多信息，请参阅 Amazon S3 Storage Lens 存储统计管理工具指标词汇表。

先决条件

要在 S3 Storage Lens 存储统计管理工具控制面板中查看 Detailed status code metrics（详细状态代码指标），您必须启用 S3 Storage Lens 存储统计管理工具 Advanced metrics and recommendations（高级指标和建议），然后选择 Detailed status code metrics（详细状态代码指标）。有关更多信息，请参阅 使用 S3 控制台。

主题

- 步骤 1：对单个 HTTP 状态代码进行趋势分析
- 步骤 2：按桶分析错误计数
- 步骤 3：排除错误

步骤 1：对单个 HTTP 状态代码进行趋势分析

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Storage Lens 和 Dashboards（控制面板）。
3. 在 Dashboards（控制面板）列表中，选择您要查看的控制面板的名称。
4. 在 Trends and distributions（趋势和分布）部分中，对于 Primary metric（主要指标），从 Detailed status codes（详细状态代码）类别中选择 403 Forbidden error count（403 禁止错误计数）。对于 Secondary metric（辅助指标），选择 % 403 Forbidden errors（403 禁止错误百分比）。
5. 向下滚动到 Top N overview for date（日期的前 N 个概览）部分。对于 Metrics（指标），从 Detailed status codes（详细状态代码）类别中选择 403 Forbidden error count（403 禁止错误计数）或 % 403 Forbidden errors（403 禁止错误百分比）。

   Top N overview for date（日期的前 N 个概览）部分将更新，以显示按账户、Amazon Web Services 区域 和桶显示排名靠前的 403 禁止错误计数。

步骤 2：按桶分析错误计数

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Storage Lens 和 Dashboards（控制面板）。
3. 在 Dashboards（控制面板）列表中，选择您要查看的控制面板的名称。

4. 在 Storage Lens 存储统计管理工具控制面板中，选择 Bucket（桶）选项卡。
5. 向下滚动到 Bucket（桶）部分。对于 Metrics categories（指标类别），选择 Detailed status code（详细状态代码）指标。然后清除 Summary（摘要）。

   Buckets（桶）列表将更新，以显示所有可用的详细状态代码指标。您可以使用这些信息来查看哪些桶具有很大比例的特定 HTTP 状态代码，以及哪些状态代码在桶中是常见的。
6. 要筛选 Buckets（桶）列表以仅显示特定的详细状态代码指标，请选择首选项图标（  ）。
7. 清除您不想在 Buckets（桶）列表中看到的任何详细状态代码指标的切换开关。
8. （可选）在 Page size（页面大小）下，选择要在列表中显示的桶数。
9. 选择确认。

   Buckets（桶）列表显示您指定的桶数量的错误计数指标。您可以使用这些信息来识别出现许多错误的特定桶，并按桶排除错误。

步骤 3：排除错误

在识别出具有高比例的特定 HTTP 状态代码的桶后，您可以排除这些错误。有关更多信息，请参阅下列内容：

- 当我尝试在 Amazon S3 中上载文件时，为什么会出现 403 Forbidden（403 禁止）错误？
- 当我尝试在 Amazon S3 中修改桶策略时，为什么会出现 403 Forbidden（403 禁止）错误？
- 如何排除所有资源都来自相同 Amazon Web Services 账户的 Amazon S3 桶中的 403 Forbidden（403 禁止）错误？
- 如何排除来自 Amazon S3 的 HTTP 500 或 503 错误？

## 将 Amazon S3 Storage Lens 存储统计管理工具与 Amazon Organizations 结合使用

Amazon S3 Storage Lens 存储统计管理工具是一项云存储分析功能，您可以使用它在整个组织范围内了解对象存储的使用情况和活动。您可以使用 S3 Storage Lens 存储统计管理工具指标生成摘要见解，例如，了解整个组织中有多少存储空间，或增长最快的桶和前缀是哪些。还可以使用 Amazon S3 Storage Lens 存储统计管理工具收集属于 Amazon Organizations 层次结构一部分的所有 Amazon Web Services 账户的存储指标和用量数据。为此，您必须使用 Amazon Organizations，并且必须使用您的 Amazon Organizations 管理账户启用 S3 Storage Lens 存储统计管理工具可信访问权限。

启用可信访问权限后，向组织中的账户添加委派管理员访问权限。委派管理员账户用于创建 S3 Storage Lens 存储统计管理工具配置和控制面板，以收集组织范围的存储指标和用户数据。有关启用可信访问权限的更多信息，请参阅《Amazon Organizations 用户指南》中的 Amazon S3 Storage Lens 存储统计管理工具和 Amazon Organizations。

主题


- 为 S3 Storage Lens 存储统计管理工具启用可信访问权限
- 为 S3 Storage Lens 存储统计管理工具禁用可信访问权限
- 为 S3 Storage Lens 存储统计管理工具注册委托管理员
- 为 S3 Storage Lens 存储统计管理工具取消注册委托管理员


## 为 S3 Storage Lens 存储统计管理工具启用可信访问权限

通过启用可信访问权限，可让 Amazon S3 Storage Lens 存储统计管理工具通过 Amazon Organizations API 操作访问 Amazon Organizations 层次结构、成员资格和结构。然后，S3 Storage Lens 存储统计管理工具便成为整个组织结构的可信服务。

无论何时创建控制面板配置，S3 Storage Lens 存储统计管理工具都会在组织的管理或委托管理员账户中创建服务相关角色。服务相关角色向 S3 Storage Lens 存储统计管理工具授予执行以下操作的权限：

- 描述组织
- 列出账户
- 验证组织的 Amazon Web Services 服务访问权限列表
- 为组织获取委托管理员

随后，S3 Storage Lens 存储统计管理工具可以确保它具有相应的访问权限，可收集组织中账户的跨账户指标。有关更多信息，请参阅使用面向 Amazon S3 Storage Lens 存储统计管理工具的服务相关角色。

启用可信访问权限后，您可以为组织中的账户分配委托管理员访问权限。当账户被标记为服务的委托管理员时，该账户将获得访问所有只读组织 API 操作的授权。此访问权限向委托管理员提供了对您组织成员和结构的可见性，以便他们也可以创建 S3 Storage Lens 存储统计管理工具控制面板。

> **Note**
>
> - 只能由管理账户启用可信访问权限。

- 只有管理账户和委托管理员才能为您的组织创建 S3 Storage Lens 存储统计管理工具控制面板或配置。

使用 S3 控制台

使 S3 Storage Lens 存储统计管理工具拥有 Amazon Organizations 可信访问权限

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，导航到 Storage Lens 存储统计管理工具。
3. 选择 Amazon Organizations 设置。将显示 Storage Lens 存储统计管理工具的 Amazon Organizations 访问权限页面。
4. 在 Amazon Organizations 可信访问权限下，选择编辑。

   将显示 Amazon Organizations 访问权限页面。
5. 选择启用，以便为 S3 Storage Lens 存储统计管理工具控制面板启用可信访问权限。
6. 选择保存更改。

使用 Amazon CLI

Example

以下示例显示了如何在 Amazon CLI 中为 S3 Storage Lens 存储统计管理工具启用 Amazon Organizations 可信访问权限。

```
aws organizations enable-aws-service-access --service-principal storage-
lens.s3.amazonaws.com
```

使用适用于 Java 的 Amazon SDK

Example – 使用适用于 Java 的 SDK 为 S3 Storage Lens 存储统计管理工具启用 Amazon Organizations 可信访问权限

以下示例显示了如何在适用于 Java 的 SDK 中为 S3 Storage Lens 存储统计管理工具启用可信访问权限。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
```

```
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.organizations.AWSOrganizations;
import com.amazonaws.services.organizations.AWSOrganizationsClient;
import com.amazonaws.services.organizations.model.EnableAWSServiceAccessRequest;

public class EnableOrganizationsTrustedAccess {
 private static final String S3_STORAGE_LENS_SERVICE_PRINCIPAL = "storage-
lens.s3.amazonaws.com";

 public static void main(String[] args) {
  try {
            AWSOrganizations organizationsClient = AWSOrganizationsClient.builder()
                .withCredentials(new ProfileCredentialsProvider())
                .withRegion(Regions.US_EAST_1)
                .build();

            organizationsClient.enableAWSServiceAccess(new
 EnableAWSServiceAccessRequest()
                .withServicePrincipal(S3_STORAGE_LENS_SERVICE_PRINCIPAL));
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon Organizations couldn't
 process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon Organizations couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon Organizations.
            e.printStackTrace();
        }
 }
}
```

## 为 S3 Storage Lens 存储统计管理工具禁用可信访问权限

以委派管理员身份移除账户或禁用可信访问权限，会将账户拥有者的 S3 Storage Lens 存储统计管理工具控制面板指标限制为仅在账户级别起作用。然后，每个账户持有人所能看到的 S3 Storage Lens 存储统计管理工具的优势仅限于其账户的有限范围，而不是整个组织范围。

在 S3 Storage Lens 存储统计管理工具中禁用可信访问权限时，任何需要可信访问权限的控制面板都不再更新。所创建的任何组织控制面板也不再更新。相反，您只能查询 S3 Storage Lens 存储统计管理工具控制面板的历史数据（当这些数据仍然可用时）。

> **Note**
>
> - 禁用对 S3 Storage Lens 存储统计管理工具的可信访问还会自动阻止所有组织级控制面板收集和聚合存储指标。这是因为 S3 Storage Lens 存储统计管理工具不再对组织账户拥有可信访问权限。
> - 管理账户和委派管理员账户仍可以查看任何禁用的控制面板的历史数据。这些账户还可以在历史数据仍可用时查询这些数据。

使用 S3 控制台

为 S3 Storage Lens 存储统计管理工具禁用可信访问权限

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，导航到 Storage Lens 存储统计管理工具。
3. 选择 Amazon Organizations 设置。将显示 Storage Lens 存储统计管理工具的 Amazon Organizations 访问权限页面。
4. 在 Amazon Organizations 可信访问权限下，选择编辑。

   将显示 Amazon Organizations 访问权限页面。
5. 选择禁用，以便为 S3 Storage Lens 存储统计管理工具控制面板禁用可信访问权限。
6. 选择保存更改。

使用 Amazon CLI

Example

以下示例使用 Amazon CLI 为 S3 Storage Lens 存储统计管理工具禁用可信访问权限。

```
aws organizations disable-aws-service-access --service-principal storage-
lens.s3.amazonaws.com
```

使用适用于 Java 的 Amazon SDK

Example – 为 S3 Storage Lens 存储统计管理工具禁用 Amazon Organizations 可信访问权限

以下示例显示了如何在适用于 Java 的 SDK 中为 S3 Storage Lens 存储统计管理工具禁用 Amazon Organizations 可信访问权限。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.organizations.AWSOrganizations;
import com.amazonaws.services.organizations.AWSOrganizationsClient;
import com.amazonaws.services.organizations.model.DisableAWSServiceAccessRequest;

public class DisableOrganizationsTrustedAccess {
 private static final String S3_STORAGE_LENS_SERVICE_PRINCIPAL = "storage-
lens.s3.amazonaws.com";

 public static void main(String[] args) {
  try {
            AWSOrganizations organizationsClient = AWSOrganizationsClient.builder()
                .withCredentials(new ProfileCredentialsProvider())
                .withRegion(Regions.US_EAST_1)
                .build();

            // Make sure to remove any existing delegated administrator for S3 Storage
 Lens
            // before disabling access; otherwise, the request will fail.
            organizationsClient.disableAWSServiceAccess(new
 DisableAWSServiceAccessRequest()
                .withServicePrincipal(S3_STORAGE_LENS_SERVICE_PRINCIPAL));
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon Organizations couldn't
 process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon Organizations couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon Organizations.
            e.printStackTrace();
        }
```

```
  }
}
```

## 为 S3 Storage Lens 存储统计管理工具注册委托管理员

您可以使用组织的管理账户或委托管理员账户创建组织级控制面板。委托管理员账户允许除管理账户以外的其他账户创建组织级控制面板。只有组织的管理账户才能将其他账户注册为组织的委托管理员以及取消其注册。

启用可信访问权限后，可以通过 management account，使用 Amazon Organizations REST API、Amazon CLI 或 SDK 对组织中的账户注册委派管理员访问权限。（有关更多信息，请参阅《Amazon Organizations API 参考》中的 RegisterDelegatedAdministrator。）当账户注册为委派管理员后，该账户将获得访问所有只读 Amazon Organizations API 操作的授权。这就提供了对您组织成员和结构的可见性，以便他们可以代表您创建 S3 Storage Lens 存储统计管理工具控制面板。

> **Note**
>
> 在使用 Amazon Organizations REST API、Amazon CLI 或 SDK 指定委托管理员之前，必须调用 EnableAWSOrganizationsAccess 操作。

### 使用 S3 控制台

为 S3 Storage Lens 存储统计管理工具注册委托管理员

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，导航到 Storage Lens 存储统计管理工具。
3. 选择 Amazon Organizations 设置。
4. 在委派管理员下，选择注册账户。
5. 添加 Amazon Web Services 账户 ID，以便将该账户注册为委派管理员。委派管理员可以为组织中的所有账户和存储创建组织级别控制面板。
6. 选择注册账户。

使用 Amazon CLI

Example

以下示例显示了如何使用 Amazon CLI 为 S3 Storage Lens 存储统计管理工具注册组织委派管理员。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
aws organizations register-delegated-administrator --service-principal storage-
lens.s3.amazonaws.com --account-id 111122223333
```

使用适用于 Java 的 Amazon SDK

Example – 为 S3 Storage Lens 存储统计管理工具注册组织委派管理员

以下示例显示了如何在适用于 Java 的 SDK 中为 S3 Storage Lens 存储统计管理工具注册 Amazon Organizations 委派管理员。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.organizations.AWSOrganizations;
import com.amazonaws.services.organizations.AWSOrganizationsClient;
import
 com.amazonaws.services.organizations.model.RegisterDelegatedAdministratorRequest;

public class RegisterOrganizationsDelegatedAdministrator {
 private static final String S3_STORAGE_LENS_SERVICE_PRINCIPAL = "storage-
lens.s3.amazonaws.com";

 public static void main(String[] args) {
  try {
            String delegatedAdminAccountId = "111122223333"; // Account Id for the
 delegated administrator.
            AWSOrganizations organizationsClient = AWSOrganizationsClient.builder()
                .withCredentials(new ProfileCredentialsProvider())
                .withRegion(Regions.US_EAST_1)
                .build();

            organizationsClient.registerDelegatedAdministrator(new
 RegisterDelegatedAdministratorRequest()
```

```
                .withAccountId(delegatedAdminAccountId)
                .withServicePrincipal(S3_STORAGE_LENS_SERVICE_PRINCIPAL));
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon Organizations couldn't
 process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon Organizations couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon Organizations.
            e.printStackTrace();
        }
 }
}
```

## 为 S3 Storage Lens 存储统计管理工具取消注册委托管理员

启用可信访问权限后，还可以对组织中的账户注销委派管理员访问权限。委派管理员账户可让除 management account 以外的其它账户创建组织级别控制面板。只有组织的管理账户才能以组织的委托管理员身份取消注册账户。

还可以通过管理账户，使用 Amazon Organizations Amazon Web Services Management Console、REST API、Amazon CLI 或 Amazon SDK 来注销委派管理员。有关更多信息，请参阅 Amazon Organizations API 参考中的 DeregisterDelegatedAdministrator。

当账户被注销委派管理员时，该账户将失去对以下各项的访问权限：

- 所有只读 Amazon Organizations API 操作，这些操作可提供组织成员和结构的可见性。
- 委派管理员创建的所有组织级别控制面板。取消注册委托管理员还会自动阻止该委托管理员创建的所有组织级控制面板聚合新的存储指标。

> **Note**
>
> 如果注销的委派管理员创建的已禁用控制面板的历史数据仍可供查询，则这些管理员仍然可以查看这些数据。

使用 S3 控制台

为 S3 Storage Lens 存储统计管理工具注销委派管理员

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，导航到 Storage Lens 存储统计管理工具。
3. 选择 Amazon Organizations 设置。
4. 在委派管理员下，选择您希望注销的账户。
5. 选择注销账户。已注销的账户不再是委派管理员，且现在无法为组织中的所有账户和存储创建组织级别控制面板。
6. 选择注册账户。

使用 Amazon CLI

Example

以下示例显示了如何使用 Amazon CLI 为 S3 Storage Lens 存储统计管理工具注销组织委派管理员。要使用此示例，请将 *111122223333* 替换为您自己的 Amazon Web Services 账户 ID。

```
aws organizations deregister-delegated-administrator --service-principal storage-
lens.s3.amazonaws.com --account-id 111122223333
```

使用适用于 Java 的 Amazon SDK

Example – 为 S3 Storage Lens 存储统计管理工具注销组织委派管理员

以下示例显示了如何使用适用于 Java 的 SDK 为 S3 Storage Lens 存储统计管理工具注销组织委派管理员。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.organizations.AWSOrganizations;
import com.amazonaws.services.organizations.AWSOrganizationsClient;
import
 com.amazonaws.services.organizations.model.DeregisterDelegatedAdministratorRequest;
```

```
public class DeregisterOrganizationsDelegatedAdministrator {
 private static final String S3_STORAGE_LENS_SERVICE_PRINCIPAL = "storage-
lens.s3.amazonaws.com";

 public static void main(String[] args) {
  try {
            String delegatedAdminAccountId = "111122223333"; // Account Id for the
 delegated administrator.
            AWSOrganizations organizationsClient = AWSOrganizationsClient.builder()
                .withCredentials(new ProfileCredentialsProvider())
                .withRegion(Regions.US_EAST_1)
                .build();

            organizationsClient.deregisterDelegatedAdministrator(new
 DeregisterDelegatedAdministratorRequest()
                .withAccountId(delegatedAdminAccountId)
                .withServicePrincipal(S3_STORAGE_LENS_SERVICE_PRINCIPAL));
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon Organizations couldn't
 process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon Organizations couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon Organizations.
            e.printStackTrace();
        }
 }
}
```

## 使用 S3 Storage Lens 组筛选和汇总指标

Amazon S3 Storage Lens 存储统计管理工具组使用基于对象元数据的自定义筛选条件聚合指标。Storage Lens 组可帮助您深入了解数据的特征，例如按龄期划分的对象分布、最常见的文件类型等。例如，您可以按对象标签筛选指标以识别增长最快的数据集，或者根据对象大小和龄期可视化存储，为制定存储存档策略提供信息。因此，Amazon S3 Storage Lens 存储统计管理工具组可以帮助您更好地了解和优化 S3 存储。

使用 Storage Lens 组时，您可以使用对象元数据（例如前缀、后缀、对象标签、对象大小或对象龄期）来分析和筛选 S3 Storage Lens 存储统计管理工具指标。您也可以组合应用这些筛选条件。将 Storage Lens 组附加到 S3 Storage Lens 存储统计管理工具控制面板后，您可以直接在控制面板中查看 Amazon S3 Storage Lens 存储统计管理工具组聚合的 S3 Storage Lens 存储统计管理工具指标。

例如，您还可以按对象大小或龄段筛选指标，以确定存储的哪一部分由小对象组成。然后，您可以将此信息与 S3 Intelligent-Tiering 或 S3 生命周期结合使用，将小对象过渡到不同的存储类，以实现成本和存储优化。

主题


- S3 Storage Lens 组工作原理
- 使用 Storage Lens 组


## S3 Storage Lens 组工作原理

您可以通过 Storage Lens 组，使用基于对象元数据的自定义筛选条件来聚合指标。定义自定义筛选条件时，可以使用前缀、后缀、对象标签、对象大小、对象期龄或这些自定义筛选条件的组合。在创建 Storage Lens 组期间，您还可以包括一个或多个筛选条件。要指定多个筛选条件，请使用 `And` 或 `Or` 逻辑运算符。

创建和配置 Storage Lens 组时，该 Storage Lens 组本身将充当要将该组附加到的控制面板中的自定义筛选条件。然后，在控制面板中，您可以使用 Storage Lens 组筛选条件，根据您在组中定义的自定义筛选条件来获取存储指标。

要在 S3 Storage Lens 存储统计管理工具控制面板中查看 Storage Lens 组的数据，您必须在创建该组后将其附加到控制面板。将 Storage Lens 组关联到 Storage Lens 存储统计管理工具控制面板后，您的控制面板将在 48 小时内收集存储使用情况指标。然后，您可以在 Storage Lens 存储统计管理工具控制面板中可视化这些数据，也可以通过指标导出将其导出。如果您忘记将 Storage Lens 组附加到控制面板，则不会在任何地方捕获或显示您的 Storage Lens 组数据。

> **Note**
>
> - 创建 S3 Storage Lens 组时，您将创建一个 Amazon 资源。因此，每个 Storage Lens 组都有自己的 Amazon 资源名称 (ARN)，您可以在将 Storage Lens 组附加到 S3 Storage Lens 存储统计管理工具控制面板或将其从该控制面板排除时指定该名称。
> - 如果您的 Storage Lens 组未附加到控制面板，则创建 Storage Lens 组不会产生任何额外费用。
> - S3 Storage Lens 存储统计管理工具聚合了所有匹配的 Storage Lens 组下某个对象的使用情况指标。因此，如果某个对象与两个或更多 Storage Lens 组的筛选条件相匹配，则在整个存储使用情况中，您会看到同一对象的重复计数。

您可以在指定的（支持的 Amazon Web Services 区域 列表中的）主区域中创建账户级别的 Storage Lens 组。然后，您可以将您的 Storage Lens 组附加到多个 Storage Lens 存储统计管理工具控制面板，前提是这些控制面板位于同一个 Amazon Web Services 账户和主区域中。您最多可以为每个 Amazon Web Services 账户中的每个主区域创建 50 个 Storage Lens 组。

您可以使用 Amazon S3 控制台、Amazon Command Line Interface (Amazon CLI)、Amazon SDK 或 Amazon S3 REST API 创建和管理 S3 Storage Lens 组。

主题


- 查看 Storage Lens 组聚合指标
- Storage Lens 组权限
- Storage Lens 组配置
- Amazon 资源标签
- Storage Lens 组指标导出


## 查看 Storage Lens 组聚合指标

您可以通过将 Storage Lens 组附加到控制面板来查看这些组的聚合指标。要附加的 Storage Lens 组必须位于控制面板账户中指定的主区域内。

要将 Storage Lens 组附加到控制面板，您必须在控制面板配置的 Storage Lens 组聚合部分指定该组。如果您有多个 Storage Lens 组，则可以筛选 Storage Lens 组聚合结果，使其根据需要仅包括或排除某些组。有关将组附加到控制面板的更多信息，请参阅 the section called “附加或移除 Storage Lens 组”。

附加组后，您将在 48 小时内在控制面板中看到新增的 Storage Lens 组聚合数据。

> **Note**
>
> 要查看您的 Storage Lens 组的聚合指标，您必须将该组附加到 S3 Storage Lens 存储统计管理工具控制面板。

## Storage Lens 组权限

Storage Lens 组需要 Amazon Identity and Access Management (IAM) 中的某些权限才能授权访问 S3 Storage Lens 组操作。要授予这些权限，您可以使用基于身份的 IAM policy。您可以将此策略附加到

IAM 用户、组或角色，以授予其权限。此类权限可能包括创建或删除 Storage Lens 组、查看其配置或管理其标签。

您授予权限的 IAM 用户或角色必须属于创建或拥有 Storage Lens 组的账户。

要使用 Storage Lens 组和查看您的 Storage Lens 组指标，您必须首先拥有使用 S3 Storage Lens 存储统计管理工具的相应权限。有关更多信息，请参阅 the section called “设置权限”。

要创建和管理 S3 Storage Lens 组，您必须拥有以下 IAM 权限，具体取决于您要执行的操作：

| 操作 | IAM 权限 |
| --- | --- |
| 新建 Storage Lens 组 | `s3:CreateStorageLensGroup` |
| 使用标签新建 Storage Lens 组 | `s3:CreateStorageLensGroup` ， `s3:TagResource` |
| 更新现有 Storage Lens 组 | `s3:UpdateStorageLensGroup` |
| 返回 Storage Lens 组配置的详细信息 | `s3:GetStorageLensGroup` |
| 列出主区域中的所有 Storage Lens 组 | `s3:ListStorageLensGroups` |
| 删除 Storage Lens 组 | `s3:DeleteStorageLensGroup` |
| 列出已添加到 Storage Lens 组的标签 | `s3:ListTagsForResource` |
| 为现有 Storage Lens 组添加或更新 Storage Lens 组标签 | `s3:TagResource` |
| 从 Storage Lens 组删除标签 | `s3:UntagResource` |

以下是如何在创建 Storage Lens 组的账户中配置 IAM policy 的示例。要使用此策略，请将 *`us-east-1`* 替换为您的 Storage Lens 组所在的主区域。将 *`111122223333`* 替换为您的 Amazon Web Services 账户 ID，然后将 *`example-storage-lens-group`* 替换为您的 Storage Lens 组的名称。要将这些权限应用于所有 Storage Lens 组，请将 *`example-storage-lens-group`* 替换为 *。

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "EXAMPLE-Statement-ID",
            "Effect": "Allow",
            "Action": [
                "s3:CreateStorageLensGroup",
                "s3:UpdateStorageLensGroup",
                "s3:GetStorageLensGroup",
                "s3:ListStorageLensGroups",
                "s3:DeleteStorageLensGroup,
                "s3:TagResource",
                "s3:UntagResource",
                "s3:ListTagsForResource"
                ],
            "Resource": "arn:aws:s3:us-east-1:111122223333:storage-lens-group/example-storage-lens-group"
        }
    ]
}
```

有关 S3 Storage Lens 存储统计管理工具权限的更多信息，请参阅 设置 Amazon S3 Storage Lens 存储统计管理工具权限。有关 IAM policy 语言的更多信息，请参阅 Amazon S3 中的策略和权限。

Storage Lens 组配置

S3 Storage Lens 组名称

我们建议您使用 Storage Lens 组的用途为其命名，这样您就可以轻松确定要将哪些组附加到控制面板。要将 Storage Lens 组附加到控制面板，您必须在控制面板配置的 Storage Lens 组聚合部分指定该组。

账户中的 Storage Lens 组名称必须唯一。长度不得超过 64 个字符，只能包含字母（a-z、A-Z）、数字 (0-9)、连字符 (-) 和下划线 (_)。

主区域

主区域是创建和维护 Storage Lens 组的 Amazon Web Services 区域。您的 Storage Lens 组是在与 Amazon S3 Storage Lens 存储统计管理工具控制面板相同的主区域创建的。Storage Lens 组配置和指标也存储在该区域中。您最多可以在主区域中创建 50 个 Storage Lens 组。

创建 Storage Lens 组后，您无法编辑主区域。

范围

要将对象包含在 Storage Lens 组中，这些对象必须在 Amazon S3 Storage Lens 存储统计管理工具控制面板的范围内。Storage Lens 存储统计管理工具控制面板的范围由您在 S3 Storage Lens 存储统计管理工具控制面板配置的控制面板范围中包含的桶决定。

您可以为对象使用不同的筛选条件来定义 Storage Lens 组的范围。要在 S3 Storage Lens 存储统计管理工具控制面板中查看这些 Storage Lens 组指标，对象必须与您在 Storage Lens 组中包含的筛选条件相匹配。例如，假设您的 Storage Lens 组要包括带有前缀 `marketing` 和后缀 `.png` 的对象，但没有对象与这些条件相匹配。在这种情况下，在您的每日指标导出中不会生成此 Storage Lens 组的指标，并且您的控制面板中也不会显示该组的指标。

筛选条件

您可以在 S3 Storage Lens 组中使用以下筛选条件：

- 前缀 – 指定要包括的对象的前缀，该前缀是对象键名称开头的一串字符。例如，如果前缀筛选条件的值为 `images`，则将包括带有以下任何前缀的对象：`images/`、`images-marketing` 和 `images/production`。前缀的最大长度是 1024 个字节。
- 后缀 – 指定要包括的对象的后缀（例如 `.png`、`.jpeg` 或 `.csv`）。后缀的最大长度是 1024 个字节。
- 对象标签 – 指定要用于筛选的对象标签列表。标签键不能超过 128 个 Unicode 字符，标签值不能超过 256 个 Unicode 字符。请注意，如果将对象标签值字段留空，则 S3 Storage Lens 组仅将该对象与标签值也为空的其它对象进行匹配。
- 龄期 – 指定要包括的对象的对象龄期范围（以天为单位）。仅支持整数。
- 大小 – 指定要包括的对象的对象大小范围（以字节为单位）。仅支持整数。允许的最大值为 5 TB。

Storage Lens 组对象标签

您可以创建最多包含 10 个对象标签筛选条件的 Storage Lens 组。以下示例包含两个对象标签键值对作为名为 *`Marketing-Department`* 的 Storage Lens 组的筛选条件。要使用此示例，请使用您的组名称替换 *`Marketing-Department`*，并将 *`object-tag-key-1`*、*`object-tag-value-1`* 等替换为要用于筛选的对象标签键值对。

```
{
    "Name": "Marketing-Department",
    "Filter": {
```

```
     "MatchAnyTag":[
                {
                    "Key": "object-tag-key-1",
                    "Value": "object-tag-value-1"
                },
                {
                    "Key": "object-tag-key-2",
                    "Value": "object-tag-value-2"
                }
            ]
    }
}
```

### 逻辑运算符（**And** 或 **Or**）

要在 Storage Lens 组中包含多个筛选条件，可以使用逻辑运算符（And 或 Or）。在以下示例中，名为 *Marketing-Department* 的 Storage Lens 组使用 And 运算符包含 Prefix、ObjectAge 和 ObjectSize 筛选条件。由于使用 And 运算符，因此只有与所有这些筛选条件匹配的对象才会包括在 Storage Lens 组的范围内。

要使用此示例，请将 *user input placeholders* 替换为要用于筛选的值。

```
{
    "Name": "Marketing-Department",
    "Filter": {
        "And": {
            "MatchAnyPrefix": [
                "prefix-1",
                "prefix-2",
                "prefix-3/sub-prefix-1"
            ],
             "MatchObjectAge": {
                "DaysGreaterThan": 10,
                "DaysLessThan": 60
            },
            "MatchObjectSize": {
                "BytesGreaterThan": 10,
                "BytesLessThan": 60
            }
        }
    }
}
```

> **Note**
>
> 如果要包括与任何筛选条件相匹配的对象，请将此示例中的 And 逻辑运算符替换为 Or 逻辑运算符。

### Amazon 资源标签

每个 S3 Storage Lens 组都视为一个 Amazon 资源，有自己的 Amazon 资源名称 (ARN)。因此，在配置 Storage Lens 组时，可以选择向该组添加 Amazon 资源标签。最多可以为每个 Storage Lens 组添加 50 个标签。要创建带标签的 Storage Lens 组，您必须拥有 `s3:CreateStorageLensGroup` 和 `s3:TagResource` 权限。

您可以使用 Amazon 资源标签根据部门、业务线或项目对资源进行分类。如果您有许多相同类型的资源，这样做会非常有用。通过应用标签，您可以根据分配给特定 Storage Lens 组的标签快速识别该组。您还可以使用标签对成本进行跟踪和分配。

此外，当您向 Storage Lens 组添加 Amazon 资源标签时，将激活基于属性的访问权限控制 (ABAC)。ABAC 是一种基于属性（在本文中，也就是标签）定义权限的授权策略。您还可以在 IAM policy 中使用指定资源标签的条件，从而控制对 Amazon 资源的访问。

您可以修改标签的键和值，还可以随时删除资源的标签。此外，请注意以下限制：

- 标签键和标签值区分大小写。
- 如果您添加的标签的值与该实例上现有标签的值相同，新的值就会覆盖旧值。
- 如果删除资源，资源的所有标签也会被删除。
- 不要在 Amazon 资源标签中包含隐私或敏感数据。
- 不支持系统标签（或标签键以 `aws:` 开头的标签）。
- 每个标签键的长度不能超过 128 个字符。每个标签值的长度不能超过 256 个字符。

### Storage Lens 组指标导出

S3 Storage Lens 组指标包含在 Storage Lens 组所附加到的控制面板的 Amazon S3 Storage Lens 存储统计管理工具指标导出中。有关 Storage Lens 指标导出功能的一般信息，请参阅 使用数据导出查看 Amazon S3 Storage Lens 存储统计管理工具指标。

Storage Lens 组的指标导出包括您将 Storage Lens 组附加到的控制面板范围内的任何 S3 Storage Lens 指标。导出还包括 Storage Lens 组的其它指标数据。

创建 Storage Lens 组后，您的指标导出每天都会发送到您在为组所附加到的控制面板配置指标导出时选择的桶。您最长可能需要 48 小时才能收到第一份指标导出。

要在每日导出中生成指标，对象必须与您在 Storage Lens 组中包含的筛选条件相匹配。如果没有对象与您在 Storage Lens 组中包含的筛选条件相匹配，则不会生成任何指标。但是，如果某个对象与两个或更多 Storage Lens 组相匹配，则当该对象出现在指标导出中时，该对象将针对每个组单独列出。

您可以通过在控制面板指标导出的 `record_type` 列中查找以下值之一来识别 Storage Lens 组的指标：

- `STORAGE_LENS_GROUP_BUCKET`
- `STORAGE_LENS_GROUP_ACCOUNT`

`record_value` 列显示 Storage Lens 组的资源 ARN（例如 `arn:aws:s3:us-east-1:111122223333:storage-lens-group/Marketing-Department`）。

## 使用 Storage Lens 组

Amazon S3 Storage Lens 存储统计管理工具组使用基于对象元数据的自定义筛选条件聚合指标。您可以使用前缀、后缀、对象标签、对象大小或对象龄期来分析和筛选 S3 Storage Lens 存储统计管理工具指标。使用 Amazon S3 Storage Lens 存储统计管理工具组，您还可以在 Amazon S3 桶内以及跨多个桶，对使用情况进行分类。因此，您将能够更好地了解和优化 S3 存储。

要开始可视化 Storage Lens 组的数据，必须先将 Storage Lens 组附加到 S3 Storage Lens 存储统计管理工具控制面板。如果您需要在控制面板中管理 Storage Lens 组，可以编辑控制面板配置。要查看您的账户下有哪些 Storage Lens 组，您可以将其列出。要查看哪些 Storage Lens 组已附加到控制面板，您可以随时查看控制面板中的 Storage Lens 组选项卡。要查看或更新现有 Storage Lens 组的范围，可以查看其详细信息。您还可以永久删除 Storage Lens 组。

要管理权限，您可以创建用户定义的 Amazon 资源标签并将其添加到 Storage Lens 组。您可以使用 Amazon 资源标签根据部门、业务线或项目对资源进行分类。如果您有许多相同类型的资源，这样做会非常有用。通过应用标签，您可以根据分配给特定 Storage Lens 组的标签快速识别该组。

此外，当您向 Storage Lens 组添加 Amazon 资源标签时，将激活基于属性的访问权限控制 (ABAC)。ABAC 是一种基于属性（在本文中，也就是标签）定义权限的授权策略。您还可以在 IAM policy 中使用指定资源标签的条件，从而控制对 Amazon 资源的访问。

主题

- 创建 Storage Lens 组

- 将 S3 Storage Lens 组附加到控制面板或从控制面板移除
- 可视化 Storage Lens 组数据
- 更新 Storage Lens 组
- 使用 Storage Lens 组管理 Amazon 资源标签
- 列出所有 Storage Lens 组
- 查看 Storage Lens 组详细信息
- 删除 Storage Lens 组

创建 Storage Lens 组

以下示例演示如何使用 Amazon S3 控制台、Amazon Command Line Interface (Amazon CLI) 和 适用于 Java 的 Amazon SDK 创建 Amazon S3 Storage Lens 存储统计管理工具组。

使用 S3 控制台

创建 Storage Lens 组

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在页面顶部的导航栏中，选择当前所显示 Amazon 区域的名称。接下来，选择要切换到的区域。
3. 在左侧导航窗格中，选择 Storage Lens 组。
4. 选择创建 Storage Lens 组。
5. 在常规下，查看您的主区域，然后输入 Storage Lens 组名称。
6. 在范围下，选择要应用于 Storage Lens 组的筛选条件。要应用多个筛选条件，请选择您的筛选条件，然后选择 AND 或 OR 逻辑运算符。

    - 对于前缀筛选条件，请选择前缀，然后输入前缀字符串。要添加多个前缀，请选择添加前缀。要移除前缀，请选择要移除的前缀旁的移除。
    - 对于对象标签筛选条件，请选择对象标签，然后输入对象的键值对。然后选择添加标签。要移除标签，请选择要移除的标签旁的移除。
    - 对于后缀筛选条件，请选择后缀，然后输入后缀字符串。要添加多个后缀，请选择添加后缀。要移除后缀，请选择要移除的后缀旁的移除。
    - 对于龄期筛选条件，请以天为单位指定对象的龄期范围。选择指定最小对象龄期，然后输入最小对象龄期。然后，选择指定最大对象龄期并输入最大对象龄期。

- 对于大小筛选条件，请指定对象大小范围和衡量单位。选择指定最小对象大小，然后输入最小对象大小。选择指定最大对象大小，然后输入最大对象大小。

7. （可选）对于 Amazon 资源标签，请添加键值对，然后选择添加标签。
8. 选择创建 Storage Lens 组。

使用 Amazon CLI

以下示例 Amazon CLI 命令将创建一个 Storage Lens 组。要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control create-storage-lens-group --account-id 111122223333 \
--region us-east-1 --storage-lens-group=file://./marketing-department.json
```

以下示例 Amazon CLI 命令将创建一个具有两个 Amazon 资源标签的 Storage Lens 组。要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control create-storage-lens-group --account-id 111122223333 \
--region us-east-1 --storage-lens-group=file://./marketing-department.json \
--tags Key=k1,Value=v1 Key=k2,Value=v2
```

有关示例 JSON 配置，请参阅 Storage Lens 组配置。

使用适用于 Java 的 Amazon SDK

以下 适用于 Java 的 Amazon SDK 示例将创建一个 Storage Lens 组。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

Example – 创建包含单个筛选条件的 Storage Lens 组

以下示例将创建一个名为 *Marketing-Department* 的 Storage Lens 组。该组有一个对象龄期筛选条件，指定了 *30* 至 *90* 天的龄期范围。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
```

```
import software.amazon.awssdk.services.s3control.model.CreateStorageLensGroupRequest;
import software.amazon.awssdk.services.s3control.model.MatchObjectAge;
import software.amazon.awssdk.services.s3control.model.StorageLensGroup;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupFilter;

public class CreateStorageLensGroupWithObjectAge {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            StorageLensGroupFilter objectAgeFilter = StorageLensGroupFilter.builder()
                    .matchObjectAge(MatchObjectAge.builder()
                            .daysGreaterThan(30)
                            .daysLessThan(90)
                            .build())
                    .build();

            StorageLensGroup storageLensGroup = StorageLensGroup.builder()
                    .name(storageLensGroupName)
                    .filter(objectAgeFilter)
                    .build();

            CreateStorageLensGroupRequest createStorageLensGroupRequest =
 CreateStorageLensGroupRequest.builder()
                    .storageLensGroup(storageLensGroup)
                    .accountId(accountId).build();

            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.createStorageLensGroup(createStorageLensGroupRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
```

```
}
```

Example – 使用 **AND** 运算符创建包含多个筛选条件的 Storage Lens 组

以下示例将创建一个名为 *Marketing-Department* 的 Storage Lens 组。该组使用 AND 运算符来指示对象必须匹配所有筛选条件。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.CreateStorageLensGroupRequest;
import software.amazon.awssdk.services.s3control.model.MatchObjectAge;
import software.amazon.awssdk.services.s3control.model.MatchObjectSize;
import software.amazon.awssdk.services.s3control.model.S3Tag;
import software.amazon.awssdk.services.s3control.model.StorageLensGroup;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupAndOperator;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupFilter;


public class CreateStorageLensGroupWithAndFilter {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            // Create object tags.
            S3Tag tag1 = S3Tag.builder()
                    .key("object-tag-key-1")
                    .value("object-tag-value-1")
                    .build();
            S3Tag tag2 = S3Tag.builder()
                    .key("object-tag-key-2")
                    .value("object-tag-value-2")
                    .build();

            StorageLensGroupAndOperator andOperator =
 StorageLensGroupAndOperator.builder()
                    .matchAnyPrefix("prefix-1", "prefix-2", "prefix-3/sub-prefix-1")
```

```
                    .matchAnySuffix(".png", ".gif", ".jpg")
                    .matchAnyTag(tag1, tag2)
                    .matchObjectAge(MatchObjectAge.builder()
                            .daysGreaterThan(30)
                            .daysLessThan(90).build())
                    .matchObjectSize(MatchObjectSize.builder()
                            .bytesGreaterThan(1000L)
                            .bytesLessThan(6000L).build())
                    .build();

            StorageLensGroupFilter andFilter = StorageLensGroupFilter.builder()
                    .and(andOperator)
                    .build();

            StorageLensGroup storageLensGroup = StorageLensGroup.builder()
                    .name(storageLensGroupName)
                    .filter(andFilter)
                    .build();

            CreateStorageLensGroupRequest createStorageLensGroupRequest =
 CreateStorageLensGroupRequest.builder()
                    .storageLensGroup(storageLensGroup)
                    .accountId(accountId).build();

            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.createStorageLensGroup(createStorageLensGroupRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Example – 使用 **OR** 运算符创建包含多个筛选条件的 Storage Lens 组

以下示例将创建一个名为 *Marketing-Department* 的 Storage Lens 组。该组使用 OR 运算符来应用前缀筛选条件（*prefix-1*、*prefix-2*、*prefix3/sub-prefix-1*）或对象大小筛选条件（大小范围在 *1000* 字节至 *6000* 字节之间）。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.CreateStorageLensGroupRequest;
import software.amazon.awssdk.services.s3control.model.MatchObjectSize;
import software.amazon.awssdk.services.s3control.model.StorageLensGroup;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupFilter;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupOrOperator;

public class CreateStorageLensGroupWithOrFilter {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            StorageLensGroupOrOperator orOperator =
 StorageLensGroupOrOperator.builder()
                    .matchAnyPrefix("prefix-1", "prefix-2", "prefix-3/sub-prefix-1")
                    .matchObjectSize(MatchObjectSize.builder()
                            .bytesGreaterThan(1000L)
                            .bytesLessThan(6000L)
                            .build())
                    .build();

            StorageLensGroupFilter orFilter = StorageLensGroupFilter.builder()
                    .or(orOperator)
                    .build();

            StorageLensGroup storageLensGroup = StorageLensGroup.builder()
                    .name(storageLensGroupName)
                    .filter(orFilter)
                    .build();
```

```
            CreateStorageLensGroupRequest createStorageLensGroupRequest =
 CreateStorageLensGroupRequest.builder()
                    .storageLensGroup(storageLensGroup)
                    .accountId(accountId).build();

            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.createStorageLensGroup(createStorageLensGroupRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Example – 使用单个筛选条件和两个 Amazon 资源标签创建 Storage Lens 组

以下示例将创建一个名为 *Marketing-Department* 的 Storage Lens 组，该组具有后缀筛选条件。此示例还向 Storage Lens 组添加了两个 Amazon 资源标签。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.CreateStorageLensGroupRequest;
import software.amazon.awssdk.services.s3control.model.StorageLensGroup;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupFilter;
import software.amazon.awssdk.services.s3control.model.Tag;

public class CreateStorageLensGroupWithResourceTags {
    public static void main(String[] args) {
```

```
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            // Create Amazon resource tags.
            Tag resourceTag1 = Tag.builder()
                    .key("resource-tag-key-1")
                    .value("resource-tag-value-1")
                    .build();
            Tag resourceTag2 = Tag.builder()
                    .key("resource-tag-key-2")
                    .value("resource-tag-value-2")
                    .build();

            StorageLensGroupFilter suffixFilter = StorageLensGroupFilter.builder()
                    .matchAnySuffix(".png", ".gif", ".jpg")
                    .build();

            StorageLensGroup storageLensGroup = StorageLensGroup.builder()
                    .name(storageLensGroupName)
                    .filter(suffixFilter)
                    .build();

            CreateStorageLensGroupRequest createStorageLensGroupRequest =
CreateStorageLensGroupRequest.builder()
                    .storageLensGroup(storageLensGroup)
                    .tags(resourceTag1, resourceTag2)
                    .accountId(accountId).build();

            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.createStorageLensGroup(createStorageLensGroupRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
```

```
}
```

有关示例 JSON 配置，请参阅 Storage Lens 组配置。

将 S3 Storage Lens 组附加到控制面板或从控制面板移除

在 Amazon S3 Storage Lens 存储统计管理工具中升级到高级级别后，您可以将 Storage Lens 组附加到控制面板。如果您有多个 Storage Lens 组，则可以根据需要包括或排除组。

您的 Storage Lens 组必须位于控制面板账户中指定的主区域内。将 Storage Lens 组附加到控制面板后，您将在 48 小时内在指标导出中收到新增的 Storage Lens 组聚合数据。

> **Note**
>
> 如果要查看 Storage Lens 组的聚合指标，则必须将其附加到 Storage Lens 控制面板。有关 Storage Lens 组 JSON 配置文件的示例，请参阅 JSON 格式的 S3 Storage Lens 存储统计管理工具示例配置（带 Storage Lens 组）。

使用 S3 控制台

将 Storage Lens 组附加到 Storage Lens 控制面板

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，在 Storage Lens 下选择控制面板。
3. 选择要将 Storage Lens 组附加到的 Storage Lens 控制面板的选项按钮。
4. 选择编辑。
5. 在 Metrics selection（指标选择）下方，请选择 Advanced metrics and recommendations（高级指标和建议）。
6. 选择 Storage Lens 组聚合。

   > **Note**
   >
   > 默认情况下，还会选中高级指标。但是，您也可以取消选中此设置，因为聚合 Storage Lens 组数据并非必须。

7. 向下滚动到 Storage Lens 组聚合，然后指定要在数据聚合中包括或排除的一个或多个 Storage Lens 组。您可以使用以下筛选条件选项：

- 如果要包括某些 Storage Lens 组，请选择包括 Storage Lens 组。在要包括的 Storage Lens 组下，选择您的 Storage Lens 组。
- 如果要包括所有 Storage Lens 组，请选择包括此账户中主区域中的所有 Storage Lens 组。
- 如果要排除某些 Storage Lens 组，请选择排除 Storage Lens 组。在要排除的 Storage Lens 组下，选择要排除的 Storage Lens 组。

8. 选择保存更改。如果您正确配置了 Storage Lens 组，则将在 48 小时内在控制面板中看到新增的 Storage Lens 组聚合数据。

从 S3 Storage Lens 存储统计管理工具控制面板移除 Storage Lens 组

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，在 Storage Lens 下选择控制面板。
3. 选择要从中移除 Storage Lens 组的 Storage Lens 控制面板的选项按钮。
4. 选择查看控制面板配置。
5. 选择编辑。
6. 向下滚动到指标选择部分。
7. 在 Storage Lens 组聚合下，选择要移除的 Storage Lens 组旁的 X。这将移除 Storage Lens 组。

   如果您在控制面板中包括了所有 Storage Lens 组，请清除包括此账户中主区域中的所有 Storage Lens 组旁的复选框。
8. 选择保存更改。

> **Note**
>
> 最多需要等待 48 小时，控制面板才会反映配置更新。

使用适用于 Java 的 Amazon SDK

Example – 将所有 Storage Lens 组附加到控制面板

以下 Java 版 SDK 示例将账户 *111122223333* 中的所有 Storage Lens 组附加到 *DashBoardConfigurationId* 控制面板：

```
package aws.example.s3control;
```

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.BucketLevel;
import com.amazonaws.services.s3control.model.PutStorageLensConfigurationRequest;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.model.AccountLevel;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;
import com.amazonaws.services.s3control.model.StorageLensGroupLevel;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class CreateDashboardWithStorageLensGroups {
    public static void main(String[] args) {
        String configurationId = "ExampleDashboardConfigurationId";
        String sourceAccountId = "111122223333";

        try {
            StorageLensGroupLevel storageLensGroupLevel = new StorageLensGroupLevel();

            AccountLevel accountLevel = new AccountLevel()
                    .withBucketLevel(new BucketLevel())
                    .withStorageLensGroupLevel(storageLensGroupLevel);

            StorageLensConfiguration configuration = new StorageLensConfiguration()
                    .withId(configurationId)
                    .withAccountLevel(accountLevel)
                    .withIsEnabled(true);

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.putStorageLensConfiguration(new
 PutStorageLensConfigurationRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
                    .withStorageLensConfiguration(configuration)
            );
        } catch (AmazonServiceException e) {
```

```
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Example – 将两个 Storage Lens 组附加到控制面板

以下 适用于 Java 的 Amazon SDK 示例将两个 Storage Lens 组（*StorageLensGroupName1* 和 *StorageLensGroupName2*）附加到 *ExampleDashboardConfigurationId* 控制面板。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.AccountLevel;
import com.amazonaws.services.s3control.model.BucketLevel;
import com.amazonaws.services.s3control.model.PutStorageLensConfigurationRequest;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;
import com.amazonaws.services.s3control.model.StorageLensGroupLevel;
import com.amazonaws.services.s3control.model.StorageLensGroupLevelSelectionCriteria;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class CreateDashboardWith2StorageLensGroups {
    public static void main(String[] args) {
        String configurationId = "ExampleDashboardConfigurationId";
        String storageLensGroupName1 = "StorageLensGroupName1";
        String storageLensGroupName2 = "StorageLensGroupName2";
        String sourceAccountId = "111122223333";

        try {
            StorageLensGroupLevelSelectionCriteria selectionCriteria = new
 StorageLensGroupLevelSelectionCriteria()
                    .withInclude(
```

```
                            "arn:aws:s3:" + US_WEST_2.getName() + ":" + sourceAccountId
 + ":storage-lens-group/" + storageLensGroupName1,
                            "arn:aws:s3:" + US_WEST_2.getName() + ":" + sourceAccountId
 + ":storage-lens-group/" + storageLensGroupName2);

            System.out.println(selectionCriteria);
            StorageLensGroupLevel storageLensGroupLevel = new StorageLensGroupLevel()
                    .withSelectionCriteria(selectionCriteria);

            AccountLevel accountLevel = new AccountLevel()
                    .withBucketLevel(new BucketLevel())
                    .withStorageLensGroupLevel(storageLensGroupLevel);

            StorageLensConfiguration configuration = new StorageLensConfiguration()
                    .withId(configurationId)
                    .withAccountLevel(accountLevel)
                    .withIsEnabled(true);

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.putStorageLensConfiguration(new
 PutStorageLensConfigurationRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
                    .withStorageLensConfiguration(configuration)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

### Example – 附加除排除项之外的所有 Storage Lens 组

以下 Java 版 SDK 示例将所有 Storage Lens 组附加到 *ExampleDashboardConfigurationId* 控制面板，但不包括指定的两个组（*StorageLensGroupName1* 和 *StorageLensGroupName2*）：

```
package aws.example.s3control;


import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.AccountLevel;
import com.amazonaws.services.s3control.model.BucketLevel;
import com.amazonaws.services.s3control.model.PutStorageLensConfigurationRequest;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;
import com.amazonaws.services.s3control.model.StorageLensGroupLevel;
import com.amazonaws.services.s3control.model.StorageLensGroupLevelSelectionCriteria;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class CreateDashboardWith2StorageLensGroupsExcluded {
    public static void main(String[] args) {
        String configurationId = "ExampleDashboardConfigurationId";
        String storageLensGroupName1 = "StorageLensGroupName1";
        String storageLensGroupName2 = "StorageLensGroupName2";
        String sourceAccountId = "111122223333";

        try {
            StorageLensGroupLevelSelectionCriteria selectionCriteria = new
 StorageLensGroupLevelSelectionCriteria()
                    .withInclude(
                            "arn:aws:s3:" + US_WEST_2.getName() + ":" + sourceAccountId
 + ":storage-lens-group/" + storageLensGroupName1,
                            "arn:aws:s3:" + US_WEST_2.getName() + ":" + sourceAccountId
 + ":storage-lens-group/" + storageLensGroupName2);

            System.out.println(selectionCriteria);
            StorageLensGroupLevel storageLensGroupLevel = new StorageLensGroupLevel()
                    .withSelectionCriteria(selectionCriteria);

            AccountLevel accountLevel = new AccountLevel()
                    .withBucketLevel(new BucketLevel())
```

```
                    .withStorageLensGroupLevel(storageLensGroupLevel);

            StorageLensConfiguration configuration = new StorageLensConfiguration()
                    .withId(configurationId)
                    .withAccountLevel(accountLevel)
                    .withIsEnabled(true);

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.putStorageLensConfiguration(new
 PutStorageLensConfigurationRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
                    .withStorageLensConfiguration(configuration)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

可视化 Storage Lens 组数据

通过将 Storage Lens 组附加到 Amazon S3 Storage Lens 存储统计管理工具控制面板，您可以将该组数据可视化。在控制面板配置中将 Storage Lens 组包含在 Storage Lens 组聚合中后，最长可能需要 48 小时才能在控制面板中显示 Storage Lens 组的数据。

更新控制面板配置后，任何新附加的 Storage Lens 组都将显示在 Storage Lens 组选项卡下的可用资源列表中。您还可以在概览选项卡中，通过按其它维度对数据进行切片，来进一步分析存储使用情况。例如，您可以选择前 3 个类别下列出的项目之一，然后选择分析依据，按另一个维度对数据进行切片。不能应用与筛选条件本身相同的维度。

> **Note**
>
> 您不能将 Storage Lens 组筛选条件与前缀筛选条件一起应用，反之亦然。您也无法使用前缀筛选条件进一步分析 Storage Lens 组。

您可以使用 Amazon S3 Storage Lens 存储统计管理工具控制面板中的 Storage Lens 组选项卡，为附加到控制面板的 Storage Lens 组自定义数据可视化。您可以可视化附加到控制面板的某些 Storage Lens 组的数据，也可以将所有组的数据可视化。

在 S3 Storage Lens 存储统计管理工具控制面板中可视化 Storage Lens 组数据时，请注意以下几点：

- S3 Storage Lens 存储统计管理工具聚合了所有匹配的 Storage Lens 组下某个对象的使用情况指标。因此，如果某个对象与两个或更多 Storage Lens 组的筛选条件相匹配，则在整个存储使用情况中，您会看到同一对象的重复计数。
- 对象必须与您在 Storage Lens 组中包含的筛选条件相匹配。如果没有对象与您在 Storage Lens 组中包含的筛选条件相匹配，则不会生成任何指标。要确定是否有任何未分配的对象，请在控制面板中查看账户级别和桶级别的对象总数。

### 更新 Storage Lens 组

以下示例演示如何更新 Amazon S3 Storage Lens 存储统计管理工具组。您可以使用 Amazon S3 控制台、Amazon Command Line Interface (Amazon CLI) 和 适用于 Java 的 Amazon SDK 更新 Storage Lens 组。

#### 使用 S3 控制台

更新 Storage Lens 组

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Storage Lens 组。
3. 在 Storage Lens 组下，选择要更新的 Storage Lens 组。
4. 在范围下，选择编辑。
5. 在范围页面上，选择要应用于 Storage Lens 组的筛选条件。要应用多个筛选条件，请选择您的筛选条件，然后选择 AND 或 OR 逻辑运算符。

- 对于前缀筛选条件，请选择前缀，然后输入前缀字符串。要添加多个前缀，请选择添加前缀。要移除前缀，请选择要移除的前缀旁的移除。
- 对于对象标签筛选条件，请输入对象的键值对。然后选择添加标签。要移除标签，请选择要移除的标签旁的移除。
- 对于后缀筛选条件，请选择后缀，然后输入后缀字符串。要添加多个后缀，请选择添加后缀。要移除后缀，请选择要移除的后缀旁的移除。
- 对于龄期筛选条件，请以天为单位指定对象的龄期范围。选择指定最小对象龄期，然后输入最小对象龄期。对于指定最大对象龄期，请输入最大对象龄期。
- 对于大小筛选条件，请指定对象大小范围和衡量单位。选择指定最小对象大小，然后输入最小对象大小。对于指定最大对象大小，请输入最大对象大小。

6. 选择保存更改。将显示 Storage Lens 组的详细信息页面。
7. （可选）如果要添加新的 Amazon 资源标签，请滚动到 Amazon 资源标签部分，然后选择添加标签。此时将显示添加标签页面。

   添加新的键值对，然后选择保存更改。将显示 Storage Lens 组的详细信息页面。
8. （可选）如果要移除现有 Amazon 资源标签，请滚动到 Amazon 资源标签部分，然后选择资源标签。然后选择 Delete(删除)。将出现删除 Amazon 标签对话框。

   再次选择删除可永久删除 Amazon 资源标签。

   > **Note**
   >
   > 永久删除 Amazon 资源标签后，该标签将无法还原。

使用 Amazon CLI

以下 Amazon CLI 示例命令将返回名为 *marketing-department* 的 Storage Lens 组的配置详细信息。要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control get-storage-lens-group --account-id 111122223333 \
--region us-east-1 --name marketing-department
```

以下 Amazon CLI 示例将更新 Storage Lens 组。要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control update-storage-lens-group --account-id 111122223333 \
--region us-east-1 --storage-lens-group=file://./marketing-department.json
```

有关示例 JSON 配置，请参阅 Storage Lens 组配置。

使用适用于 Java 的 Amazon SDK

以下 适用于 Java 的 Amazon SDK 示例将返回账户 *111122223333* 中 *Marketing-Department* Storage Lens 组的配置详细信息。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.GetStorageLensGroupRequest;
import software.amazon.awssdk.services.s3control.model.GetStorageLensGroupResponse;

public class GetStorageLensGroup {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            GetStorageLensGroupRequest getRequest =
 GetStorageLensGroupRequest.builder()
                    .name(storageLensGroupName)
                    .accountId(accountId).build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            GetStorageLensGroupResponse response =
 s3ControlClient.getStorageLensGroup(getRequest);
            System.out.println(response);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
```

```
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

以下示例将更新账户 *111122223333* 中名为 *Marketing-Department* 的 Storage Lens 组。此示例将更新控制面板范围，使其包含与以下任何后缀匹配的对象：*.png*、*.gif*、*.jpg* 或 *.jpeg*。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.StorageLensGroup;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupFilter;
import software.amazon.awssdk.services.s3control.model.UpdateStorageLensGroupRequest;

public class UpdateStorageLensGroup {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            // Create updated filter.
            StorageLensGroupFilter suffixFilter = StorageLensGroupFilter.builder()
                    .matchAnySuffix(".png", ".gif", ".jpg", ".jpeg")
                    .build();

            StorageLensGroup storageLensGroup = StorageLensGroup.builder()
                    .name(storageLensGroupName)
                    .filter(suffixFilter)
                    .build();

            UpdateStorageLensGroupRequest updateStorageLensGroupRequest =
 UpdateStorageLensGroupRequest.builder()
                    .name(storageLensGroupName)
                    .storageLensGroup(storageLensGroup)
                    .accountId(accountId)
```

```
                    .build();

            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.updateStorageLensGroup(updateStorageLensGroupRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

有关示例 JSON 配置，请参阅 Storage Lens 组配置。

使用 Storage Lens 组管理 Amazon 资源标签

每个 Amazon S3 Storage Lens 存储统计管理工具组都视为一个 Amazon 资源，具有自己的 Amazon 资源名称 (ARN)。因此，在配置 Storage Lens 组时，可以选择向该组添加 Amazon 资源标签。最多可以为每个 Storage Lens 组添加 50 个标签。要创建带标签的 Storage Lens 组，您必须拥有 `s3:CreateStorageLensGroup` 和 `s3:TagResource` 权限。

您可以使用 Amazon 资源标签根据部门、业务线或项目对资源进行分类。如果您有许多相同类型的资源，这样做会非常有用。通过应用标签，您可以根据分配给特定 Storage Lens 组的标签快速识别该组。您还可以使用标签对成本进行跟踪和分配。

此外，当您向 Storage Lens 组添加 Amazon 资源标签时，将激活基于属性的访问权限控制 (ABAC)。ABAC 是一种基于属性（在本文中，也就是标签）定义权限的授权策略。您还可以在 IAM policy 中使用指定资源标签的条件，从而控制对 Amazon 资源的访问。

您可以修改标签的键和值，还可以随时删除资源的标签。此外，请注意以下限制：

- 标签键和标签值区分大小写。
- 如果您添加的标签的值与该实例上现有标签的值相同，新的值就会覆盖旧值。
- 如果删除资源，资源的所有标签也会被删除。

- 不要在 Amazon 资源标签中包含隐私或敏感数据。
- 不支持系统标签（标签键以 aws: 开头）。
- 每个标签键的长度不能超过 128 个字符。每个标签值的长度不能超过 256 个字符。

以下示例演示如何将 Amazon 资源标签与 Storage Lens 组配合使用。

主题


- 向 Storage Lens 组添加 Amazon 资源标签
- 更新 Storage Lens 组标签值
- 从 Storage Lens 组删除 Amazon 资源标签
- 列出 Storage Lens 组标签


## 向 Storage Lens 组添加 Amazon 资源标签

以下示例演示如何将 Amazon 资源标签添加到 Amazon S3 Storage Lens 存储统计管理工具组。您可以使用 Amazon S3 控制台、Amazon Command Line Interface (Amazon CLI) 和 适用于 Java 的 Amazon SDK 添加资源标签。

### 使用 S3 控制台

向 Storage Lens 组添加 Amazon 资源标签

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Storage Lens 组。
3. 在 Storage Lens 组下，选择要更新的 Storage Lens 组。
4. 在 Amazon 资源标签下，选择添加标签。
5. 在添加标签页面上，添加新的键值对。

> **Note**
>
> 如果添加的新标签与现有标签具有相同的键，则将覆盖之前的标签值。

6. （可选）要添加多个新标签，请再次选择添加标签以继续添加新条目。您最多可以将 50 个 Amazon 资源标签添加到 Storage Lens 组。
7. （可选）如果要移除新添加的条目，请选择要移除的标签旁的移除。

8. 选择保存更改。

### 使用 Amazon CLI

以下示例 Amazon CLI 命令将向名为 *marketing-department* 的现有 Storage Lens 组添加两个资源标签。要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control tag-resource --account-id 111122223333 \
--resource-arn arn:aws:s3:us-east-1:111122223333:storage-lens-group/marketing-
department \
--region us-east-1 --tags Key=k1,Value=v1 Key=k2,Value=v2
```

### 使用适用于 Java 的 Amazon SDK

以下 适用于 Java 的 Amazon SDK 示例将向现有 Storage Lens 组添加两个 Amazon 资源标签。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.Tag;
import software.amazon.awssdk.services.s3control.model.TagResourceRequest;

public class TagResource {
    public static void main(String[] args) {
        String resourceARN = "Resource_ARN";
        String accountId = "111122223333";

        try {
            Tag resourceTag1 = Tag.builder()
                .key("resource-tag-key-1")
                .value("resource-tag-value-1")
                .build();
            Tag resourceTag2 = Tag.builder()
                    .key("resource-tag-key-2")
                    .value("resource-tag-value-2")
                    .build();
            TagResourceRequest tagResourceRequest = TagResourceRequest.builder()
```

```
                    .resourceArn(resourceARN)
                    .tags(resourceTag1, resourceTag2)
                    .accountId(accountId)
                    .build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.tagResource(tagResourceRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

更新 Storage Lens 组标签值

以下示例演示如何使用 Amazon S3 控制台、Amazon Command Line Interface (Amazon CLI) 和 适用于 Java 的 Amazon SDK 更新 Storage Lens 组标签值。

使用 S3 控制台

更新 Storage Lens 组的 Amazon 资源标签

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Storage Lens 组。
3. 在 Storage Lens 组下，选择要更新的 Storage Lens 组。
4. 在 Amazon 资源标签下，选择要更新的标签。
5. 使用与要更新的键值对相同的键添加新标签值。选择对勾图标以更新标签值。

> **Note**
>
> 如果添加的新标签与现有标签具有相同的键，则将覆盖之前的标签值。

6. （可选）如果要添加新标签，请选择添加标签以添加新条目。此时将显示添加标签页面。

   最多可以为 Storage Lens 组添加 50 个 Amazon 资源标签。添加完新标签后，选择保存更改。

7. （可选）如果要移除新添加的条目，请选择要移除的标签旁的移除。完成移除标签后，选择保存更改。

使用 Amazon CLI

以下示例 Amazon CLI 命令将更新名为 *marketing-department* 的 Storage Lens 组的两个标签值。要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control tag-resource --account-id 111122223333 \
--resource-arn arn:aws:s3:us-east-1:111122223333:storage-lens-group/marketing-
department \
--region us-east-1 --tags Key=k1,Value=v3 Key=k2,Value=v4
```

使用适用于 Java 的 Amazon SDK

以下 适用于 Java 的 Amazon SDK 示例将更新 Storage Lens 组的两个标签值。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.Tag;
import software.amazon.awssdk.services.s3control.model.TagResourceRequest;

public class UpdateTagsForResource {
    public static void main(String[] args) {
        String resourceARN = "Resource_ARN";
        String accountId = "111122223333";

        try {
            Tag updatedResourceTag1 = Tag.builder()
                .key("resource-tag-key-1")
                .value("resource-tag-updated-value-1")
                .build();
```

```
            Tag updatedResourceTag2 = Tag.builder()
                    .key("resource-tag-key-2")
                    .value("resource-tag-updated-value-2")
                    .build();
            TagResourceRequest tagResourceRequest = TagResourceRequest.builder()
                    .resourceArn(resourceARN)
                    .tags(updatedResourceTag1, updatedResourceTag2)
                    .accountId(accountId)
                    .build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.tagResource(tagResourceRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

从 Storage Lens 组删除 Amazon 资源标签

以下示例演示如何从 Storage Lens 组删除 Amazon 资源标签。您可以使用 Amazon S3 控制台、Amazon Command Line Interface (Amazon CLI) 和 适用于 Java 的 Amazon SDK 删除标签。

使用 S3 控制台

从 Storage Lens 组删除 Amazon 资源标签

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Storage Lens 组。
3. 在 Storage Lens 组下，选择要更新的 Storage Lens 组。
4. 在 Amazon 资源标签下，选择要删除的键值对。
5. 选择删除。将出现删除 Amazon 资源标签对话框。

> **Note**
>
> 如果使用标签控制访问，则继续执行此操作可能会影响相关资源。永久删除标签后，该标签将无法还原。

6. 选择删除，永久性删除该键值对。

使用 Amazon CLI

以下 Amazon CLI 命令将从现有 Storage Lens 组中删除两个 Amazon 资源标签：要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control untag-resource --account-id 111122223333 \
--resource-arn arn:aws:s3:us-east-1:111122223333:storage-lens-group/Marketing-Department \
--region us-east-1 --tag-keys k1 k2
```

使用适用于 Java 的 Amazon SDK

以下 适用于 Java 的 Amazon SDK 示例将从账户 *111122223333* 中具有您所指定的 Amazon 资源名称 (ARN) 的 Storage Lens 组中，删除两个 Amazon 资源标签。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.UntagResourceRequest;

public class UntagResource {
    public static void main(String[] args) {
        String resourceARN = "Resource_ARN";
        String accountId = "111122223333";

        try {
            String tagKey1 = "resource-tag-key-1";
            String tagKey2 = "resource-tag-key-2";
```

```
            UntagResourceRequest untagResourceRequest = UntagResourceRequest.builder()
                    .resourceArn(resourceARN)
                    .tagKeys(tagKey1, tagKey2)
                    .accountId(accountId)
                    .build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.untagResource(untagResourceRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

列出 Storage Lens 组标签

以下示例演示如何列出与 Storage Lens 组关联的 Amazon 资源标签。您可以使用 Amazon S3 控制台、Amazon Command Line Interface (Amazon CLI) 和 适用于 Java 的 Amazon SDK 列出标签。

使用 S3 控制台

查看 Storage Lens 组的标签和标签值列表

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Storage Lens 组。
3. 在 Storage Lens 组下，选择您感兴趣的 Storage Lens 组。
4. 向下滚动到 Amazon 资源标签部分。所有添加到您的 Storage Lens 组的用户定义的 Amazon 资源标签及其标签值都将列出。

使用 Amazon CLI

以下 Amazon CLI 示例命令将列出名为 *marketing-department* 的 Storage Lens 组的所有 Storage Lens 组标签值。要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control list-tags-for-resource --account-id 111122223333 \
--resource-arn arn:aws:s3:us-east-1:111122223333:storage-lens-group/marketing-
department \
--region us-east-1
```

使用适用于 Java 的 Amazon SDK

以下 适用于 Java 的 Amazon SDK 示例将为您指定的 Storage Lens 组 Amazon 资源名称 (ARN) 列出 Storage Lens 组标签值。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.ListTagsForResourceRequest;
import software.amazon.awssdk.services.s3control.model.ListTagsForResourceResponse;

public class ListTagsForResource {
    public static void main(String[] args) {
        String resourceARN = "Resource_ARN";
        String accountId = "111122223333";

        try {
            ListTagsForResourceRequest listTagsForResourceRequest =
 ListTagsForResourceRequest.builder()
                    .resourceArn(resourceARN)
                    .accountId(accountId)
                    .build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            ListTagsForResourceResponse response =
 s3ControlClient.listTagsForResource(listTagsForResourceRequest);
            System.out.println(response);
```

```
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

列出所有 Storage Lens 组

以下示例演示如何列出 Amazon Web Services 账户和主区域中的所有 Amazon S3 Storage Lens 存储统计管理工具组。这些示例显示了如何使用 Amazon S3 控制台、Amazon Command Line Interface (Amazon CLI) 和 适用于 Java 的 Amazon SDK 列出所有 Storage Lens 组。

使用 S3 控制台

列出账户和主区域中的所有 Storage Lens 组

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Storage Lens 组。
3. 在 Storage Lens 组下，将显示您账户中的 Storage Lens 组列表。

使用 Amazon CLI

以下 Amazon CLI 示例将列出您账户的所有 Storage Lens 组。要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control list-storage-lens-groups --account-id 111122223333 \
--region us-east-1
```

使用适用于 Java 的 Amazon SDK

以下 适用于 Java 的 Amazon SDK 示例将列出账户 *111122223333* 的 Storage Lens 组。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.ListStorageLensGroupsRequest;
import software.amazon.awssdk.services.s3control.model.ListStorageLensGroupsResponse;

public class ListStorageLensGroups {
    public static void main(String[] args) {
        String accountId = "111122223333";

        try {
            ListStorageLensGroupsRequest listStorageLensGroupsRequest =
 ListStorageLensGroupsRequest.builder()
                    .accountId(accountId)
                    .build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            ListStorageLensGroupsResponse response =
 s3ControlClient.listStorageLensGroups(listStorageLensGroupsRequest);
            System.out.println(response);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

### 查看 Storage Lens 组详细信息

以下示例演示如何查看 Amazon S3 Storage Lens 存储统计管理工具组配置详细信息。您可以使用 Amazon S3 控制台、Amazon Command Line Interface (Amazon CLI) 和 适用于 Java 的 Amazon SDK 查看这些详细信息。

使用 S3 控制台

查看 Storage Lens 组配置详细信息

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Storage Lens 组。
3. 在 Storage Lens 组下，选择您感兴趣的 Storage Lens 组旁的选项按钮。
4. 请选择查看详细信息。现在，您可以查看 Storage Lens 组的详细信息。

使用 Amazon CLI

以下 Amazon CLI 示例将返回 Storage Lens 组的配置详细信息。要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control get-storage-lens-group --account-id 111122223333 \
--region us-east-1 --name marketing-department
```

使用适用于 Java 的 Amazon SDK

以下 适用于 Java 的 Amazon SDK 示例将返回账户 *111122223333* 中名为 *Marketing-Department* 的 Storage Lens 组的配置详细信息。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.GetStorageLensGroupRequest;
import software.amazon.awssdk.services.s3control.model.GetStorageLensGroupResponse;

public class GetStorageLensGroup {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";
```

```
        try {
            GetStorageLensGroupRequest getRequest =
 GetStorageLensGroupRequest.builder()
                    .name(storageLensGroupName)
                    .accountId(accountId).build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            GetStorageLensGroupResponse response =
 s3ControlClient.getStorageLensGroup(getRequest);
            System.out.println(response);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

删除 Storage Lens 组

以下示例演示如何使用 Amazon S3 控制台、Amazon Command Line Interface (Amazon CLI) 和 适用于 Java 的 Amazon SDK 删除 Amazon S3 Storage Lens 存储统计管理工具组。

使用 S3 控制台

删除 Storage Lens 组

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择 Storage Lens 组。
3. 在 Storage Lens 组下，选择要删除的 Storage Lens 组旁的选项按钮。
4. 选择删除。将显示删除 Storage Lens 组对话框。
5. 再次选择删除即可永久删除 Storage Lens 组。

> **Note**
>
> Storage Lens 组在删除后无法还原。

使用 Amazon CLI

以下 Amazon CLI 示例将删除名为 *marketing-department* 的 Storage Lens 组。要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws s3control delete-storage-lens-group --account-id 111122223333 \
--region us-east-1 --name marketing-department
```

使用适用于 Java 的 Amazon SDK

以下 适用于 Java 的 Amazon SDK 示例将删除账户 *111122223333* 中名为 *Marketing-Department* 的 Storage Lens 组。要使用此示例，请将 *user input placeholders* 替换为您自己的信息。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.DeleteStorageLensGroupRequest;

public class DeleteStorageLensGroup {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            DeleteStorageLensGroupRequest deleteStorageLensGroupRequest =
 DeleteStorageLensGroupRequest.builder()
                    .name(storageLensGroupName)
                    .accountId(accountId).build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
```

```
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.deleteStorageLensGroup(deleteStorageLensGroupRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

# 使用 S3 清单对数据进行编目和分析

您可以使用 Amazon S3 清单来帮助管理您的存储。例如，您可以出于业务、合规性和法规需要，使用该清单来审核和报告对象的复制和加密状态。您还可以使用 Amazon S3 清单简化和加快业务工作流和大数据任务，此清单可以有计划地取代 Amazon S3 同步 `List` API 操作。Amazon S3 清单不使用 `List` API 操作来审计对象且不会影响存储桶的请求速率。

Amazon S3 清单每天或每周为 S3 存储桶或具有共享前缀的对象（即，其名称以通用字符串开头的对象），提供用于列出您的对象及其对应元数据的逗号分隔值（CSV）、Apache 优化的行列式（ORC）或 Apache Parquet 输出文件。如果您设置每周清单，则在初始报告后的每个星期日（UTC 时区）生成一份报告。有关 Amazon S3 清单定价的信息，请参阅 Amazon S3 定价。

您可以为存储桶配置多个清单列表。配置清单列表时，可以指定以下内容：

- 清单中应包含哪些对象元数据
- 是列出所有对象版本，还是仅列出当前版本
- 在哪里存储清单列表文件输出
- 是每天生成清单，还是每周生成清单
- 是否加密清单列表文件

您可以通过 Amazon Athena、Amazon Redshift Spectrum 以及其他工具（如 Presto、Apache Hive 和 Apache Spark）使用标准 SQL 查询 Amazon S3 清单。有关使用 Athena 查询清单文件的更多信息，请参阅the section called “使用 Athena 查询清单”。

> **Note**
>
> Amazon S3 交付第一份清单报告可能需要长达 48 小时。

## 源存储桶和目标存储桶

由清单列出其对象的存储桶称为源存储桶。在其中存储清单列表文件的存储桶称为目标存储桶。

源存储桶

清单列出了源存储桶中存储的对象。您可以获得整个存储桶的清单列表，也可以通过对象键名称前缀筛选此列表。

源存储桶：

- 包含在清单中列出的对象
- 包含清单的配置

目标存储桶

Amazon S3 清单列表文件将写入目标存储桶。要对目标存储桶内公共位置中的所有清单列表文件进行分组，您可以在清单配置中指定目标前缀。

目标存储桶：

- 包含清单文件列表。
- 包含清单文件，其中列出了存储在目标存储桶中的所有清单列表文件。有关更多信息，请参阅 清单 Manifest。
- 必须具有向 Amazon S3 授予验证存储桶的所有权的权限和将文件写入存储桶的权限的存储桶策略。
- 必须与源存储桶位于同一 Amazon Web Services 区域。
- 可以与源存储桶相同。
- 可以由与拥有源存储桶的账户不同的 Amazon Web Services 账户 拥有。

## Amazon S3 清单列表

清单列表文件包含源存储桶中对象的列表以及每个对象的元数据。清单列表文件按以下格式之一存储在目标存储桶中：

- 作为使用 GZIP 压缩的 CSV 文件
- 作为使用 ZLIB 压缩的 Apache 优化行列式（ORC）文件
- 作为使用 Snappy 压缩的 Apache Parquet 文件

> **Note**
>
> 不能保证会以任何顺序对 Amazon S3 清单报告中的对象排序。

清单列表文件包含源存储桶中对象的列表以及每个所列对象的元数据：

- Bucket name (存储桶名称) – 清单所针对的存储桶的名称。
- 键名称 – 唯一地标识存储桶中的对象的对象键名（或键）。当您使用 CSV 文件格式时，键名称采用 URL 编码形式，必须解码，然后才能使用。
- 版本 ID – 对象版本 ID。在存储桶上启用版本控制后，Amazon S3 会为添加到存储桶的对象指定版本号。有关更多信息，请参阅 使用 S3 版本控制保留对象的多个版本。（如果仅为对象的当前版本配置列表，则不包括此字段。）
- IsLatest – 如果对象的版本为最新，则设置为 `True`。（如果仅为对象的当前版本配置列表，则不包括此字段。）
- 删除标记 – 如果对象是删除标记，则设置为 `True`。有关更多信息，请参阅 使用 S3 版本控制保留对象的多个版本。（如果您已将您的报告配置为包含您的对象的所有版本，则此字段将自动添加到报告）。
- 大小 - 以字节为单位的对象大小，不包括未完成的分段上传、对象元数据和删除标记的大小。
- Last modified date (上次修改日期) – 对象创建日期或上次修改日期（以较晚者为准）。
- ETag – 实体标签（ETag）是对象的哈希。ETag 仅反映对于对象的内容的更改，而不反映对于对象的元数据的更改。ETag 可能是对象数据的 MD5 摘要。是与不是取决于对象的创建方式和加密方式。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 Object。
- 存储类 – 用于存储对象的存储类。设置为 `STANDARD`、`REDUCED_REDUNDANCY`、`STANDARD_IA`、`ONEZONE_IA`、`INTELLIGENT_TIERING`、`GLACIER` 或 `SNOW`。有关更多信息，请参阅 了解和管理 Amazon S3 存储类。

> **Note**
>
> S3 清单不支持 S3 Express One Zone。

- Multipart upload flag (分段上传标记) – 如果对象以分段上传形式上传，则设置为 `True`。有关更多信息，请参阅 在 Amazon S3 中使用分段上传来上传和复制对象。
- 复制状态 – 设置为 `PENDING`、`COMPLETED`、`FAILED` 或 `REPLICA`。有关更多信息，请参阅 获取复制状态信息。
- 加密状态 – 服务器端加密状态，具体取决于使用哪种加密密钥：采用 Amazon S3 托管式密钥的服务器端加密（SSE-S3）、采用 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）、采用 Amazon KMS 密钥的双层服务器端加密（DSSE-C）或采用客户提供的密钥的服务器端加密（SSE-C）。设置为 `SSE-S3`、`SSE-KMS`、`DSSE-KMS`、`SSE-C` 或 `NOT-SSE`。`NOT-SSE` 状态表示对象未使用服务器端加密进行加密。有关更多信息，请参阅 利用加密来保护数据。
- S3 对象锁定保留截止日期 – 在此日期之前无法删除锁定的对象。有关更多信息，请参阅 使用对象锁定以锁定对象。
- S3 对象锁定保留模式 – 对于已锁定的对象，设置为 `Governance` 或 `Compliance`。有关更多信息，请参阅 使用对象锁定以锁定对象。
- S3 对象锁定依法保留状态 – 如果依法保留已应用于对象，则设置为 `On`。否则，其设置为 `Off`。有关更多信息，请参阅 使用对象锁定以锁定对象。
- S3 Intelligent-Tiering 访问层 – 如果对象存储在 S3 Intelligent-Tiering 存储类中，则为对象的访问层（频繁或不频繁）。设置为 `FREQUENT`、`INFREQUENT`、`ARCHIVE_INSTANT_ACCESS`、`ARCHIVE` 或 `DEEP_ARCHIVE`。有关更多信息，请参阅 用于自动优化访问模式不断变化或未知的数据的存储类。
- S3 存储桶密钥状态 – 设置为 `ENABLED` 或者 `DISABLED`。指示对象是否将 S3 存储桶密钥用于 SSE-KMS。有关更多信息，请参阅 使用 Amazon S3 存储桶密钥。
- 校验和算法 – 表示用于创建对象的校验和的算法。有关更多信息，请参阅 使用支持的校验和算法。
- 对象访问控制列表 – 每个对象的访问控制列表（ACL），用于定义哪个 Amazon Web Services 账户或组被授予对此对象的访问权限以及授予的访问权限类型。“对象 ACL”字段以 JSON 格式定义。S3 清单报告包括与源存储桶中的对象关联的 ACL，即使已为该存储桶禁用了 ACL 仍会包括。有关更多信息，请参阅使用“对象 ACL”字段和访问控制列表 (ACL) 概述。

> **Note**
>
> “对象 ACL”字段以 JSON 格式定义。清单报告将“对象 ACL”字段的值显示为以 base64 编码的字符串。
>
> 例如，假设您有以下采用 JSON 格式的“对象 ACL”字段：
>
> ```
> {
> ```

```
        "version": "2022-11-10",
        "status": "AVAILABLE",
        "grants": [{
            "canonicalId": "example-canonical-user-ID",
            "type": "CanonicalUser",
            "permission": "READ"
        }]
}
```

“对象 ACL”字段经过编码并显示为以下以 base64 编码的字符串：

```
eyJ2ZXJzaW9uIjoiMjAyMi0xMS0xMCIsInN0YXR1cyI6IkFWQUlMQUJMRSIsImdyYW50cyI6W3siY2Fub25pY2Fs
```

要以 JSON 格式获取“对象 ACL”字段的解码值，可以在 Amazon Athena 中查询此字段。有关示例查询，请参阅使用 Amazon Athena 查询 Amazon S3 清单。

- 对象拥有者：对象拥有者的规范用户 ID。有关更多信息，请参阅《Amazon 账户管理参考指南》中的 Find the canonical user ID for your Amazon account。

> **Note**
>
> 在对象根据其生命周期配置的生存期结束后，Amazon S3 会将该对象加入移除队列并异步移除它。因此，过期日期和 Amazon S3 删除对象的日期之间可能会有一段延迟。清单报告包括已过期但尚未移除的对象。有关 S3 生命周期中的过期操作的更多信息，请参阅即将过期的对象。

以下是清单报告示例，其中包含由四条记录组成的其它元数据字段。

```
amzn-s3-demo-bucket1    example-object-1    EXAMPLEDC8l.XJCENlF7LePaNIIvs001    TRUE
     1500    2024-08-15T15:28:26.0004    EXAMPLE21e1518b92f3d92773570f600    STANDARD
  FALSE    COMPLETED    SSE-KMS    2025-01-25T15:28:26.000Z    COMPLIANCE    Off
 ENABLED
 eyJ2ZXJzaW9uIjoiMjAyMi0xMS0xMCIsInN0YXR1cyI6IkFWQUlMQUJMRSIsImdyYW50cyI6W3sicGVybWlzc2lvbiI6Ik
    EXAMPLE766e8f6b115d93d41df2eac420aa4a465d177c1398bc6a088c76b7000
amzn-s3-demo-bucket1    example-object-2    EXAMPLEDC8l.XJCENlF7LePaNIIvs002
 TRUE        200    2024-08-21T15:28:26.000Z    EXAMPLE21e1518b92f3d92773570f601
  INTELLIGENT_TIERING    FALSE    COMPLETED    SSE-KMS    2025-01-25T15:28:26.000Z
    COMPLIANCE    Off    INFREQUENT    ENABLED    SHA-256
```

```
 eyJ2ZXJzaW9uIjoiMjAyMi0xMS0xMCIsInN0YXR1cyI6IkFWQUlMQUJMRSIsImdyYW50cyI6W3sicGVybWlzc2lvbiI6Ik
    EXAMPLE766e8f6b115d93d41df2eac420aa4a465d177c1398bc6a088c76b7001
amzn-s3-demo-bucket1    example-object-3    EXAMPLEDC8l.XJCENlF7LePaNIIvs003    TRUE
      12500    2023-01-15T15:28:30.000Z    EXAMPLE21e1518b92f3d92773570f602    STANDARD
    FALSE    REPLICA    SSE-KMS    2025-01-25T15:28:26.000Z    GOVERNANCE    On
 ENABLED
 eyJ2ZXJzaW9uIjoiMjAyMi0xMS0xMCIsInN0YXR1cyI6IkFWQUlMQUJMRSIsImdyYW50cyI6W3sicGVybWlzc2lvbiI6Ik
    EXAMPLE766e8f6b115d93d41df2eac420aa4a465d177c1398bc6a088c76b7002
amzn-s3-demo-bucket1    example-object-4    EXAMPLEDC8l.XJCENlF7LePaNIIvs004    TRUE
      100    2021-02-15T15:28:27.000Z    EXAMPLE21e1518b92f3d92773570f603    STANDARD
  FALSE    COMPLETED    SSE-KMS    2025-01-25T15:28:26.000Z    COMPLIANCE    Off
 ENABLED
 eyJ2ZXJzaW9uIjoiMjAyMi0xMS0xMCIsInN0YXR1cyI6IkFWQUlMQUJMRSIsImdyYW50cyI6W3sicGVybWlzc2lvbiI6Ik
    EXAMPLE766e8f6b115d93d41df2eac420aa4a465d177c1398bc6a088c76b7003
```

我们建议创建一个删除旧清单列表的生命周期策略。有关更多信息，请参阅 管理对象的生命周期。

`s3:PutInventoryConfiguration` 权限允许用户在配置清单列表时选择之前为每个对象列出的所有元数据字段，也可以指定存储清单的目标存储桶。对目标存储桶中的对象具有读取权限的用户可以访问清单列表中提供的所有对象元数据字段。要限制对于清单报告的访问权限，请参阅向 S3 清单和 S3 分析功能授予权限。

## 清单一致性

并非所有对象都会显示每个清单列表中。清单列表提供了（新对象和覆盖）的 PUT 请求的最终一致性，并提供了 DELETE 请求的最终一致性。存储桶的每个清单列表都是存储桶项目的快照。这些列表最终是一致的（也就是说，列表可能不包括最近添加或删除的对象）。

要在对于对象执行操作之前验证对象的状态，我们建议您执行 `HeadObject` REST API 请求以检索对象的元数据，或在 Amazon S3 控制台中检查对象的属性。您还可以使用 Amazon CLI 或 Amazon SDK 检查对象元数据。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 `HeadObject`。

有关使用 Amazon S3 清单的更多信息，请参阅以下主题。

主题

- 配置 Amazon S3 清单
- 查找清单列表
- 设置清单完成时的 Amazon S3 事件通知
- 使用 Amazon Athena 查询 Amazon S3 清单

- 将 Amazon S3 库存报告中的空版本 ID 字符串转换为空字符串
- 使用“对象 ACL”字段

# 配置 Amazon S3 清单

Amazon S3 清单每天根据您定义的时间表，提供您的对象和元数据的平面文件列表。您可以使用 S3 清单作为 Amazon S3 同步 `List` API 操作的计划替代方案。S3 清单提供逗号分隔值（CSV）、经过 Apache 优化的行列式（ORC）或 Apache Parquet (Parquet) 输出文件，这些文件列出了对象及其相应的元数据。

您可以将 S3 清单配置为每天或每周为 S3 存储桶或为共享前缀的对象（名称以相同字符串开头的对象）创建清单列表。有关更多信息，请参阅 使用 S3 清单对数据进行编目和分析。

本部分介绍了如何设置清单，包括有关清单源存储桶和目标存储桶的详细信息。

主题


- 概览
- 创建目标存储桶策略
- 向 Amazon S3 授予权限以使用客户自主管理型密钥进行加密
- 使用 S3 控制台配置清单
- 使用 REST API 处理 S3 清单


## 概览

Amazon S3 清单将帮助您按预定的计划创建 S3 存储桶中的对象的列表，由此管理存储。您可以为桶配置多个清单列表。清单列表将发布到目标存储桶中的 CSV、ORC 或 Parquet 文件。

设置清单的最简单方法是使用 Amazon S3 控制台，不过您也可以使用 Amazon S3 REST API、Amazon Command Line Interface (Amazon CLI) 或 Amazon SDK。控制台将为您执行以下过程的第一步：将存储桶策略添加到目标存储桶。

为 S3 存储桶设置 Amazon S3 清单

1. 为目标存储桶添加存储桶策略。

   您必须在目标存储桶上创建存储桶策略，以向 Amazon S3 授予将对象写入已定义位置的存储桶的权限。有关策略示例，请参阅向 S3 清单和 S3 分析功能授予权限。
2. 配置一个清单以列出源存储桶中的对象并将该列表发布到目标存储桶。

当您为源存储桶配置清单列表时，您应指定用于存储该列表的目标存储桶，以及是每天还是每周生成一次列表。您还可以配置是列出所有对象版本还是仅列出当前版本，以及要包含哪些对象元数据。

S3 清单报告配置中的某些对象元数据字段是可选的，这意味着它们在默认情况下是可用的，但是当您向用户授予 `s3:PutInventoryConfiguration` 权限时，它们可能会受到限制。您可以使用 `s3:InventoryAccessibleOptionalFields` 条件键控制用户能否在报告中包含这些可选元数据字段。

有关 S3 清单中可用的可选元数据字段的更多信息，请参阅《Amazon Simple Storage Service API Reference》中的 OptionalFields。有关在清单配置中限制对某些可选元数据字段的访问的更多信息，请参阅控制 S3 清单报告配置的创建。

您可以指定使用具有 Amazon S3 托管式密钥 (SSE-S3) 或具有 Amazon Key Management Service (Amazon KMS) 客户自主管理型密钥（SSE-KMS）的服务器端加密来加密清单列表文件。

> **Note**
>
> 使用 S3 清单进行的 SSE-KMS 加密不支持 Amazon 托管式密钥 (`aws/s3`)。

有关 SSE-S3 和 SSE-KMS 的更多信息，请参阅 使用服务器端加密保护数据。如果您打算使用 SSE-KMS 加密，请参阅步骤 3。

- 有关如何使用控制台配置清单列表的信息，请参阅使用 S3 控制台配置清单。
- 要使用 Amazon S3 API 配置清单列表，请使用 PutBucketInventoryConfiguration REST API 操作，或者使用 Amazon CLI 或 Amazon SDK 中的等效操作。

3. 要使用 SSE-KMS 加密清单列表文件，授予 Amazon S3 使用 Amazon KMS key 的权限。

   您可以使用 Amazon S3 控制台、Amazon S3 REST API、Amazon CLI 或 Amazon SDK，为清单列表文件配置加密。无论选择哪种方式，您都必须授予 Amazon S3 相应权限使用客户托管密钥来加密清单文件。可通过修改要用于加密清单文件的客户托管密钥的密钥策略，向 Amazon S3 授予权限。有关更多信息，请参阅 向 Amazon S3 授予权限以使用客户自主管理型密钥进行加密。

   存储清单列表文件的目标存储桶可以由与拥有源存储桶的账户不同的 Amazon Web Services 账户拥有。如果您使用 SSE-KMS 加密功能执行 Amazon S3 清单跨账户操作，则在配置 S3 清单时，建议您使用完全限定的 KMS 密钥 ARN。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的使用 SSE-KMS 加密进行跨账户操作和 ServerSideEncryptionByDefault。

## 创建目标存储桶策略

如果您通过 Amazon S3 控制台创建清单配置，Amazon S3 会在目标存储桶上自动创建一个存储桶策略，以授予 Amazon S3 对存储桶的写入权限。但是，如果您通过 Amazon CLI、Amazon SDK 或 Amazon S3 REST API 创建清单配置，则必须在目标存储桶上手动添加存储桶策略。S3 清单目标存储桶策略允许 Amazon S3 将清单报告数据写入存储桶。

下面是一个示例存储桶策略。

```
{
      "Version": "2012-10-17",
      "Statement": [
        {
            "Sid": "InventoryExamplePolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
            ],
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:::DOC-EXAMPLE-SOURCE-BUCKET"
                },
                "StringEquals": {
                    "aws:SourceAccount": "source-account-id",
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
            }
        }
    ]
}
```

有关更多信息，请参阅 向 S3 清单和 S3 分析功能授予权限。

如果在您尝试创建存储桶策略出现错误，则将为您提供相关修复说明。例如，如果您选择了其他 Amazon Web Services 账户 中的目标存储桶，而没有权限读取和写入存储桶策略，则您会看到一条错误消息。

在这种情况下，目标存储桶拥有者必须将存储桶策略添加到目标存储桶中。如果策略未添加到目标存储桶中，则您不会获得清单报告，因为 Amazon S3 无权写入目标存储桶。如果源桶属于其他账户而非当前用户的账户，则必须在策略中替换源桶拥有者的正确账户 ID。

> **Note**
>
> 确保没有向目标存储桶策略中添加任何会阻止向该存储桶传送清单报告的拒绝语句。有关更多信息，请参阅为什么无法生成 Amazon S3 清单报告？

## 向 Amazon S3 授予权限以使用客户自主管理型密钥进行加密

要向 Amazon S3 授予使用 Amazon Key Management Service（Amazon KMS）客户自主管理型密钥进行服务器端加密的权限，必须使用密钥策略。要更新密钥策略，以便您能够使用客户自主管理型密钥，请使用以下过程。

授予 Amazon S3 使用客户自主管理型密钥进行加密的权限

1. 使用拥有客户自主管理型密钥的 Amazon Web Services Management Console，登录 Amazon Web Services 账户。
2. 从 https://console.aws.amazon.com/kms 打开 Amazon KMS 控制台。
3. 要更改 Amazon Web Services 区域，请使用页面右上角的区域选择器。
4. 在左侧导航窗格中，选择 Customer managed keys (客户托管密钥)。
5. 在客户自主管理型密钥下，选择要用于加密清单文件的客户托管密钥。
6. 在 Key Policy (密钥策略) 部分中，选择 Switch to policy view (切换到策略视图)。
7. 要更新密钥策略，选择 Edit (编辑)。
8. 在编辑密钥策略页上，将以下各行添加到现有密钥策略。对于 *source-account-id* 和 *amzn-s3-demo-source-bucket*，为您的用例提供适当的值。

```
{
    "Sid": "Allow Amazon S3 use of the customer managed key",
    "Effect": "Allow",
    "Principal": {
        "Service": "s3.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey"
    ],
```

```
    "Resource": "*",
    "Condition":{
      "StringEquals":{
         "aws:SourceAccount":"source-account-id"
     },
      "ArnLike":{
        "aws:SourceARN": "arn:aws:s3:::amzn-s3-demo-source-bucket"
     }
   }
}
```

9. 选择保存更改。

有关创建客户托管密钥和使用密钥策略的更多信息，请参阅 Amazon Key Management Service 开发人员指南中的以下链接：

- 管理密钥
- Amazon KMS 中的密钥策略

> **Note**
>
> 确保没有向目标存储桶策略中添加任何会阻止向该存储桶传送清单报告的拒绝语句。有关更多信息，请参阅为什么无法生成 Amazon S3 清单报告？

## 使用 S3 控制台配置清单

按照以下说明使用 S3 控制台配置清单。

> **Note**
>
> Amazon S3 交付第一份清单报告可能需要长达 48 小时。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在存储桶列表中，选择要为其配置 Amazon S3 清单的存储桶的名称。

4. 选择管理选项卡。
5. 在 Inventory configurations (清单配置) 下，选择 Create inventory configuration (创建清单配置)。
6. 对于清单配置名称，输入名称。
7. 对于清单范围，请执行以下操作：
   - 输入可选的前缀。
   - 选择要包括的对象版本：仅当前版本或包括所有版本。
8. 在 Report details (报告详细信息) 下，选择要将报告保存到的 Amazon Web Services 账户 的位置：此账户或另一个账户。
9. 在目标下，选择要将清单报告保存到的目标存储桶。

   目标存储桶必须位于与您为其设置清单的桶相同的 Amazon Web Services 区域 中。目标存储桶可处于不同的 Amazon Web Services 账户 中。指定目标存储桶时，您还可以添加可选前缀，以将清单报告组合在一起。

   在目标存储桶字段下，您将看到目标存储桶权限声明，该声明添加到目标存储桶策略中以允许 Amazon S3 在该桶中放置数据。有关更多信息，请参阅 创建目标存储桶策略。
10. 在频率下，选择生成报告的频率：每日或每周。
11. 对于输出格式，为报告选择以下格式之一：
    - CSV – 如果您计划将此清单报告用于 S3 批量操作，或者如果您想在其他工具（例如 Microsoft Excel）中分析此报告，请选择 CSV。
    - Apache ORC
    - Apache Parquet
12. 在 Status (状态) 下，选择 Enable (启用) 或 Disable (禁用)。
13. 要配置服务器端加密，请在清单报告加密下执行以下步骤：
    a. 在服务器端加密下，选择不要指定加密密钥或指定加密密钥来加密数据。
       - 要在将对象存储在 Amazon S3 中时保留适用于对象原定设置服务器端加密的桶设置，请选择不要指定加密密钥。只要桶目标启用了 S3 存储桶密钥，复制操作就将在目标存储桶上应用 S3 存储桶密钥。

> **Note**
>
> 如果指定目标的存储桶策略要求在将对象存储到 Amazon S3 之前对其进行加密，则必须指定加密密钥。否则，将对象复制到目标将失败。

- 要在将对象存储到 Amazon S3 之前对其进行加密，请选择指定加密密钥。

b. 如果您选择指定加密密钥，那么在加密类型下，您必须选择 Amazon S3 托管密钥（SSE-S3）或 Amazon Key Management Service 密钥（SSE-KMS）。

SSE-S3 使用最强的数据块密码之一 [即 256 位高级加密标准（AES-256）] 来加密每个对象。SSE-KMS 为您提供了对密钥的更多控制。有关 SSE-S3 的更多信息，请参阅使用具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3）。有关 SSE-KMS 的更多信息，请参阅使用具有 Amazon KMS 密钥的服务器端加密（SSE-KMS）。

> **Note**
>
> 要使用 SSE-KMS 加密清单列表文件，必须授予 Amazon S3 使用客户自主管理型密钥的权限。有关说明，请参阅授予 Amazon S3 使用 KMS 密钥进行加密的权限。

c. 如果您选择了 Amazon Key Management Service 密钥（SSE-KMS），则在 Amazon KMS key 之下，您可以通过以下选项之一指定 Amazon KMS 密钥。

> **Note**
>
> 如果存储清单列表文件的目标存储桶由其他 Amazon Web Services 账户拥有，请确保使用完全限定的 KMS 密钥 ARN 来指定您的 KMS 密钥。

- 要从可用 KMS 密钥列表中进行选择，请选择从您的 Amazon KMS 密钥中进行选择，然后从可用密钥列表中选择对称加密 KMS 密钥。确保该 KMS 密钥与您的存储桶位于同一区域。

> **Note**
>
> Amazon 托管式密钥 (aws/s3) 和您的客户自主管理型密钥都显示在列表中。但是，使用 S3 清单进行的 SSE-KMS 加密不支持 Amazon 托管式密钥 (aws/s3)。

- 要输入 KMS 密钥 ARN，请选择输入 Amazon KMS 密钥 ARN，然后在显示的字段中输入您的 KMS 密钥 ARN。
- 要在 Amazon KMS 控制台中创建新的客户自主管理型密钥，请选择创建 KMS 密钥。

14. 对于其他元数据字段，从下面选择一项或多项以添加到清单报告：

- 大小 - 以字节为单位的对象大小，不包括未完成的分段上传、对象元数据和删除标记的大小。
- Last modified date (上次修改日期) – 对象创建日期或上次修改日期（以较晚者为准）。
- 分段上传 – 指定对象以分段上传形式上传。有关更多信息，请参阅 在 Amazon S3 中使用分段上传来上传和复制对象。
- Replication status (复制状态) – 对象的复制状态。有关更多信息，请参阅 获取复制状态信息。
- 加密状态 – 用于加密对象的服务器端加密类型。有关更多信息，请参阅 使用服务器端加密保护数据。
- 桶密钥状态 – 指示是否将 Amazon KMS 生成的桶级密钥应用于对象。有关更多信息，请参阅 使用 Amazon S3 存储桶密钥降低 SSE-KMS 的成本。
- 对象访问控制列表 – 每个对象的访问控制列表（ACL），用于定义哪个 Amazon Web Services 账户或组被授予对此对象的访问权限以及授予的访问权限类型。有关此字段的更多信息，请参阅使用“对象 ACL”字段。有关 ACL 的更多信息，请参阅 访问控制列表 (ACL) 概述。
- 对象拥有者 – 对象的拥有者。
- 存储类 – 用于存储对象的存储类。
- 智能分层：访问层 – 如果存储在“S3 智能分层”存储类中，则表示对象的访问层（频繁或不频繁）。有关更多信息，请参阅 用于自动优化访问模式不断变化或未知的数据的存储类。
- ETag – 实体标签（ETag）是对象的哈希。ETag 仅反映对于对象的内容的更改，而不反映对于对象的元数据的更改。ETag 可能是该对象数据的 MD5 摘要，也可能不是。是与不是取决于对象的创建方式和加密方式。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 Object。
- 校验和算法 – 表示用于创建对象的校验和的算法。有关更多信息，请参阅 使用支持的校验和算法。
- 所有对象锁定配置 – 对象的对象锁定状态，包括以下设置：
  - 对象锁定：保留模式 – 应用于对象的保护级别，可以是监管或合规。
  - 对象锁定：保留截止日期 – 在此日期之前无法删除锁定的对象。
  - 对象锁定：依法保留状态 – 锁定对象的依法保留状态。

  有关 S3 对象锁定的更多信息，请参阅S3 对象锁定的工作原理。

有关清单报告内容的更多信息，请参阅 Amazon S3 清单列表。

有关在清单配置中限制对某些可选元数据字段的访问的更多信息，请参阅控制 S3 清单报告配置的创建。

15. 选择创建。

### 使用 REST API 处理 S3 清单

下面是可用于处理 Amazon S3 清单的 REST 操作。

- DeleteBucketInventoryConfiguration
- GetBucketInventoryConfiguration
- ListBucketInventoryConfigurations
- PutBucketInventoryConfiguration

## 查找清单列表

在清单列表发布后，Manifest 文件将发布到目标存储桶中的以下位置。

```
destination-prefix/amzn-s3-demo-source-bucket/config-ID/YYYY-MM-DDTHH-MMZ/manifest.json
 destination-prefix/amzn-s3-demo-source-bucket/config-ID/YYYY-MM-DDTHH-MMZ/
manifest.checksum
 destination-prefix/amzn-s3-demo-source-bucket/config-ID/hive/dt=YYYY-MM-DD-HH-MM/
symlink.txt
```

- *destination-prefix* 是对象键名称前缀，可以选择在资源清单配置中指定。您可以使用此前缀对目标存储桶内公共位置中的所有清单列表文件进行分组。
- *amzn-s3-demo-source-bucket* 是清单列表所针对的源存储桶。添加源存储桶名称是为了防止在将不同源存储桶中的多个清单报告发送到同一目标存储桶时发生冲突。
- 为防止从同一源存储桶发送到同一目标存储桶的多个清单报告发生冲突，添加了 *config-ID*。*config-ID* 来自清单报告配置，是在设置过程中定义的报告的名称。
- *YYYY-MM-DDTHH-MMZ* 是时间戳，包含清单报告生成过程开始扫描存储桶的开始时间和日期；例如，2016-11-06T21-32Z。
- manifest.json 是 Manifest 文件。

- `manifest.checksum` 是 `manifest.json` 文件内容的 MD5 哈希。
- `symlink.txt` 是 Apache Hive 兼容的清单文件。

清单列表每天或每周发布到目标存储桶中的以下位置。

```
destination-prefix/amzn-s3-demo-source-bucket/config-ID/data/example-file-name.csv.gz
...
destination-prefix/amzn-s3-demo-source-bucket/config-ID/data/example-file-name-1.csv.gz
```

- *destination-prefix* 是对象键名称前缀，可以选择在资源清单配置中指定。您可以使用此前缀对目标存储桶内公共位置中的所有清单列表文件进行分组。
- *amzn-s3-demo-source-bucket* 是清单列表所针对的源存储桶。添加源存储桶名称是为了防止在将不同源存储桶中的多个清单报告发送到同一目标存储桶时发生冲突。
- *example-file-name*`.csv.gz` 是 CSV 清单文件之一。ORC 清单名称以文件扩展名 `.orc` 结尾，Parquet 清单名称以文件扩展名 `.parquet` 结尾。

## 清单 Manifest

Manifest 文件 `manifest.json` 和 `symlink.txt` 描述清单文件的位置。每次交付新的清单列表时，它均带有一组新的 Manifest 文件。这些文件可能会互相覆盖。在启用了版本控制的存储桶中，Amazon S3 会创建清单文件的新版本。

`manifest.json` 文件中包含的每个 Manifest 均提供了有关清单的元数据和其他基本信息。这些信息包含：

- 源存储桶名称
- 目标存储桶名称
- 清单的版本
- 采用纪元日期格式的创建时间戳，包含清单报告生成过程开始扫描存储桶的开始时间和日期
- 清单文件的格式和架构
- 目标存储桶中清单文件的列表

每当写入 `manifest.json` 文件后，它都会附带一个 `manifest.checksum` 文件（作为 `manifest.json` 文件内容的 MD5 哈希）。

### Example **manifest.json** 文件中的清单 Manifest

以下示例显示了采用 CSV、ORC 和 Parquet 格式的清单的 manifest.json 文件中的清单列表。

#### CSV

下面是 CSV 格式清单的 manifest.json 文件中的 Manifest 示例。

```
{
    "sourceBucket": "amzn-s3-demo-source-bucket",
    "destinationBucket": "arn:aws:s3:::example-inventory-destination-bucket",
    "version": "2016-11-30",
    "creationTimestamp" : "1514944800000",
    "fileFormat": "CSV",
    "fileSchema": "Bucket, Key, VersionId, IsLatest, IsDeleteMarker,
 Size, LastModifiedDate, ETag, StorageClass, IsMultipartUploaded,
 ReplicationStatus, EncryptionStatus, ObjectLockRetainUntilDate, ObjectLockMode,
 ObjectLockLegalHoldStatus, IntelligentTieringAccessTier, BucketKeyStatus,
 ChecksumAlgorithm, ObjectAccessControlList, ObjectOwner",
    "files": [
        {
            "key": "Inventory/amzn-s3-demo-source-bucket/2016-11-06T21-32Z/
files/939c6d46-85a9-4ba8-87bd-9db705a579ce.csv.gz",
            "size": 2147483647,
            "MD5checksum": "f11166069f1990abeb9c97ace9cdfabc"
        }
    ]
}
```

#### ORC

下面是 ORC 格式清单的 manifest.json 文件中的 Manifest 示例。

```
{
    "sourceBucket": "amzn-s3-demo-source-bucket",
    "destinationBucket": "arn:aws:s3:::example-destination-bucket",
    "version": "2016-11-30",
    "creationTimestamp" : "1514944800000",
    "fileFormat": "ORC",
    "fileSchema":
 "struct<bucket:string,key:string,version_id:string,is_latest:boolean,is_delete_marker:boole
    "files": [
        {
```

```
            "key": "inventory/amzn-s3-demo-source-bucket/data/
d794c570-95bb-4271-9128-26023c8b4900.orc",
            "size": 56291,
            "MD5checksum": "5925f4e78e1695c2d020b9f6eexample"
        }
    ]
}
```

Parquet

下面是 manifest.json 格式清单的 Parquet 文件中的清单示例。

```
{
    "sourceBucket": "amzn-s3-demo-source-bucket",
    "destinationBucket": "arn:aws:s3:::example-destination-bucket",
    "version": "2016-11-30",
    "creationTimestamp" : "1514944800000",
    "fileFormat": "Parquet",
    "fileSchema": "message s3.inventory { required binary bucket (UTF8);
 required binary key (UTF8); optional binary version_id (UTF8); optional boolean
 is_latest; optional boolean is_delete_marker; optional int64 size; optional
 int64 last_modified_date (TIMESTAMP_MILLIS); optional binary e_tag (UTF8);
 optional binary storage_class (UTF8); optional boolean is_multipart_uploaded;
 optional binary replication_status (UTF8); optional binary encryption_status
 (UTF8); optional int64 object_lock_retain_until_date (TIMESTAMP_MILLIS); optional
 binary object_lock_mode (UTF8); optional binary object_lock_legal_hold_status
 (UTF8); optional binary intelligent_tiering_access_tier (UTF8); optional binary
 bucket_key_status (UTF8); optional binary checksum_algorithm (UTF8); optional
 binary object_access_control_list (UTF8); optional binary object_owner (UTF8);}",
    "files": [
        {
           "key": "inventory/amzn-s3-demo-source-bucket/data/
d754c470-85bb-4255-9218-47023c8b4910.parquet",
            "size": 56291,
            "MD5checksum": "5825f2e18e1695c2d030b9f6eexample"
        }
    ]
}
```

symlink.txt 文件是一个与 Apache Hive 兼容的清单文件，它使 Hive 能够自动发现清单文件及其关联的数据文件。与 Hive 兼容的清单文件可以与 Hive 兼容的服务 Athena 和 Amazon Redshift

Spectrum 一起使用。它还可用于与 Hive 兼容的应用程序，包括 Presto、Apache Hive、Apache Spark 以及许多其他应用程序。

> **Important**
>
> `symlink.txt` Apache Hive 兼容的清单文件当前不适用于 Amazon Glue。
> 对于 ORC 和 Parquet 格式的清单文件，不支持使用 Apache Hive 和 Apache Spark 读取 `symlink.txt` 文件。

## 设置清单完成时的 Amazon S3 事件通知

您可以设置 Amazon S3 事件通知以在创建清单校验和文件后接收通知，该通知将指示库存列表已添加到目标存储桶。清单是目标位置的所有库存列表的最新列表。

Amazon S3 可以将事件发布到 Amazon Simple Notification Service (Amazon SNS) 主题、Amazon Simple Queue Service (Amazon SQS) 队列或 Amazon Lambda 函数。有关更多信息，请参阅 Amazon S3 事件通知。

以下通知配置定义了新添加到目标存储桶的所有 `manifest.checksum` 文件将由 Amazon Lambda `cloud-function-list-write` 处理。

```
<NotificationConfiguration>
  <QueueConfiguration>
      <Id>1</Id>
      <Filter>
          <S3Key>
              <FilterRule>
                  <Name>prefix</Name>
                  <Value>destination-prefix/source-bucket</Value>
              </FilterRule>
              <FilterRule>
                  <Name>suffix</Name>
                  <Value>checksum</Value>
              </FilterRule>
          </S3Key>
      </Filter>
      <CloudFunction>arn:aws:lambda:us-west-2:222233334444:cloud-function-list-write</
CloudFunction>
      <Event>s3:ObjectCreated:*</Event>
  </QueueConfiguration>
```

```
</NotificationConfiguration>
```

有关更多信息，请参阅《Amazon Lambda 开发人员指南》中的Amazon Lambda 与 Amazon S3 结合使用。

## 使用 Amazon Athena 查询 Amazon S3 清单

您可以在 Athena 可用的所有区域中，通过 Amazon Athena 使用标准 SQL 查询来查询 Amazon S3 清单文件。要检查 Amazon Web Services 区域 可用性，请参阅 Amazon Web Services 区域 表。

Athena 可以采用经 Apache 优化的行列式（ORC）、Apache Parquet 或逗号分隔值（CSV）格式来查询 Amazon S3 清单文件。当您使用 Athena 查询清单文件时，我们建议您使用 ORC 格式或 Parquet 格式的清单文件。ORC 和 Parquet 格式提供了更快的查询性能并能够降低查询成本。ORC 和 Parquet 是自我描述、可感知类型的列式文件格式，专为 Apache Hadoop 而设计。列式格式允许读取器仅读取、解压缩并处理当前查询所需的列。所有 Amazon Web Services 区域均提供 ORC 和 Parquet 格式的 Amazon S3 清单。

使用 Athena 查询 Amazon S3 清单文件

1. 创建 Athena 表。有关创建表的信息，请参阅《Amazon Athena 用户指南》中的在 Amazon Athena 中创建表。
2. 使用以下示例查询模板之一创建查询，具体取决于您查询的是 ORC 格式、Parquet 格式还是 CSV 格式的清单报告。

   - 当您使用 Athena 查询 ORC 格式的清单报告时，请使用以下示例查询作为模板。

     下面的示例查询在 ORC 格式的清单报告中包含所有可选字段。

     要使用此示例查询，请执行以下操作：

     - 将 *your_table_name* 替换为您创建的 Athena 表的名称。
     - 删除您没有为清单选择的所有可选字段，以便查询对应于您的清单的选定字段。
     - 根据您的配置替换以下桶名称和清单位置（配置 ID）。

       s3://*amzn-s3-demo-bucket*/*config-ID*/hive/

     - 将 `projection.dt.range` 下的 *2022-01-01-00-00* 日期替换为在 Athena 中对数据进行分区的时间范围的第一天。有关更多信息，请参阅 Athena 中的分区数据。

```
CREATE EXTERNAL TABLE your_table_name(
         bucket string,
```

```
          key string,
          version_id string,
          is_latest boolean,
          is_delete_marker boolean,
          size bigint,
          last_modified_date timestamp,
          e_tag string,
          storage_class string,
          is_multipart_uploaded boolean,
          replication_status string,
          encryption_status string,
          object_lock_retain_until_date bigint,
          object_lock_mode string,
          object_lock_legal_hold_status string,
          intelligent_tiering_access_tier string,
          bucket_key_status string,
          checksum_algorithm string,
          object_access_control_list string,
          object_owner string
) PARTITIONED BY (
        dt string
)
ROW FORMAT SERDE 'org.apache.hadoop.hive.ql.io.orc.OrcSerde'
  STORED AS INPUTFORMAT 'org.apache.hadoop.hive.ql.io.SymlinkTextInputFormat'
  OUTPUTFORMAT 'org.apache.hadoop.hive.ql.io.IgnoreKeyTextOutputFormat'
  LOCATION 's3://source-bucket/config-ID/hive/'
  TBLPROPERTIES (
    "projection.enabled" = "true",
    "projection.dt.type" = "date",
    "projection.dt.format" = "yyyy-MM-dd-HH-mm",
    "projection.dt.range" = "2022-01-01-00-00,NOW",
    "projection.dt.interval" = "1",
    "projection.dt.interval.unit" = "HOURS"
  );
```

- 当您使用 Athena 查询 Parquet 格式的清单报告时，请使用 ORC 格式报告的示例查询。但是，请使用以下 Parquet SerDe 代替 `ROW FORMAT SERDE` 语句中的 ORC SerDe。

```
ROW FORMAT SERDE 'org.apache.hadoop.hive.ql.io.parquet.serde.ParquetHiveSerDe'
```

- 当您使用 Athena 查询 CSV 格式的清单报告时，请使用以下示例查询作为模板。

  下面的示例查询在 CSV 格式的清单报告中包含所有可选字段。

要使用此示例查询，请执行以下操作：

- 将 *your_table_name* 替换为您创建的 Athena 表的名称。
- 删除您没有为清单选择的所有可选字段，以便查询对应于您的清单的选定字段。
- 根据您的配置替换以下桶名称和清单位置（配置 ID）。

  s3://*amzn-s3-demo-bucket*/*config-ID*/hive/

- 将 projection.dt.range 下的 *2022-01-01-00-00* 日期替换为在 Athena 中对数据进行分区的时间范围的第一天。有关更多信息，请参阅 Athena 中的分区数据。

```
CREATE EXTERNAL TABLE your_table_name(
         bucket string,
         key string,
         version_id string,
         is_latest boolean,
         is_delete_marker boolean,
         size string,
         last_modified_date string,
         e_tag string,
         storage_class string,
         is_multipart_uploaded boolean,
         replication_status string,
         encryption_status string,
         object_lock_retain_until_date string,
         object_lock_mode string,
         object_lock_legal_hold_status string,
         intelligent_tiering_access_tier string,
         bucket_key_status string,
         checksum_algorithm string,
         object_access_control_list string,
         object_owner string
) PARTITIONED BY (
        dt string
)
ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.OpenCSVSerde'
  STORED AS INPUTFORMAT 'org.apache.hadoop.hive.ql.io.SymlinkTextInputFormat'
  OUTPUTFORMAT 'org.apache.hadoop.hive.ql.io.IgnoreKeyTextOutputFormat'
  LOCATION 's3://source-bucket/config-ID/hive/'
  TBLPROPERTIES (
    "projection.enabled" = "true",
    "projection.dt.type" = "date",
    "projection.dt.format" = "yyyy-MM-dd-HH-mm",
```

```
    "projection.dt.range" = "2022-01-01-00-00,NOW",
    "projection.dt.interval" = "1",
    "projection.dt.interval.unit" = "HOURS"
  );
```

3. 现在，您可以对清单运行各种查询，如以下示例所示。将每个 *user input placeholder* 替换为您自己的信息。

```
# Get a list of the latest inventory report dates available.
SELECT DISTINCT dt FROM your_table_name ORDER BY 1 DESC limit 10;

# Get the encryption status for a provided report date.
SELECT encryption_status, count(*) FROM your_table_name WHERE dt = 'YYYY-MM-DD-HH-
MM' GROUP BY encryption_status;

# Get the encryption status for inventory report dates in the provided range.
SELECT dt, encryption_status, count(*) FROM your_table_name
WHERE dt > 'YYYY-MM-DD-HH-MM' AND dt < 'YYYY-MM-DD-HH-MM' GROUP BY dt,
 encryption_status;
```

当您配置 S3 清单以将对象访问控制列表（对象 ACL）字段添加到清单报告时，报告将“对象 ACL”字段的值显示为以 base64 编码的字符串。要以 JSON 格式获取“对象 ACL”字段的解码值，可以使用 Athena 查询此字段。请参阅以下查询示例。有关“对象 ACL”字段的更多信息，请参阅使用“对象 ACL”字段。

```
# Get the S3 keys that have Object ACL grants with public access.
WITH grants AS (
    SELECT key,
        CAST(
            json_extract(from_utf8(from_base64(object_access_control_list)),
 '$.grants') AS ARRAY(MAP(VARCHAR, VARCHAR))
        ) AS grants_array
    FROM your_table_name
)
SELECT key,
       grants_array,
       grant
FROM grants, UNNEST(grants_array) AS t(grant)
WHERE element_at(grant, 'uri') = 'http://acs.amazonaws.com/groups/global/AllUsers'
```

```
# Get the S3 keys that have Object ACL grantees in addition to the object owner.
WITH grants AS
    (SELECT key,
    from_utf8(from_base64(object_access_control_list)) AS
 object_access_control_list,
         object_owner,
         CAST(json_extract(from_utf8(from_base64(object_access_control_list)),
         '$.grants') AS ARRAY(MAP(VARCHAR, VARCHAR))) AS grants_array
    FROM your_table_name)
SELECT key,
       grant,
       objectowner
FROM grants, UNNEST(grants_array) AS t(grant)
WHERE cardinality(grants_array) > 1 AND element_at(grant, 'canonicalId') !=
 object_owner;
```

```
# Get the S3 keys with READ permission that is granted in the Object ACL.
WITH grants AS (
    SELECT key,
        CAST(
            json_extract(from_utf8(from_base64(object_access_control_list)),
 '$.grants') AS ARRAY(MAP(VARCHAR, VARCHAR))
        ) AS grants_array
    FROM your_table_name
)
SELECT key,
       grants_array,
       grant
FROM grants, UNNEST(grants_array) AS t(grant)
WHERE element_at(grant, 'permission') = 'READ';
```

```
# Get the S3 keys that have Object ACL grants to a specific canonical user ID.
WITH grants AS (
    SELECT key,
        CAST(
            json_extract(from_utf8(from_base64(object_access_control_list)),
 '$.grants') AS ARRAY(MAP(VARCHAR, VARCHAR))
        ) AS grants_array
    FROM your_table_name
```

```
)
SELECT key,
       grants_array,
       grant
FROM grants, UNNEST(grants_array) AS t(grant)
WHERE element_at(grant, 'canonicalId') = 'user-canonical-id';
```

```
# Get the number of grantees on the Object ACL.
SELECT key,
       object_access_control_list,
       json_array_length(json_extract(object_access_control_list,'$.grants')) AS
 grants_count
FROM your_table_name;
```

有关使用 Athena 的更多信息，请参阅 Amazon Athena 用户指南。

## 将 Amazon S3 库存报告中的空版本 ID 字符串转换为空字符串

> **Note**
>
> 下面的过程只适用于包含所有版本的 Amazon S3 库存报告，并且只有当"所有版本"的报告作为 S3 分批操作在已启用 S3 版本的存储桶上的显示时才适用。您无需为仅指定当前版本的 S3 清单报告转换字符串。

您可以使用 S3 清单报告作为 S3 分批操作的清单。但是，在存储桶上启用 S3 版本控制时，包括所有版本的 S3 清单报告将在版本 ID 字段中用空字符串标记任何空版本控制的对象。当库存报告包含所有对象版本 ID 时，分批操作将 `null` 字符串识别为版本 ID，但不是空字符串。

当 S3 分批操作任务使用“所有版本”S3 清单报告作为清单时，它会使版本 ID 字段中有空字符串的对象上的所有任务失败。要将 S3 库存报告版本 ID 字段中的空字符串转换为分批操作 `null` 字符串，使用以下过程。

更新 Amazon S3 库存报告以便与分批操作一起使用

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。

2. 导航至 S3 清单报告。库存报告位于您在配置库存报告时指定的目标存储桶中。有关查找清单报告的更多信息，请参阅 查找清单列表。

   a. 选择目标存储桶。

   b. 选择 文件夹。该文件夹以原始源存储桶命名。

   c. 选择以清单配置命名的文件夹。

   d. 选择名为 hive 的文件夹旁边的勾选框。在页面顶部，选择 Copy S3 URI（复制 S3 URI）以为文件夹复制 S3 URI。

3. 从 https://console.aws.amazon.com/athena/ 打开 Amazon Athena 控制台。

4. 在查询编辑器中，选择 Settings（设置），然后选择 Manage（管理）。在存储库的 Manage settings（管理设置）页面中，针对 Location of query result（查询结果的位置），选择用于存储查询结果的 S3 存储桶。

5. 在查询编辑器中，使用以下命令创建 Athena 表以保存库存报告中的数据。将 *table_name* 替换为您所选择的名称，然后在 LOCATION 子句中，插入之前复制的 S3 URI。然后选择 Run（运行），以运行查询。

```
CREATE EXTERNAL TABLE table_name(bucket string, key string,
 version_id string) PARTITIONED BY (dt string)ROW FORMAT SERDE
 'org.apache.hadoop.hive.serde2.OpenCSVSerde'STORED AS INPUTFORMAT
 'org.apache.hadoop.hive.ql.io.SymlinkTextInputFormat' OUTPUTFORMAT
 'org.apache.hadoop.hive.ql.io.IgnoreKeyTextOutputFormat' LOCATION 'Copied S3 URI';
```

6. 要清除查询编辑器，请选择 Clear（清除）。然后使用以下命令将清单报告加载到表中。将 *table_name* 替换为您在上一步所选择的项。然后选择 Run（运行），以运行查询。

```
MSCK REPAIR TABLE table_name;
```

7. 要清除查询编辑器，请选择 Clear（清除）。运行以下 SELECT 查询以检索原始库存报告中的所有条目，并将任何空版本 ID 替换为 null 字符串。将 *table_name* 替换为先前所选择的项，然后将 WHERE 子句中的 *YYYY-MM-DD-HH-MM* 替换为您想要此工具运行的库存报告的日期。然后选择 Run（运行），以运行查询。

```
SELECT bucket as Bucket, key as Key, CASE WHEN version_id = '' THEN 'null' ELSE
 version_id END as VersionId FROM table_name WHERE dt = 'YYYY-MM-DD-HH-MM';
```

8. 返回 Amazon S3 控制台 (https://console.aws.amazon.com/s3/)，然后导航到稍早您为 Location of query result（查询结果位置）选择的 S3 存储桶。其内部应该有一系列以日期结束的文件夹。

例如，您将看到类似于 s3://*amzn-s3-demo-bucket*/*query-result-location*/Unsaved/2021/10/07/ 的内容。您将看到包含您运行的 SELECT 查询的结果的 .csv 文件。

选择具有最新修改日期的 CSV 文件。将此文件下载到本地计算机以进行下一步。

9. 生成的 CSV 文件包含标题行。要使用此 CSV 文件作为 S3 分批操作任务的输入，您必须移除标题行，因为分批操作不支持 CSV 清单上的标题行。

   要移除标题行，可以对文件运行以下命令之一。将 *file.csv* 替换为 CSV 文件的名称。

   对于 macOS 和 Linux 计算机，在终端窗口运行 tail 命令。

   ```
   tail -n +2 file.csv > tmp.csv && mv tmp.csv file.csv
   ```

   对于 Windows 计算机，在 Windows PowerShell 窗口中运行以下脚本。将 *File-location* 替换为文件的路径，将 *file.csv* 替换为文件名。

   ```
   $ins = New-Object System.IO.StreamReader File-location\file.csv
   $outs = New-Object System.IO.StreamWriter File-location\temp.csv
   try {
       $skip = 0
       while ( !$ins.EndOfStream ) {
           $line = $ins.ReadLine();
           if ( $skip -ne 0 ) {
               $outs.WriteLine($line);
           } else {
               $skip = 1
           }
       }
   } finally {
       $outs.Close();
       $ins.Close();
   }
   Move-Item File-location\temp.csv File-location\file.csv -Force
   ```

10. 从 CSV 文件中移除标题行后，您可以在 S3 分批操作任务中将其用作清单。将 CSV 文件上载到 S3 存储桶或您选择的位置，然后使用 CSV 文件作为清单创建分批操作任务。

    有关创建 S3 分批操作任务的更多信息，请参阅 创建 S3 批量操作任务。

# 使用“对象 ACL”字段

Amazon S3 清单报告包含 S3 源桶中对象的列表以及每个对象的元数据。“对象访问控制列表（ACL）”字段是 Amazon S3 清单中提供的一个元数据字段。具体而言，“对象 ACL”字段包含每个对象的访问控制列表（ACL）。对象的 ACL 定义了哪个 Amazon Web Services 账户或组被授予对此对象的访问权限以及所授予的访问权限类型。有关更多信息，请参阅访问控制列表 (ACL) 概述和Amazon S3 清单列表。

Amazon S3 清单报告中的“对象 ACL”字段以 JSON 格式定义。JSON 数据包含以下字段：

- `version` – 清单报告中“对象 ACL”字段格式的版本。它采用日期格式 `yyyy-mm-dd`。
- `status` – 可能的值为 `AVAILABLE` 或 `UNAVAILABLE`，指明对象 ACL 是否可用于某个对象。当对象 ACL 的状态为 `UNAVAILABLE` 时，清单报告中“对象拥有者”字段的值也是 `UNAVAILABLE`。
- `grants` – 被授权者/权限对，列出了对象 ACL 授予的每个被授权者的权限状态。被授权者的可用值为 `CanonicalUser` 和 `Group`。有关被授权者的更多信息，请参阅访问控制列表中的被授权者。

  对于类型为 `Group` 的被授权者，被授权者/权限对包括以下属性：

  - `uri` – 预定义的 Amazon S3 组。
  - `permission` – 所授予的对于对象的 ACL 权限。有关更多信息，请参阅对于对象的 ACL 权限。
  - `type` – 类型为 `Group`，表示被授权者是组。

  对于类型为 `CanonicalUser` 的被授权者，被授权者/权限对包括以下属性：

  - `canonicalId`— 一种经过混淆处理的 Amazon Web Services 账户 ID 形式。Amazon Web Services 账户的规范用户 ID 特定于该账户。您可以检索规范用户 ID。有关更多信息，请参阅《Amazon 账户管理参考指南》中的 Find the canonical user ID for your Amazon Web Services 账户。

    > **Note**
    >
    > 如果 ACL 中的被授权者是 Amazon Web Services 账户的电子邮件地址，S3 清单使用该 Amazon Web Services 账户的 `canonicalId` 和 `CanonicalUser` 类型来指定此授权者。有关更多信息，请参阅访问控制列表中的被授权者。

  - `permission` – 所授予的对于对象的 ACL 权限。有关更多信息，请参阅对于对象的 ACL 权限。
  - `type` – 类型为 `CanonicalUser`，表示被授权者是 Amazon Web Services 账户。

以下示例显示了“对象 ACL”字段的可能值，采用 JSON 格式：

```
{
    "version": "2022-11-10",
    "status": "AVAILABLE",
    "grants": [{
        "uri": "http://acs.amazonaws.com/groups/global/AllUsers",
        "permission": "READ",
        "type": "Group"
    }, {
        "canonicalId": "example-canonical-id",
        "permission": "FULL_CONTROL",
        "type": "CanonicalUser"
    }]
}
```

**Note**

“对象 ACL”字段以 JSON 格式定义。清单报告将“对象 ACL”字段的值显示为以 base64 编码的字符串。
例如，假设您有以下采用 JSON 格式的“对象 ACL”字段：

```
{
        "version": "2022-11-10",
        "status": "AVAILABLE",
        "grants": [{
            "canonicalId": "example-canonical-user-ID",
            "type": "CanonicalUser",
            "permission": "READ"
        }]
}
```

“对象 ACL”字段经过编码并显示为以下以 base64 编码的字符串：

```
eyJ2ZXJzaW9uIjoiMjAyMi0xMS0xMCIsInN0YXR1cyI6IkFWQUlMQUJMRSIsImdyYW50cyI6W3siY2Fub25pY2FsSW
```

要以 JSON 格式获取“对象 ACL”字段的解码值，可以在 Amazon Athena 中查询此字段。有关示例查询，请参阅使用 Amazon Athena 查询 Amazon S3 清单。

# 最佳实践设计模式：优化 Amazon S3 性能

当从 Amazon S3 上传和检索存储时，您的应用程序可以轻松地实现每秒数千个事务的请求性能。Amazon S3 自动扩展到高请求速率。例如，您的应用程序可以实现每秒每个分区的 Amazon S3 前缀至少 3500 个PUT/COPY/POST/DELETE 或 5500 个 GET/HEAD 请求。对存储桶中的前缀数量没有限制。您可以通过使用并行来增加读取或写入性能。例如，如果您在 Amazon S3 存储桶中创建 10 个前缀以并行处理读取，则可以将读取性能扩展到每秒 55,000 个读取请求。同样，您可以通过写入多个前缀来扩展写入操作。在读写操作的情况下，扩展是逐渐发生的，而不是瞬时完成的，实际性能将根据您的特定工作负载特征、使用规律和系统配置而有所不同。当 Amazon S3 扩展到新的更高请求速率时，您可能会看到一些 503（减速）错误。扩展完成后，这些错误将消失。有关创建和使用前缀的更多信息，请参阅使用前缀组织对象。

Amazon S3 上的某些数据湖应用程序对于运行超过 PB 级数据的查询扫描数百万或数十亿个对象。这些数据湖应用程序实现的单一实例传输速率可最大限度地提高 Amazon EC2 实例的网络接口利用率，这在单一实例上可高达 100 Gb/s。然后，这些应用程序跨多个实例聚合吞吐量，以获得每秒多个 Tb 的级别。

另外一些应用程序对延迟很敏感，例如社交媒体消息传递应用程序。这些应用程序可实现一致的小对象延迟（对于较大对象，为第一个字节输出延迟），延迟时间大约为 100 - 200 毫秒。

其他 Amazon 服务也可帮助加快不同应用程序架构的性能。例如，如果您希望通过单一 HTTP 连接实现较高的传输速率，或需要单一位毫秒延迟，请使用 Amazon CloudFront 或 Amazon ElastiCache 以通过 Amazon S3 进行缓存。

此外，如果您希望在客户端与 S3 存储桶之间获得较快的长距离数据传输速度，请使用 使用 Amazon S3 Transfer Acceleration 配置快速、安全的文件传输。Transfer Acceleration 使用 CloudFront 中的全球分布式边缘站点来加快跨地理距离的数据传输。如果 Amazon S3 工作负载使用具有 Amazon KMS 的服务器端加密，请参阅《Amazon Key Management Service 开发人员指南》中的 Amazon KMS 限制，以获取有关使用案例支持的请求速率的信息。

下面的主题介绍的最佳实践准则和设计模式用于优化使用 Amazon S3 的应用程序的性能。有关对 Amazon S3 进行性能优化的最新信息，请参阅 Amazon S3 的性能准则 和 Amazon S3 的性能设计规律。

> **Note**
>
> 有关将 Amazon S3 Express One Zone 存储类与目录存储桶配合使用的更多信息，请参阅 S3 Express One Zone 和使用目录存储桶。

主题


- Amazon S3 的性能准则
- Amazon S3 的性能设计规律


# Amazon S3 的性能准则

当构建用于从 Amazon S3 上传和检索对象的应用程序时，请遵循我们的最佳实践准则以优化性能。我们还提供了更详细的 Amazon S3 的性能设计规律 。

要在 Amazon S3 上获得应用程序的最佳性能，我们建议遵循以下准则。

主题


- 衡量性能
- 水平扩展存储连接
- 使用字节范围提取
- 延迟敏感型应用程序的重试请求
- 在同一 Amazon Web Services 区域中结合 Amazon S3（存储）和 Amazon EC2（计算）
- 使用 Amazon S3 Transfer Acceleration 最大限度地减少因距离导致的延迟
- 使用最新版本的 Amazon SDK


## 衡量性能

当优化性能时，查看网络吞吐量、CPU 和 DRAM 要求。根据针对这些不同资源的组合需求，可能需要评估不同的 Amazon EC2 实例类型。有关实例类型的信息，请参阅《Amazon EC2 用户指南》中的实例类型。

它还有助于在衡量性能时使用 HTTP 分析工具查看 DNS 查找时间、延迟和数据传输速度。

要了解性能要求并优化应用程序的性能，还可以监控收到的 503 错误响应。监控某些性能指标可能会产生额外费用。有关更多信息，请参阅 Amazon S3 定价。

### 监控 503（减速）状态错误响应的数量

要监控收到的 503 状态错误响应的数量，可以使用以下选项之一：

- 使用 Amazon S3 的 Amazon CloudWatch 请求指标。CloudWatch 请求指标包括一个用于 5xx 状态响应的指标。有关 CloudWatch 请求指标的更多信息，请参阅使用 Amazon CloudWatch 监控指标。
- 使用 Amazon S3 Storage Lens 存储统计管理工具的高级指标部分中提供的 503（服务不可用）错误计数。有关更多信息，请参阅 使用 S3 Storage Lens 存储统计管理工具指标提高性能。
- 使用 Amazon S3 服务器访问日志记录。通过服务器访问日志记录，您可以筛选和查看所有收到 503（内部错误）响应的请求。还可以使用 Amazon Athena 解析日志。有关服务器访问日志记录的更多信息，请参阅 使用服务器访问日志记录来记录请求。

通过监控 HTTP 503 状态错误代码的数量，您通常可以获得宝贵的见解，了解哪些前缀、密钥或存储桶获得的节流请求最多。

## 水平扩展存储连接

跨许多连接分布请求是一种常用的横向扩展性能的设计模式。当构建高性能应用程序时，将 Amazon S3 视为非常大的分布式系统，而不是类似于传统存储服务器的单个网络端点。您可以通过将多个并行请求发到 Amazon S3 来实现最佳性能。将这些请求分布在不同的连接，以最大限度地利用 Amazon S3 的可访问带宽。Amazon S3 对与存储桶建立的连接数没有任何限制。

## 使用字节范围提取

通过在 GET Object 请求中使用 Range HTTP 标头，您可以从对象中提取字节范围，而只传输指定的部分。您可以使用到 Amazon S3 的并行连接，从相同对象中提取不同的字节范围。这有助于您通过单一整个对象请求实现更高的聚合吞吐量。通过提取较小范围的大型对象，您的应用程序还可以在请求中断时改善重试次数。有关更多信息，请参阅 下载对象。

字节范围请求的典型大小为 8 MB 或 16 MB。如果使用分段上传来 PUT 对象，则最佳实践是以相同的分段大小来 GET 它们（或者至少与分段边界相符）以获得最佳性能。GET 请求可以直接面向单独的分段；例如，`GET ?partNumber=N`.

## 延迟敏感型应用程序的重试请求

大量的超时和重试会导致持续不断的延迟。考虑到 Amazon S3 的大规模，如果第一个请求较慢，则退出的请求可能采取不同的路径并快速成功。Amazon SDK 具有可配置的超时和重试值，您可以进行调整以符合特定应用程序的容限。

## 在同一 Amazon Web Services 区域中结合 Amazon S3（存储）和 Amazon EC2（计算）

尽管 S3 存储桶名称是全局唯一的，但每个存储桶都存储在您创建它时所选择的区域中。要了解有关存储桶命名准则的更多信息，请参阅存储桶概述和存储桶命名规则。为了优化性能，我们建议您尽可能从位于同一 Amazon Web Services 区域的 Amazon EC2 实例中访问此存储桶。这可以减少网络延迟和数据传输成本。

## 使用 Amazon S3 Transfer Acceleration 最大限度地减少因距离导致的延迟

使用 Amazon S3 Transfer Acceleration 配置快速、安全的文件传输 可在客户端与 S3 存储桶之间管理快速、轻松和安全的长地理距离文件传输。Transfer Acceleration 利用 Amazon CloudFront 中的全球分布式边缘站点。当数据到达某个边缘站点时，会通过经过优化的网络路径路由至 Amazon S3。Transfer Acceleration 适合定期跨大洲传输 GB 到 TB 的数据。它也适用于全球各地需要上传到集中式存储桶的客户。

可以使用 Amazon S3 Transfer Acceleration 速度比较工具来比较各个 Amazon S3 区域内加快的上传速度和未加快的上传速度。此速度比较工具使用分段上传来将文件从浏览器传输到各种使用和未使用 Amazon S3 Transfer Acceleration 的 Amazon S3 区域。

## 使用最新版本的 Amazon SDK

Amazon SDK 为许多用于优化 Amazon S3 性能的建议准则提供内置的支持。这些 SDK 提供了更简单的 API 以便从应用程序内部利用 Amazon S3，并定期更新以遵循最新的最佳实践。例如，这些 SDK 包含自动对 HTTP 503 错误重试请求的逻辑，并投资编写代码来应对和适应慢速连接。

这些 SDK 还提供传输管理器，以便在适当的时机使用字节范围请求来自动横向扩展连接，从而实现每秒数千个请求。务必使用最新版本的 Amazon SDK，以获取最新的性能优化特征。

您还可以在使用 HTTP REST API 请求时优化性能。当使用 REST API 时，您应遵循属于 SDK 一部分的相同最佳实践。对于慢速连接允许超时和重试，并使用多个连接以允许并行提取对象数据。有关使用 REST API 的信息，请参阅 Amazon Simple Storage Service API 参考。

# Amazon S3 的性能设计规律

当设计应用程序以从 Amazon S3 上传和检索对象时，使用我们的最佳实践设计模式，以实现应用程序的最佳性能。我们还提供 Amazon S3 的性能准则 ，供您在规划您的应用程序架构时考虑。

要优化性能，您可以使用以下设计模式。

主题


- 对频繁访问的内容使用缓存
- 延迟敏感型应用程序的超时和重试
- 水平扩缩和请求并行化以实现高吞吐量
- 使用 Amazon S3 Transfer Acceleration 加快地理位置分散的数据传输速度


## 对频繁访问的内容使用缓存

许多在 Amazon S3 中存储数据的应用程序会提供用户反复请求的数据的一个“工作集”。如果工作负载针对一组常用对象发送重复的 GET 请求，则可以使用 Amazon CloudFront、Amazon ElastiCache 或 AWS Elemental MediaStore 等缓存来优化性能。成功地采用缓存可能导致低延迟和较高的数据传输速率。使用缓存的应用程序还会向 Amazon S3 发送少量的直接请求，这可帮助降低请求成本。

Amazon CloudFront 是一个快速内容交付网络 (CDN)，它透明地在一大组地理位置分散的节点 (PoP) 中缓存 Amazon S3 中的数据。当可能从多个区域或通过 Internet 访问对象时，CloudFront 允许在访问对象的用户附近缓存数据。这样就可以实现常见 Amazon S3 内容的高性能交付。有关 CloudFront 的更多信息，请参阅 Amazon CloudFront 开发人员指南。

Amazon ElastiCache 是一个托管的内存中缓存。通过 ElastiCache，您可以预配置在内存中缓存对象的 Amazon EC2 实例。这种缓存会导致 GET 延迟下降若干个数量级，并显著增加下载吞吐量。要使用 ElastiCache，请修改应用程序逻辑，以便用热门对象填充缓存和检查缓存中的热门对象，然后从 Amazon S3 中请求它们。有关使用 ElastiCache 提高 Amazon S3 GET 性能的示例，请参阅博客文章使用 Amazon ElastiCache for Redis 增强 Amazon S3。

AWS Elemental MediaStore 是一个专为 Amazon S3 中的视频工作流和媒体交付构建的缓存和内容分配系统。MediaStore 提供专用于视频的端到端存储 API，推荐用于性能敏感型视频工作负载。有关 MediaStore 的更多信息，请参阅 AWS Elemental MediaStore 用户指南。

## 延迟敏感型应用程序的超时和重试

在某些情况下，应用程序会收到来自 Amazon S3 的响应，指示需要重试。Amazon S3 将存储桶和对象名称映射到与其关联的对象数据。如果应用程序生成高的请求率（通常针对少量对象持续超过每秒 5,000 个请求的速率），则它可能会收到 HTTP 503 速度下降 响应。如果出现这些错误，每个 Amazon SDK 都会使用指数退避来实现自动重试逻辑。如果您不使用 Amazon SDK，则应在收到 HTTP 503 错误时实施重试逻辑。有关回退技术的信息，请参阅《Amazon SDK 和工具参考指南》中的 Retry behavior。

Amazon S3 自动扩展以应对持续的新请求速率，同时动态地优化性能。尽管 Amazon S3 在内部针对新的请求速率进行优化，但您将临时收到 HTTP 503 请求响应，直至优化完成。当 Amazon S3 在内部针对新的请求速率优化性能后，通常无需重试就能正常应对所有请求。

对于延迟密集型应用程序，Amazon S3 建议跟踪和主动重试较慢的操作。当重试请求时，我们建议您使用到 Amazon S3 的新连接并执行全新 DNS 查找。

当您发出大型可变大小的请求（例如，超过 128 MB）时，我们建议跟踪所实现的吞吐量并重试最慢 5% 的请求。当您发出较小的请求（例如，小于 512 KB）时，其中，延迟时间中值通常处于数十毫秒的范围内，好的指导原则是在 2 秒后重试 GET 或 PUT 操作。如果需要更多重试，则最佳实践是退避。例如，我们建议您在 2 秒后发出一次重试，然后 4 秒后再发出一次重试。

如果应用程序对 Amazon S3 发出固定大小的请求，则应预期对于其中每个请求获得更一致的响应时间。在这种情况下，一个简单的策略是确定最慢的 1% 的请求并重试这些请求。甚至一次重试也会频繁、有效地减少延迟。

如果您使用 Amazon Key Management Service（Amazon KMS）进行服务器端加密，请参阅《Amazon Key Management Service 开发人员指南》中的 Quotas，以获取有关您的使用案例支持的请求速率的信息。

## 水平扩缩和请求并行化以实现高吞吐量

Amazon S3 是一个非常大的分布式系统。为了帮助您利用其规模，我们建议您将并行请求横向扩展到 Amazon S3 服务端点。除了在 Amazon S3 中分布请求之外，这种类型的扩展方法还有助于将负载分布到整个网络中的多个路径。

对于高吞吐量传输，Amazon S3 建议使用并行利用多个连接来 GET 或 PUT 数据的应用程序。例如，Amazon Java SDK 中的 Amazon S3 Transfer Manager 支持上述功能，大多数其他 Amazon SDK 也提供类似的构造。对于某些应用程序，您可以实现并行连接，具体方法为：在不同的应用程序线程或不同的应用程序实例中并行启动多个连接。要采取的最佳方法取决于应用程序以及您访问的对象的结构。

您可以使用 Amazon SDK 直接发出 GET 和 PUT 请求，而不是利用 Amazon SDK 中的传输管理。这种方法让您可以更直接地调整工作负载，同时仍受益于软件工具包支持重试和处理任何可能发生的 HTTP 503 响应。通常来说，当您将某个区域中的大型对象从 Amazon S3 下载到 Amazon EC2 时，我们建议您以 8-16 MB 的粒度向对象的字节范围发出并行请求。对于每个 85-90 MB/s 的所需网络吞吐量发出一个并行请求。要使 10 Gb/s 网络接口卡 (NIC) 达到饱和，您可以通过单独的连接使用大约 15 个并行请求。您可以通过更多连接扩展并行请求以使速度更快的 NIC 达到饱和，如 25 Gb/s 或 100 Gb/s NIC。

当您调整并行发出的请求数量时，衡量性能至关重要。我们建议一次只用一个请求为起点。衡量所实现的网络带宽以及应用程序用于处理数据的其他资源的使用情况。然后，您可以确定瓶颈资源（也即使用率最高的资源），进而确定可能有用的请求数。例如，如果一次处理一个请求会导致 CPU 利用率达到 25%，则建议可以容纳多达四个并行请求。衡量是必不可少的，随着请求速率增加，务必确认资源使用情况。

如果应用程序使用 REST API 直接向 Amazon S3 发出请求，我们建议您使用 HTTP 连接池，并对一系列请求重用每个连接。通过避免逐个请求连接设置，可消除对每个连接执行 TCP 慢速启动和安全套接字层 (SSL) 握手的需要。有关使用 REST API 的信息，请参阅 Amazon Simple Storage Service API 参考。

最后，务必注意 DNS 并仔细检查请求正在分散到广泛的 Amazon S3 IP 地址池。对于 Amazon S3 的 DNS 查询会循环经过一个很大的 IP 端点列表。但是，缓存解析程序或重用单一 IP 地址的应用程序代码不会受益于地址多样性和由此产生的负载平衡。网络实用工具（如 `netstat` 命令行工具）可以显示用来与 Amazon S3 通信的 IP 地址，并且我们提供要使用的 DNS 配置的准则。有关这些准则的更多信息，请参阅《Amazon S3 API 参考》中的 Making requests。

## 使用 Amazon S3 Transfer Acceleration 加快地理位置分散的数据传输速度

使用 Amazon S3 Transfer Acceleration 配置快速、安全的文件传输 通过使用 Amazon S3，有效地将由于全球分散的客户端与区域性应用程序之间的地理距离所导致的延迟降至最小甚至消除。Transfer Acceleration 使用 CloudFront 中的全球分布式边缘站点进行数据传输。Amazon 边缘网络在超过 50 个站点具有节点。目前，它用于通过 CloudFront 分布内容，并向针对 Amazon Route 53 发出的 DNS 查询提供快速响应。

边缘网络还有助于加速进出 Amazon S3 的数据传输。它对具有以下特点的应用程序是理想之选：跨大洲或在大洲之间传输数据、具有快速 Internet 连接、使用大型对象，或具有大量要上传的内容。当数据到达某个边缘站点时，数据会被经过优化的网络路径路由至 Amazon S3。通常，您与 Amazon S3 区域之间的距离越远，使用 Transfer Acceleration 可预期获得的速度改进就越大。

您可以对新的或现有的存储桶设置 Transfer Acceleration。您可以通过单独的 Amazon S3 Transfer Acceleration 端点来使用 Amazon 边缘站点。测试 Transfer Acceleration 是否有助于提高客户端请求性能的最佳方法是使用 Amazon S3 Transfer Acceleration 速度比较工具。网络配置和条件随时间或站点不同而可能发生变化。因此，我们只对 Amazon S3 Transfer Acceleration 可能会改进上传性能的传输向您收费。有关将 Transfer Acceleration 与不同的 Amazon SDK 结合使用的信息，请参阅 启用和使用 S3 Transfer Acceleration。

# 使用 Amazon S3 托管静态网站

您可以使用 Amazon S3 托管静态网站。在静态网站上，单独的网页包含静态内容。它们也可能包含客户端脚本。

> **Note**
>
> 我们建议您使用 Amazon Amplify Hosting 来托管存储在 S3 上的静态网站内容。Amplify Hosting 是一项完全托管式服务，可让您轻松地在由 Amazon CloudFront 提供支持的全球可用内容分发网络（CDN）上部署您的网站，并可实现安全的静态网站托管。
> 借助 Amazon Amplify Hosting，您可以选择对象在通用存储桶中的位置，将内容部署到托管式 CDN，并为网站生成一个公有 HTTPS URL 以供在任何地方访问。有关 Amplify Hosting 的更多信息，请参阅从 S3 通用存储桶将静态网站部署到 Amazon Amplify Hosting 和《Amazon Amplify Console User Guide》中的 Deploying a static website from S3 using the Amplify console。

有关在 Amazon S3 上托管静态网站的更多信息（包括说明和分步演练），请参阅以下主题。

主题


- 网站端点
- 启用网站托管
- 配置索引文档
- 配置自定义错误文档
- 设置访问网站的权限
- （可选）记录 Web 流量
- （可选）配置网页重定向
- 使用跨源资源共享 (CORS)
- 静态网站教程


## 网站端点

当您将存储桶配置为静态网站时，该网站在存储桶的 Amazon Web Services 区域 特定的网站端点上可用。网站端点不同于您在其上发送 REST API 请求的端点。有关端点之间的差异的更多信息，请参阅网站端点和 REST API 端点之间的主要区别。

根据您所在的区域，Amazon S3 网站端点采用以下两种格式之一。

- s3-website 短横线 (-) 区域 - `http://bucket-name.s3-website-Region.amazonaws.com`
- s3-网站 点 (.) 区域 - `http://bucket-name.s3-website.Region.amazonaws.com`

此 URL 将返回您为该网站配置的默认索引文档。有关 Amazon S3 网站端点的完整列表，请参阅 Amazon S3 网站端点。

> **Note**
>
> 为了增强 Amazon S3 静态网站的安全性，Amazon S3 网站端点域（例如 s3-website-us-east-1.amazonaws.com 或 s3-website.ap-south-1.amazonaws.com）已在 Public Suffix List (PSL)中注册。为进一步增强安全性，如果您需要在 Amazon S3 静态网站的域名中设置敏感 Cookie，我们建议您使用带 `__Host-` 前缀的 Cookie。这将有助于保护您的域，防范跨站点请求伪造 (CSRF) 攻击。要了解更多信息，请参阅 Mozilla 开发者网络中的 Set-Cookie 页面。

如果您希望您的网站公开，您必须使您的所有内容对您的客户公开可读，以便您的客户可以在网站端点访问这些内容。有关更多信息，请参阅 设置访问网站的权限。

> **Important**
>
> - Amazon S3 网站端点不支持 HTTPS 或接入点。如果要使用 HTTPS，可以执行以下操作之一：
>   - （建议）使用 Amazon Amplify Hosting 来托管存储在 S3 上的静态网站内容。Amplify Hosting 是一项完全托管式服务，可让您轻松地在由 Amazon CloudFront 提供支持的全球可用内容分发网络（CDN）上部署您的网站，并可实现安全的静态网站托管。
>
>     借助 Amazon Amplify Hosting，您可以选择对象在通用存储桶中的位置，将内容部署到托管式 CDN，并为网站生成一个公有 HTTPS URL 以供在任何地方访问。有关 Amplify Hosting 的更多信息，请参阅从 S3 通用存储桶将静态网站部署到 Amazon Amplify Hosting 和《Amazon Amplify Console User Guide》中的 Deploying a static website from S3 using the Amplify console。
>   - 使用 Amazon CloudFront 为 Amazon S3 上托管的静态网站提供服务。有关更多信息，请参阅如何使用 CloudFront 为我的 Amazon S3 存储桶提供 HTTPS 请求？ 要使用自定义域的 HTTPS，请参阅使用注册到 Route 53 的自定义域配置静态网站。

- 申请方付款存储桶不允许通过网站端点进行访问。对此类存储桶的任何请求都会收到 403 拒绝访问响应。有关更多信息，请参阅 使用申请方付款通用存储桶进行存储传输和使用。

主题


- 网站端点示例
- 添加 DNS 别名记录
- 将自定义域与 Route 53 结合使用
- 网站端点和 REST API 端点之间的主要区别


## 网站端点示例

以下示例演示如何访问配置为静态网站的 Amazon S3 存储桶。

Example – 请求根级别的对象

要请求存储在存储桶根级别的特定对象，请使用以下 URL 结构。

```
http://bucket-name.s3-website.Region.amazonaws.com/object-name
```

例如，以下 URL 请求存储在存储桶中根级别的 photo.jpg 对象。

```
http://example-bucket.s3-website.us-west-2.amazonaws.com/photo.jpg
```

Example – 请求前缀中的对象

要请求存储在存储桶的文件夹中的对象，请使用此 URL 结构。

```
http://bucket-name.s3-website.Region.amazonaws.com/folder-name/object-name
```

以下 URL 请求存储桶中的 docs/doc1.html 对象。

```
http://example-bucket.s3-website.us-west-2.amazonaws.com/docs/doc1.html
```

## 添加 DNS 别名记录

如果您拥有已注册的域，则可以添加指向 Amazon S3 网站端点的 DNS CNAME 条目。例如，如果您注册了 www.example-bucket.com 域，则可以创建存储桶 www.example-bucket.com，

并添加指向 www.example-bucket.com.s3-website.*Region*.amazonaws.com 的 DNS CNAME 记录。对 http://www.example-bucket.com 的所有请求都将路由到 www.example-bucket.com.s3-website.*Region*.amazonaws.com。

有关更多信息，请参阅 使用 CNAME 记录自定义 Amazon S3 URL。

## 将自定义域与 Route 53 结合使用

您可以使用自己的向 Amazon Route 53 注册的域（例如，example.com）来提供您的内容，而不是使用 Amazon S3 网站端点访问网站。您可以将 Amazon S3 与 Route 53 结合使用以在根域中托管网站。例如，如果您拥有根域 example.com 且在 Amazon S3 上托管您的网站，则您的网站访问者可以通过输入 http://www.example.com 或 http://example.com 从他们的浏览器访问该站点。

有关示例演练的信息，请参阅 教程：使用注册到 Route 53 的自定义域配置静态网站。

## 网站端点和 REST API 端点之间的主要区别

Amazon S3 网站端点针对通过 Web 浏览器访问进行了优化。下表总结 REST API 端点和网站端点之间的主要区别。

| 主要区别 | REST API 端点 | 网站端点 |
| --- | --- | --- |
| 访问控制 | 同时支持公有和私有内容 | 仅支持公开可读的内容 |
| 错误消息处理 | 返回 XML 格式的错误响应 | 返回 HTML 文档 |
| 重定向支持 | 不适用 | 同时支持对象级和存储桶级重定向 |
| 支持的请求 | 支持所有存储桶和对象操作 | 仅支持针对对象的 GET 和 HEAD 请求 |
| 对存储桶根级的 GET 和 HEAD 请求的响应 | 返回存储桶中对象键的列表 | 返回在网站配置中指定的索引文档 |
| 安全套接字层 (SSL) 支持 | 支持 SSL 连接 | 不支持 SSL 连接 |

有关 Amazon S3 端点的完整列表，请参阅《Amazon Web Services 一般参考》中的 Amazon S3 端点和限额。

# 启用网站托管

将存储桶配置为静态网站时，您必须启用静态网站托管、配置索引文档和设置权限。

您可以使用 Amazon S3 控制台、REST API、Amazon SDK、Amazon CLI 或 Amazon CloudFormation 启用静态网站托管。

要使用自定义域配置您的网站，请参阅 教程：使用注册到 Route 53 的自定义域配置静态网站。

## 使用 S3 控制台

启用静态网站托管

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在存储桶列表中，选择要为其启用静态网站托管的存储桶的名称。
4. 选择属性。
5. 在静态网站托管下，请选择编辑。
6. 请选择使用此存储桶托管网站。
7. 在静态网站托管下，请选择启用。
8. 在 Index document (索引文档) 中，输入索引文档的文件名，通常为 `index.html`。

   索引文档名称区分大小写，并且必须与您计划上传到 S3 存储桶的 HTML 索引文档的文件名完全匹配。当您为网站托管配置存储桶时，您必须指定索引文档。当对根域或任何子文件夹发出请求时，Amazon S3 将返回此索引文档。有关更多信息，请参阅 配置索引文档。
9. 要为 4XX 类错误提供您自己的自定义错误文档，请在错误文档中输入自定义错误文档文件名。

   错误文档名称区分大小写，并且必须与您计划上传到 S3 存储桶的 HTML 错误文档的文件名完全匹配。如果未指定自定义错误文档并发生错误，Amazon S3 返回默认 HTML 错误文档。有关更多信息，请参阅 配置自定义错误文档。
10. （可选）如果要指定高级重定向规则，请在 Redirection rules（重定向规则）中，输入 JSON 来描述规则。

例如，您可以根据请求中的特定对象键名或前缀按条件路由请求。有关更多信息，请参阅 配置重新导向规则以使用高级条件重新导向。

11. 选择 Save changes（保存更改）。

    Amazon S3 为您的存储桶启用静态网站托管。在页面底部的静态网站托管下，您可以看到存储桶的网站端点。

12. 在静态网站托管下，记下端点。

    端点是存储桶的 Amazon S3 网站端点。将存储桶配置为静态网站后，您可以使用此端点来测试您的网站。

## 使用 REST API

有关直接发送 REST 请求以启用静态网站托管的更多信息，请参阅《Amazon Simple Storage Service API 参考》中的以下部分：

- PUT Bucket website
- GET Bucket website
- DELETE Bucket website

## 使用 Amazon SDK

若要在 Amazon S3 上托管静态网站，需要为网站托管配置 Amazon S3 存储桶，然后将您的网站内容上传到该存储桶。您还可以使用 Amazon SDK 以编程方式创建、更新和删除网站配置。SDK 围绕 Amazon S3 REST API 提供封装类。如果应用程序需要它，可以直接从应用程序发送 REST API 请求。

.NET

以下示例说明如何使用 适用于 .NET 的 Amazon SDK 管理存储桶的网站配置。要将网站配置添加到存储桶，请提供存储桶名称和网站配置。网站配置必须包含索引文档，并且可包含可选的错误文档。这些文档必须存储在存储桶中。有关更多信息，请参阅 PUT Bucket 网站。有关 Amazon S3 网站功能的更多信息，请参阅 使用 Amazon S3 托管静态网站。

以下 C# 代码示例将网站配置添加到指定的存储桶。该配置指定索引文档和错误文档名称。有关设置和运行代码示例的信息，请参阅《适用于 .NET 的 Amazon SDK 开发人员指南》中的适用于 .NET 的 Amazon SDK 入门。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class WebsiteConfigTest
    {
        private const string bucketName = "*** bucket name ***";
        private const string indexDocumentSuffix = "*** index object key ***"; //
 For example, index.html.
        private const string errorDocument = "*** error object key ***"; // For
 example, error.html.
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;
        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            AddWebsiteConfigurationAsync(bucketName, indexDocumentSuffix,
 errorDocument).Wait();
        }

        static async Task AddWebsiteConfigurationAsync(string bucketName,
                                                string indexDocumentSuffix,
                                                string errorDocument)
        {
            try
            {
                // 1. Put the website configuration.
                PutBucketWebsiteRequest putRequest = new PutBucketWebsiteRequest()
                {
                    BucketName = bucketName,
                    WebsiteConfiguration = new WebsiteConfiguration()
                    {
                        IndexDocumentSuffix = indexDocumentSuffix,
                        ErrorDocument = errorDocument
                    }
                };
```

```
                PutBucketWebsiteResponse response = await
 client.PutBucketWebsiteAsync(putRequest);

                // 2. Get the website configuration.
                GetBucketWebsiteRequest getRequest = new GetBucketWebsiteRequest()
                {
                    BucketName = bucketName
                };
                GetBucketWebsiteResponse getResponse = await
 client.GetBucketWebsiteAsync(getRequest);
                Console.WriteLine("Index document: {0}",
 getResponse.WebsiteConfiguration.IndexDocumentSuffix);
                Console.WriteLine("Error document: {0}",
 getResponse.WebsiteConfiguration.ErrorDocument);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
        }
    }
}
```

PHP

以下 PHP 示例将网站配置添加到指定的存储桶。`create_website_config` 方法显式提供索引文档和错误文档名称。该示例还检索网站配置并输出响应。有关 Amazon S3 网站功能的更多信息，请参阅 使用 Amazon S3 托管静态网站。

有关适用于 Ruby 的 Amazon 开发工具包 API 的更多信息，请转到适用于 Ruby 的 Amazon 开发工具包 – 版本 2。

```
 require 'vendor/autoload.php';

use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';
```

```
$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);


// Add the website configuration.
$s3->putBucketWebsite([
    'Bucket'                => $bucket,
    'WebsiteConfiguration'  => [
        'IndexDocument' => ['Suffix' => 'index.html'],
        'ErrorDocument' => ['Key' => 'error.html']
    ]
]);

// Retrieve the website configuration.
$result = $s3->getBucketWebsite([
    'Bucket' => $bucket
]);
echo $result->getPath('IndexDocument/Suffix');

// Delete the website configuration.
$s3->deleteBucketWebsite([
    'Bucket' => $bucket
]);
```

### 使用 Amazon CLI

有关使用 Amazon CLI 将 S3 存储桶配置为静态网站的更多信息，请参阅《Amazon CLI 命令参考》中的网站。

接下来，您必须配置索引文档并设置权限。有关信息，请参阅 配置索引文档 和 设置访问网站的权限。

还可以有选择性地配置错误文档、Web 流量日志记录或重定向。

## 配置索引文档

启用网站托管时，还必须配置和上传索引文档。索引文档 是在对网站的根或任何子文件夹发出请求时 Amazon S3 返回的网页。例如，如果用户在浏览器中输入 `http://www.example.com`，则该用户没有请求任何特定页面。在这种情况下，Amazon S3 将提供索引文档，该文档有时也可称为默认页面。

当您为存储桶启用静态网站托管时，您可以输入索引文档的名称（例如，index.html）。为存储桶启用静态网站托管后，您可以将具有索引文档名称的 HTML 文件上传到存储桶。

根级 URL 的尾部斜杠是可选的。例如，如果您将具有 index.html 的网站配置为索引文档，以下任意一个 URL 将返回 index.html。

```
http://example-bucket.s3-website.Region.amazonaws.com/
http://example-bucket.s3-website.Region.amazonaws.com
```

有关 Amazon S3 网站端点的更多信息，请参阅 网站端点。

## 索引文档和文件夹

在 Amazon S3 中，存储桶是对象的平面容器。它不会像计算机上的文件系统那样提供任何分层组织。但是，您可以通过使用表示文件夹结构的对象键名创建逻辑层级结构。

例如，考虑具有三个对象（具有以下键名）的存储桶。虽然它们没有按任何物理分层组织进行存储，但您可以从键名推断以下逻辑文件夹结构：

- sample1.jpg — 对象位于存储桶的根级。
- photos/2006/Jan/sample2.jpg — 对象位于 photos/2006/Jan 子文件夹中。
- photos/2006/Feb/sample3.jpg — 对象位于 photos/2006/Feb 子文件夹中。

在 Amazon S3 控制台中，您还可以在存储桶中创建文件夹。例如，您可以创建名为 photos 的文件夹。您可以将对象上传到存储桶或该存储桶中的 photos 文件夹。如果您将对象 sample.jpg 添加到存储桶，则键名为 sample.jpg。如果您将对象上传到 photos 文件夹，则对象键名为 photos/sample.jpg。

如果您在存储桶中创建了文件夹结构，则您必须在每个级别上都具有索引文档。在每个文件夹中，索引文档必须具有相同的名称，例如，index.html。当用户指定类似于文件夹查找的 URL 时，是否存在尾部斜杠将决定网站的行为。例如，以下具有尾部反斜杠的 URL 将返回 photos/index.html 索引文档。

```
http://bucket-name.s3-website.Region.amazonaws.com/photos/
```

但是，如果您从之前的 URL 排除了尾部斜杠，则 Amazon S3 将首先在存储段中查找对象 photos。如果未找到 photos 对象，它将搜索索引文档 photos/index.html。如果找到该文档，则 Amazon S3 将返回 302 Found 消息并指向 photos/ 密钥。对于对 photos/ 的后续请求，Amazon S3 将返回 photos/index.html。如果未找到索引文档，Amazon S3 将返回错误。

# 配置索引文档

要使用 S3 控制台配置索引文档，请使用以下步骤。您还可以使用 REST API、Amazon SDK、Amazon CLI 或 Amazon CloudFormation 配置索引文档。

> **Note**
>
> 在启用版本控制的存储桶中，您可以上传 `index.html` 的多个副本，但只解析为最新的版本。有关使用 S3 版本控制的更多信息，请参阅使用 S3 版本控制保留对象的多个版本。

当您为存储桶启用静态网站托管时，您可以输入索引文档的名称（例如，**`index.html`**）。为存储桶启用静态网站托管后，您可以将具有此索引文档名称的 HTML 文件上传到存储桶。

配置索引文档

1. 创建 `index.html` 文件。

   如果您没有 `index.html` 文件，则可以使用以下 HTML 创建一个：

   ```
   <html xmlns="http://www.w3.org/1999/xhtml" >
   <head>
       <title>My Website Home Page</title>
   </head>
   <body>
     <h1>Welcome to my website</h1>
     <p>Now hosted on Amazon S3!</p>
   </body>
   </html>
   ```

2. 将索引文件保存在本地。

   索引文档文件名必须与您在静态网站托管对话框中输入的索引文档名称完全匹配。索引文档名称区分大小写。例如，如果在静态网站托管对话框中为索引文档名称输入 `index.html`，则索引文档文件名也必须是 `index.html`，而不是 `Index.html`。

3. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。

4. 在左侧导航窗格中，选择通用存储桶。

5. 在存储桶列表中，选择要用于托管静态网站的存储桶的名称。

6. 为您的存储桶启用静态网站托管，并输入索引文档的确切名称（例如 `index.html`）。有关更多信息，请参阅 启用网站托管。

   启用静态网站托管后，继续执行步骤 6。

7. 要将索引文档上传到存储桶，请执行以下操作之一：

   - 将索引文件拖放到控制台存储桶列表中。
   - 选择上传，然后按照提示选择并上传索引文件。

   如需分步指导，请参阅 上传对象。

8. （可选）将其他网站内容上传到您的存储桶。

接下来，您必须设置用于访问网站的权限。有关信息，请参阅 设置访问网站的权限。

还可以有选择性地配置错误文档、Web 流量日志记录或重定向。

# 配置自定义错误文档

将存储桶配置为静态网站后，当出现错误时，Amazon S3 返回 HTML 错误文档。您可以选择使用自定义错误文档配置存储桶，以便在发生错误时 Amazon S3 返回该文档。

> **Note**
>
> 当出现错误时，某些浏览器将显示自己的错误消息，而忽略 Amazon S3 返回的错误文档。例如，当出现 HTTP 404 Not Found (HTTP 404 未找到) 错误时，Google Chrome 可能忽略 Amazon S3 返回的错误文档并显示自己的错误。

主题


- Amazon S3 HTTP 响应代码
- 配置自定义错误文档


## Amazon S3 HTTP 响应代码

下表列出了出现错误时 Amazon S3 返回的 HTTP 响应代码的子集。

| HTTP 错误代码 | 描述 |
| --- | --- |
| 301 永久移动 | 当用户将请求直接发送到 Amazon S3 网站端点（`http://s3-website.` *`Region`*`.amazonaws.com/` ）时，Amazon S3 将返回 301 Moved Permanently（301 永久移动）响应并将这些请求重定向到 `https://aws.amazon.com/s3/` 。 |
| 302 Found (302 已找到) | 当 Amazon S3 接收对不包含尾部斜杠的键 x (`http://`*`bucket-name`*`.s3-website.` *`Region`*`.amazonaws.com/x` ) 的请求时，它首先查找键名为 x 的对象。如果未找到对象，则 Amazon S3 确定该请求是针对子文件夹 x 发出的，并通过在末尾添加斜杠重定向请求并返回 302 Found (302 已找到)。 |
| 304 Not Modified (304 未修改) | Amazon S3 使用请求标头 `If-Modified-Since` 、`If-Unmodified-Since` 、`If-Match` 和/或 `If-None-Match` 来确定请求的对象与客户端具有的缓存副本是否相同。如果对象相同，网站端点将返回 304 Not Modified 响应。 |
| 400 Malformed Request | 当用户尝试通过错误的地区端点访问存储桶时，网站端点的响应包含 400 Malformed Request。 |
| 403 禁止访问 | 当用户请求转换为不可公开读取的对象时，网站端点的响应包含 403 禁止访问。对象所有者必须使用存储桶策略或 ACL 使该对象公开可读。 |
| 404 未找到 | 由于以下原因，网站端点的响应包含 404 Not Found：<br>• Amazon S3 确定网站 URL 引用了不存在的对象键。<br>• Amazon S3 推断该请求针对不存在的索引文档。<br>• 在 URL 中指定的存储桶不存在。<br>• URL 中指定的存储桶存在，但未配置为网站。 |

| HTTP 错误代码 | 描述 |
| --- | --- |
| | 您可以创建为 404 Not Found 返回的自定义文档。确保该文档已上传到配置为网站的存储桶，且网站托管配置已设置为使用该文档。<br><br>有关 Amazon S3 如何将 URL 当作对对象或索引文档的请求的信息，请参阅配置索引文档。 |
| 500 Service Error | 当出现内部服务器错误时，网站端点的响应包含 500 Service Error。 |
| 503 服务不可用 | 当 Amazon S3 确定您需要降低请求率时，网站端点的响应包含 503 Service Unavailable（503 服务不可用）。 |

对于其中每个错误，Amazon S3 都返回一条预定义的 HTML 消息。以下是对 403 Forbidden 响应返回的 HTML 消息示例。



403 Forbidden

- Code: AccessDenied
- Message: Access Denied
- RequestId: 873CA367A51F7EC7
- HostId: DdQezl9vkuw5luD5HKsFaTDm9KH4PZzCPRkW3igimILbTu1DiYlvXjgyd7pVxq32

An Error Occurred While Attempting to Retrieve a Custom Error Document

- Code: AccessDenied
- Message: Access Denied

## 配置自定义错误文档

将存储桶配置为静态网站时，您可以提供包含用户友好错误消息和其他帮助的自定义错误文档。Amazon S3 将仅为 HTTP 4XX 类的错误代码返回您的自定义错误文档。

要使用 S3 控制台配置自定义错误文档，请执行以下步骤。您还可以使用 REST API、Amazon SDK、Amazon CLI 或 Amazon CloudFormation 配置错误文档。有关更多信息，请参阅下列内容：

- 《Amazon Simple Storage Service API 参考》中的 PutBucketWebsite

- 《Amazon CloudFormation 用户指南》中的 AWS::S3::Bucket WebsiteConfiguration
- 《Amazon CLI 命令参考》中的 put-bucket-website

当您为存储桶启用静态网站托管时，请输入错误文档的名称（例如，**404.html**）。为存储桶启用静态网站托管后，您可以将具有此错误文档名称的 HTML 文件上传到存储桶。

要配置错误文档

1. 创建错误文档，例如 404.html。
2. 将错误文档文件保存在本地。

   错误文档名称区分大小写，必须与启用静态网站托管时输入的名称完全匹配。例如，如果在静态网站托管对话框中为错误文档名称输入 404.html，则错误文档文件名也必须是 404.html。
3. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
4. 在左侧导航窗格中，选择通用存储桶。
5. 在存储桶列表中，选择要用于托管静态网站的存储桶的名称。
6. 为您的存储桶启用静态网站托管，并输入错误文档的确切名称（例如 404.html）。有关更多信息，请参阅启用网站托管和配置自定义错误文档。

   启用静态网站托管后，继续执行步骤 6。
7. 要将错误文档上传到存储桶，请执行以下操作之一：

   - 将错误文档文件拖放到控制台存储桶列表中。
   - 选择上传，然后按照提示选择并上传索引文件。

   如需分步指导，请参阅 上传对象。

# 设置访问网站的权限

将存储桶配置为静态网站时，如果希望网站成为公有网站，则可以授予公有读取访问权限。要使存储桶公开可读，您必须禁用存储桶的阻止公有访问设置并编写一条授予公有读取访问权限的存储桶策略。如果存储桶包含并非由存储桶拥有者拥有的对象，您可能还需要添加对象访问控制列表 (ACL)，以便向所有人授予读取访问权限。

如果您不想禁用存储桶的阻止公共访问设置，但仍希望将自己的网站公开，则可以创建 Amazon CloudFront 分配来为静态网站提供服务。有关更多信息，请参阅使用 Amazon CloudFront 为网站提速或《Amazon Route 53 开发人员指南》中的使用 Amazon CloudFront 分配为静态网站提供服务。

> **Note**
>
> 在网站端点上，如果用户请求了不存在的对象，则 Amazon S3 将返回 HTTP 响应代码 404 (Not Found)。如果该对象存在，但您尚未授予对对象的读取权限，则网站端点将返回 HTTP 响应代码 403 (Access Denied)。用户可以使用该响应代码推断特定对象是否存在。如果您不需要此行为，则不应启用对存储桶的网站支持。

主题


- 步骤 1：编辑 S3 阻止公有访问设置
- 步骤 2：添加存储桶策略
- 对象访问控制列表


## 步骤 1：编辑 S3 阻止公有访问设置

如果要将现有存储桶配置为具有公有访问权限的静态网站，您必须编辑该存储桶的阻止公有访问设置。您可能还必须编辑账户级别的阻止公有访问设置。Amazon S3 会应用限制性最强的存储桶级别和账户级别的阻止公有访问设置的组合。

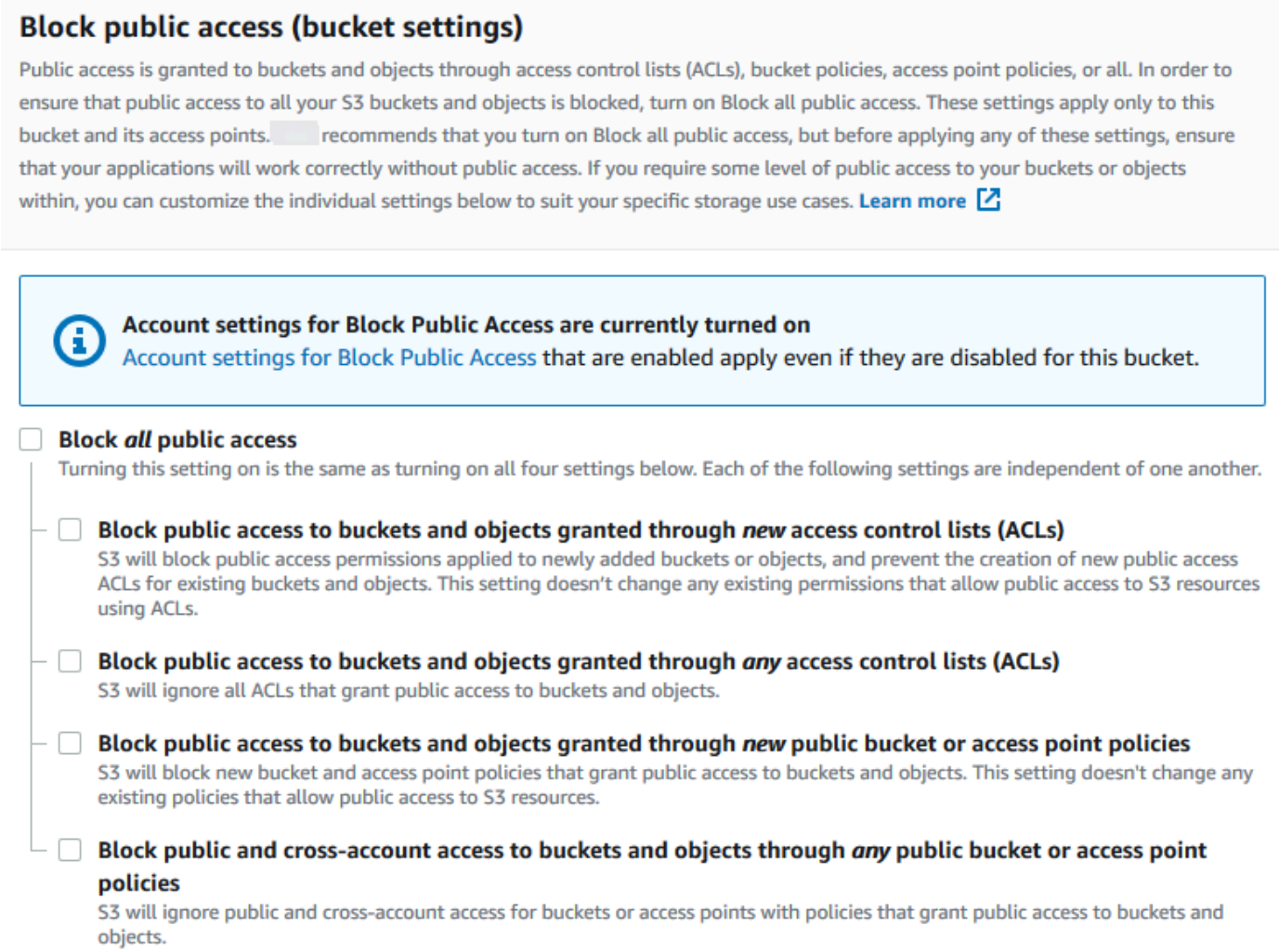
例如，如果您允许对存储桶进行公有访问，但阻止账户级别的所有公有访问权限，则 Amazon S3 将继续阻止对存储桶进行公有访问。在这种情况下，您将必须编辑存储桶级别和账户级别的阻止公有访问设置。有关更多信息，请参阅 阻止对您的 Amazon S3 存储的公有访问。

默认情况下，Amazon S3 阻止对您的账户和存储桶的公有访问权限。如果要使用存储桶托管静态网站，您可以使用以下步骤编辑您的屏蔽公共访问权限设置。

> **Warning**
>
> 在完成这些步骤之前，请查看阻止对您的 Amazon S3 存储的公有访问，来确保您了解并接受支持公共访问权限所涉及的风险。当您关闭屏蔽公共访问权限设置以使您的存储桶变为公有时，Internet 上的任何人都可以访问您的存储桶。我们建议您阻止对存储桶的所有公有访问。

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。

2. 请选择已配置为静态网站的存储桶的名称。
3. 选择权限。
4. 在屏蔽公共访问权限（存储桶设置）下，请选择编辑。
5. 清除阻止所有公有访问，然后选择保存更改。




Amazon S3 关闭了存储桶的屏蔽公共访问权限设置。要创建公有静态网站，可能还必须为您的账户配置屏蔽公共访问权限设置，然后再添加存储桶策略。如果当前已开启账户的屏蔽公共访问权限设置，您将在屏蔽公共访问权限（存储桶设置）下看到一条备注。

## 步骤 2：添加存储桶策略

要使存储桶中的对象公开可读，您必须编写一条向所有人授予 `s3:GetObject` 权限的存储桶策略。

在编辑 S3 阻止公有访问设置后，您可以添加存储桶策略以授予对存储桶的公有读取访问权限。当您授予公有读取访问权限时，Internet 上的任何人都可以访问您的存储桶。

> **Important**
>
> 下面的策略仅供举例说明，仍允许完全访问您存储桶的内容。在继续执行此步骤之前，请查看如何保护 Amazon S3 存储桶中的文件？，以确保您了解保护 S3 存储桶中文件的最佳实践以及授予公有访问权限所涉及的风险。

1. 在存储桶 下，请选择存储桶的名称。
2. 选择权限。
3. 在存储桶策略下，请选择编辑。
4. 要授予对网站的公有读取访问权限，请复制以下存储桶策略，将其粘贴到存储桶策略编辑器中。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicReadGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::Bucket-Name/*"
            ]
        }
    ]
}
```

5. 将 `Resource` 更新为您的存储桶名称。

   在上述示例存储桶策略中，*Bucket-Name* 是存储桶名称的占位符。要将此存储桶策略用于您自己的存储桶，您必须更新此名称以匹配您的存储桶名称。

6. 选择保存更改。

   此时将显示一条消息，指示存储桶策略已成功添加。

如果您看到显示 `Policy has invalid resource` 的错误，请确认存储桶策略中的存储桶名称与您的存储桶名称匹配。有关添加存储桶策略的信息，请参阅如何添加 S3 存储桶策略？

如果您收到错误消息且无法保存存储桶策略，请检查您的账户和存储桶的阻止公有访问设置以确认您允许对存储桶进行公有访问。

## 对象访问控制列表

您可以使用存储桶策略来授予对对象的公共读取权限。但是，存储桶策略仅适用于存储桶拥有者所拥有的对象。如果存储桶包含并非由存储桶拥有者拥有的对象，则存储桶拥有者应使用对象访问控制列表 (ACL) 授予对这些对象的公有 READ 权限。

S3 对象所有权是 Amazon S3 存储桶级别的设置，您可以使用该设置来控制上传到存储桶的对象的所有权和禁用或启用 ACL。默认情况下，对象所有权设为强制存储桶拥有者设置，并且所有 ACL 均处于禁用状态。禁用 ACL 后，存储桶拥有者拥有存储桶中的所有对象，并使用访问管理策略来专门管理对这些对象的访问权限。

Amazon S3 中的大多数现代使用案例不再需要使用 ACL。我们建议您将 ACL 保持为禁用状态，除非有需要单独控制每个对象的访问权限的特殊情况。禁用 ACL 后，您可以使用策略来控制对存储桶中所有对象的访问权限，无论是谁将对象上传到您的存储桶。有关更多信息，请参阅 为您的存储桶控制对象所有权和禁用 ACL。。

> **Important**
>
> 如果通用存储桶针对 S3 对象所有权使用强制存储桶拥有者设置，则必须使用策略来授予对通用存储桶及其中对象的访问权限。启用强制存储桶拥有者设置后，设置访问控制列表（ACL）或更新 ACL 的请求将失败并返回 `AccessControlListNotSupported` 错误代码。我们仍然支持读取 ACL 的请求。

要使用 ACL 使对象公开可读，您可以向 `AllUsers` 组授予 READ 权限，如以下授权元素所示。可以将此授权元素添加到对象 ACL 中。有关管理 ACL 的信息，请参阅 访问控制列表 (ACL) 概述。

```
<Grant>
  <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
           xsi:type="Group">
    <URI>http://acs.amazonaws.com/groups/global/AllUsers</URI>
  </Grantee>
```

```
  <Permission>READ</Permission>
</Grant>
```

# （可选）记录 Web 流量

您可以选择为配置为静态网站的存储桶启用 Amazon S3 服务器访问日志记录。服务器访问日志记录详细地记录了对您的存储桶提出的各种请求。有关更多信息，请参阅 使用服务器访问日志记录来记录请求。如果您计划使用 Amazon CloudFront 来为网站提速，也可以使用 CloudFront 日志记录。有关更多信息，请参阅《Amazon CloudFront 开发人员指南》中的配置和使用访问日志。

为静态网站存储桶启用服务器访问日志记录

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 例如，在您创建存储桶（配置为静态网站）的同一区域中，创建用于日志记录的通用存储桶（例如 `logs.example.com`）。
3. 为服务器访问日志记录日志文件创建文件夹（例如，`logs`）。
4. （可选）如果要使用 CloudFront 提高网站性能，请为 CloudFront 日志文件创建一个文件夹（例如，`cdn`）。

   有关更多信息，请参阅 使用 Amazon CloudFront 为网站提速。
5. 在 Buckets (存储桶) 列表中，请选择您的存储桶。
6. 请选择属性。
7. 在 Server access logging（服务器访问日志记录）下，请选择 Edit（编辑）。
8. 请选择 Enable。
9. 在 Target bucket（目标存储桶）下，请选择服务器访问日志的存储桶和文件夹目标：
   - 浏览到文件夹和存储桶位置：
     1. 请选择 Browse S3（浏览 S3）。
     2. 请选择存储桶名称，然后选择日志文件夹。
     3. 请选择 Choose path（选择路径）。
   - 输入 S3 存储桶路径，例如 **`s3://logs.example.com/logs/`**。
10. 选择保存更改。

    在日志存储桶中，您现在可以访问日志。Amazon S3 每 2 小时将网站访问日志写入您的日志存储桶一次。

# （可选）配置网页重定向

如果为静态网站托管配置了 Amazon S3 存储桶，您可以为存储桶或其中的对象配置重新导向。您可以使用以下选项来配置重新导向。

主题


- 针对存储桶的网站端点的请求重新导向到另一个存储桶或域
- 配置重新导向规则以使用高级条件重新导向
- 重新导向对于对象的请求


## 针对存储桶的网站端点的请求重新导向到另一个存储桶或域

您可以将针对存储桶的网站端点的所有请求重新导向到另一个存储桶或域。如果您重新导向所有请求，则对网站端点所做的任何请求都将重新导向至指定的存储桶或域。

例如，假设您的根域为 `example.com`，而您需要服务 `http://example.com` 和 `http://www.example.com` 的请求，则必须创建两个分别名为 `example.com` 和 `www.example.com` 的存储桶。然后，将内容保留在 `example.com` 存储桶中，然后配置另一个 `www.example.com` 存储桶以将所有请求重定向至 `example.com` 存储桶。有关更多信息，请参阅使用自定义域名配置静态网站。

重定向对存储桶网站端点的请求

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets（存储桶）下，请选择要从中重定向请求的存储桶的名称（例如 `www.example.com`）。
3. 请选择属性。
4. 在静态网站托管下，选择编辑。
5. 请选择 Redirect requests for an object（重定向对于对象的请求）。
6. 在 Host name（主机名）框中，输入存储桶或自定义域的网站端点。

   例如，如果您正在重定向到根域地址，则输入 **`example.com`**。
7. 对于 Protocol（协议），请选择重定向请求的协议（none（无）、http 或 https）。

   如果未指定协议，则默认选项为 none (无)。
8. 选择保存更改。

# 配置重新导向规则以使用高级条件重新导向

利用高级重定向规则，您可以根据特定对象键名、请求中的前缀或者响应代码来按条件路由请求。例如，假设您在存储桶中删除或重命名了某个对象。您可以添加一个将请求重定向到其他对象的路由规则。如果您要使文件夹不可用，则可以添加路由规则将请求重定向至其他网页。处理错误时，您还可以通过将返回错误的请求路由到其他域来添加一个处理错误条件的路由规则。

当为存储桶启用静态网站托管时，您可以选择指定高级重新导向规则。Amazon S3 对每个网站配置的路由规则限制为 50 条。如果您需要 50 个以上的路由规则，则可以使用对象重定向。有关更多信息，请参阅 使用 S3 控制台。

有关使用 REST API 配置路由规则的更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 PutBucketWebsite。

> **Important**
>
> 要在新的 Amazon S3 控制台中创建重定向规则，您必须使用 JSON。有关 JSON 示例，请参阅重定向规则示例。

为静态网站配置重定向规则

要为已启用静态网站托管的存储桶添加重定向规则，请执行以下步骤。

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在存储桶列表中，选择已配置为静态网站的存储桶的名称。
4. 请选择属性。
5. 在 Static website hosting（静态网站托管）下，请选择 Edit (编辑)。
6. 在 Redirection rules (重定向规则) 框中，输入使用 JSON 的重定向规则。

   在 S3 控制台中，您可以使用 JSON 描述规则。有关 JSON 示例，请参阅重定向规则示例。Amazon S3 对每个网站配置的路由规则限制为 50 条。
7. 选择保存更改。

## 路由规则元素

以下是在 JSON 和 XML 中的网站配置中定义路由规则的一般语法。要在新的 S3 控制台中配置重定向规则，必须使用 JSON。有关 JSON 示例，请参阅重定向规则示例。

JSON

```
[
    {
      "Condition": {
        "HttpErrorCodeReturnedEquals": "string",
        "KeyPrefixEquals": "string"
      },
      "Redirect": {
        "HostName": "string",
        "HttpRedirectCode": "string",
        "Protocol": "http"|"https",
        "ReplaceKeyPrefixWith": "string",
        "ReplaceKeyWith": "string"
      }
    }
  ]

Note: Redirect must each have at least one child element. You can have either
 ReplaceKeyPrefix with or ReplaceKeyWith but not both.
```

XML

```
<RoutingRules> =
    <RoutingRules>
         <RoutingRule>...</RoutingRule>
         [<RoutingRule>...</RoutingRule>
         ...]
    </RoutingRules>

<RoutingRule> =
   <RoutingRule>
      [ <Condition>...</Condition> ]
      <Redirect>...</Redirect>
   </RoutingRule>

<Condition> =
   <Condition>
```

```
      [ <KeyPrefixEquals>...</KeyPrefixEquals> ]
      [ <HttpErrorCodeReturnedEquals>...</HttpErrorCodeReturnedEquals> ]
   </Condition>
    Note: <Condition> must have at least one child element.

<Redirect> =
   <Redirect>
      [ <HostName>...</HostName> ]
      [ <Protocol>...</Protocol> ]
      [ <ReplaceKeyPrefixWith>...</ReplaceKeyPrefixWith>  ]
      [ <ReplaceKeyWith>...</ReplaceKeyWith> ]
      [ <HttpRedirectCode>...</HttpRedirectCode> ]
   </Redirect>

Note: <Redirect> must have at least one child element. You can have either
 ReplaceKeyPrefix with or ReplaceKeyWith but not both.
```

下表描述了路由规则中的元素。

| 名称 | 描述 |
| --- | --- |
| RoutingRules | 用于收集 RoutingRule 元素的容器。 |
| RoutingRule | 标识在满足条件时应用的条件和重定向的规则。<br>条件：<br>• RoutingRules 容器必须包含至少一个路由规则。 |
| Condition | 对于要应用的指定的重定向，用于描述必须满足的条件的容器。如果路由规则不包含条件，则该规则将应用于所有请求。 |
| KeyPrefixEquals | 从中重定向请求的对象键名的前缀。<br>KeyPrefixEquals 如果未指定 HttpErrorCodeReturnedEquals ，则需要 。如果同时指定 KeyPrefixEquals 和 |

| 名称 | 描述 |
| --- | --- |
| | HttpErrorCodeReturnedEquals ，则两者都必须为真才能满足条件。 |
| HttpErrorCodeReturnedEquals | 要应用的重定向必须匹配的 HTTP 错误代码。如果出现错误，并且错误代码满足此值，则应用指定的重定向。<br><br>HttpErrorCodeReturnedEquals 如果未指定 KeyPrefixEquals ，则需要 。如果同时指定 KeyPrefixEquals 和 HttpErrorCodeReturnedEquals ，则两者都必须为真才能满足条件。 |
| Redirect | 提供用于重定向请求的说明的容器元素。您可以将请求重定向到其他主机或其他页面，或者也可以指定要使用的其他协议。RoutingRule 必须具有 Redirect 元素。Redirect 元素必须至少包含以下一个同级元素：Protocol、HostName、ReplaceKeyPrefixWith 、ReplaceKeyWith 或 HttpRedirectCode 。 |
| Protocol | 响应中返回的 http 标头中将要使用的协议（https 或 Location）。<br><br>如果提供了一个同级，则 Protocol 不是必需的。 |
| HostName | 可在响应中返回的 Location 标头中使用的主机名。<br><br>如果提供了一个同级，则 HostName 不是必需的。 |
| ReplaceKeyPrefixWith | 将替换重定向请求中的 KeyPrefixEquals 值的对象键名的前缀。<br><br>如果提供了一个同级，则 ReplaceKeyPrefixWith 不是必需的。仅在不提供 ReplaceKeyWith 时提供它。 |

| 名称 | 描述 |
| --- | --- |
| ReplaceKeyWith | 可在响应中返回的 Location 标头中使用的对象键。<br><br>如果提供了一个同级，则 ReplaceKeyWith 不是必需的。仅在不提供 ReplaceKeyPrefixWith 时提供它。 |
| HttpRedirectCode | 可在响应中返回的 Location 标头中使用的 HTTP 重定向代码。<br><br>如果提供了一个同级，则 HttpRedirectCode 不是必需的。 |

重定向规则示例

以下示例介绍了常见的重定向任务：

> **Important**
> 要在新的 Amazon S3 控制台中创建重定向规则，您必须使用 JSON。

Example 1：保留键前缀后进行重定向

假设您的存储桶包含以下对象：

- index.html
- docs/article1.html
- docs/article2.html

您决定将文件夹从 docs/ 重命名为 documents/。做出此更改后，您需要将对前缀 docs/ 的请求重定向至 documents/。例如，对 docs/article1.html 的请求将重定向至 documents/article1.html。

在这种情况下，您可以将以下路由规则添加到网站配置。

JSON

```
[
```

```
    {
        "Condition": {
            "KeyPrefixEquals": "docs/"
        },
        "Redirect": {
            "ReplaceKeyPrefixWith": "documents/"
        }
    }
]
```

XML

```
  <RoutingRules>
    <RoutingRule>
    <Condition>
      <KeyPrefixEquals>docs/</KeyPrefixEquals>
    </Condition>
    <Redirect>
      <ReplaceKeyPrefixWith>documents/</ReplaceKeyPrefixWith>
    </Redirect>
    </RoutingRule>
  </RoutingRules>
```

Example 2：将对已删除文件夹的请求重定向到页面

假设您删除了 images/ 文件夹 (即，删除了具有键前缀 images/ 的所有对象)。您可以添加路由规则以将具有键前缀 images/ 的任何对象的请求重定向至名为 folderdeleted.html 的页。

JSON

```
[
    {
        "Condition": {
            "KeyPrefixEquals": "images/"
        },
        "Redirect": {
            "ReplaceKeyWith": "folderdeleted.html"
        }
    }
]
```

XML

```
  <RoutingRules>
    <RoutingRule>
    <Condition>
       <KeyPrefixEquals>images/</KeyPrefixEquals>
    </Condition>
    <Redirect>
      <ReplaceKeyWith>folderdeleted.html</ReplaceKeyWith>
    </Redirect>
    </RoutingRule>
  </RoutingRules>
```

Example 3：为 HTTP 错误进行重定向

假设在未找到请求的对象时，您需要将请求重定向到 Amazon Elastic Compute Cloud (Amazon EC2) 实例。添加重定向规则，以便当返回 HTTP 状态代码 404 (未找到) 时，站点访问者可重定向到将处理该请求的 Amazon EC2 实例。

以下示例也将在重定向中插入对象键前缀 `report-404/`。例如，如果您请求了页面 `ExamplePage.html` 并且它导致了 HTTP 404 错误，该请求将重定向到指定 Amazon EC2 实例上的 `report-404/ExamplePage.html` 页面。如果没有路由规则且发生了 HTTP 错误 404，将返回配置中指定的错误文档。

JSON

```
[
    {
        "Condition": {
            "HttpErrorCodeReturnedEquals": "404"
        },
        "Redirect": {
            "HostName": "ec2-11-22-333-44.compute-1.amazonaws.com",
            "ReplaceKeyPrefixWith": "report-404/"
        }
    }
]
```

XML

```
  <RoutingRules>
```

```
    <RoutingRule>
    <Condition>
      <HttpErrorCodeReturnedEquals>404</HttpErrorCodeReturnedEquals >
    </Condition>
    <Redirect>
      <HostName>ec2-11-22-333-44.compute-1.amazonaws.com</HostName>
      <ReplaceKeyPrefixWith>report-404/</ReplaceKeyPrefixWith>
    </Redirect>
    </RoutingRule>
  </RoutingRules>
```

## 重新导向对于对象的请求

您可以通过在对象的元数据中设置网站重定向位置，以将对于对象的请求重定向到另一个对象或 URL。您可以通过将 `x-amz-website-redirect-location` 属性添加到对象元数据来设置重定向。在 Amazon S3 控制台上，您可以在对象的元数据中设置 Website Redirect Location (网站重定向位置)。如果您使用 Amazon S3 API，请设置 `x-amz-website-redirect-location`。然后，该网站将该对象解释为 301 重定向。

要重定向对其他对象的请求，您可以将重定向位置设置为目标对象的键。要重定向对外部 URL 的请求，您可以将重定向位置设置为所需的 URL。有关对象元数据的更多信息，请参阅 系统定义的对象元数据。

当您设置页面重定向时，您可以保留或删除源对象内容。例如，如果您的存储桶中有一个 `page1.html` 对象，则可以将针对此页面的任何请求重定向到另一个对象 `page2.html`。您有两种选择：

- 保留 `page1.html` 对象的内容和重定向页面请求。
- 删除 `page1.html` 的内容并上传名为 `page1.html` 的零字节对象以替换现有对象和重定向页面请求。

使用 S3 控制台

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets（存储桶）列表中，请选择已配置为静态网站的存储桶的名称（例如 `example.com`）。
3. 在 Objects (对象) 下，选择您的对象。
4. 请选择 Actions（操作），然后选择 Edit metadata（编辑元数据）。

5. 请选择 Metadata（元数据）。
6. 请选择 Add Metadata（添加元数据）。
7. 在 Type（类型）下，请选择 System Defined（系统定义）。
8. 在 Key (键) 中，请选择 x-amz-website-redirect-location。
9. 在 Value (值)中，输入要重定向到的对象的键名，例如 `/page2.html`。

   对于同一存储桶中的另一个对象，值中的 / 前缀是必需的。您也可以将该值设置为外部 URL，例如 `http://www.example.com`。
10. 请选择 Edit metadata（编辑元数据）。

使用 REST API

以下 Amazon S3 API 操作支持请求中的 `x-amz-website-redirect-location` 标头。Amazon S3 存储对象元数据中的标头值作为 `x-amz-website-redirect-location`。

- PUT Object
- 开始分段上传
- POST 对象
- PUT Object – 复制

为网站托管配置的存储桶具有网站端点和 REST 端点。对配置为 301 重定向的页面的请求具有以下可能的结果，具体取决于请求的端点：

- 特定于区域的网站端点 – Amazon S3 根据 `x-amz-website-redirect-location` 属性的值重定向页面请求。
- REST 端点 – Amazon S3 不会重定向页面请求。它将返回请求的对象。

有关端点的更多信息，请参阅 网站端点和 REST API 端点之间的主要区别。

设置页面重定向时，您可以保留或删除对象内容。例如，假设您的存储桶中有 `page1.html` 对象。

- 若要保留 `page1.html` 的内容并仅重定向页面请求，您可以提交 PUT 对象 – 复制请求来创建新的 `page1.html` 对象，该对象使用现有 `page1.html` 对象作为源。在您的请求中，您可以设置 `x-amz-website-redirect-location` 标头。当请求完成时，您将拥有未更改其内容的原始页面，但 Amazon S3 会将对该页面的任何请求重定向到您指定的重定向位置。

- 要删除 page1.html 对象的内容并重定向对该页面的请求，您可以发送 PUT Object 请求，以上传具有相同对象键的零字节对象 page1.html。在 PUT 请求中，您可以将 x-amz-website-redirect-location 的 page1.html 设置为新对象。当请求完成时，page1.html 将不包含任何内容，且后续请求将被重定向到由 x-amz-website-redirect-location 指定的位置。

当使用 GET Object 操作以及其他对象元数据检索该对象时，Amazon S3 在响应中返回 x-amz-website-redirect-location 标头。

# 使用跨源资源共享 (CORS)

跨源资源共享 (CORS) 定义了在一个域中加载的客户端 Web 应用程序与另一个域中的资源交互的方式。借助 CORS 支持，您可以使用 Amazon S3 构建各种富客户端 Web 应用程序，并选择性地允许跨源访问您的 Amazon S3 资源。

本部分提供 CORS 概述。副主题介绍如何通过使用 Amazon S3 控制台或通过以编程方式使用 Amazon S3 REST API 和 Amazon SDK 来启用 CORS。

## 跨源资源共享：使用案例场景

以下是有关使用 CORS 的示例场景。

方案 1

假设您在名为 website 的 Amazon S3 存储桶中托管网站（如 使用 Amazon S3 托管静态网站 中所述）。您的用户加载了网站端点。

```
http://website.s3-website.us-east-1.amazonaws.com
```

现在，您想要使用此存储桶中存储的网页上的 JavaScript，以使用该存储桶的 Amazon S3 API 端点 website.s3.us-east-1.amazonaws.com 向同一存储桶发送经身份验证的 GET 和 PUT 请求。浏览器通常会阻止 JavaScript 允许这些请求，但借助 CORS，您可以配置您的存储桶以显式支持来自 website.s3-website.us-east-1.amazonaws.com 的跨源请求。

方案 2

假设您想要托管来自您的 S3 存储桶的 Web 字体。浏览器会再次要求对正在加载的 Web 字体进行 CORS 检查 (也称为预检)。您可以配置托管 Web 字体的存储桶，以允许任何源发出这些请求。

## Amazon S3 如何评估针对存储桶的 CORS 配置？

Amazon S3 收到来自浏览器的预检请求后，它将为存储桶评估 CORS 配置，并使用第一个匹配传入浏览器请求的 CORSRule 规则来允许跨源请求。要使规则实现匹配，必须满足以下条件：

- 向存储桶发出的 CORS 请求中的 Origin 标头必须与 CORS 配置的 AllowedOrigins 元素中的源相匹配。
- 在向存储桶发出的 CORS 请求的 Access-Control-Request-Method 中指定的 HTTP 方法，必须与在 CORS 配置的 AllowedMethods 元素中列出的一个或多个方法相匹配。
- 预检请求的 Access-Control-Request-Headers 标头中列出的标头必须与 CORS 配置的 AllowedHeaders 元素中的标头相匹配。

> **Note**
>
> 对存储桶启用 CORS 时，ACL 和策略将继续适用。

## 对象 Lambda 接入点如何支持 CORS

当 S3 对象 Lambda 收到来自浏览器的请求或包含 Origin 标头的请求时，S3 对象 Lambda 始终会添加 "AllowedOrigins":"*" 标头字段。

有关使用 CORS 的更多信息，请参阅以下主题。

主题

- CORS 配置的元素
- 配置跨源资源共享 (CORS)
- 测试 CORS
- CORS 问题排查

## CORS 配置的元素

要将您的存储桶配置为允许跨源请求，创建一个 CORS 配置。CORS 配置是一个包含元素的文档，这些元素标识可访问您的存储桶的源、对于每个源将支持的操作（HTTP 方法）以及其它操作特定的信息。您可以向配置添加最多 100 条规则。您可以将 CORS 配置作为 cors 子资源添加到存储桶中

如果要在 S3 控制台中配置 CORS，则必须使用 JSON 来创建 CORS 配置。新的 S3 控制台仅支持 JSON CORS 配置。

有关 CORS 配置及其中元素的更多信息，请参阅以下主题。有关如何添加 CORS 配置的说明，请参阅配置跨源资源共享 (CORS)。

> **Important**
>
> 在 S3 控制台中，CORS 配置必须是 JSON。

主题


- AllowedMethods 元素
- AllowedOrigins 元素
- AllowedHeaders 元素
- ExposeHeaders 元素
- MaxAgeSeconds 元素
- CORS 配置的示例


## `AllowedMethods` 元素

在 CORS 配置中，您可以为 `AllowedMethods` 元素指定以下值。

- GET
- PUT
- POST
- DELETE
- HEAD

## `AllowedOrigins` 元素

在 `AllowedOrigins` 元素中，可指定您希望允许从中发送跨源请求的源，例如 `http://www.example.com`。源字符串只能包含至少一个 `*` 通配符，例如 `http://*.example.com`。您可以选择将 `*` 指定为源，以允许所有源发送跨源请求。您还可以指定 `https` 只允许安全的源。

### `AllowedHeaders` 元素

`AllowedHeaders` 元素通过 `Access-Control-Request-Headers` 标头指定预检请求中允许哪些标头。`Access-Control-Request-Headers` 标头中的每个标头名称必须匹配元素中的相应条目。Amazon S3 将仅发送请求的响应中允许的标头。有关适用于发送至 Amazon S3 的请求中的标头示例列表，请参阅 Amazon Simple Storage Service API 参考指南中的常见请求标头。

配置中的每个 AllowedHeaders 字符串都可以包含至少一个 * 通配符。例如，`<AllowedHeader>x-amz-*</AllowedHeader>` 将允许所有特定于 Amazon 的标头。

### `ExposeHeaders` 元素

每个 `ExposeHeader` 元素标识您希望客户能够从其应用程序 (例如，从 JavaScript `XMLHttpRequest` 对象) 进行访问的响应标头。有关常见的 Amazon S3 响应标头的列表，请参阅 Amazon Simple Storage Service API 参考指南中的常见响应标头。

### `MaxAgeSeconds` 元素

`MaxAgeSeconds` 元素指定在预检请求被资源、HTTP 方法和源识别之后，浏览器将为预检请求缓存响应的时间 (以秒为单位)。

## CORS 配置的示例

您可以使用您自己的域 ( 例如 `example1.com` ) 提供您的内容，而不是通过使用 Amazon S3 网站端点访问网站。有关如何使用您自己的域的信息，请参阅 教程：使用注册到 Route 53 的自定义域配置静态网站。

以下示例 CORS 配置具有三个规则，这些规则被指定为 `CORSRule` 元素：

- 第一个规则允许来自 `http://www.example1.com` 源的跨源 PUT、POST 和 DELETE 请求。该规则还通过 `Access-Control-Request-Headers` 标头允许预检 OPTIONS 请求中的所有标头。作为对预检 OPTIONS 请求的响应，Amazon S3 将返回请求的标头。
- 第二个规则允许与第一个规则具有相同的跨源请求，但第二个规则应用于另一个源 `http://www.example2.com`。
- 第三个规则允许来自所有源的跨源 GET 请求。* 通配符将引用所有源。

JSON

```
[
```

```
    {
        "AllowedHeaders": [
            "*"
        ],
        "AllowedMethods": [
            "PUT",
            "POST",
            "DELETE"
        ],
        "AllowedOrigins": [
            "http://www.example1.com"
        ],
        "ExposeHeaders": []
    },
    {
        "AllowedHeaders": [
            "*"
        ],
        "AllowedMethods": [
            "PUT",
            "POST",
            "DELETE"
        ],
        "AllowedOrigins": [
            "http://www.example2.com"
        ],
        "ExposeHeaders": []
    },
    {
        "AllowedHeaders": [],
        "AllowedMethods": [
            "GET"
        ],
        "AllowedOrigins": [
            "*"
        ],
        "ExposeHeaders": []
    }
]
```

## XML

```
<CORSConfiguration>
```

```
 <CORSRule>
   <AllowedOrigin>http://www.example1.com</AllowedOrigin>

   <AllowedMethod>PUT</AllowedMethod>
   <AllowedMethod>POST</AllowedMethod>
   <AllowedMethod>DELETE</AllowedMethod>

   <AllowedHeader>*</AllowedHeader>
 </CORSRule>
 <CORSRule>
   <AllowedOrigin>http://www.example2.com</AllowedOrigin>

   <AllowedMethod>PUT</AllowedMethod>
   <AllowedMethod>POST</AllowedMethod>
   <AllowedMethod>DELETE</AllowedMethod>

   <AllowedHeader>*</AllowedHeader>
 </CORSRule>
 <CORSRule>
   <AllowedOrigin>*</AllowedOrigin>
   <AllowedMethod>GET</AllowedMethod>
 </CORSRule>
</CORSConfiguration>
```

CORS 配置还允许可选的配置参数，如下面的 CORS 配置所示。在本示例中，CORS 配置允许来自 `http://www.example.com` 源的跨源 PUT、POST 和 DELETE 请求。

JSON

```
[
    {
        "AllowedHeaders": [
            "*"
        ],
        "AllowedMethods": [
            "PUT",
            "POST",
            "DELETE"
        ],
        "AllowedOrigins": [
            "http://www.example.com"
        ],
```

```
        "ExposeHeaders": [
            "x-amz-server-side-encryption",
            "x-amz-request-id",
            "x-amz-id-2"
        ],
        "MaxAgeSeconds": 3000
    }
]
```

XML

```
<CORSConfiguration>
 <CORSRule>
   <AllowedOrigin>http://www.example.com</AllowedOrigin>
   <AllowedMethod>PUT</AllowedMethod>
   <AllowedMethod>POST</AllowedMethod>
   <AllowedMethod>DELETE</AllowedMethod>
   <AllowedHeader>*</AllowedHeader>
  <MaxAgeSeconds>3000</MaxAgeSeconds>
  <ExposeHeader>x-amz-server-side-encryption</
ExposeHeader>
  <ExposeHeader>x-amz-request-id</
ExposeHeader>
  <ExposeHeader>x-amz-id-2</ExposeHeader>
 </CORSRule>
</CORSConfiguration>
```

上述配置中的 CORSRule 元素包括以下可选元素：

- MaxAgeSeconds — 指定在 Amazon S3 针对特定资源的预检 OPTIONS 请求作出响应后，浏览器缓存该响应的时间（以秒为单位，在本示例中为 3000 秒）。通过缓存响应，在需要重复原始请求时，浏览器无需向 Amazon S3 发送预检请求。
- ExposeHeaders – 识别可让客户从应用程序 (例如，从 JavaScript x-amz-server-side-encryption 对象) 进行访问的响应标头 (在本示例中，为 x-amz-request-id、x-amz-id-2 和 XMLHttpRequest)。

# 配置跨源资源共享 (CORS)

跨源资源共享 (CORS) 定义了在一个域中加载的客户端 Web 应用程序与另一个域中的资源交互的方式。借助 CORS 支持，您可以使用 Amazon S3 构建各种富客户端 Web 应用程序，并选择性地允许跨源访问您的 Amazon S3 资源。

本节将向您介绍如何使用 Amazon S3 控制台、Amazon S3 REST API 和 Amazon SDK 来启用 CORS。要将您的存储桶配置为允许跨源请求，您可以将 CORS 配置添加到存储桶中。CORS 配置是一个定义规则的文档，这些规则标识可访问您的存储桶的源、每个源支持的操作（HTTP 方法）以及其他操作特定的信息。在 S3 控制台中，CORS 配置必须是 JSON 文档。

有关 JSON 和 XML 中的 CORS 配置示例，请参阅 CORS 配置的元素。

使用 S3 控制台

本节说明如何使用 Amazon S3 控制台向 S3 存储桶添加跨源资源共享（CORS）配置。

在存储桶上启用 CORS 时，访问控制列表（ACL）和其他访问权限策略仍适用。

> **Important**
>
> 在 S3 控制台中，CORS 配置必须是 JSON。有关 JSON 和 XML 中的 CORS 配置示例，请参阅 CORS 配置的元素。

将 CORS 配置添加到 S3 存储桶

1. 登录到Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在存储桶列表中，选择要为其创建存储桶策略的存储桶的名称。
4. 选择 Permissions (权限)。
5. 在 Cross-origin resource sharing（CORS）（跨源资源共享（CORS））部分中，请选择 Edit（编辑）。
6. 在 CORS configuration editor (CORS 配置编辑器) 文本框中，键入或复制并粘贴新的 CORS 配置，或者编辑现有配置。

   CORS 配置是一个 JSON 文件。您在编辑器中键入的文本必须是有效的 JSON。有关更多信息，请参阅 CORS 配置的元素。

7. 请选择保存更改。

> **Note**
>
> Amazon S3 在 CORS configuration editor（CORS 配置编辑器）标题旁边显示存储桶的 Amazon Resource Name（ARN）。有关 ARN 的更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon 资源名称（ARN）和 Amazon 服务命名空间。

使用 Amazon SDK

您可以使用 Amazon SDK 管理存储桶的跨源资源共享（CORS）。有关 CORS 的更多信息，请参阅使用跨源资源共享 (CORS)。

以下示例：

- 创建 CORS 配置并对存储桶设置该配置
- 通过添加规则来检索并修改配置
- 向存储桶添加修改过的配置
- 删除配置

Java

Example

Example

有关如何创建和测试有效示例的说明，请参阅《适用于 Java 的 Amazon SDK 开发人员指南》中的入门。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.BucketCrossOriginConfiguration;
import com.amazonaws.services.s3.model.CORSRule;
```

```
import java.io.IOException;
import java.util.ArrayList;
import java.util.Arrays;
import java.util.List;

public class CORS {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";

        // Create two CORS rules.
        List<CORSRule.AllowedMethods> rule1AM = new
 ArrayList<CORSRule.AllowedMethods>();
        rule1AM.add(CORSRule.AllowedMethods.PUT);
        rule1AM.add(CORSRule.AllowedMethods.POST);
        rule1AM.add(CORSRule.AllowedMethods.DELETE);
        CORSRule rule1 = new
 CORSRule().withId("CORSRule1").withAllowedMethods(rule1AM)
                .withAllowedOrigins(Arrays.asList("http://*.example.com"));

        List<CORSRule.AllowedMethods> rule2AM = new
 ArrayList<CORSRule.AllowedMethods>();
        rule2AM.add(CORSRule.AllowedMethods.GET);
        CORSRule rule2 = new
 CORSRule().withId("CORSRule2").withAllowedMethods(rule2AM)
                .withAllowedOrigins(Arrays.asList("*")).withMaxAgeSeconds(3000)
                .withExposedHeaders(Arrays.asList("x-amz-server-side-encryption"));

        List<CORSRule> rules = new ArrayList<CORSRule>();
        rules.add(rule1);
        rules.add(rule2);

        // Add the rules to a new CORS configuration.
        BucketCrossOriginConfiguration configuration = new
 BucketCrossOriginConfiguration();
        configuration.setRules(rules);

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();
```

```
            // Add the configuration to the bucket.
            s3Client.setBucketCrossOriginConfiguration(bucketName, configuration);

            // Retrieve and display the configuration.
            configuration = s3Client.getBucketCrossOriginConfiguration(bucketName);
            printCORSConfiguration(configuration);

            // Add another new rule.
            List<CORSRule.AllowedMethods> rule3AM = new
ArrayList<CORSRule.AllowedMethods>();
            rule3AM.add(CORSRule.AllowedMethods.HEAD);
            CORSRule rule3 = new
CORSRule().withId("CORSRule3").withAllowedMethods(rule3AM)
                    .withAllowedOrigins(Arrays.asList("http://www.example.com"));

            rules = configuration.getRules();
            rules.add(rule3);
            configuration.setRules(rules);
            s3Client.setBucketCrossOriginConfiguration(bucketName, configuration);

            // Verify that the new rule was added by checking the number of rules in
the
            // configuration.
            configuration = s3Client.getBucketCrossOriginConfiguration(bucketName);
            System.out.println("Expected # of rules = 3, found " +
configuration.getRules().size());

            // Delete the configuration.
            s3Client.deleteBucketCrossOriginConfiguration(bucketName);
            System.out.println("Removed CORS configuration.");

            // Retrieve and display the configuration to verify that it was
            // successfully deleted.
            configuration = s3Client.getBucketCrossOriginConfiguration(bucketName);
            printCORSConfiguration(configuration);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
```

```
    }

    private static void printCORSConfiguration(BucketCrossOriginConfiguration
 configuration) {
        if (configuration == null) {
            System.out.println("Configuration is null.");
        } else {
            System.out.println("Configuration has " +
 configuration.getRules().size() + " rules\n");

            for (CORSRule rule : configuration.getRules()) {
                System.out.println("Rule ID: " + rule.getId());
                System.out.println("MaxAgeSeconds: " + rule.getMaxAgeSeconds());
                System.out.println("AllowedMethod: " + rule.getAllowedMethods());
                System.out.println("AllowedOrigins: " + rule.getAllowedOrigins());
                System.out.println("AllowedHeaders: " + rule.getAllowedHeaders());
                System.out.println("ExposeHeader: " + rule.getExposedHeaders());
                System.out.println();
            }
        }
    }
}
```

.NET

Example

有关设置和运行代码示例的信息，请参阅《适用于 .NET 的 Amazon SDK 开发人员指南》中的适用于 .NET 的 Amazon SDK 入门。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class CORSTest
    {
        private const string bucketName = "*** bucket name ***";
        // Specify your bucket region (an example region is shown).
```

```
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            CORSConfigTestAsync().Wait();
        }
        private static async Task CORSConfigTestAsync()
        {
            try
            {
                // Create a new configuration request and add two rules
                CORSConfiguration configuration = new CORSConfiguration
                {
                    Rules = new System.Collections.Generic.List<CORSRule>
                        {
                          new CORSRule
                          {
                            Id = "CORSRule1",
                            AllowedMethods = new List<string> {"PUT", "POST",
 "DELETE"},
                            AllowedOrigins = new List<string> {"http://
*.example.com"}
                          },
                          new CORSRule
                          {
                            Id = "CORSRule2",
                            AllowedMethods = new List<string> {"GET"},
                            AllowedOrigins = new List<string> {"*"},
                            MaxAgeSeconds = 3000,
                            ExposeHeaders = new List<string> {"x-amz-server-side-
encryption"}
                          }
                        }
                };

                // Add the configuration to the bucket.
                await PutCORSConfigurationAsync(configuration);

                // Retrieve an existing configuration.
                configuration = await RetrieveCORSConfigurationAsync();
```

```
                // Add a new rule.
                configuration.Rules.Add(new CORSRule
                {
                    Id = "CORSRule3",
                    AllowedMethods = new List<string> { "HEAD" },
                    AllowedOrigins = new List<string> { "http://www.example.com" }
                });

                // Add the configuration to the bucket.
                await PutCORSConfigurationAsync(configuration);

                // Verify that there are now three rules.
                configuration = await RetrieveCORSConfigurationAsync();
                Console.WriteLine();
                Console.WriteLine("Expected # of rulest=3; found:{0}",
configuration.Rules.Count);
                Console.WriteLine();
                Console.WriteLine("Pause before configuration delete. To continue,
click Enter...");
                Console.ReadKey();

                // Delete the configuration.
                await DeleteCORSConfigurationAsync();

                // Retrieve a nonexistent configuration.
                configuration = await RetrieveCORSConfigurationAsync();
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
        }

        static async Task PutCORSConfigurationAsync(CORSConfiguration configuration)
        {

            PutCORSConfigurationRequest request = new PutCORSConfigurationRequest
            {
```

```
                BucketName = bucketName,
                Configuration = configuration
            };

            var response = await s3Client.PutCORSConfigurationAsync(request);
        }

        static async Task<CORSConfiguration> RetrieveCORSConfigurationAsync()
        {
            GetCORSConfigurationRequest request = new GetCORSConfigurationRequest
            {
                BucketName = bucketName

            };
            var response = await s3Client.GetCORSConfigurationAsync(request);
            var configuration = response.Configuration;
            PrintCORSRules(configuration);
            return configuration;
        }

        static async Task DeleteCORSConfigurationAsync()
        {
            DeleteCORSConfigurationRequest request = new
DeleteCORSConfigurationRequest
            {
                BucketName = bucketName
            };
            await s3Client.DeleteCORSConfigurationAsync(request);
        }

        static void PrintCORSRules(CORSConfiguration configuration)
        {
            Console.WriteLine();

            if (configuration == null)
            {
                Console.WriteLine("\nConfiguration is null");
                return;
            }

            Console.WriteLine("Configuration has {0} rules:",
configuration.Rules.Count);
            foreach (CORSRule rule in configuration.Rules)
            {
```

```
                Console.WriteLine("Rule ID: {0}", rule.Id);
                Console.WriteLine("MaxAgeSeconds: {0}", rule.MaxAgeSeconds);
                Console.WriteLine("AllowedMethod: {0}", string.Join(", ",
 rule.AllowedMethods.ToArray()));
                Console.WriteLine("AllowedOrigins: {0}", string.Join(", ",
 rule.AllowedOrigins.ToArray()));
                Console.WriteLine("AllowedHeaders: {0}", string.Join(", ",
 rule.AllowedHeaders.ToArray()));
                Console.WriteLine("ExposeHeader: {0}", string.Join(", ",
 rule.ExposeHeaders.ToArray()));
            }
        }
    }
}
```

使用 REST API

要对存储桶设置 CORS 配置，您可以使用 Amazon Web Services Management Console。如果您的应用程序需要它，您也可以直接发送 REST 请求。Amazon Simple Storage Service API 参考的下面几节描述了与 CORS 配置相关的 REST API 操作：

- PutBucketCors
- GetBucketCors
- DeleteBucketCors
- OPTIONS object

## 测试 CORS

要测试 CORS 配置，可以使用 OPTIONS 方法发送 CORS 预检请求，以便服务器在可以接受发送该请求的情况下做出响应。Amazon S3 收到预检请求后，S3 会为存储桶评估 CORS 配置，并使用第一个与传入请求匹配的 CORSRule 规则来启用跨源请求。要使规则实现匹配，必须满足以下条件：

- 向存储桶发出的 CORS 请求中的 Origin 标头必须与 CORS 配置的 AllowedOrigins 元素中的源相匹配。
- 在向存储桶发出的 CORS 请求的 Access-Control-Request-Method 中指定的 HTTP 方法，必须与在 CORS 配置的 AllowedMethods 元素中列出的一个或多个方法相匹配。
- 预检请求的 Access-Control-Request-Headers 标头中列出的标头必须与 CORS 配置的 AllowedHeaders 元素中的标头相匹配。

以下是 CORS 配置示例。要创建 CORS 配置，请参阅配置 CORS。有关 CORS 配置的更多示例，请参阅 CORS 配置的元素。

JSON

```
[
    {
        "AllowedHeaders": [
            "Authorization"
        ],
        "AllowedMethods": [
            "GET",
            "PUT",
            "POST",
            "DELETE"
        ],
        "AllowedOrigins": [
            "http://www.example1.com"
        ],
        "ExposeHeaders":  [
             "x-amz-meta-custom-header"
        ]

    }
]
```

要测试 CORS 配置，可以使用以下 CURL 命令发送预检 OPTIONS 检查。CURL 是一个命令行工具，可用于与 S3 进行交互。有关更多信息，请参阅 CURL。

```
curl -v -X OPTIONS \
 -H "Origin: http://www.example1.com" \
 -H "Access-Control-Request-Method: PUT" \
 -H "Access-Control-Request-Headers: Authorization" \
 -H "Access-Control-Expose-Headers: x-amz-meta-custom-header"\
    "http://bucket_name.s3.amazonaws.com/object_prefix_name"
```

在上面的示例中，`curl -v -x OPTIONS` 命令用于向 S3 发送预检请求，来查询 S3 是否支持从跨源 `http://www.example1.com` 发送对于对象的 PUT 请求。标头 `Access-Control-Request-Headers` 和 `Access-Control-Expose-Headers` 是可选的。

- 为响应预检 OPTIONS 请求中的 Access-Control-Request-Method 标头，如果请求的方法匹配，Amazon S3 会返回受支持方法的列表。
- 为响应预检 OPTIONS 请求中的 Access-Control-Request-Headers 标头，如果请求的标头匹配，Amazon S3 会返回受支持标头的列表。
- 为响应预检 OPTIONS 请求中的 Access-Control-Expose-Headers 标头，如果请求的标头与浏览器中运行的脚本可以访问的受支持标头匹配，Amazon S3 会返回受支持标头的列表。

> **Note**
>
> 发送预检请求时，如果不支持使用任何 CORS 请求标头，则不会返回任何响应 CORS 标头。

为响应此预检 OPTIONS 请求，您将收到 200 OK 响应。有关测试 CORS 时收到的常见错误代码以及解决 CORS 相关问题的更多信息，请参阅 CORS 问题排查。

```
< HTTP/1.1 200 OK
< Date: Fri, 12 Jul 2024 00:23:51 GMT
< Access-Control-Allow-Origin: http://www.example1.com
< Access-Control-Allow-Methods: GET, PUT, POST, DELETE
< Access-Control-Allow-Headers: Authorization
< Access-Control-Expose-Headers: x-amz-meta-custom-header
< Access-Control-Allow-Credentials: true
< Vary: Origin, Access-Control-Request-Headers, Access-Control-Request-Method
< Server: AmazonS3
< Content-Length: 0
```

## CORS 问题排查

以下主题有助于排查与 S3 相关的一些常见 CORS 问题。

主题

- 403 禁止错误：未为此存储桶启用 CORS
- 403 禁止错误：不支持此 CORS 请求
- 在 CORS 响应中找不到标头
- 有关 S3 代理集成的 CORS 的注意事项

## 403 禁止错误：未为此存储桶启用 CORS

当跨源请求发送到 Amazon S3 但未在 S3 存储桶上配置 CORS 时，会发生以下 403 Forbidden 错误。

错误：HTTP/1.1 403 禁止 CORS 响应：未为此存储桶启用 CORS。

CORS 配置是一个包含规则的文档或策略，这些规则标识可访问您的存储桶的源、每个源将支持的操作（HTTP 方法）以及其它操作特定的信息。请参阅如何使用 Amazon S3 控制台、Amazon SDK 和 REST API 在 S3 上配置 CORS。有关 CORS 的更多信息以及 CORS 配置示例，请参阅 CORS 的元素。

## 403 禁止错误：不支持此 CORS 请求

当 CORS 配置中的 CORS 规则与请求中的数据不匹配时，会收到以下 403 Forbidden 错误。

错误：HTTP/1.1 403 禁止 CORS 响应：不支持此 CORS 请求。

因此，出现此 403 Forbidden 错误的原因可能有多种：

- 不支持源。
- 不支持方法。
- 不支持请求的标头。

对于 Amazon S3 收到的每个请求，CORS 配置中必须具有与请求中的数据匹配的 CORS 规则。

不支持源

向存储桶发出的 CORS 请求中的 Origin 标头必须与 CORS 配置的 AllowedOrigins 元素中的源相匹配。AllowedOrigins 元素中的通配符 ("*") 将匹配所有 HTTP 方法。有关如何更新 AllowedOrigins 元素的更多信息，请参阅配置跨源资源共享（CORS）。

例如，如果 AllowedOrigins 元素中仅包含 http://www.example1.com 域，则从 http://www.example2.com 域发送的 CORS 请求将收到 403 Forbidden 错误。

以下示例显示 CORS 配置的一部分，它在 AllowedOrigins 元素中包含 http://www.example1.com 域。

```
"AllowedOrigins":[
   "http://www.example1.com"
```

```
]
```

要使从 http://www.example2.com 域发送的 CORS 请求获得成功，应将 http://www.example2.com 域包含在 CORS 配置的 AllowedOrigins 元素中。

```
"AllowedOrigins":[
   "http://www.example1.com"
   "http://www.example2.com"
]
```

不支持方法

在向存储桶发出的 CORS 请求的 Access-Control-Request-Method 中指定的 HTTP 方法，必须与在 CORS 配置的 AllowedMethods 元素中列出的一个或多个方法相匹配。AllowedMethods 中的通配符 ("*") 将匹配所有 HTTP 方法。有关如何更新 AllowedOrigins 元素的更多信息，请参阅配置跨源资源共享（CORS）。

在 CORS 配置中，您可以在 AllowedMethods 元素中指定以下方法：

- GET
- PUT
- POST
- DELETE
- HEAD

以下示例显示 CORS 配置的一部分，该配置在 AllowedMethods 元素中包含 GET 方法。只有包含 GET 方法的请求才会获得成功。

```
"AllowedMethods":[
   "GET"
]
```

如果在 CORS 请求中使用了 HTTP 方法（例如 PUT），或者该方法包含在对存储桶的预检 CORS 请求中但不存在于 CORS 配置中，则该请求将导致 403 Forbidden 错误。要支持此 CORS 请求或 CORS 预检请求，必须将 PUT 方法添加到 CORS 配置中。

```
"AllowedMethods":[
   "GET"
```

```
    "PUT"
]
```

不支持请求的标头

预检请求的 Access-Control-Request-Headers 标头中列出的标头必须与 CORS 配置的 AllowedHeaders 元素中的标头相匹配。有关可以在对 Amazon S3 的请求中使用的常见标头的列表，请参阅 Common Request Headers。有关如何更新 AllowedHeaders 元素的更多信息，请参阅配置跨源资源共享（CORS）。

以下示例显示 CORS 配置的一部分，该配置在 AllowedHeaders 元素中包含 Authorization 标头。只有对 Authorization 标头的请求才会获得成功。

```
"AllowedHeaders":  [
    "Authorization"
]
```

如果 CORS 请求中包含标头（例如 Content-MD5），但该标头不存在于 CORS 配置中，则该请求将导致 403 Forbidden 错误。要支持此 CORS 请求，必须将 Content-MD5 标头添加到 CORS 配置中。如果您要在 CORS 请求中同时将 Authorization 和 Content-MD5 标头传递到存储桶，请确认这两个标头都包含在 CORS 配置的 AllowedHeaders 元素中。

```
"AllowedHeaders":  [
    "Authorization"
    "Content-MD5"
]
```

## 在 CORS 响应中找不到标头

CORS 配置中的 ExposeHeaders 元素确定了您希望在浏览器中运行的脚本和应用程序可以访问哪些响应标头，以便响应 CORS 请求。

如果存储在 S3 存储桶中的对象具有用户定义的元数据（例如 x-amz-meta-custom-header）以及响应数据，则此自定义标头可能包含您要从客户端 JavaScript 代码访问的其它元数据或信息。但出于安全考虑，默认情况下，浏览器会阻止访问自定义标头。要支持客户端 JavaScript 访问自定义标头，需要在 CORS 配置中包含该标头。

在下面的示例中，x-amz-meta-custom-header1 标头包含在 ExposeHeaders 元素中。x-amz-meta-custom-header2 未包含在 ExposeHeaders 元素中，并且 CORS 配置中也缺少此标头。在响应中，仅返回 ExposeHeaders 元素中包含的值。如果请求在 Access-Control-Expose-

Headers 标头中包含了 x-amz-meta-custom-header2 标头，则响应仍会返回 200 OK。但是，只有允许的标头（例如 x-amz-meta-custom-header）才会返回并显示在响应中。

```
"ExposeHeaders":  [
    "x-amz-meta-custom-header1"
]
```

为确保所有标头都出现在响应中，请将所有允许的标头添加到 CORS 配置中的 ExposeHeaders 元素，如下所示。

```
"ExposeHeaders":  [
    "x-amz-meta-custom-header1",
    "x-amz-meta-custom-header2"
]
```

## 有关 S3 代理集成的 CORS 的注意事项

如果您遇到错误且已经检查了 S3 存储桶上的 CORS 配置，并且跨源请求已发送到 Amazon CloudFront 等代理，请尝试以下操作：

- 将设置配置为支持 HTTP 请求使用 OPTIONS 方法。
- 将代理配置为转发以下标头：Origin、Access-Control-Request-Headers 和 Access-Control-Request-Method。
- 将代理设置配置为在其缓存密钥中包含 origin 标头。

一些代理为 CORS 请求提供预定义的功能。例如，在 CloudFront 中，您可以配置一个策略，该策略包括的标头

可在源为 Amazon S3 存储桶时启用跨源资源共享（CORS）请求。

此策略包含以下设置：

- 源请求中包含的标头：

  Origin

  Access-Control-Request-Headers

  Access-Control-Request-Method
- 源请求中包含的 Cookie：无

- 源请求中包含的查询字符串：无

有关更多信息，请参阅《CloudFront 开发人员指南》中的使用策略来控制源请求和使用托管式源请求策略。

# 静态网站教程

以下教程或演练提供了完整的过程，旨在介绍如何创建和配置 Amazon S3 通用存储桶来实施静态网站托管和托管点播视频流。此类教程的目的是提供一般指导。这些教程适用于实验室类型的环境，使用了示例存储桶名称、用户名等。在未进行仔细审核并进行改进以满足组织环境的独特需求的情况下，这些过程不适合在您的生产环境中直接使用。

- Hosting on-demand streaming video with Amazon S3, Amazon CloudFront, and Amazon Route 53：可以将 Amazon S3 与 Amazon CloudFront 结合使用，以安全和可扩展的方式托管视频，供点播观看。在将视频打包成正确的格式之后，可以将其存储在服务器或 S3 通用存储桶中，然后在查看者请求视频时使用 CloudFront 提供视频。在本教程中，您将了解如何配置通用存储桶来托管点播视频流，使用 CloudFront 进行传输，并使用 Amazon Route 53 进行域名系统（DNS）和自定义域管理。CloudFront 从其缓存中提供视频，只有在尚未缓存的情况下才从通用存储桶中检索视频。这种缓存管理特征可以通过低延迟、高吞吐量和高传输速度加快向全球观众传送视频的速度。有关 CloudFront 缓存管理的更多信息，请参阅 Amazon CloudFront 开发人员指南中的优化缓存和可用性。
- 配置静态网站：可以配置一个通用存储桶，使其像网站一样运行。本教程将为您演练在 Amazon S3 上托管网站的步骤，包括创建存储桶、在 S3 控制台中启用静态网站托管、创建索引文档和创建错误文档。有关更多信息，请参阅使用 Amazon S3 托管静态网站。
- 使用注册到 Route 53 的自定义域配置静态网站：可以创建和配置一个通用存储桶来托管静态网站，并在 S3 上为网站（具有注册到 Amazon Route 53 的自定义域名）创建重定向。您使用 Route 53 来注册域，并定义要将域的互联网流量路由到何处。本教程介绍如何创建 Route 53 别名记录，来将域和子域的流量路由到包含 HTML 文件的通用存储桶。有关更多信息，请参阅《Amazon Route 53 开发人员指南》中的 Use your domain for a static website in an Amazon S3 bucket。完成本教程后，可以选择使用 CloudFront 来提高网站的性能。有关更多信息，请参阅使用 Amazon CloudFront 为网站提速。
- Deploying a static website to Amazon Amplify Hosting from an S3 general purpose bucket：我们建议您使用 Amazon Amplify Hosting 来托管存储在 S3 上的静态网站内容。Amplify Hosting 是一项完全托管式服务，可让您轻松地在由 Amazon CloudFront 提供支持的全球可用内容分发网络（CDN）上部署您的网站，无需大量设置即可实现安全的静态网站托管。借助 Amazon Amplify Hosting，您可以选择对象在通用存储桶中的位置，将内容部署到托管式 CDN，并为网站生成一个公有 HTTPS

URL 以供在任何地方访问。有关更多信息，请参阅《Amazon Amplify Hosting 用户指南》中的 Deploying a static website from S3 using the Amplify console。

## 教程：使用 Amazon S3、Amazon CloudFront 和 Amazon Route 53 托管点播流视频

您可以将 Amazon S3 与 Amazon CloudFront 结合使用托管视频，实现以安全和可扩展的方式进行点播观看。点播视频 (VOD) 流代表您的视频内容存储在服务器上，观看者能够随时观看。

CloudFront 是一项快速、高度安全和可编程内容传送网络 (CDN) 服务。CloudFront 可以通过 HTTPS 从全球所有 CloudFront 节点安全地交付您的内容。有关 CloudFront 的更多信息，请参阅 Amazon CloudFront 开发人员指南中的什么是 Amazon CloudFront？。

CloudFront 缓存减少了源服务器必须直接响应的请求数量。观看者（最终用户）请求您使用 CloudFront 提供的视频时，请求将路由到离观看者所在位置更近的附近边缘站点。CloudFront 从其缓存中提供视频，只有在尚未缓存的情况下才从 S3 存储桶中检索视频。这种缓存管理特征可以通过低延迟、高吞吐量和高传输速度加快向全球观众传送视频的速度。有关 CloudFront 缓存管理的更多信息，请参阅 Amazon CloudFront 开发人员指南中的优化缓存和可用性。

目标

在本教程中，您将配置 S3 存储桶以托管点播视频流，用 CloudFront 进行传输，并用 Amazon Route 53 进行域名系统（DNS）和自定义域管理。

主题


- 先决条件：用 Route 53 注册并配置自定义域
- 步骤 1：创建 S3 存储桶
- 步骤 2：将视频上传到 S3 存储桶
- 步骤 3：创建 CloudFront 源访问身份
- 步骤 4：创建 CloudFront 分配
- 步骤 5：通过 CloudFront 分配访问视频
- 步骤 6：配置您的 CloudFront 分配以使用自定义域名
- 步骤 7：用自定义域名通过 CloudFront 分配访问 S3 视频
- （可选）步骤 8：查看有关您的 CloudFront 分配接收的请求的数据
- 步骤 9：清除
- 后续步骤

## 先决条件：用 Route 53 注册并配置自定义域

开始本教程之前，您必须用 Route 53 注册和配置自定义域（例如，**example.com**），从而可将 CloudFront 分配配置为以后使用自定义域名。

如果没有自定义域名，并可通过 CloudFront 从类似于以下内容的 URL 中公开访问和托管您的 S3 视频：

```
https://CloudFront distribution domain name/Path to an S3 video
```

例如，**https://d111111abcdef8.cloudfront.net/sample.mp4**。

将您的 CloudFront 分配配置来使用配置了 Route 53 的自定义域名后，可以公开访问您的 S3 视频并通过 CloudFront 托管，URL 看起来类似于以下内容：

```
https://CloudFront distribution alternate domain name/Path to an S3 video
```

例如，**https://www.example.com/sample.mp4**。自定义域名对于观看者来说更简单、更直观。

若要注册自定义域，请参阅 Amazon Route 53 开发人员指南中的使用 Route 53 注册新域名。

用 Route 53 注册域名时，Route 53 会为您创建稍后在本教程中使用的托管区域。此托管区域用于存储有关如何为域路由流量的信息，例如路由到 Amazon EC2 实例或 CloudFront 分配。

您的域名注册、您的托管区域和域名收到的 DNS 查询会产生相关费用。有关更多信息，请参阅 Amazon Route 53 定价。

> **Note**
>
> 注册域名时，会立即产生费用，这是不可逆转的。您可以选择不自动续订域名，但要预先支付域名年费。有关更多信息，请参阅 Amazon Route 53 开发人员指南中的注册新域。

## 步骤 1：创建 S3 存储桶

创建存储桶来存储计划流式传输的原始视频。

创建存储桶

1. 登录到Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。

2. 在页面顶部的导航栏中，选择当前所显示 Amazon Web Services 区域的名称。接下来，选择要在其中创建存储桶的区域。

   > **Note**
   >
   > 要最大程度地减少延迟和成本以及满足法规要求，请选择一个靠近您的区域。在某一区域存储的对象将一直留在该区域，除非您特意将其转移到其他区域。有关 Amazon S3 Amazon Web Services 区域的列表，请参阅《Amazon Web Services 一般参考》中的 Amazon Web Services 服务 端点。

3. 在左侧导航窗格中，选择通用存储桶。
4. 选择创建存储桶。此时将打开创建存储桶页面。
5. 对于存储桶名称，输入您的存储桶的名称（例如 **`tutorial-bucket`**）。

   有关 Amazon S3 存储桶命名的更多信息，请参阅 通用存储桶命名规则。
6. 对于区域，选择要放置存储桶的 Amazon Web Services 区域。

   如果可能，您应选择最接近大多数观看者的区域位置。有关存储桶区域的更多信息，请参阅 通用存储桶概述。
7. 对于阻止此存储桶的公有访问设置，保留默认设置（阻止全部公有访问权限已启用）。

   即使启用阻止全部公有访问，观看者仍然可以通过 CloudFront 访问上传的视频。此特征使用 CloudFront 托管存储在 S3 中视频的主要优势。

   除非需要为您的用例关闭一个或多个设置，我们建议您启用所有设置。有关阻止公有访问的更多信息，请参阅 阻止对您的 Amazon S3 存储的公有访问。
8. 对于其余设置，保留默认值。

   （可选）如果要为您的特定用例配置其他存储桶设置，请参阅 创建通用存储桶。
9. 选择创建存储桶。

## 步骤 2：将视频上传到 S3 存储桶

以下过程介绍了如何使用控制台将视频文件上传到 S3 存储桶。如果将许多大型视频文件上传到 S3 时，您还可以使用 Amazon S3 Transfer Acceleration 配置快速安全的文件传输。Transfer Acceleration 可以加快视频上传到 S3 存储桶的速度，以便远距离传输较大的视频。有关更多信息，请参阅 使用 Amazon S3 Transfer Acceleration 配置快速、安全的文件传输。

将文件上传到存储桶

1. 登录到Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在通用存储桶列表中，选择您在步骤 1 中创建的存储桶名称（例如 **tutorial-bucket**），以便将您的文件上传到其中。
4. 在存储桶的对象 选项卡上，选择上传。
5. 在上传页面的文件和文件夹下，选择添加文件。
6. 选择要上传的文件，然后选择打开。

   例如，您可以上传名为`sample.mp4`的视频文件。
7. 选择上传。

## 步骤 3：创建 CloudFront 源访问身份

要限制从 S3 存储桶直接访问视频，请创建一个称为源访问身份（OAI）的特殊 CloudFront 用户。您会在本教程的后面部分中将 OAI 与您的分配关联。通过使用 OAI，您可以确保观看者无法绕过 CloudFront 并直接从 S3 存储桶获取视频。只有 CloudFront OAI 才能访问 S3 存储桶中的文件。有关更多信息，请参阅 Amazon CloudFront 开发人员指南中的使用 OAI 限制对 Amazon S3 内容的访问。

创建 CloudFront OAI

1. 登录 Amazon Web Services Management Console，并通过以下网址打开 CloudFront 控制台：https://console.amazonaws.cn/cloudfront/v4/home。
2. 在左侧导航窗格的安全部分，选择来源访问。
3. 在身份选项卡下，选择创建来源访问身份。
4. 输入名称（例如，**S3-OAI**) 作为新的源访问身份。
5. 选择创建。

## 步骤 4：创建 CloudFront 分配

要使用 CloudFront 在您的 S3 存储桶中提供和分发视频，您必须创建 CloudFront 分配。

分步

- 创建 CloudFront 分配。
- 查看存储桶策略

创建 CloudFront 分配。

1. 登录 Amazon Web Services Management Console，并通过以下网址打开 CloudFront 控制台：https://console.amazonaws.cn/cloudfront/v4/home。
2. 在左侧导航窗格中，选择分发。
3. 选择创建分发。
4. 在源部分中，针对源域，选择以您在步骤 1 中创建的 S3 存储桶的名称开头的 S3 源域名（例如，**tutorial-bucket**）。
5. 对于来源访问，请选择遗留访问身份。
6. 在源访问身份下，选择您在步骤 3 中创建的现有源访问身份（例如，**S3-OAI**）。
7. 在存储桶策略下，选择是，更新存储桶策略。
8. 对于默认缓存行为部分，在观看者协议策略下，选择重新定向 HTTP 至 HTTPS。

   当您选择此特征时，HTTP 请求会自动重定向到 HTTPS，保护您的网站并保护观看者的数据。
9. 对于默认缓存行为 部分中的其他设置，请保留默认值。

   （可选）您还可以控制文件在 CloudFront 转发另一请求到您的源之前留在 CloudFront 缓存中的时长。减少持续时间让您可提供动态内容。增加持续时间意味着您的观看者将获得更好的性能，因为直接从边缘缓存提供文件的可能性更大。较长的持续时间还会减少源的负载。有关更多信息，请参阅 Amazon CloudFront 开发人员指南中的管理内容在边缘缓存中保留的时长（过期时间）。
10. 对于其他部分，将其余设置保留设置为默认值。

    有关不同设置选项的更多信息，请参阅 Amazon CloudFront 开发人员指南中的您创建或更新分发时指定的值。
11. 在页面底部，选择创建分发。
12. 在 CloudFront 的常规选项卡中，在详细信息下，上次修改列中的分发值从部署中更改为上次修改分发的时间戳。该过程通常需要花费几分钟的时间。

查看存储桶策略

1. 登录到Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。

2. 在左侧导航窗格中，选择存储桶。
3. 在存储桶列表中，选择您之前用作 CloudFront 分配源的存储桶名称（例如，**tutorial-bucket**）。
4. 选择权限选项卡。
5. 在存储桶策略部分中，确认您看到类似于存储桶策略文本中以下内容的语句：

```
{
    "Version": "2008-10-17",
    "Id": "PolicyForCloudFrontPrivateContent",
    "Statement": [
        {
            "Sid": "1",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access
 Identity EH1HDMB1FH2TC"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::tutorial-bucket/*"
        }
    ]
}
```

这是您之前选择是，更新存储桶策略时 CloudFront 分配添加到存储桶策略的语句。

此存储桶策略更新表示您已成功配置 CloudFront 分配以限制对 S3 存储桶的访问。由于存在此限制，只能通过 CloudFront 分配访问存储桶中的对象。

## 步骤 5：通过 CloudFront 分配访问视频

现在，CloudFront 可以为存储在 S3 存储桶中的视频提供服务。要通过 CloudFront 访问您的视频，您必须将 CloudFront 分配域名与 S3 存储桶中视频路径组合在一起。

用 CloudFront 分配域名创建 S3 视频的 URL

1. 登录 Amazon Web Services Management Console，并通过以下网址打开 CloudFront 控制台：https://console.amazonaws.cn/cloudfront/v4/home。
2. 在左侧导航窗格中，选择分发。
3. 要获取分发域名，请执行以下操作：

a. 在源列中，通过查找其源名称来识别正确的 CloudFront 分配，该名称以步骤 1 中创建的 S3 存储桶开头（例如，**tutorial-bucket**）。

b. 从列表中找到分布后，扩大域名列，复制域名值来获取您的 CloudFront 分配。

4. 在新浏览器选项卡中，粘贴您之前复制的分发域名。
5. 返回到上一个浏览器选项卡，然后通过以下网址打开 S3 控制台：https://console.aws.amazon.com/s3/。
6. 在左侧导航窗格中，选择存储桶。
7. 在存储桶列表中，选择您在步骤 1 中创建的存储桶名称（例如，**tutorial-bucket**）。
8. 在对象列表中，选择您在步骤 2 中上传的视频名称（例如，`sample.mp4`）。
9. 在对象详细信息页面上的对象概述部分中，复制密钥值。此值是指向 S3 存储桶中上传视频对象的路径。
10. 返回您之前粘贴分发域名的浏览器选项卡，在分发域名之后输入正斜杠 (**/**)，然后粘贴您之前复制的视频的路径（例如，`sample.mp4`）。

    现在，您的 S3 视频可以公开访问，并通过 CloudFront 托管在类似于以下的 URL 中：

    ```
    https://CloudFront distribution domain name/Path to the S3 video
    ```

    使用适当的值替换 *CloudFront ####*和 *S3 #####*。示例 URL 为 **https://d111111abcdef8.cloudfront.net/sample.mp4**

## 步骤 6：配置您的 CloudFront 分配以使用自定义域名

要使用自己的域名而非 URL 中的 CloudFront 域名来访问 S3 视频，您必须在 CloudFront 分配中添加备用域名。

分步

- 请求 SSL 证书
- 将备用域名添加到您的 CloudFront 分配。
- 创建 DNS 记录，将备用域名的流量路由到您的 CloudFront 分配的域名
- 检查是否为您的分发启用了 IPv6，并根据需要创建另一个 DNS 记录

### 请求 SSL 证书

要允许观看者在视频流的 URL 中使用 HTTPS 和自定义域名，请使用 Amazon Certificate Manager (ACM) 以请求安全套接字层 (SSL) 证书。SSL 证书建立了指向网站的加密网络连接。

1. 登录到 Amazon Web Services Management Console 并通过 https://console.aws.amazon.com/acm/ 打开 ACM 控制台。
2. 如果显示介绍页面，请在设置证书中，选择开始。
3. 在请求证书页面上，选择请求公有证书，然后选择请求证书。
4. 在添加域名页面上，键入您要使用 SSL/TLS 证书保护的站点的完全限定域名 (FQDN)。使用星号 (*) 创建通配符证书保护同一域中的多个站点名称。具体来说，在本教程中，键入 ***** 和您在先决条件中配置的自定义域名。例如，输入 ***.example.com**，然后选择下一步。

   有关更多信息，请参阅 Amazon Certificate Manager 用户指南中的请求 ACM 公有证书（控制台）。
5. 在选择验证方法页面上，选择 DNS 验证。然后选择下一步。

   如果您可以编辑 DNS 配置，建议使用 DNS 域验证而不是电子邮件验证。相对于电子邮件验证，DNS 验证有多种优势。有关更多信息，请参阅 Amazon Certificate Manager 用户指南中的选项 1：DNS 验证。
6. （可选）在添加标签页面上，您可以选择用元数据标记证书。
7. 选择审核。
8. 在审核页面上，验证域名和验证方法下的信息都正确无误。然后，选择确认和请求。

   验证页面显示正在处理您的请求，并且正在验证证书域。等待验证的证书处于等待验证状态。
9. 在验证页面上，选择自定义域名左侧的向下箭头，然后选择在 Route 53 中创建记录以通过 DNS 验证您的域所有权。

   这将添加由 Amazon Certificate Manager 提供的 CNAME 记录到您的 DNS 配置。
10. 在在 Route 53 中创建记录对话框中，选择创建。

    验证页面应在底部显示成功状态通知。
11. 选择继续查看证书列表页。

    新证书的状态将在 30 分钟内从等待验证更改为已颁发。

将备用域名添加到您的 CloudFront 分配。

1. 登录 Amazon Web Services Management Console，并通过以下网址打开 CloudFront 控制台：https://console.amazonaws.cn/cloudfront/v4/home。
2. 在左侧导航窗格中，选择分发。
3. 为您在步骤 4 中创建的分发选择 ID。
4. 在常规选项卡，转到设置部分，然后选择编辑。
5. 在编辑设置页面上，对于备用域名（CNAME）- 可选，选择添加项目以添加要在此 CloudFront 分配提供的 S3 视频 URL 中使用的自定义域名。

   例如，在本教程中，如果您要路由子域，如 `www.example.com`，请输入带域名 (`example.com`) 的子域名 (`www`)。具体来说，输入 **`www.example.com`**。

   > **Note**
   >
   > 您添加的备用域名（CNAME）必须包含您之前附加到 CloudFront 分配的 SSL 证书。

6. 对于自定义 SSL 证书 - 可选，选择您在之前请求的 SSL 证书（例如，**`*.example.com`**）。

   > **Note**
   >
   > 如果在请求后没有立即看到 SSL 证书，则可以等待 30 分钟，然后刷新列表，直到 SSL 证书可供您选择。

7. 对于其余设置，保留默认值。选择 Save changes（保存更改）。
8. 在分发的常规选项卡中，请等待上次修改的值从部署中更改为上次修改分发的时间戳。

创建 DNS 记录，将备用域名的流量路由到您的 CloudFront 分配的域名

1. 登录 Amazon Web Services Management Console，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在左侧导航窗格中，选择托管区域。
3. 在托管区域页面上，选择 Route 53 在先决条件中为您创建的托管区域名称（例如，**`example.com`**）。
4. 选择创建记录，然后使用快速创建记录方法。
5. 对于记录名称，请保持记录名称的值与您在之前添加的 CloudFront 分配的备用域名相同。

在本教程中，要将流量路由到子域，如 `www.example.com`，请输入不带域名的子域名。例如，在您的自定义域名之前仅输入 **`www`** 文本字段。

6. 在记录类型中，选择 A – 将流量路由到 IPv4 地址和某些 Amazon 资源。
7. 对于值，选择别名切换以启用别名资源。
8. 在将流量路由至下，从下拉列表中选择别名到 CloudFront 分配。
9. 在选择分发搜索框中，选择您在步骤 4 中创建的 CloudFront 分配的域名。

   要查找您的 CloudFront 分配域名，请执行以下操作：

   a. 在新浏览器选项卡中，登录到 Amazon Web Services Management Console 并通过 https://console.amazonaws.cn/cloudfront/v3/home 打开 CloudFront 控制台。
   b. 在左侧导航窗格中，选择分发。
   c. 在源列中，通过查找其源名称来识别正确的 CloudFront 分配，该名称以步骤 1 中创建的 S3 存储桶开头（例如，**`tutorial-bucket`**）。
   d. 从列表中找到分发后，扩大域名列，查找域名来获取您的 CloudFront 分配。
10. 在 Route 53 控制台中的创建记录页面上，对于其余设置，请保留默认值。
11. 选择创建记录。

检查是否为您的分发启用了 IPv6，并根据需要创建另一个 DNS 记录

如果为您的分发启用了 IPv6，则必须创建另一个 DNS 记录。

1. 要检查是否为分发启用了 IPv6，请执行以下操作：

   a. 登录 Amazon Web Services Management Console，并通过以下网址打开 CloudFront 控制台：https://console.amazonaws.cn/cloudfront/v4/home。
   b. 在左侧导航窗格中，选择分发。
   c. 选择您在步骤 4 中创建的 CloudFront 分配的 ID。
   d. 在常规选项卡上，在设置下，请检查是否启用 IPv6。

      如果为您的分发启用了 IPv6，则必须创建另一个 DNS 记录。
2. 如果为分发启用了 IPv6，请执行以下操作来创建 DNS 记录：

   a. 登录 Amazon Web Services Management Console，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。

b. 在左侧导航窗格中，选择托管区域。

c. 在托管区域页面上，选择 Route 53 在先决条件中为您创建的托管区域名称（例如，**example.com**）。

d. 选择创建记录，然后使用快速创建记录方法。

e. 对于记录名称，在自定义域名之前的文本字段中，输入您在之前创建 IPv4 DNS 记录时键入的相同值。例如，在本教程中，要将流量路由到子域 `www.example.com`，请仅输入 **www**。

f. 对于记录类型，选择 AAAA-将流量路由到 IPv6 地址和 Amazon 一些资源。

g. 对于值，选择别名切换以启用别名资源。

h. 在将流量路由至下，从下拉列表中选择别名到 CloudFront 分配。

i. 在选择分发搜索框中，选择您在步骤 4 中创建的 CloudFront 分配的域名。

j. 对于其余设置，保留默认值。

k. 选择创建记录。

## 步骤 7：用自定义域名通过 CloudFront 分配访问 S3 视频

要用自定义 URL 访问 S3 视频，您必须将备用域名与 S3 存储桶中视频路径结合起来。

创建自定义 URL 通过 CloudFront 分配访问 S3 视频

1. 登录 Amazon Web Services Management Console，并通过以下网址打开 CloudFront 控制台：https://console.amazonaws.cn/cloudfront/v4/home。
2. 在左侧导航窗格中，选择分发。
3. 要获取您的 CloudFront 分配的备用域名，请执行以下操作：

   a. 在源列中，通过在步骤 1 中创建的 S3 存储桶名称查找源名称来识别正确的 CloudFront 分配（例如，**tutorial-bucket**）。

   b. 从列表中找到分发后，扩大备用域名列，复制 CloudFront 分配的备用域名值。
4. 在新的浏览器选项卡中，粘贴 CloudFront 分配的备用域名。
5. 返回到上一个浏览器选项卡，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
6. 查找步骤 5 中解释的 S3 视频的路径。
7. 返回到之前粘贴备用域名的浏览器选项卡，键入正斜杠 (**/**)，然后粘贴 S3 视频的路径（例如，`sample.mp4`）。

现在，您的 S3 视频可以公开访问，并可通过 CloudFront 从类似于以下的自定义 URL 中托管：

```
https://CloudFront distribution alternate domain name/Path to the S3 video
```

使用适当的值替换 *CloudFront ######*和 *S3 #####*。示例 URL 为 **https://www.example.com/sample.mp4**。

## （可选）步骤 8：查看有关您的 CloudFront 分配接收的请求的数据

查看有关您的 CloudFront 分配接收的请求数据

1. 登录 Amazon Web Services Management Console，并通过以下网址打开 CloudFront 控制台：https://console.amazonaws.cn/cloudfront/v4/home。
2. 在左侧窗格中，在报告和分析中，从控制台中选择报告，范围从缓存统计数据、常见对象、顶级推荐人、使用和观看者。

   您可以筛选每个报告仪表板。有关更多信息，请参阅 Amazon CloudFront 开发人员指南中的控制台中的 CloudFront 报告。
3. 要筛选数据，请选择您在步骤 4 中创建的 CloudFront 分配的 ID。

## 步骤 9：清除

如果您仅使用 CloudFront 和 Route 53 托管 S3 串流视频作为学习练习，请删除您分派的 Amazon 资源，使其不再产生费用。

> **Note**
>
> 注册域名时，会立即产生费用，这是不可逆转的。您可以选择不自动续订域名，但要预先支付域名年费。有关更多信息，请参阅 Amazon Route 53 开发人员指南中的注册新域。

分步

- 删除 CloudFront 分配
- 删除 DNS 记录
- 删除您的自定义域公有托管区域

- 从 Route 53 中删除自定义域名
- 删除 S3 源存储桶中的原始视频
- 删除 S3 源存储桶

删除 CloudFront 分配

1. 登录 Amazon Web Services Management Console，并通过以下网址打开 CloudFront 控制台：https://console.amazonaws.cn/cloudfront/v4/home。
2. 在左侧导航窗格中，选择分发。
3. 在源列中，通过在步骤 1 中创建的 S3 存储桶名称查找以其开头的源名称，识别正确的 CloudFront 分配（例如，**`tutorial-bucket`**）。
4. 要删除 CloudFront 分配，必须先将其禁用。
   - 如果状态列的值为已启用，上次修改的值是上次修改分发的时间戳，请继续禁用分发，然后再删除它。
   - 如果状态的值为已启用，并且上次修改的值为部署中，请等待状态的值更改为上次修改分发的时间戳。然后继续禁用分发，再删除它。
5. 要禁用 CloudFront 分配，请执行以下操作：
   a. 在分发列表中，选中要删除分发的 ID 旁边的复选框。
   b. 要禁用分发，选择禁用，然后选择禁用确认。

      如果禁用的分发包含一个相关的备用域名，则 CloudFront 会停止接受该域名（例如，`www.example.com`）的流量，即便另一个分发有一个包含通配符 (`*`) 且匹配同样域的备用域名（例如，`*.example.com`）。
   c. 状态的值立即变为禁用。等到上次修改的值从部署中变为上次修改分发的时间戳。

      由于 CloudFront 必须将此更改传播到所有边缘站点，所以可能需要几分钟时间才能完成更新，并且删除选项可供您删除分发。
6. 要删除禁用的分发，请执行以下操作：
   a. 选中要删除分发的 ID 旁边的复选框。
   b. 选择删除，然后选择删除以确认。

### 删除 DNS 记录

如果要删除域的公有托管区域（包括 DNS 记录），请参阅 Amazon Route 53 开发人员指南中的 删除您的自定义域公有托管区域。如果您只想删除在步骤 6 中创建的 DNS 记录，执行以下操作：

1. 登录 Amazon Web Services Management Console，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在左侧导航窗格中，选择托管区域。
3. 在托管区域页面上，选择 Route 53 在先决条件中为您创建的托管区域名称（例如，**`example.com`**）。
4. 在记录列表中，选择要删除的记录旁边的复选框（在步骤 6 中创建的记录）。

   > **Note**
   >
   > 您不能删除类型值为 NS或 SOA 的记录。

5. 选择删除记录。
6. 要确认删除，请选择删除。

   对记录的更改需要一定时间才会传播到 Route 53 DNS 服务器。目前，验证更改是否已传播的唯一方式是使用 GetChange API 操作。更改通常在 60 秒内传播到所有 Route 53 服务器。

### 删除您的自定义域公有托管区域

> **Warning**
>
> 如果您希望保留域注册，但停止将互联网流量路由到您的网站或 Web 应用程序，建议您删除托管区域（如前一节所述）中的记录，而不是删除托管区域。
> 如果删除托管区域，其他人可以劫持域并使用您的域名将流量路由到他们自己的资源。
> 此外，如果您删除托管区域，则无法取消删除它。您必须创建新的托管区域并更新域注册的名称服务器，这最多需要 48 个小时生效。
> 如果您想要使域在互联网上不可用，可以将 DNS 服务转移到免费的 DNS 服务，然后删除 Route 53 托管区域。这可防止以后的 DNS 查询可能被错误路由。

1. 如果已经用 Route 53 注册域，请参阅 Amazon Route 53 开发人员指南中的为域添加或更改名称服务器和粘附记录，了解有关将 Route 53 名称服务器替换为新 DNS 服务的名称服务器的信息。
2. 如果此域已向其他注册商注册，请使用注册商提供的方法更改此域的名称服务器。

> **Note**
>
> 如果要删除子域 (www.example.com) 的托管区域，则不需要更改域 (example.com) 的名称服务器。

1. 登录 Amazon Web Services Management Console，并通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在左侧导航窗格中，选择托管区域。
3. 在托管区域页面上，选择您要删除的托管区域所对应的行。
4. 在托管区域的记录选项卡上，请确认您要删除的托管区域仅包含 NS 和 SOA 记录。

   如果它包含其他记录，请先将其删除。

   如果您为子域的托管区域创建了任何 NS 记录，请也删除此类记录。
5. 在托管区的 DNSSEC 签署选项卡上，禁用 DNSSEC 签名（如果启用）。有关更多信息，请参阅 Amazon Route 53 开发人员指南中的禁用 DNSSEC 签名。
6. 在托管区域的详细信息页面顶部，选择删除区域。
7. 若要确认删除，请输入 **delete**，然后选择删除。

从 Route 53 中删除自定义域名

对于大多数顶级域 (TLD)，可在不需要域时删除域注册。如果在注册的计划到期时间之前从 Route 53 删除域名注册，Amazon 将不退还注册费。有关更多信息，请参阅 Amazon Route 53 开发人员指南中的删除域名注册。

> **Important**
>
> 如果您想在 Amazon Web Services 账户 之间转移域或将域转移到另一个注册商，请不要删除域并期望立即重新注册。相反，请参阅 Amazon Route 53 开发人员指南中的适用文档：
>
> - 将域转移到其他 Amazon Web Services 账户
> - 将域从 Amazon Route 53 转移到另一注册商

删除 S3 源存储桶中的原始视频

1. 登录到Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 在存储桶列表中，选择您在步骤 2 中将视频上传到其中的存储桶名称（例如，**tutorial-bucket**）。
4. 在对象选项卡上，选中要删除的对象名称左侧的复选框（例如，`sample.mp4`）。
5. 选择删除。
6. 在永久删除对象？下方，输入 **permanently delete** 以确认您要删除此对象。
7. 选择删除对象。

删除 S3 源存储桶

1. 登录到Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 在存储桶列表中，选择您在步骤 1 中创建的存储桶名称旁边的选项按钮（例如，**tutorial-bucket**）。
4. 选择删除。
5. 在删除存储桶页面上，通过在文本字段中输入存储桶名称来确认要删除存储桶，然后选择删除存储桶。

## 后续步骤

完成本教程后，您可以进一步探索以下相关使用案例：

- 将 S3 视频转换为特定电视或连接设备所需的流媒体格式，然后再使用 CloudFront 分配托管这些视频。

  要使用 Amazon S3 批量操作、Amazon Lambda 和 AWS Elemental MediaConvert 将视频集批量转码为各种输出媒体格式，请参阅教程：使用 S3 批量操作对视频进行批量转码。
- 使用 CloudFront 和 Route 53 托管存储在 S3 中的其他对象，如图像、音频、动态图形、样式表、HTML、JavaScript、反应应用等。

有关示例，请参阅 教程：使用注册到 Route 53 的自定义域配置静态网站 和 使用 Amazon CloudFront 为网站提速。

- 使用 Amazon S3 Transfer Acceleration 配置快速安全的文件传输。Transfer Acceleration 可以加快视频上传到 S3 存储桶的速度，以便远距离传输较大的视频。Transfer Acceleration 通过 CloudFront 全球分布的边缘站点和 Amazon 骨干网络路由流量，提高传输性能。它还利用网络协议优化。有关更多信息，请参阅 使用 Amazon S3 Transfer Acceleration 配置快速、安全的文件传输。

## 教程：在 Amazon S3 上配置静态网站

> **Important**
>
> Amazon S3 现在将具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）作为 Amazon S3 中每个存储桶的基本加密级别。从 2023 年 1 月 5 日起，上传到 Amazon S3 的所有新对象都将自动加密，不会产生额外费用，也不会影响性能。S3 存储桶默认加密配置和上传的新对象的自动加密状态可在 Amazon CloudTrail 日志、S3 清单、S3 Storage Lens 存储统计管理工具、Amazon S3 控制台中获得，并可用作 Amazon Command Line Interface 和 Amazon SDK 中的附加 Amazon S3 API 响应标头。有关更多信息，请参阅默认加密常见问题解答。

您可以配置 Amazon S3 存储桶，使其功能与网站相似。本示例向您演练了在 Amazon S3 上托管网站的步骤。

> **Important**
>
> 以下教程需要禁用“屏蔽公共访问权限”。我们建议将“屏蔽公共访问权限”保持为启用状态。如果要将所有四个“屏蔽公共访问权限”设置保持为启用状态并托管静态网站，则可以使用 Amazon CloudFront 来源访问控制（OAC）。Amazon CloudFront 提供了设置安全静态网站所需的功能。Amazon S3 静态网站仅支持 HTTP 端点。Amazon CloudFront 使用 Amazon S3 的持久存储，同时提供额外的安全标头，如 HTTPS。HTTPS 通过加密正常 HTTP 请求并防范常见的网络攻击来增强安全性。有关更多信息，请参阅《Amazon CloudFront 开发人员指南》中的安全静态网站入门。

主题

- 步骤 1：创建存储桶
- 步骤 2：启用静态网站托管

- 步骤 3：编辑屏蔽公共访问权限设置
- 步骤 4：添加可使您的存储桶内容公开可用的存储桶策略
- 步骤 5：配置索引文档
- 步骤 6：配置错误文档
- 步骤 7：测试您的网站端点
- 步骤 8：清除


## 步骤 1：创建存储桶

以下说明概述了如何创建存储桶以用于网站托管。有关创建存储桶的详细分步说明，请参阅创建通用存储桶。

创建存储桶

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 选择 Create bucket（创建存储桶）。
3. 输入 Bucket name（存储桶名称）（例如 **`example.com`**）。
4. 请选择要在其中创建存储桶的区域。

   请选择一个在地理上靠近您的区域可最大程度地减少延迟和成本，或满足法规要求。您选择的区域决定了您的 Amazon S3 网站端点。有关更多信息，请参阅 网站端点。
5. 要接受默认设置并创建存储桶，请选择 Create（创建）。

## 步骤 2：启用静态网站托管

创建存储桶后，您可以为存储桶启用静态网站托管。您可以创建新存储桶或使用现有存储桶。

启用静态网站托管

1. 登录到Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在存储桶列表中，选择要为其启用静态网站托管的存储桶的名称。
4. 选择属性。

5. 在静态网站托管下，请选择编辑。
6. 请选择使用此存储桶托管网站。
7. 在静态网站托管下，请选择启用。
8. 在 Index document (索引文档) 中，输入索引文档的文件名，通常为 `index.html`。

   索引文档名称区分大小写，并且必须与您计划上传到 S3 存储桶的 HTML 索引文档的文件名完全匹配。当您为网站托管配置存储桶时，您必须指定索引文档。当对根域或任何子文件夹发出请求时，Amazon S3 将返回此索引文档。有关更多信息，请参阅 配置索引文档。
9. 要为 4XX 类错误提供您自己的自定义错误文档，请在错误文档中输入自定义错误文档文件名。

   错误文档名称区分大小写，并且必须与您计划上传到 S3 存储桶的 HTML 错误文档的文件名完全匹配。如果未指定自定义错误文档并发生错误，Amazon S3 返回默认 HTML 错误文档。有关更多信息，请参阅 配置自定义错误文档。
10. （可选）如果要指定高级重定向规则，请在 Redirection rules（重定向规则）中，输入 JSON 来描述规则。

    例如，您可以根据请求中的特定对象键名或前缀按条件路由请求。有关更多信息，请参阅 配置重新导向规则以使用高级条件重新导向。
11. 选择 Save changes（保存更改）。

    Amazon S3 为您的存储桶启用静态网站托管。在页面底部的静态网站托管下，您可以看到存储桶的网站端点。
12. 在静态网站托管下，记下端点。

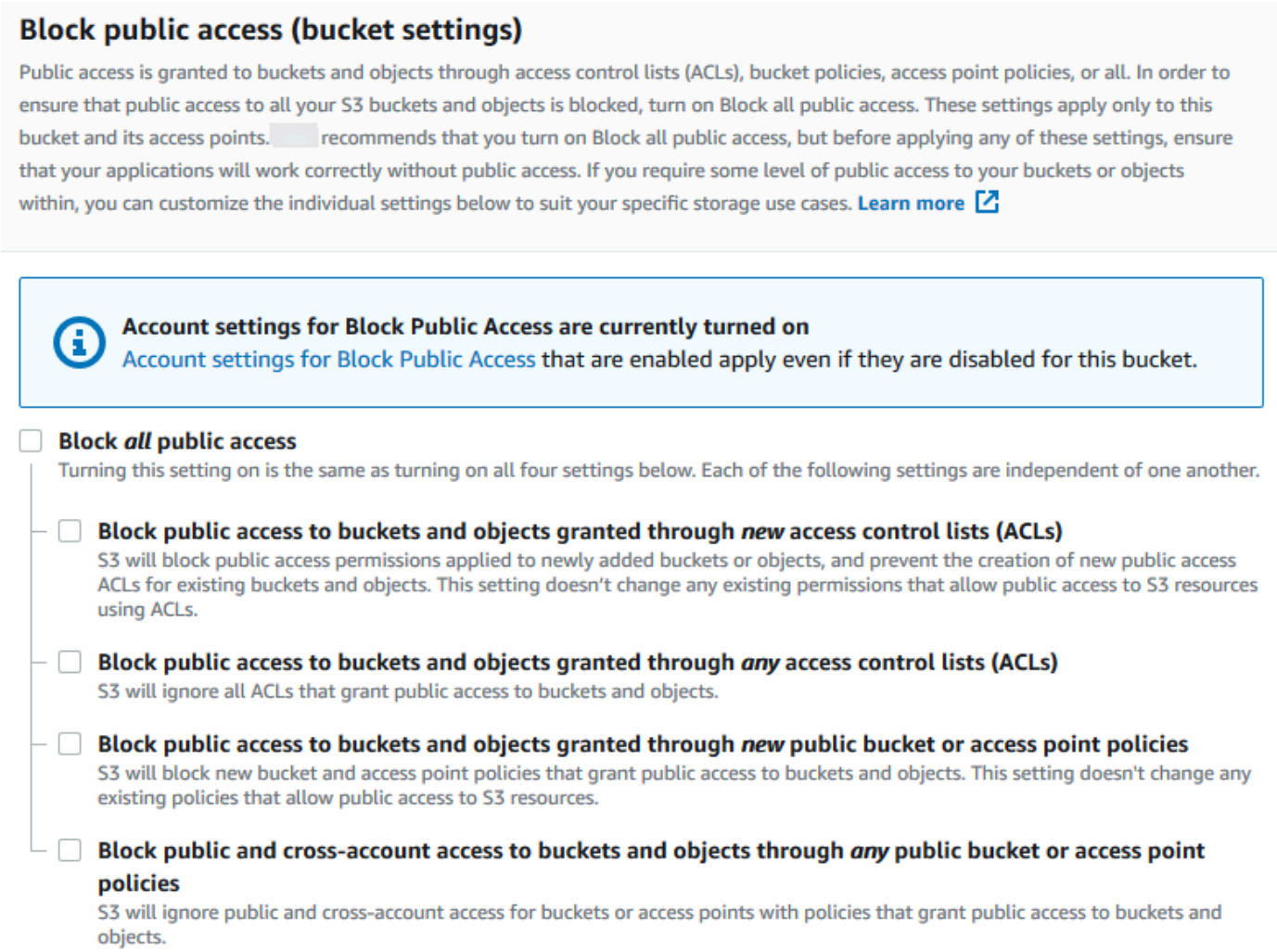
    端点是存储桶的 Amazon S3 网站端点。将存储桶配置为静态网站后，您可以使用此端点来测试您的网站。

## 步骤 3：编辑屏蔽公共访问权限设置

默认情况下，Amazon S3 阻止对您的账户和存储桶的公有访问权限。如果要使用存储桶托管静态网站，您可以使用以下步骤编辑您的屏蔽公共访问权限设置。

> **Warning**
>
> 在完成这些步骤之前，请查看阻止对您的 Amazon S3 存储的公有访问，来确保您了解并接受支持公共访问权限所涉及的风险。当您关闭屏蔽公共访问权限设置以使您的存储桶变为公有时，Internet 上的任何人都可以访问您的存储桶。我们建议您阻止对存储桶的所有公有访问。

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 请选择已配置为静态网站的存储桶的名称。
3. 选择权限。
4. 在屏蔽公共访问权限（存储桶设置）下，请选择编辑。
5. 清除阻止所有公有访问，然后选择保存更改。



Amazon S3 关闭了存储桶的屏蔽公共访问权限设置。要创建公有静态网站，可能还必须为您的账户配置屏蔽公共访问权限设置，然后再添加存储桶策略。如果当前已开启账户的屏蔽公共访问权限设置，您将在屏蔽公共访问权限（存储桶设置）下看到一条备注。

## 步骤 4：添加可使您的存储桶内容公开可用的存储桶策略

在编辑 S3 屏蔽公共访问权限设置后，您可以添加存储桶策略以授予对存储桶的公有读取访问权限。当您授予公有读取访问权限时，Internet 上的任何人都可以访问您的存储桶。

> **Important**
>
> 下面的策略仅供举例说明，仍允许完全访问您存储桶的内容。在继续执行此步骤之前，请查看如何保护 Amazon S3 存储桶中的文件？，以确保您了解保护 S3 存储桶中文件的最佳实践以及授予公有访问权限所涉及的风险。

1. 在存储桶 下，请选择存储桶的名称。
2. 选择权限。
3. 在存储桶策略下，请选择编辑。
4. 要授予对网站的公有读取访问权限，请复制以下存储桶策略，将其粘贴到存储桶策略编辑器中。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicReadGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::Bucket-Name/*"
            ]
        }
    ]
}
```

5. 将 `Resource` 更新为您的存储桶名称。

在上述示例存储桶策略中，*Bucket-Name* 是存储桶名称的占位符。要将此存储桶策略用于您自己的存储桶，您必须更新此名称以匹配您的存储桶名称。

6. 选择保存更改。

   此时将显示一条消息，指示存储桶策略已成功添加。

   如果您看到显示 Policy has invalid resource 的错误，请确认存储桶策略中的存储桶名称与您的存储桶名称匹配。有关添加存储桶策略的信息，请参阅如何添加 S3 存储桶策略？

   如果您收到错误消息且无法保存存储桶策略，请检查您的账户和存储桶的屏蔽公共访问权限设置以确认您允许对存储桶进行公有访问。

## 步骤 5：配置索引文档

当您为存储桶启用静态网站托管时，您可以输入索引文档的名称（例如，**index.html**）。为存储桶启用静态网站托管后，您可以将具有此索引文档名称的 HTML 文件上传到存储桶。

配置索引文档

1. 创建 index.html 文件。

   如果您没有 index.html 文件，则可以使用以下 HTML 创建一个：

```
<html xmlns="http://www.w3.org/1999/xhtml" >
<head>
    <title>My Website Home Page</title>
</head>
<body>
  <h1>Welcome to my website</h1>
  <p>Now hosted on Amazon S3!</p>
</body>
</html>
```

2. 将索引文件保存在本地。

   索引文档文件名必须与您在静态网站托管对话框中输入的索引文档名称完全匹配。索引文档名称区分大小写。例如，如果在静态网站托管对话框中为索引文档名称输入 index.html，则索引文档文件名也必须是 index.html，而不是 Index.html。

3. 登录到Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
4. 在左侧导航窗格中，选择通用存储桶。
5. 在存储桶列表中，选择要用于托管静态网站的存储桶的名称。
6. 为您的存储桶启用静态网站托管，并输入索引文档的确切名称（例如 `index.html`）。有关更多信息，请参阅 启用网站托管。

   启用静态网站托管后，继续执行步骤 6。
7. 要将索引文档上传到存储桶，请执行以下操作之一：

   - 将索引文件拖放到控制台存储桶列表中。
   - 选择上传，然后按照提示选择并上传索引文件。

   如需分步指导，请参阅 上传对象。
8. （可选）将其他网站内容上传到您的存储桶。

## 步骤 6：配置错误文档

当您为存储桶启用静态网站托管时，请输入错误文档的名称（例如，**`404.html`**）。为存储桶启用静态网站托管后，您可以将具有此错误文档名称的 HTML 文件上传到存储桶。

要配置错误文档

1. 创建错误文档，例如 `404.html`。
2. 将错误文档文件保存在本地。

   错误文档名称区分大小写，必须与启用静态网站托管时输入的名称完全匹配。例如，如果在静态网站托管对话框中为错误文档名称输入 `404.html`，则错误文档文件名也必须是 `404.html`。
3. 登录到Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
4. 在左侧导航窗格中，选择通用存储桶。
5. 在存储桶列表中，选择要用于托管静态网站的存储桶的名称。
6. 为您的存储桶启用静态网站托管，并输入错误文档的确切名称（例如 `404.html`）。有关更多信息，请参阅启用网站托管 和配置自定义错误文档。

   启用静态网站托管后，继续执行步骤 6。

7. 要将错误文档上传到存储桶，请执行以下操作之一：

   - 将错误文档文件拖放到控制台存储桶列表中。
   - 选择上传，然后按照提示选择并上传索引文件。

   如需分步指导，请参阅 上传对象。

## 步骤 7：测试您的网站端点

为存储桶配置静态网站托管后，您可以测试您的网站端点。

> **Note**
>
> Amazon S3 不支持对该网站进行 HTTPS 访问。如果要使用 HTTPS，则可以使用 Amazon CloudFront 为 Amazon S3 上托管的静态网站提供服务。
> 有关更多信息，请参阅如何使用 CloudFront 为 Amazon S3 上托管的静态网站提供服务？以及要求在查看器和 CloudFront 之间使用 HTTPS 进行通信。

1. 在 Buckets（存储桶）下，请选择存储桶的名称。
2. 请选择属性。
3. 在页面底部的 Static website hosting（静态网站托管）下，请选择 Bucket website endpoint（存储桶网站端点）。

   您的索引文档将在单独的浏览器窗口中打开。

现在，您已拥有在 Amazon S3 上托管的网站。该网站在 Amazon S3 网站端点上可用。但是，您可能有要用来从已创建的网站提供内容的域 (如 `example.com`)。您可能还需要使用 Amazon S3 的根域支持来响应对 `http://www.example.com` 和 `http://example.com` 的请求。此操作需要其他步骤。有关示例，请参阅教程：使用注册到 Route 53 的自定义域配置静态网站。

## 步骤 8：清除

如果您仅出于练习目的创建静态网站，则删除您所分配的 Amazon 资源，使其不再产生费用。删除 Amazon 资源后，您的网站将不再可用。有关更多信息，请参阅 删除通用存储桶。

# 在中国托管 Amazon S3 静态网站

> **Important**
>
> 在 2025 年 1 月 6 日之前，您应该重访您的静态网站和 S3 存储桶配置，以确保您通过 ICP 备案或 ICP 许可证使用自定义域名。否则，您的网站可能会受到中国监管要求的影响。

Amazon Web Services 提供多种托管静态网站的方式。Amazon S3 使用服务器端呈现将预构建的 HTML、CSS 和 JavaScript 文件呈现给网络浏览器，这为托管来自 S3 存储桶的网页提供了解决方案。您可以在 S3 存储桶中托管您的网站，并将您的域名直接链接到该网站。您还可以将 Amazon S3 与内容分发网络（CDN）（如 Amazon CloudFront）结合使用来交付网页。CDN 可将延迟减少到毫秒，从而加速向客户交付网站内容。

本主题概述了在 Amazon Web Services 中国（北京）和中国（宁夏）区域取得互联网内容提供商（ICP）备案和通过自定义域名访问您的网站的流程。要在中国托管静态网站，中国法规要求您首先从 ICP 备案系统取得备案或从政府主管部门获得 ICP 许可证。没有 ICP 备案或 ICP 许可证的域不得在中国提供互联网信息服务。除了帮助您遵守法规外，自定义域还比 S3 网站端点更具优势。自定义域比 S3 网站端点更易于记住。搜索引擎也会记录自定义域并将它们编入索引，这可以帮助客户找到您的网站。

## 先决条件

在将自定义域配置为在 Amazon Web Services 中国（北京）区域和中国（宁夏）区域托管 S3 静态网站之前，您必须满足以下先决条件。

### 取得 ICP 备案

如果您的域名通过 Amazon Web Services 中国（宁夏）区域中由宁夏西云数据科技有限公司（NWCD）运营的服务器进行公共访问，您必须通过 NWCD 申请 ICP 备案。

如果您的域名通过 Amazon Web Services 中国（北京）区域中由北京光环新网科技股份有限公司（Sinnet）运营的服务器进行公共访问，您必须通过 Sinnet 申请 ICP 备案。

如果您申请 ICP 备案，则审核过程可能需要 3-20 天。有关 ICP 备案过程的更多信息，包括常见问题解答、下载和详细说明，请参阅 ICP 备案。

### 确认域名是否有 ICP 备案

如果您不知道自己是否已经有 ICP 备案，可以在工业和信息化部网站上查看现有的 ICP 备案。

1. 打开工业和信息化部的 ICP 备案网站，网址为 https://beian.miit.gov.cn。
2. 根据网站上的说明输入查询关键字。
3. 要查看您的域名或实体是否已提交 ICP 备案，请在搜索框中输入您的信息。

### 配置 Amazon S3 静态网站

将自定义域映射到 S3 端点之前，您必须满足以下先决条件。如果您尚未完成这些先决条件，请参阅教程：使用注册到 Route 53 的自定义域配置静态网站中的步骤 1–10。

1. 向域名注册商注册您的自定义域。
2. 创建域存储桶和可选的子域存储桶：
   a. 对于您的域存储桶，启用静态网站托管，然后上传您的网站内容。启用静态网站托管后，您的域存储桶会被分配一个 S3 网站端点，例如 `www.example.com.cn.s3-website.cn-north-1.amazonaws.com.cn`。您将使用此网站端点配置 Route 53 自定义域。
   b. 对于您的子域存储桶，在静态网站托管下，为对象配置重定向请求，以重定向至上传到您的域存储桶的网站内容。

   您的域存储桶包含构成您网站的文件。您的子域存储桶会将请求重新路由到您的域存储桶。例如，如果客户进入 `www.example.com.cn`，您的子域存储桶会将请求转发到您的域存储桶：`example.com.cn`。
3. 清除所有四种 S3 屏蔽公共访问权限设置。您必须清除所有“屏蔽公共访问权限”设置，以便您可以添加允许对存储桶进行公共读取访问的存储桶策略。
4. 添加允许对您的存储桶进行公共读取访问的存储桶策略。当您添加授予公共读取访问权限的存储桶策略时，客户可以访问您的网站内容。

## 使用 Route 53 配置自定义域

在取得 ICP 备案并完成在 Amazon S3 中配置静态网站的先决条件后，您可以将自定义域名映射到 Amazon S3 静态网站并通过自定义域访问您的网站。以下过程使用 Route 53 作为域名管理器。如果您使用其他域名注册商而不是 Route 53，则必须按照适用于该域名注册商的类似步骤，将自定义域映射到 S3 网站端点。有关详细步骤，请联系您的域名注册商。

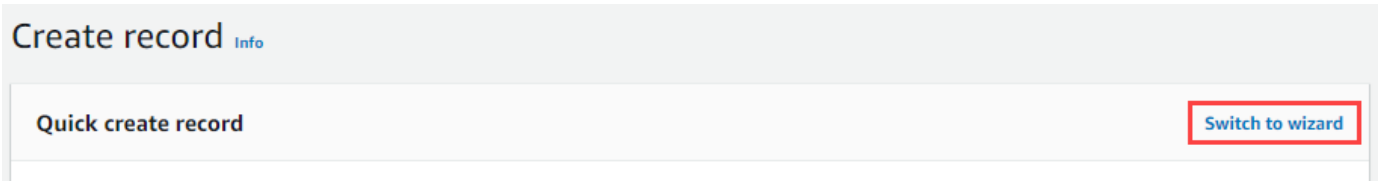
将您的自定义域映射到 S3 网站端点

完成在 Amazon S3 中配置静态网站的先决条件后，您就有了网站端点，例如 `www.example.com.cn.s3-website.cn-north-1.amazonaws.com.cn`（`www.example.com.cn`）。要为您的域和子域配置别名记录，请按照以下步骤操作：

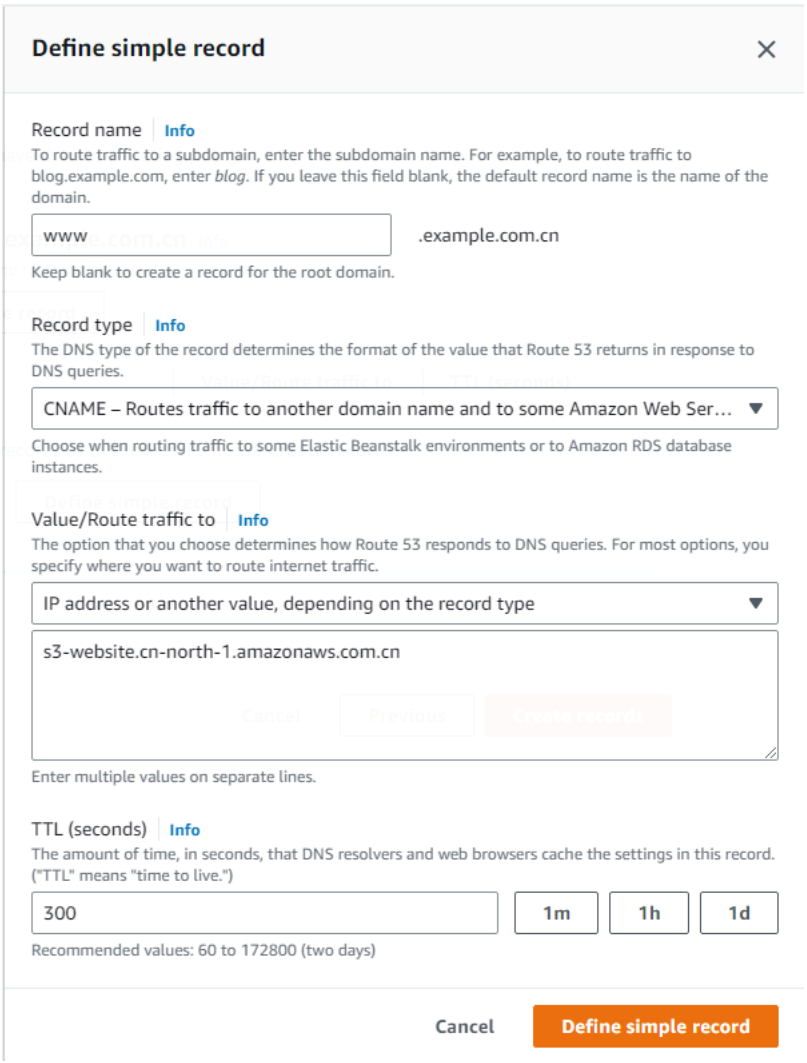
1. 通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 请选择托管区域。
3. 在托管区域列表中，请选择与您的域名匹配的托管区域的名称。
4. 要为您的托管区创建别名记录，请选择创建记录。




5. 请选择切换到向导。




6. 请选择简单路由，然后选择下一步。
7. 请选择定义简单记录。




a. 对于记录名称，接受默认值。

b. 对于记录类型，选择 CNAME 将流量路由到另一个域名和某些 Amazon Web Services 资源。

c. 对于值/流量路由至，选择根据记录类型选择 IP 地址或其他值。在文本框中，输入 S3 网站端点：**`s3-website.cn-north-1.amazonaws.com.cn`**。

d. 请选择定义简单记录。

8. （可选）如果您为子域存储桶配置了重定向，请为子域存储桶执行步骤 2-7。

9. 验证您的网站和重定向是否有效：

a. 通过自定义域名（例如 `http://example.com.cn`）访问您的网站。

b. 如果您配置了子域存储桶，请通过您的子域（例如 `http://www.example.com.cn`）访问您的网站。

## 重新配置在 Amazon S3 中托管的网站

如果您已经有一个在 Amazon S3 中托管的静态网站，并且您的域名已有 ICP 备案，则可以通过四种方式将您的域名直接链接到 S3 存储桶。Amazon S3 提供以下选项：

- 将域链接到 S3 存储桶 - 如果 S3 存储桶名称与网站域名相同（例如，存储桶名称为 `example.cn`，网站名称为 `example.cn`），请按照域名提供商提供的说明将您的域链接到 S3 存储桶。这些说明因每个提供商而异。

  创建 S3 存储桶后，您无法更改存储桶名称。如果存储桶名称与网站域名不同，则可以执行以下操作之一：

- 购买新域 - 您可以购买名称与存储桶名称相同的新域，获取 ICP 备案，然后按照域名提供商提供的步骤将域名链接到存储桶。
- 将网站内容移至名称与域名相同的新存储桶 - 您可以使用与网站域名相同的名称创建一个新存储桶，获取 ICP 记录，然后按照域提供商提供的步骤将域链接到网站存储桶。如果存储桶名称不可用，则可以使用 Amazon CloudFront，如下一个要点所述。
- 使用 Amazon CloudFront 将域映射到域名与存储桶名称不同的存储桶名称 – 要使用 CloudFront 将您的域名映射到您的存储桶，请执行以下操作：
  - 按照步骤 2：创建 CloudFront 分配来创建映射到存储桶的 CloudFront 分配。对于来源配置中的来源访问权限，请使用来源访问身份（OAI），但不要接受其默认值。
  - 按照添加备用域名向您的 CloudFront 分配添加备用域名。
  - 在 CloudFront 分配正常运行后，禁用 S3 静态网站托管，并从您的存储桶策略中删除公共读取访问声明。

> **Note**
>
> 除非您的域名有 ICP 备案，否则 CloudFront 不会处理您的请求。

## 通过您的自定义域访问您的网站

将静态网站配置为使用自定义域后，必须更新所有位置中之前通过引用 S3 网站端点 URL 而指向 S3 网站的所有链接。例如，您必须更新您的文档页面、电子邮件新闻稿等，让它们使用新的自定义域。您的自定义域将更容易被您的客户记住，当客户在搜索中使用关键字时，他们将能够在搜索引擎中找到您的网站。

# 教程：使用注册到 Route 53 的自定义域配置静态网站

假设您要在 Amazon S3 上托管静态网站。您向 Amazon Route 53 注册了一个域（如 `example.com`），希望从 Amazon S3 内容响应对 `http://www.example.com` 和 `http://example.com` 的请求。您可以使用本演练了解如何托管静态网站以及在 Amazon S3 上为具有注册到 Route 53 的自定义域名的网站创建重定向。您可以使用要在 Amazon S3 上托管的现有网站，也可以使用本演练从头开始。

完成本演练后，您可以选择使用 Amazon CloudFront 来提高网站的性能。有关更多信息，请参阅 使用 Amazon CloudFront 为网站提速。

> **Note**
>
> Amazon S3 网站端点不支持 HTTPS 或接入点。如果要使用 HTTPS，则可以使用 Amazon CloudFront 为 Amazon S3 上托管的静态网站提供服务。
> 有关如何使用 CloudFront 和 Amazon S3 安全地托管内容的教程，请参阅教程：使用 Amazon S3、Amazon CloudFront 和 Amazon Route 53 托管点播流视频。有关更多信息，请参阅如何使用 CloudFront 为 Amazon S3 上托管的静态网站提供服务？以及要求在查看器和 CloudFront 之间使用 HTTPS 进行通信。

使用 Amazon CloudFormation 模板自动设置静态网站

可以使用 Amazon CloudFormation 模板自动设置静态网站。Amazon CloudFormation 模板设置托管安全静态网站所需的组件，这样您便能更多地关注网站内容而不是配置组件。

Amazon CloudFormation 模板包含以下组件：

- Amazon S3 – 创建一个 Amazon S3 存储桶来托管静态网站。
- CloudFront – 创建 CloudFront 分配来为静态网站提速。
- Lambda@Edge – 使用 Lambda@Edge 向每个服务器响应添加安全标头。安全标头是 Web 服务器响应中的一组标头，它们告诉 Web 浏览器采取额外的安全预防措施。有关更多信息，请参阅博客文章：使用 Lambda@Edge 和 Amazon CloudFront 添加 HTTP 安全标头。

此 Amazon CloudFormation 模板可供您下载和使用。有关信息和说明，请参阅《Amazon CloudFront 开发人员指南》中的安全静态网站入门。

主题

- 开始前的准备工作
- 步骤 1：将自定义域注册到 Route 53
- 步骤 2：创建两个存储桶
- 步骤 3：为网站托管配置根域存储桶
- 步骤 4：为网站重定向配置子域存储桶
- 步骤 5：配置网站流量的日志记录
- 步骤 6：上传索引和网站内容
- 步骤 7：上传错误文档
- 步骤 8：编辑 S3 屏蔽公共访问权限设置
- 步骤 9：附加存储桶策略
- 步骤 10：测试您的域端点
- 步骤 11：为您的域和子域添加别名记录
- 步骤 12：测试网站
- 使用 Amazon CloudFront 为网站提速
- 清理示例资源


## 开始前的准备工作

在按照此示例中的步骤操作时，您将使用以下服务：

Amazon Route 53 – 您使用 Route 53 注册域，并定义要将您的域的 Internet 流量路由到何处。此示例介绍如何创建 Route 53 别名记录，以便将您的域（`example.com`）和子域（`www.example.com`）的流量路由到包含 HTML 文件的 Amazon S3 存储桶。

Amazon S3 – 您将使用 Amazon S3 创建存储桶、上传示例网站页面、配置权限以便每个人都可以查看内容，然后为网站托管配置存储桶。

## 步骤 1：将自定义域注册到 Route 53

如果您还没有已注册的域名（如 `example.com`），则可向 Route 53 注册一个域名。有关更多信息，请参阅 Amazon Route 53 开发人员指南中的注册新域。注册您的域名后，您可以为网站托管创建并配置 Amazon S3 存储桶。

## 步骤 2：创建两个存储桶

要同时支持来自根域和子域的请求，您需要创建以下两个存储桶。

- 域存储桶 – example.com
- 子域存储桶 – www.example.com

这两个存储桶的名称必须与您的域名完全匹配。在此示例中，域名为 example.com。您将您的内容托管在根域存储桶（example.com）之外。您为子域存储桶（www.example.com）创建重定向请求。如果有人在其浏览器中输入 www.example.com，他们将重定向到 example.com 并看到该名称的 Amazon S3 存储桶中托管的内容。

为网站托管创建存储桶

以下说明概述了如何创建存储桶以用于网站托管。有关创建存储桶的详细分步说明，请参阅创建通用存储桶。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 选择根域存储桶：

   a. 在页面顶部的导航栏中，选择当前所显示 Amazon Web Services 区域的名称。接下来，选择要在其中创建存储桶的区域。

   > **Note**
   >
   > 要最大程度地减少延迟和成本以及满足法规要求，请选择一个靠近您的区域。在某一区域存储的对象将一直留在该区域，除非您特意将其转移到其他区域。有关 Amazon S3 Amazon Web Services 区域的列表，请参阅《Amazon Web Services 一般参考》中的 Amazon Web Services 服务 端点。

   b. 在左侧导航窗格中，选择通用存储桶。

   c. 选择创建存储桶。此时将打开创建存储桶页面。

   d. 输入 Bucket name（存储桶名称）（例如 **example.com**）。

   e. 请选择要在其中创建存储桶的区域。

      请选择一个在地理上靠近您的区域可最大程度地减少延迟和成本，或满足法规要求。您选择的区域决定了您的 Amazon S3 网站端点。有关更多信息，请参阅 网站端点。

   f. 要接受默认设置并创建存储桶，请选择 Create（创建）。

3. 创建您的子域存储桶：

a. 请选择 Create bucket（创建存储桶）。

b. 输入 Bucket name（存储桶名称）（例如 **www.example.com**）。

c. 请选择要在其中创建存储桶的区域。

   请选择一个在地理上靠近您的区域可最大程度地减少延迟和成本，或满足法规要求。您选择的区域决定了您的 Amazon S3 网站端点。有关更多信息，请参阅 网站端点。

d. 要接受默认设置并创建存储桶，请选择 Create（创建）。

在下一步中，您配置 example.com 进行网站托管。

## 步骤 3：为网站托管配置根域存储桶

在此步骤中，您将根域存储桶（example.com）配置为网站。该存储桶将包含您的网站内容。为网站托管配置存储桶时，您可以使用网站端点访问网站。

启用静态网站托管

1. 登录到Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择通用存储桶。
3. 在存储桶列表中，选择要为其启用静态网站托管的存储桶的名称。
4. 选择属性。
5. 在静态网站托管下，请选择编辑。
6. 请选择使用此存储桶托管网站。
7. 在静态网站托管下，请选择启用。
8. 在 Index document (索引文档) 中，输入索引文档的文件名，通常为 index.html。

   索引文档名称区分大小写，并且必须与您计划上传到 S3 存储桶的 HTML 索引文档的文件名完全匹配。当您为网站托管配置存储桶时，您必须指定索引文档。当对根域或任何子文件夹发出请求时，Amazon S3 将返回此索引文档。有关更多信息，请参阅 配置索引文档。

9. 要为 4XX 类错误提供您自己的自定义错误文档，请在错误文档中输入自定义错误文档文件名。

   错误文档名称区分大小写，并且必须与您计划上传到 S3 存储桶的 HTML 错误文档的文件名完全匹配。如果未指定自定义错误文档并发生错误，Amazon S3 返回默认 HTML 错误文档。有关更多信息，请参阅 配置自定义错误文档。

10. （可选）如果要指定高级重定向规则，请在 Redirection rules（重定向规则）中，输入 JSON 来描述规则。

    例如，您可以根据请求中的特定对象键名或前缀按条件路由请求。有关更多信息，请参阅 配置重新导向规则以使用高级条件重新导向。

11. 选择 Save changes（保存更改）。

    Amazon S3 为您的存储桶启用静态网站托管。在页面底部的静态网站托管下，您可以看到存储桶的网站端点。

12. 在静态网站托管下，记下端点。

    端点是存储桶的 Amazon S3 网站端点。将存储桶配置为静态网站后，您可以使用此端点来测试您的网站。

在编辑屏蔽公共访问权限设置并添加允许公有读取访问的存储桶策略后，您可以使用网站端点访问您的网站。

在下一步中，您将子域 (`www.example.com`) 配置为将请求重定向到您的域 (`example.com`)。

## 步骤 4：为网站重定向配置子域存储桶

在为网站托管配置了根域存储桶后，可以将子域存储桶配置为将所有请求重定向到该域。在此示例中，对 `www.example.com` 的所有请求都重定向到 `example.com`。

配置重定向请求

1. 在 Amazon S3 控制台上的通用存储桶列表中，选择子域存储桶名称（在本例中为 `www.example.com`）。
2. 选择属性。
3. 在静态网站托管下，选择编辑。
4. 请选择 Redirect requests for an object（重新导向对于对象的请求）。
5. 在 Target bucket（目标存储桶）框中，输入您的根域（例如 **`example.com`**）。
6. 对于 Protocol（协议），请选择 http。
7. 选择保存更改。

## 步骤 5：配置网站流量的日志记录

如果想要跟踪访问您的网站的访问者人数，则可以选择对根域存储桶启用日志记录。有关更多信息，请参阅 使用服务器访问日志记录来记录请求。如果您计划使用 Amazon CloudFront 来为网站提速，也可以使用 CloudFront 日志记录。

为根域存储桶启用服务器访问日志记录

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 例如，在您创建存储桶（配置为静态网站）的同一区域中，创建用于日志记录的存储桶（例如 `logs.example.com`）。
3. 为服务器访问日志记录日志文件创建文件夹（例如，`logs`）。
4. （可选）如果要使用 CloudFront 提高网站性能，请为 CloudFront 日志文件创建一个文件夹（例如，`cdn`）。

   > **Important**
   >
   > 当您创建或更新分配并启用 CloudFront 日志记录时，CloudFront 会更新存储桶访问控制列表（ACL），以提供 `awslogsdelivery` 账户授予将日志写入存储桶的 `FULL_CONTROL` 权限。有关更多信息，请参阅 Amazon CloudFront Developer Guide（Amazon CloudFront 开发人员指南）中的 Permissions required to configure standard logging and to access your log files（配置标准日志和访问日志文件所需的权限）。如果存储日志的存储桶使用 S3 对象所有权的强制存储桶拥有者设置来禁用 ACL，则 CloudFront 无法将日志写入存储桶。有关更多信息，请参阅 为您的存储桶控制对象所有权和禁用 ACL。。

5. 在 Buckets（存储桶）列表中，请选择您的根域存储桶。
6. 请选择属性。
7. 在 Server access logging（服务器访问日志记录）下，请选择 Edit（编辑）。
8. 请选择 Enable。
9. 在 Target bucket（目标存储桶）下，请选择服务器访问日志的存储桶和文件夹目标：

   - 浏览到文件夹和存储桶位置：
     1. 请选择 Browse S3（浏览 S3）。
     2. 请选择存储桶名称，然后选择日志文件夹。
     3. 请选择 Choose path（选择路径）。

- 输入 S3 存储桶路径，例如 `s3://logs.example.com/logs/`。

10. 选择保存更改。

    在日志存储桶中，您现在可以访问日志。Amazon S3 每 2 小时将网站访问日志写入您的日志存储桶一次。

## 步骤 6：上传索引和网站内容

在此步骤中，您可以将索引文档和可选网站内容上传到您的根域存储桶。

当您为存储桶启用静态网站托管时，您可以输入索引文档的名称（例如，**`index.html`**）。为存储桶启用静态网站托管后，您可以将具有此索引文档名称的 HTML 文件上传到存储桶。

配置索引文档

1. 创建 `index.html` 文件。

   如果您没有 `index.html` 文件，则可以使用以下 HTML 创建一个：

   ```
   <html xmlns="http://www.w3.org/1999/xhtml" >
   <head>
       <title>My Website Home Page</title>
   </head>
   <body>
     <h1>Welcome to my website</h1>
     <p>Now hosted on Amazon S3!</p>
   </body>
   </html>
   ```

2. 将索引文件保存在本地。

   索引文档文件名必须与您在静态网站托管对话框中输入的索引文档名称完全匹配。索引文档名称区分大小写。例如，如果在静态网站托管对话框中为索引文档名称输入 `index.html`，则索引文档文件名也必须是 `index.html`，而不是 `Index.html`。

3. 登录到Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
4. 在左侧导航窗格中，选择通用存储桶。
5. 在存储桶列表中，选择要用于托管静态网站的存储桶的名称。

6. 为您的存储桶启用静态网站托管，并输入索引文档的确切名称（例如 `index.html`）。有关更多信息，请参阅 启用网站托管。

   启用静态网站托管后，继续执行步骤 6。

7. 要将索引文档上传到存储桶，请执行以下操作之一：

   - 将索引文件拖放到控制台存储桶列表中。
   - 选择上传，然后按照提示选择并上传索引文件。

   如需分步指导，请参阅 上传对象。

8. （可选）将其他网站内容上传到您的存储桶。

## 步骤 7：上传错误文档

当您为存储桶启用静态网站托管时，请输入错误文档的名称（例如，**`404.html`**）。为存储桶启用静态网站托管后，您可以将具有此错误文档名称的 HTML 文件上传到存储桶。

要配置错误文档

1. 创建错误文档，例如 `404.html`。
2. 将错误文档文件保存在本地。

   错误文档名称区分大小写，必须与启用静态网站托管时输入的名称完全匹配。例如，如果在静态网站托管对话框中为错误文档名称输入 `404.html`，则错误文档文件名也必须是 `404.html`。

3. 登录到Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
4. 在左侧导航窗格中，选择通用存储桶。
5. 在存储桶列表中，选择要用于托管静态网站的存储桶的名称。
6. 为您的存储桶启用静态网站托管，并输入错误文档的确切名称（例如 `404.html`）。有关更多信息，请参阅启用网站托管 和配置自定义错误文档。

   启用静态网站托管后，继续执行步骤 6。

7. 要将错误文档上传到存储桶，请执行以下操作之一：

   - 将错误文档文件拖放到控制台存储桶列表中。
   - 选择上传，然后按照提示选择并上传索引文件。

如需分步指导，请参阅 上传对象。

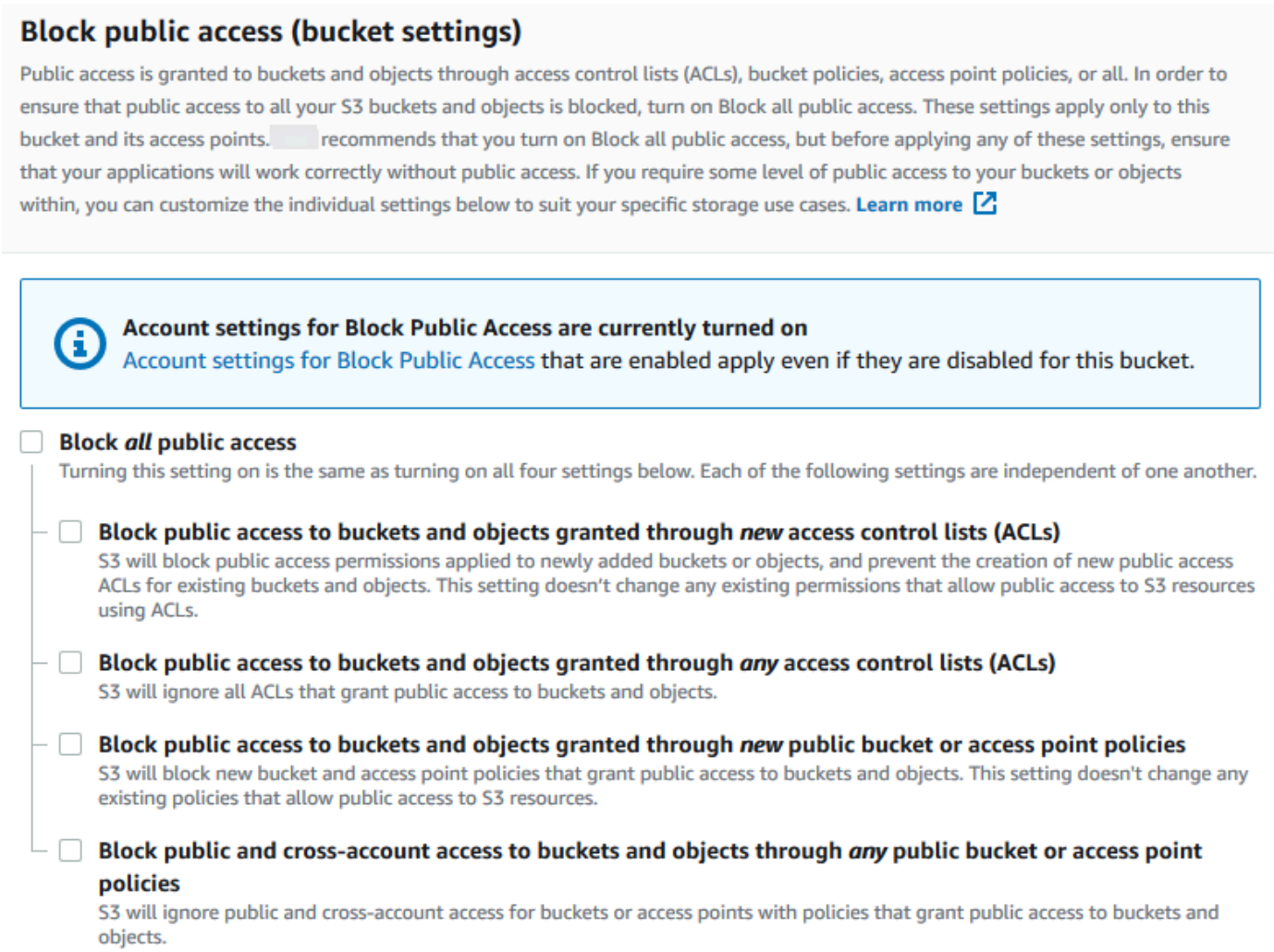
## 步骤 8：编辑 S3 屏蔽公共访问权限设置

在此示例中，您编辑域存储桶（example.com）的屏蔽公共访问权限设置以允许公有访问。

默认情况下，Amazon S3 阻止对您的账户和存储桶的公有访问权限。如果要使用存储桶托管静态网站，您可以使用以下步骤编辑您的屏蔽公共访问权限设置。

> **Warning**
>
> 在完成这些步骤之前，请查看阻止对您的 Amazon S3 存储的公有访问，来确保您了解并接受支持公共访问权限所涉及的风险。当您关闭屏蔽公共访问权限设置以使您的存储桶变为公有时，Internet 上的任何人都可以访问您的存储桶。我们建议您阻止对存储桶的所有公有访问。

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 请选择已配置为静态网站的存储桶的名称。
3. 选择权限。
4. 在屏蔽公共访问权限（存储桶设置）下，请选择编辑。
5. 清除阻止所有公有访问，然后选择保存更改。




Amazon S3 关闭了存储桶的屏蔽公共访问权限设置。要创建公有静态网站，可能还必须为您的账户配置屏蔽公共访问权限设置，然后再添加存储桶策略。如果当前已开启账户的屏蔽公共访问权限设置，您将在屏蔽公共访问权限（存储桶设置）下看到一条备注。

## 步骤 9：附加存储桶策略

在此示例中，您将存储桶策略附加到域存储桶（`example.com`）以允许进行公有读取访问。例如，您可以将示例存储桶策略中的 *`Bucket-Name`* 替换为域存储桶的名称，例如 `example.com`。

在编辑 S3 屏蔽公共访问权限设置后，您可以添加存储桶策略以授予对存储桶的公有读取访问权限。当您授予公有读取访问权限时，Internet 上的任何人都可以访问您的存储桶。

> **Important**
>
> 下面的策略仅供举例说明，仍允许完全访问您存储桶的内容。在继续执行此步骤之前，请查看如何保护 Amazon S3 存储桶中的文件？，以确保您了解保护 S3 存储桶中文件的最佳实践以及授予公有访问权限所涉及的风险。

1. 在存储桶 下，请选择存储桶的名称。
2. 选择权限。
3. 在存储桶策略下，请选择编辑。
4. 要授予对网站的公有读取访问权限，请复制以下存储桶策略，将其粘贴到存储桶策略编辑器中。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicReadGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::Bucket-Name/*"
            ]
        }
    ]
}
```

5. 将 `Resource` 更新为您的存储桶名称。

   在上述示例存储桶策略中，*`Bucket-Name`* 是存储桶名称的占位符。要将此存储桶策略用于您自己的存储桶，您必须更新此名称以匹配您的存储桶名称。

6. 选择保存更改。

   此时将显示一条消息，指示存储桶策略已成功添加。

   如果您看到显示 `Policy has invalid resource` 的错误，请确认存储桶策略中的存储桶名称与您的存储桶名称匹配。有关添加存储桶策略的信息，请参阅如何添加 S3 存储桶策略？

如果您收到错误消息且无法保存存储桶策略，请检查您的账户和存储桶的屏蔽公共访问权限设置以确认您允许对存储桶进行公有访问。

在下一步中，您可以找出您的网站端点并测试您的域端点。

## 步骤 10：测试您的域端点

在将您的域存储桶配置为托管公有网站之后，可以测试您的端点。有关更多信息，请参阅 网站端点。您只能测试域存储桶的端点，因为您的子域存储桶是为网站重定向设置的，而不是静态网络托管。

> **Note**
>
> Amazon S3 不支持对该网站进行 HTTPS 访问。如果要使用 HTTPS，则可以使用 Amazon CloudFront 为 Amazon S3 上托管的静态网站提供服务。
> 有关更多信息，请参阅如何使用 CloudFront 为 Amazon S3 上托管的静态网站提供服务？以及要求在查看器和 CloudFront 之间使用 HTTPS 进行通信。

1. 在 Buckets（存储桶）下，请选择存储桶的名称。
2. 请选择属性。
3. 在页面底部的 Static website hosting（静态网站托管）下，请选择 Bucket website endpoint（存储桶网站端点）。

   您的索引文档将在单独的浏览器窗口中打开。

接下来，您使用 Amazon Route 53 使客户能够使用这两个自定义 URL 导航到您的站点。

## 步骤 11：为您的域和子域添加别名记录

在此步骤中，您创建别名记录并将其添加到您的域的托管区域，而这些别名记录将映射 `example.com` 和 `www.example.com`。别名记录使用 Amazon S3 网站端点，而不使用 IP 地址。Amazon Route 53 保留了别名记录和 Amazon S3 存储桶所在的 IP 地址之间的映射。您创建两个别名记录，一个用于根域，一个用于子域。

为根域和子域添加别名记录

为您的根域 (**example.com**) 添加别名记录

1. 通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。

   > **Note**
   >
   > 如果您尚未使用 Route 53，请参阅 Amazon Route 53 开发人员指南中的步骤 1：注册域。完成设置后，可继续按说明操作。

2. 请选择托管区域。
3. 在托管区域列表中，请选择与您的域名匹配的托管区域的名称。
4. 请选择创建记录。
5. 请选择切换到向导。

   > **Note**
   >
   > 如果要使用快速创建来创建别名记录，请参阅配置 Route 53 以将流量路由到 S3 存储桶。

6. 请选择简单路由，然后选择下一步。
7. 请选择定义简单记录。
8. 在记录名称中，接受默认值，该值为您的托管区域和您的域的名称。
9. 在值/流量路由至中，请选择向 S3 网站端点添加别名。
10. 请选择区域。
11. 请选择 S3 存储桶。

    存储桶名称应与 Name（名称）框中显示的名称相匹配。例如，在选择 S3 存储桶列表中，存储桶名称将与创建存储桶所在区域的 Amazon S3 网站端点一起显示 `s3-website-us-west-1.amazonaws.com (example.com)`。

    如果出现以下情况，请选择 S3 存储桶将列出一个存储桶：

    - 您已将存储桶配置为静态网站。
    - 存储桶名称与您正在创建的记录的名称相同。
    - 当前 Amazon Web Services 账户 创建了存储桶。

如果您的存储桶未显示在选择 S3 存储桶列表中，请输入在其中创建存储桶的区域的 Amazon S3 网站端点，例如 **s3-website-us-west-2.amazonaws.com**。有关 Amazon S3 网站端点的完整列表，请参阅 Amazon S3 网站端点。有关别名目标的更多信息，请参阅 Amazon Route 53 开发人员指南中的 值/路由流量至。

12. 在 Record type (记录类型) 中，选择 A – Routes traffic to an IPv4 address and some Amazon resources (A – 将流量路由到 IPv4 地址和某些 Amazon 资源)。
13. 对于评估目标运行状况，请选择否。
14. 请选择定义简单记录。

为您的子域添加别名记录 (**www.example.com**)

1. 在配置记录下，请选择定义简单记录。
2. 在子域的记录名称中，键入 www。
3. 在值/流量路由至中，请选择向 S3 网站端点添加别名。
4. 请选择区域。
5. 请选择 S3 存储桶，例如 s3-website-us-west-2.amazonaws.com (www.example.com)。

   如果您的存储桶未显示在选择 S3 存储桶列表中，请输入在其中创建存储桶的区域的 Amazon S3 网站端点，例如 **s3-website-us-west-2.amazonaws.com**。有关 Amazon S3 网站端点的完整列表，请参阅 Amazon S3 网站端点。有关别名目标的更多信息，请参阅 Amazon Route 53 开发人员指南中的 值/路由流量至。
6. 在 Record type (记录类型) 中，选择 A – Routes traffic to an IPv4 address and some Amazon resources (A – 将流量路由到 IPv4 地址和某些 Amazon 资源)。
7. 对于评估目标运行状况，请选择否。
8. 请选择定义简单记录。
9. 在配置记录页面上，请选择创建记录。

> **Note**
>
> 更改通常在 60 秒内传播到所有 Route 53 服务器。传播完成后，您可以使用在此步骤中创建的别名记录的名称将流量路由到 Amazon S3 存储桶。

为根域和子域添加别名记录（旧 Route 53 控制台）

为您的根域 (**example.com**) 添加别名记录

Route 53 控制台进行了重新设计。在 Route 53 控制台中，您可以暂时使用旧控制台。如果您选择使用旧 Route 53 控制台，请使用以下过程。

1. 通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。

   > **Note**
   >
   > 如果您尚未使用 Route 53，请参阅 Amazon Route 53 开发人员指南中的步骤 1：注册域。完成设置后，可继续按说明操作。

2. 请选择 Hosted Zones (托管区域)。
3. 在托管区域列表中，请选择与您的域名匹配的托管区域的名称。
4. 请选择 Create Record Set。
5. 指定以下值：

   名称

   接受默认值，该值为您的托管区域和您的域的名称。

   对于根域，您不需要在 Name (名称) 字段中输入任何其他信息。

   类型

   请选择 A – IPv4 address（A – IPv4 地址）。

   别名

   请选择是。

   别名目标

   在列表的 S3 website endpoints（S3 网站端点）部分，请选择您的存储桶名称。

   存储桶名称应与 Name（名称）框中显示的名称相匹配。在 Alias Target（别名目标）列表中，存储桶名称后跟在其中创建存储桶的区域的 Amazon S3 网站端点，例如 `example.com (s3-website-us-west-2.amazonaws.com)`。Alias Target（别名目标）会在以下情况下列出存储桶：

   - 您已将存储桶配置为静态网站。

- 存储桶名称与您正在创建的记录的名称相同。
- 当前 Amazon Web Services 账户 创建了存储桶。

如果您的存储桶未显示在 Alias Target（别名目标）列表中，请输入在其中创建存储桶的区域的 Amazon S3 网站端点，例如 `s3-website-us-west-2`。有关 Amazon S3 网站端点的完整列表，请参阅 Amazon S3 网站端点。有关别名目标的更多信息，请参阅 Amazon Route 53 开发人员指南中的 值/路由流量至。

路由策略

接受默认值 Simple。

Evaluate Target Health

接受默认值 No。

6. 请选择创建。

为您的子域添加别名记录 (**`www.example.com`**)

1. 在您的根域 (`example.com`) 的托管区域中，请选择 Create Record Set (创建记录集)。
2. 指定以下值：

名称

对于子域，在框中输入 `www`。

类型

请选择 A – IPv4 address（A – IPv4 地址）。

别名

请选择是。

别名目标

在列表的 S3 website endpoints（S3 网站端点）部分中，请选择 Name（名称）字段中显示的相同存储桶名称，例如 `www.example.com (s3-website-us-west-2.amazonaws.com)`。

路由策略

接受默认值 Simple。

Evaluate Target Health

接受默认值 No。

3. 请选择创建。

> **Note**
>
> 更改通常在 60 秒内传播到所有 Route 53 服务器。传播完成后，您可以使用在此步骤中创建的别名记录的名称将流量路由到 Amazon S3 存储桶。

## 步骤 12：测试网站

验证网站和重定向正常工作。在浏览器中，输入 URL。在本示例中，可以尝试以下 URL：

- 域（`http://example.com`）– 显示 `example.com` 存储桶中的索引文档。
- 子域 (`http://www.example.com`) – 将您的请求重定向到 `http://example.com`。您会在 `example.com` 存储桶中看到索引文档。

如果您的网站或重定向链接不起作用，则可以尝试以下操作：

- 清除缓存 – 清除 Web 浏览器缓存。
- 检查名称服务器 – 如果在清除缓存后，您的网页和重定向链接无法正常工作，则可以比较域的名称服务器和托管区域的名称服务器。如果名称服务器不匹配，您可能需要更新域名服务器，以便匹配在托管区域下方列出的服务器。有关更多信息，请参阅为域添加或更改名称服务器和粘附记录。

在成功测试根域和子域后，您可以设置 Amazon CloudFront 分配以提高网站的性能，并提供可用于查看网站流量的日志。有关更多信息，请参阅 使用 Amazon CloudFront 为网站提速。

## 使用 Amazon CloudFront 为网站提速

您可以使用 Amazon CloudFront 来提高 Amazon S3 网站的性能。CloudFront 可将您的网站文件（如 HTML、图像和视频）提供给全球各地的数据中心（称为边缘站点）使用。当访问者从您的网站请求文件时，CloudFront 会自动将请求重定向到最近边缘站点上的文件副本。这时的下载速度会比访问者从更远的数据中心请求该内容更快。

CloudFront 会将内容在边缘站点上缓存您指定的时间。如果访问者请求已过期的缓存内容，CloudFront 会检查来源服务器，确定该内容是否有更新的版本可用。如果有更新的版本，则 CloudFront 将新版本复制到该边缘站点。当访问者请求内容时，您对原始内容所做的更改便会复制到边缘站点。

在没有 Route 53 的情况下使用 CloudFront

本页面上的教程使用 Route 53 来指向您的 CloudFront 分配。但是，如果您想在不使用 Route 53 的情况下使用 CloudFront 提供托管在 Amazon S3 存储桶中的内容，请参阅 Amazon CloudFront Tutorials: Setting up a Dynamic Content Distribution for Amazon S3。在使用 CloudFront 提供托管在 Amazon S3 存储桶中的内容时，您可以使用任何存储桶名称，并且同时支持 HTTP 和 HTTPS。

使用 Amazon CloudFormation 模板自动执行设置过程

有关使用 Amazon CloudFormation 模板配置安全静态网站以创建 CloudFront 分配来为您的网站提供服务的更多信息，请参阅《Amazon CloudFront 开发人员指南》中的安全静态网站入门。

主题


- 步骤 1：创建 CloudFront 分配
- 步骤 2：更新域和子域的记录集
- （可选）步骤 3：检查日志文件


步骤 1：创建 CloudFront 分配

首先，创建 CloudFront 分配。这将使您的网站可供全球各地的数据中心使用。

使用 Amazon S3 源创建分配

1. 通过 打开 CloudFront 控制台https://console.amazonaws.cn/cloudfront/v4/home
2. 选择 Create Distribution（创建分配）。
3. 在 Create Distribution（创建分配）页面上的 Origin Settings（源设置）部分中，对于 Origin Domain Name（源域名），输入您的存储桶的 Amazon S3 网站端点，例如 **`example.com.s3-website.us-west-1.amazonaws.com`**。

   CloudFront 将为您填写 Origin ID (源 ID)。
4. 对于 Default Cache Behavior Settings (默认缓存行为设置)，将值保留设置为默认值。

   当为查看器协议策略使用默认设置时，您可以为静态网站使用 HTTPS。有关这些配置选项的更多信息，请参阅《Amazon CloudFront 开发人员指南》中的您创建或更新 Web 分配时指定的值。

5. 对于 Distribution Settings，执行以下操作：

   a. 将 Price Class (价格级别) 的设置保留为 Use All Edge Locations (Best Performance) (使用所有节点 (最佳性能))。

   b. 将 Alternate Domain Names (CNAMEs) ( 备用域名(CNAME) ) 设置为根域和 www 子域。在本教程中，它们是 `example.com` 和 `www.example.com`。

   > **Important**
   >
   > 在执行该步骤之前，请注意使用备用域名的要求，尤其是需要使用有效的 SSL/TLS 证书。

   c. 对于 SSL 证书，选择自定义 SSL 证书 (example.com)，然后选择涵盖域名和子域名的自定义证书。

   有关更多信息，请参阅《Amazon CloudFront 开发人员指南》中的 SSL 证书。

   d. 在 Default Root Object (默认根对象) 中，输入索引文档的名称，例如 `index.html`。

   如果用于访问分配的 URL 不包含文件名，CloudFront 分配将返回索引文档。Default Root Object (默认根对象) 应该与静态网站的索引文档的名称完全匹配。有关更多信息，请参阅 配置索引文档。

   e. 将 Logging (日志记录) 设置为 On (打开)。

   > **Important**
   >
   > 当您创建或更新分配并启用 CloudFront 日志记录时，CloudFront 会更新存储桶访问控制列表 ( ACL ) ，以提供 `awslogsdelivery` 账户 `FULL_CONTROL` 权限，从而将日志写入您的存储桶。有关更多信息，请参阅 Amazon CloudFront Developer Guide ( Amazon CloudFront 开发人员指南 ) 中的 Permissions required to configure standard logging and to access your log files ( 配置标准日志和访问日志文件所需的权限 ) 。如果存储日志的存储桶使用 S3 对象所有权的强制存储桶拥有者设置来禁用 ACL，则 CloudFront 无法将日志写入存储桶。有关更多信息，请参阅 为您的存储桶控制对象所有权和禁用 ACL。 。

   f. 对于 Bucket for Logs，选择您创建的日志记录存储桶。

   有关配置日志记录存储桶的更多信息，请参阅 ( 可选 ) 记录 Web 流量。

g. 如果您要将由流量生成的日志存储到文件夹中的 CloudFront 分配，请在 Log Prefix (日志前缀) 中键入文件夹名称。

h. 将所有其他设置保留为默认值。

6. 选择 Create Distribution。
7. 要查看分配的状态，请在控制台中找到该分配，然后检查 Status 列。

   `InProgress` (进行中) 状态表示分配尚未完成部署。

   分配部署完毕后，您可以使用新的 CloudFront 域名来引用您的内容。
8. 记录 CloudFront 控制台中显示的 Domain Name (域名) 值，例如 `dj4p1rv6mvubz.cloudfront.net`。
9. 要验证您的 CloudFront 分配是否正常运行，请在 Web 浏览器中输入该分配的域名。

   如果您的网站是可见的，则 CloudFront 分配正常工作。如果您的网站具有向 Amazon Route 53 注册的自定义域，您将需要 CloudFront 域名来在下一步更新记录集。

步骤 2：更新域和子域的记录集

现在您已成功地创建 CloudFront 分配，请更新 Route 53 中的别名记录以指向新的 CloudFront 分配。

更新别名记录以指向 CloudFront 分配

1. 通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在左侧导航中，选择 Hosted zones（托管区）。
3. 在 Hosted Zones（托管区）页上，选择为您的子域创建的托管区域，例如 `www.example.com`。
4. 在 Records（记录）下，选择您为子域创建的 A 记录。
5. 在 Record details（记录详细信息）下，选择 Edit record（编辑记录）。
6. 在 Route traffic to（将流量路由至）下，选择 Alias to CloudFront distribution（别名到 CloudFront 分配）。
7. 在 Choose distribution（选择分配）下，选择 CloudFront 分配。
8. 选择 Save。
9. 要将根域的 A 记录重定向到 CloudFront 分配，请对根域重复此过程，例如 `example.com`。

   记录集的更新需要 2 – 48 小时才能生效。
10. 要查看新的 A 记录是否已生效，请在 Web 浏览器中输入您的子域 URL，例如 `http://www.example.com`。

如果您的浏览器不再重定向至根域（例如，`http://example.com`），则说明新的 A 记录已生效。当新 A 记录生效时，由新 A 记录路由到 CloudFront 分配的流量不会重定向到根域。任何使用 `http://example.com` 或 `http://www.example.com` 引用站点的访问者都会重定向到最近的 CloudFront 边缘站点，在这里可体验更快速的下载。

> **Tip**
>
> 浏览器可以缓存重定向设置。如果您认为新的 A 记录设置应该已经生效，但是您的浏览器仍然将 `http://www.example.com` 重定向至 `http://example.com`，请尝试清除浏览器的历史记录和缓存，然后关闭再重新打开浏览器应用程序，或使用其他 Web 浏览器。

（可选）步骤 3：检查日志文件

访问日志会告诉您有多少人正在访问网站。它们还包含有价值的业务数据，您可以使用 Amazon EMR 等其他服务分析这些数据。

CloudFront 日志存储在您在创建 CloudFront 分配并启用日志记录时所选择的存储桶和文件夹中。CloudFront 将在相应请求提出后的 24 小时内将日志写入您的日志存储桶。

查看网站的日志文件

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 为网站选择日志记录存储桶的名称。
3. 选择 CloudFront 日志文件夹。
4. 先下载由 CloudFront 编写的 `.gzip` 文件，然后再打开这些文件。

如果您仅出于练习目的创建网站，则可以删除您所分配的资源，使其不再产生费用。为此，请参阅清理示例资源。删除 Amazon 资源后，您的网站将不再可用。

## 清理示例资源

如果您出于学习目的创建静态网站，应删除您分配的Amazon资源，使其不再产生费用。删除 Amazon 资源后，您的网站将不再可用。

任务

- 步骤 1：删除 Amazon CloudFront 分配

- 步骤 2：删除 Route 53 托管区域
- 步骤 3：禁用日志记录并删除 S3 存储桶


### 步骤 1：删除 Amazon CloudFront 分配

在删除 Amazon CloudFront 分配之前，您必须先将其禁用。已禁用的分发不再起作用，并且不会产生费用。您可以随时启用已禁用的分发。已禁用的分发在删除后将不再可用。

#### 禁用并删除 CloudFront 分配

1. 通过 打开 CloudFront 控制台https://console.amazonaws.cn/cloudfront/v4/home
2. 选择要禁用的分配，然后选择禁用。
3. 当系统提示确认时，选择是，禁用。
4. 选择禁用的分配，然后选择删除。
5. 当系统提示进行确认时，选择 Yes, Delete。

### 步骤 2：删除 Route 53 托管区域

在删除托管区域之前，您必须先删除已创建的记录集。您不需要删除 NS 和 SOA 记录；删除托管区域时，会自动删除这些记录。

#### 删除记录集

1. 通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在域名列表中，选择您的域名，然后选择 Go to Record Sets。
3. 在记录集列表中，选择您创建的 A 记录。

   每个记录集的类型均列在 Type (类型) 列中。
4. 选择 Delete Record Set。
5. 当系统提示进行确认时，选择 Confirm。

#### 删除 Route 53 托管区域

1. 紧接上一个步骤，选择 Back to Hosted Zones。
2. 选择您的域名，然后选择 Delete Hosted Zone。
3. 当系统提示进行确认时，选择 Confirm。

步骤 3：禁用日志记录并删除 S3 存储桶

在删除您的 S3 存储桶之前，请确保已禁用该存储桶的日志记录。否则，在您删除存储桶时，Amazon 会继续将日志写入其中。

禁用存储桶的日志记录

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Buckets（存储桶）下，选择存储桶名称，然后选择 Properties（属性）。
3. 从 Properties 中选择 Logging。
4. 取消选中启用复选框。
5. 选择保存。

现在您可以删除存储桶。有关更多信息，请参阅 删除通用存储桶。

## 从 S3 通用存储桶将静态网站部署到 Amazon Amplify Hosting

我们建议您使用 Amazon Amplify Hosting 来托管存储在 S3 上的静态网站内容。Amplify Hosting 是一项完全托管式服务，可让您轻松地在由 Amazon CloudFront 提供支持的全球可用内容分发网络（CDN）上部署您的网站，无需大量设置即可实现安全的静态网站托管。借助 Amazon Amplify Hosting，您可以选择对象在通用存储桶中的位置，将内容部署到托管式 CDN，并为网站生成一个公有 HTTPS URL 以供在任何地方访问。使用 Amplify Hosting 部署静态网站可为您提供以下优势和功能：

- 部署到由 Amazon CloudFront 提供支持的 Amazon 内容分发网络（CDN）：CloudFront 是一项 Web 服务，可以加快向用户分发静态和动态 Web 内容的速度。CloudFront 通过全球数据中心（称作边缘站点）网络传输内容。当用户请求您用 CloudFront 提供的内容时，请求被路由到提供最低延迟（时间延迟）的边缘站点，从而以最佳性能、更高的可靠性和可用性交付内容。有关更多信息，请参阅《Amazon CloudFront 开发人员指南》中的 CloudFront 如何交付内容。
- HTTPS 支持：在您的网站和用户的 Web 浏览器之间提供安全的通信和数据传输。
- 自定义域：轻松将您的网站连接到从域注册商（如 Amazon Route 53）购买的自定义 URL。
- 自定义 SSL 证书：设置自定义域时，可以使用 Amplify 为您提供的默认托管证书，也可以使用从您选择的第三方证书颁发机构购买的您自己的自定义证书。
- 内置指标和 CloudWatch 监控：监控您网站的流量、错误、数据传输和延迟。
- 密码保护：通过在 Amplify 控制台中设置用户名和密码要求，限制对您网站的访问权限。
- 重定向和重写：在 Amplify 控制台中创建重定向和重写规则，以使 Web 服务器能够将导航从一个 URL 重新路由到另一个 URL。

当您将 Amazon S3 通用存储桶中存储的应用程序部署到 Amplify Hosting 时，Amazon 费用将基于 Amplify 定价模型确定。有关更多信息，请参阅 Amazon Amplify 定价。

> **Important**
>
> Amplify Hosting 并非在提供 Amazon S3 的所有 Amazon Web Services 区域 均可用。若要将静态网站部署到 Amplify Hosting，包含您的网站的 Amazon S3 通用存储桶必须位于可以使用 Amplify 的区域之中。有关可以使用 Amplify 的区域列表，请参阅《Amazon Web Services 一般参考》中的 Amplify 端点。

可以从 Amazon S3 控制台、Amplify 控制台、Amazon CLI 或 Amazon SDK 开始部署过程。您只能从位于您自己账户中的通用存储桶部署到 Amplify。Amplify 不支持跨账户 存储桶访问。

请按照以下说明，从 Amazon S3 控制台开始，将静态网站从 Amazon S3 通用存储桶部署到 Amplify Hosting。

## 从 S3 控制台将静态网站部署到 Amplify

从 Amazon S3 控制台部署静态网站

1. 登录到Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在左侧导航窗格中，选择存储桶。
3. 在存储桶列表中，选择包含您要部署到 Amplify Hosting 的网站的通用存储桶。
4. 选择属性选项卡。
5. 在静态网站托管下，选择创建 Amplify 应用程序。在此步骤中，部署过程将移至 Amplify 控制台。
6. 在使用 S3 部署页面上，执行以下步骤。
   a. 对于应用程序名称，输入应用程序或网站的名称。
   b. 对于分支名称，输入应用程序后端的名称。
   c. 对于要托管的对象的 S3 位置，请输入通用存储桶的目录路径，或选择浏览 S3 来定位和选择位置。
7. 选择保存并部署。

> **Note**
>
> 如果您为 Amplify 上托管的通用存储桶中的静态网站更新了任何对象，则必须将应用程序重新部署到 Amplify Hosting，这样才能使更改生效。Amplify Hosting 不会自动检测对存储桶的更改。有关更多信息，请参阅《Amazon Amplify Hosting 用户指南》中的 Updating a static website deployed to Amplify from an S3 bucket。

要直接从 Amplify 控制台开始，请参阅《Amazon Amplify Hosting 用户指南》中的 Deploying a static website from S3 using the Amplify console。

要开始使用 Amazon SDK，请参阅《Amazon Amplify Hosting 用户指南》中的 Creating a bucket policy to deploy a static website from S3 using the Amazon SDKs。

# 配额

对于每项 Amazon 服务，您的 Amazon Web Services 账户都具有默认配额（以前称为限制）。Amazon S3 配额包括通用存储桶、目录存储桶、接入点等的数量。可以请求增加某些配额，但并非所有配额都可以增加。我们不会立即授予这些提高，因此，您的提高请求可能需要几天才能生效。

有关 Amazon S3 配额及其默认值的列表，请参阅《Amazon Web Services 一般参考》中的 Amazon S3 配额。

## 增加配额

要请求提高限额

可以使用以下选项之一来请求增加配额：

- 从 Amazon Web Services Management Console中：打开服务配额控制台。在导航窗格中，选择 Amazon 服务。选择 Amazon S3，选择配额，然后按照说明来请求提高配额。有关说明，请参阅 Service Quotas 用户指南中的请求增加配额。
- 从 Amazon CLI 中：使用 request-service-quota-increase Amazon CLI 命令。有关说明，请参阅 Service Quotas 用户指南中的请求增加配额。

# 参考

除了 Amazon S3 控制台之外，还可以通过 Amazon S3 REST API、Amazon SDK 或 Amazon Command Line Interface（Amazon CLI）以编程方式使用 Amazon S3。

- Amazon Simple Storage Service API 参考
- 《Amazon Simple Storage Service API 参考》中的代码示例
- 《Amazon Command Line Interface 用户指南》中的 Amazon 命令行界面。
- Amazon SDK

# 文档历史记录

- 当前 API 版本：2006-03-01

下表介绍了 Amazon Simple Storage Service API 参考和 Amazon S3 用户指南的每个版本中的重要更改。要获得本文档的更新通知，您可以订阅 RSS 源。

| 变更 | 说明 | 日期 |
| --- | --- | --- |
| S3 表类数据存储服务现在使用客户自主管理型密钥支持 SSE-KMS。 | S3 表类数据存储服务现在使用客户自主管理型密钥支持具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）。您可以在表存储桶和表级别应用 SSE-KMS 加密。有关更多信息，请参阅 Using server-side encryption with Amazon KMS keys (SSE-KMS) in table buckets。 | 2025 年 4 月 16 日 |
| Amazon 本地区域中提供了目录存储桶的接入点 | 目录存储桶现在支持接入点，以简化对 Amazon S3 中共享数据集的大规模数据访问管理。借助这项新功能，您可以为每个存储桶创建数百个接入点，每个接入点都有不同的名称和为每个应用程序自定义的权限。有关更多信息，请参阅 Managing access to shared datasets in directory buckets with access points。 | 2025 年 3 月 31 日 |
| S3 表存储桶与 Amazon SageMaker 智能湖仓的集成现已正式发布 | 您可以将 S3 表存储桶与 Amazon SageMaker 智能湖仓集成，以便通过 Amazon 分 | 2025 年 3 月 13 日 |

析服务访问表，例如 Amazon Athena、Amazon Redshift 和 QuickSight。Amazon SageMaker 智能湖仓统一了您在 Amazon S3 数据湖和 Amazon Redshift 数据仓库中的数据，因此，您可以在单个数据副本上构建分析、机器学习（ML）和生成式人工智能应用程序。该集成会使用您的表资源填充 Amazon Glue Data Catalog，并与 Amazon Lake Formation 联合访问这些资源。该集成通过 Lake Formation 支持精细的访问控制，以提供额外的安全性。有关集成的更多信息，请参阅将 Amazon S3 表类数据存储服务与 Amazon 分析服务结合使用。如果您使用预览版设置集成，则可以继续使用当前的集成。但是，更新的集成流程提供了性能改进，因此我们建议进行迁移。要迁移到更新的集成，请参阅迁移到更新的集成流程。

| | | |
|---|---|---|
| Amazon S3 控制台新增了 S3 表类数据存储服务创建表和查询表支持 | S3 表类数据存储服务现在支持使用 Amazon Athena 直接从 Amazon S3 控制台执行创建表和查询表操作。有了这项新功能，您现在只需在 Amazon S3 控制台中执行几个步骤，即可创建表、为表填充数据和查询表。有关更多信息，请参阅创建 Amazon S3 表和使用 Athena 查询 Amazon S3 表。 | 2025 年 3 月 13 日 |
| S3 表类数据存储服务增加了对创建表时添加架构的支持 | 现在，可以使用 S3 表类数据存储服务 `CreateTable` API 操作，通过添加可选的元数据标志来创建带有架构的表。有关更多信息，请参阅创建表。 | 2025 年 1 月 30 日 |
| S3 表类数据存储服务增加了对创建表时添加架构的支持 | 现在，可以使用 S3 表类数据存储服务 `CreateTable` API 操作，通过添加可选的元数据标志来创建带有架构的表。有关更多信息，请参阅创建表。 | 2025 年 1 月 30 日 |

| | | |
|---|---|---|
| S3 元数据现已正式发布 | Amazon S3 元数据现已正式发布。S3 元数据通过近乎实时进行更新的自动化、可查询的元数据，协助您轻松发现和理解 S3 数据。借助 S3 元数据，您可以整理、识别和使用 S3 数据进行业务分析、人工智能和机器学习（AI/ML）模型训练等。S3 元数据支持对象元数据（包括系统定义的信息，例如对象的大小和来源）和自定义元数据（例如，带有产品 SKU、事务 ID 或内容评级等信息的标签）。有关更多信息，请参阅使用 S3 元数据加快数据发现速度。 | 2025 年 1 月 27 日 |
| Amazon 托管式策略 – 新策略 | S3 表类数据存储服务添加了两个新的 Amazon 托管式策略。 | 2024 年 12 月 6 日 |

| | | |
|---|---|---|
| S3 表类数据存储服务 | Amazon S3 表类数据存储服务提供针对分析工作负载进行优化的 S3 存储，其功能可提高查询性能，降低表的存储成本，并大规模简化数据湖的操作。S3 表类数据存储服务引入了一种新的存储桶类型：表存储桶，专为将 Apache Iceberg 表存储为子资源而构建。与 S3 通用存储桶中的自行管理的表相比，表存储桶可提供更高的每秒事务数（TPS）和更好的查询吞吐量。您可以自动将表存储桶与 Amazon 分析服务（例如 Athena、Amazon Redshift、QuickSight 等）集成。有关更多信息，请参阅使用 Amazon S3 表类数据存储服务和表存储桶。 | 2024 年 12 月 3 日 |
| S3 元数据预览版 | Amazon S3 元数据通过近乎实时进行更新的自动化、可查询的元数据，协助您轻松发现和理解 S3 数据。借助 S3 元数据，您可以整理、识别和使用 S3 数据进行业务分析、人工智能和机器学习（AI/ML）模型训练等。S3 元数据支持对象元数据（包括系统定义的信息，例如对象的大小和来源）和自定义元数据（例如，带有产品 SKU、事务 ID 或内容评级等信息的标签）。有关更多信息，请参阅使用 S3 元数据加快数据发现速度。 | 2024 年 12 月 3 日 |

| | | |
|---|---|---|
| 适用于 S3 的存储浏览器 | 适用于 S3 的存储浏览器是一个开源组件，您可以将其添加到 Web 应用程序中，为您的最终用户提供存储在 S3 中的数据的简单界面。有关更多信息，请参阅适用于 S3 的存储浏览器。 | 2024 年 12 月 1 日 |
| 新的 Amazon S3 校验和算法以及改进的校验和完整性功能 | Amazon S3 添加了 `CRC-64NVME` 校验和算法以及改进的校验和完整性功能。有关更多信息，请参阅检查 Amazon S3 中的对象完整性。 | 2024 年 12 月 1 日 |
| 数据驻留工作负载 | 在专用本地区域中，您可以创建 S3 目录存储桶来为数据驻留和隔离应用场景存储数据。有关更多信息，请参阅数据驻留工作负载。 | 2024 年 12 月 1 日 |
| 用于强制执行有条件写入的新条件键 | Amazon S3 添加了新的条件键 `s3:if-match` 和 `s3:if-none-match`，以便在存储桶策略中用于强制客户端使用 `If-None-Match` 或 `If-Match` HTTP 标头。有关更多信息，请参阅 Enforce conditional writes on Amazon S3 buckets。 | 2024 年 11 月 25 日 |

| | | |
|---|---|---|
| 适用于有条件写入的新 HTTP 标头，用于检查对象是否已更改 | Amazon S3 添加了 `If-Match` HTTP 标头，用于在为某些 API 操作写入对象之前检查对象的实体标签（ETag）。通过此标头，Amazon S3 将提供的 ETag 值与 S3 中对象的 ETag 值进行比较。如果 ETag 值不匹配，则操作会失败。有关更多信息，请参阅如何使用有条件写入来防止对象覆盖。 | 2024 年 11 月 25 日 |
| Amazon Redshift 现已与 S3 访问权限管控集成 | Amazon Redshift 客户现在可以使用 S3 访问权限管控来扩展和管理其 S3 数据的权限。这使 Amazon Redshift 客户能够使用 Amazon IAM Identity Center，为企业身份以及 IAM 用户和组扩展 S3 权限。有关更多信息，请参阅 Amazon Redshift integration with Amazon S3 Access Grants。 | 2024 年 11 月 15 日 |
| Amazon Organizations 成员账户现在可以重新获得对意外锁定的 Amazon S3 存储桶的访问权限 | Amazon Organizations 成员账户现在可以通过 Amazon Identity and Access Management（IAM）使用一个简单的流程，来重新获得对意外锁定的 Amazon S3 存储桶的访问权限。有关更多信息，请参阅《Amazon Identity and Access Management User Guide》中的 Perform a privileged task on an Amazon Organizations member account。 | 2024 年 11 月 14 日 |

| | | |
|---|---|---|
| 资源控制策略（RCP）是 Amazon Organizations 中的一种新型授权策略，也可用于 Amazon S3 存储桶 | 资源控制策略（RCP）是一项在 Amazon Organizations 中管理的新授权策略，可用于为您整个组织内的 Amazon S3 存储桶设置最大可用权限。有关更多信息，请参阅《Amazon Organizations User Guide》中的 Resource control policies (RCPs)。 | 2024 年 11 月 13 日 |
| Amazon S3 现在会自动批准将存储桶配额增加到多达 1000 个存储桶 | Amazon S3 现在会自动批准将存储桶配额增加到多达 1000 个存储桶。要查看存储桶利用率或请求增加配额，请访问服务配额控制台。 | 2024 年 9 月 30 日 |
| Amazon S3 生命周期配置的新默认最小对象大小转换行为 | Amazon S3 现在对 S3 生命周期配置应用默认行为，来防止将小于 128 KB 的对象转换到任何存储类。要了解如何覆盖此行为，请参阅支持转换小于 128 KB 的对象。 | 2024 年 9 月 24 日 |
| 目录存储桶现在使用客户自主管理型密钥支持 SSE-KMS。 | 目录存储桶现在使用客户自主管理型密钥支持具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）。可以通过更多选项来加密和管理目录存储桶中数据的安全性。有关更多信息，请参阅目录存储桶中的数据保护和加密。 | 2024 年 9 月 17 日 |

| | | |
|---|---|---|
| S3 访问权限管控支持用于列出调用方访问授权的 API 操作 | IAM 身份和 IAM Identity Center 公司目录身份现在可以使用 `ListCallerAccessGrants` API 列出这些身份可以访问的所有 Amazon S3 存储桶、前缀和对象，如其 S3 访问权限管控所定义的那样。使用此 API 可以发现 IAM 身份或公司目录身份可以通过特定 Amazon Web Services 账户中的 S3 访问权限管控访问的所有 S3 数据。有关更多信息，请参阅 List the caller's access grants。 | 2024 年 9 月 5 日 |

| | | |
|---|---|---|
| 适用于同账号请求的增强拒绝访问错误消息 | Amazon S3 现在对于对同一 Amazon Web Services 账户内的资源发出的请求，在拒绝访问（HTTP 403 Forbidden）错误中包含额外的上下文。这个新的上下文包括拒绝访问的策略类型、拒绝的原因，以及有关请求访问该资源的 Amazon Identity and Access Management（IAM）用户或角色的信息。此上下文有助于您解决访问问题，确定拒绝访问错误的根本原因，并通过更新相关策略来修复不正确的访问控制。此附加上下文也可以在 Amazon CloudTrail 日志中找到。针对同账号请求的增强拒绝访问错误消息现已在所有 Amazon Web Services 区域推出，包括 Amazon GovCloud (US) Regions和中国区域。有关更多信息，请参阅排查 Amazon S3 中的拒绝访问（403 Forbidden）错误。 | 2024 年 8 月 21 日 |
| Amazon S3 支持对 PutObject 和 CompleteMultipartUpload 使用有条件写入 | 在对上传操作使用有条件写入来创建对象之前，您可以检查存储桶中是否存在该对象。这样可以防止覆盖现有数据。有条件写入将验证存储桶中尚不存在具有相同键名称的现有对象。有关更多信息，请参阅 Conditional requests。 | 2024 年 8 月 20 日 |

| | | |
|---|---|---|
| Amazon S3 不再对多个 HTTP 错误代码收费 | Amazon S3 已完成一项更改，因此客户未发起的未经授权的请求是免费的。有关更多信息，请参阅 Amazon S3 错误响应的账单计费。 | 2024 年 8 月 19 日 |
| 不再向新客户提供 Amazon S3 Select | 不再向新客户提供 Amazon S3 Select。Amazon S3 Select 的现有客户可以像往常一样继续使用该功能。了解更多。 | 2024 年 7 月 25 日 |
| Amazon S3 清单支持 s3:InventoryAccessibleOptionalFields 条件键 | Amazon S3 清单支持 s3:InventoryAccessibleOptionalFields 条件键，以便控制用户能否在其报告中包含可选的元数据字段。有关更多信息，请参阅控制 S3 清单报告配置创建。 | 2024 年 2 月 20 日 |
| S3 on Outposts 的 IPv6 支持 | 现在，可以通过 S3 on Outposts 双堆栈端点，使用 IPv6 访问 S3 on Outposts 桶。S3 on Outposts 的 IPv6 支持可让您通过 IPv6 网络管理 S3 on Outposts 桶和控制面板资源。 | 2024 年 1 月 16 日 |
| 全新的高性能、单区 Amazon S3 存储类 – S3 Express One Zone | Amazon S3 Express One Zone 是高性能的单区 Amazon S3 存储类，专门用于为延迟要求极高的应用程序提供稳定的毫秒级数据访问。有关更多信息，请参阅 S3 Express One Zone。 | 2023 年 11 月 28 日 |

| | | |
|---|---|---|
| 适用于 Amazon S3 的 Mountpoint 增加了对 S3 Express One Zone 的支持 | 现在可以使用 Mountpoint 挂载 S3 Express One Zone 目录存储桶。 | 2023 年 11 月 28 日 |
| Lambda 调用架构版本 | Amazon S3 批量操作引入了新的 Lambda 调用架构版本，用于对目录存储桶执行的批量操作作业。有关更多信息，请参阅将 Lambda 和 Amazon S3 批量操作用于目录存储桶。 | 2023 年 11 月 28 日 |
| 目录存储桶的导入操作 | Amazon S3 引入了导入操作。导入是一种创建 Amazon S3 批量操作作业的简化方法，用于将对象从通用存储桶复制到目录存储桶。有关更多信息，请参阅将对象导入到目录存储桶。 | 2023 年 11 月 28 日 |
| 使用 S3 Access Grants 管理 S3 访问权限 | Amazon S3 Access Grants 使您能够大规模地管理 Amazon Identity and Access Management（IAM）主体的数据权限，以及来自企业目录（如 Azure AD）的目录标识。现在，您可以强制执行最低权限的 S3 权限，并根据业务需求轻松扩展这些权限。有关更多信息，请参阅使用 S3 Access Grants 管理访问权限。 | 2023 年 11 月 26 日 |
| 适用于 Amazon S3 的 Mountpoint 增加了缓存功能 | 借助 Mountpoint，您现在可以为重复访问的数据配置缓存。 | 2023 年 11 月 22 日 |

| | | |
|---|---|---|
| 增强 Amazon S3 批量操作清单生成 | 现在，您可以指示 Amazon S3 批量操作根据创建作业时指定的对象筛选条件自动生成清单。此选项适用于您在 Amazon S3 控制台中创建的批量复制任务，也适用于您使用 Amazon CLI、Amazon SDK 或 Amazon S3 REST API 创建的任何任务类型。有关更多信息，请参阅创建 Amazon S3 批量操作作业。 | 2023 年 11 月 22 日 |
| 现有的 Amazon S3 存储桶现在可以添加对象锁定配置 | 现在，您可以对现有的 Amazon S3 存储桶启用对象锁定。您可以为新的或现有的存储桶设置依法持有和保留期。有关更多信息，请参阅使用对象锁定。 | 2023 年 11 月 20 日 |
| S3 Storage Lens 存储统计管理工具前缀请求指标 | S3 Storage Lens 存储统计管理工具在 Amazon S3 存储桶中引入了前缀请求指标。有关更多信息，请参阅指标类别。 | 2023 年 11 月 17 日 |
| Amazon S3 Storage Lens 存储统计管理工具组 | S3 Storage Lens 存储统计管理工具引入了 Storage Lens 组，这是一种基于对象元数据的自定义对象筛选条件。有关更多信息，请参阅 Working with Amazon S3 Storage Lens groups。 | 2023 年 11 月 15 日 |

| | | |
|---|---|---|
| 新的 IAM 策略 | S3 on Outposts 引入了 AWSServiceRoleForS3OnOutposts ，这是一个服务相关角色，可帮助您管理网络资源。有关更多信息，请参阅使用面向 S3 on Outposts 的服务相关角色。 | 2023 年 10 月 3 日 |
| Amazon S3 提供了删除标记的 Last-Modified 时间 | Amazon S3 在 S3 Head 和 Get API 操作的响应标头中提供了删除标记的 Last-Modified 时间。有关更多信息，请参阅使用删除标记。 | 2023 年 9 月 27 日 |
| Amazon 托管式策略的 Amazon S3 更新 | Amazon S3 向 AmazonS3ReadOnlyAccess 添加了 s3:Describe* 权限。有关更多信息，请参阅 Amazon S3 的 Amazon 托管式策略。 | 2023 年 8 月 11 日 |
| 缩短了通过 S3 批量操作发出的标准还原请求的启动时间 | 现在，通过 S3 批量操作发出的还原请求的标准检索可以在几分钟内启动。有关更多信息，请参阅归档检索选项。 | 2023 年 8 月 9 日 |
| 添加了 Mountpoint，这是一款用于将 Amazon S3 存储桶作为本地文件系统挂载的高吞吐量客户端。 | 借助 Mountpoint，您的应用程序可以通过文件操作访问存储在 Amazon S3 中的对象，同时使您的应用程序能够通过文件接口访问 Amazon S3 的弹性存储和吞吐量。 | 2023 年 8 月 9 日 |

| | | |
|---|---|---|
| 具有 Amazon Key Management Service 密钥的双层服务器端加密（DSSE-KMS） | 在将对象上传到 Amazon S3 时，具有 Amazon Key Management Service（Amazon KMS）密钥的双层服务器端加密（DSSE-KMS）将会对于对象应用两层加密。有关更多信息，请参阅使用具有 Amazon KMS 密钥的双层服务器端加密。 | 2023 年 6 月 13 日 |
| Amazon S3 为所有新存储桶启用 S3 屏蔽公共访问权限并禁用 S3 访问控制列表（ACL）。 | Amazon S3 现在会自动启用 S3 屏蔽公共访问权限，并对所有 Amazon 区域中的所有新 S3 存储桶禁用 S3 访问控制列表（ACL）。有关更多信息，请参阅屏蔽 Amazon S3 存储的公共访问权限和控制对象所有权和禁用存储桶的 ACL。 | 2023 年 4 月 27 日 |
| S3 复制操作失败指标 | Amazon S3 添加了新的 Amazon CloudWatch 指标来监控 S3 复制失败。有关更多信息，请参阅使用复制指标监控进度。 | 2023 年 4 月 5 日 |
| 私有 DNS | 适用于 Amazon S3 的 Amazon PrivateLink 现在支持私有 DNS。有关更多信息，请参阅私有 DNS。 | 2023 年 3 月 14 日 |
| Amazon S3 控制台中的跨账户接入点支持 | Amazon S3 现在支持使用 Amazon S3 控制台创建跨账户接入点。有关更多信息，请参阅创建接入点。 | 2023 年 3 月 14 日 |

| | | |
|---|---|---|
| Amazon S3 on Outposts 支持 Outposts 上的 S3 复制 | 使用本地 S3 复制，您可以自动将对象复制到单个 Outposts 目标存储桶或多个目标存储桶。目标存储桶可以位于不同的 Amazon Outposts，也可以与源存储桶位于同一 Outposts 中。有关更多信息，请参阅复制 S3 on Outposts 的对象。 | 2023 年 3 月 14 日 |
| Amazon S3 对象 Lambda 接入点别名 | 当您创建对象 Lambda 接入点时，Amazon S3 会自动为您的对象 Lambda 接入点生成一个唯一的别名。您可以在接入点数据面板操作请求中使用此别名，而不使用 Amazon S3 存储桶名称或对象 Lambda 接入点 Amazon 资源名称（ARN）。有关更多信息，请参阅如何为您的对象 Lambda 接入点使用存储桶式别名。 | 2023 年 3 月 14 日 |
| Amazon S3 多区域接入点跨账户支持 | Amazon S3 现在支持使用 Amazon S3 控制台创建跨账户多区域接入点。有关更多信息，请参阅创建多区域接入点。 | 2023 年 3 月 14 日 |
| 跨账户接入点 | Amazon S3 支持创建跨账户接入点。您可以使用 Amazon Command Line Interface（Amazon CLI）或 REST API `CreateAccessPoint` 操作创建跨账户接入点。有关更多信息，请参阅创建接入点。 | 2022 年 11 月 30 日 |

| | | |
|---|---|---|
| Amazon S3 支持对 Amazon S3 多区域接入点进行失效转移控制 | Amazon S3 为多区域接入点引入了失效转移控制。这些控制措施允许您在几分钟内将通过 Amazon S3 多区域接入点路由的 S3 数据访问请求流量转移到备用 Amazon Web Services 区域，以测试和构建高可用性应用程序。有关更多信息，请参阅 Amazon S3 多区域接入点失效转移控制。 | 2022 年 11 月 28 日 |
| Amazon S3 Storage Lens 存储统计管理工具通过 34 个新指标提高了整个组织的可见性 | S3 Storage Lens 存储统计管理工具引入了 34 个附加指标，以发现更深的成本优化机会，确定数据保护最佳实践，并提高应用程序工作流的性能。有关更多信息，请参阅 S3 Storage Lens 存储统计管理工具指标。 | 2022 年 11 月 17 日 |
| Amazon S3 对于 S3 Glacier Flexible Retrieval 和 S3 Glacir Deep Archive 支持更高的还原请求速率 | 对于 S3 Glacier Flexible Retrieval 和 S3 Glacier Deep Archive 存储类，Amazon S3 支持以每个 Amazon Web Services 账户每秒最多 1000 个事务的速率发出还原请求。 | 2022 年 11 月 15 日 |
| Amazon S3 on Outposts 支持其他 S3 生命周期操作和筛选条件 | S3 on Outposts 支持其他 S3 生命周期规则，以优化容量管理。您可以随着对象的老化而使它们过期，也可以将其替换为较新的版本。通过使用前缀、对象标签或对象大小进行筛选，可以为整个存储桶或存储桶中的对象子集创建生命周期规则。有关更多信息，请参阅创建和管理生命周期配置。 | 2022 年 11 月 2 日 |

| | | |
|---|---|---|
| 对 SSE-C 对象的 S3 复制支持 | 您可以复制使用具有客户提供的加密密钥的服务器端加密创建的对象。有关复制加密对象的更多信息，请参阅复制使用服务器端加密（SSE-C、SSE-S3、SSE-KMS）创建的对象。 | 2022 年 10 月 24 日 |
| Amazon S3 on Outposts 支持接入点别名 | 对于 S3 on Outposts，您必须使用接入点访问 Outposts 存储桶中的任何对象。每次您为存储桶创建接入点时，S3 on Outposts 都会自动生成一个接入点别名。对于任何数据面板操作，您都可以使用此接入点别名，而不是接入点 ARN。有关更多信息，请参阅为 S3 on Outposts 存储桶接入点使用存储桶式别名。 | 2022 年 10 月 21 日 |
| S3 对象 Lambda 支持 `HeadObject` 、`ListObjects` 和 `ListObjectsV2` 操作 | 您可以使用自定义代码修改标准 S3 `GET`、`LIST` 或 `HEAD` 请求返回的数据，以便执行筛选行、动态调整图像大小、隐去机密数据等操作。有关更多信息，请参阅使用 S3 对象 Lambda 转换对象。 | 2022 年 10 月 4 日 |

| | | |
|---|---|---|
| Amazon S3 on Outposts 支持 S3 版本控制 | 启用后，S3 版本控制功能将对象的多个不同副本保存到同一个存储桶中。对于 Outpost 桶中存储的每个对象，您可以使用 S3 版本控制功能来保留、检索和还原其每个版本。S3 版本控制功能可帮助您从用户意外操作和应用程序故障中恢复。有关更多信息，请参阅为 S3 on Outposts 存储桶管理 S3 版本控制。 | 2022 年 9 月 21 日 |
| 适用于 Amazon S3 的 Amazon Backup | Amazon Backup 是一种完全托管式的、基于策略的服务，您可以使用它来定义中央备份策略，以保护您的 Amazon S3 数据。有关更多信息，请参阅对 Amazon S3 使用 Amazon Backup。 | 2022 年 2 月 18 日 |
| 使用 S3 分批复制以复制现有对象 | 使用 S3 分批复制，您可以复制在实施复制配置之前就已存在的对象。复制现有对象是通过使用批量操作任务完成的。S3 分批复制与实时复制不同，后者连续自动跨 Amazon S3 存储桶复制新对象。有关更多信息，请参阅使用 S3 批量复制来复制现有对象。 | 2022 年 2 月 8 日 |
| 重命名 S3 Glacier Flexible Retrieval | Glacier 存储类已重命名为 S3 Glacier Flexible Retrieval。此更改不影响 API。 | 2021 年 11 月 30 日 |

| | | |
|---|---|---|
| 用于禁用 ACL 的新 S3 对象所有权设置 | 您可以应用对象拥有权的强制存储桶拥有者设置，以对存储桶及其中的对象禁用 ACL，并获取存储桶中每个对象的拥有权。强制存储桶拥有者设置简化了对存储在 Amazon S3 中的数据的访问管理。有关更多信息，请参阅 Controlling ownership of objects and disabling ACLs for your bucket（为您的存储桶控制对象所有权和禁用 ACL）。 | 2021 年 11 月 30 日 |
| 新建 S3 Intelligent-Tiering 存储类 | S3 Intelligent-Tiering 归档即时访问是 S3 Intelligent-Tiering 下的额外存储类。有关更多信息，请参阅 S3 Intelligent-Tiering 的工作原理。 | 2021 年 11 月 30 日 |
| 新的 S3 Glacier 即时检索存储类 | 您现在可以将对象放在 S3 Glacier 即时检索存储类中。有关此存储类的更多信息，请参阅使用 Amazon S3 存储类。 | 2021 年 11 月 30 日 |
| 适用于 Amazon S3 的 Amazon Backup 预览版 | Amazon Backup 是一种完全托管式的、基于策略的服务，您可以使用它来定义中央备份策略，以保护您的 Amazon S3 数据。有关更多信息，请参阅对 Amazon S3 使用 Amazon Backup。 | 2021 年 11 月 30 日 |

| | | |
|---|---|---|
| 适用于 Amazon S3 的 Amazon Identity and Access Management Access Analyzer | IAM Access Analyzer 将根据 IAM 策略语法和最佳实践运行策略检查，以验证您的策略。要了解有关使用 IAM Access Analyzer 验证策略的更多信息，请参阅《IAM 用户指南》中的 IAM Access Analyzer 策略验证。 | 2021 年 11 月 30 日 |
| 新事件类型 | Amazon S3 事件通知添加了新事件类型，请参阅 Amazon S3 Event Notifications（Amazon S3 事件通知）。 | 2021 年 11 月 29 日 |
| 在存储桶上启用 Amazon EventBridge | 您可以在 Amazon S3 存储桶上启用 EventBridge 以将事件发送到 Amazon EventBridge，请参阅使用 EventBridge。 | 2021 年 11 月 29 日 |
| 新 S3 生命周期筛选器 | 您可以根据对象大小创建生命周期规则，也可以指定要保留多少个非当前对象版本。有关更多信息，请参阅 S3 生命周期配置示例。 | 2021 年 11 月 23 日 |

| | | |
|---|---|---|
| 将 Amazon S3 Storage Lens 存储统计管理工具指标发布到 Amazon CloudWatch | 您可以将 S3 Storage Lens 存储统计管理工具使用情况和活动指标发布到 Amazon CloudWatch，以便在 CloudWatch 控制面板中创建运营状况的统一视图。您还可以使用 CloudWatch 特征（如警报和触发操作、指标数学和异常检测）来监控 S3 Storage Lens 存储统计管理工具指标并采取措施。此外，CloudWatch API 使应用程序（包括第三方提供商）能够访问 S3 Storage Lens 存储统计管理工具指标。有关更多信息，请参阅 Monitor S3 Storage Lens metrics in CloudWatch（在 CloudWatch 中监控 S3 Storage Lens 存储统计管理工具指标）。 | 2021 年 11 月 22 日 |
| 多区域接入点 | 您可以使用多区域接入点创建全局端点，应用程序可以使用该端点来满足来自位于多个 Amazon Web Services 区域的 Amazon S3 存储桶的请求。您可以使用此多区域接入点将数据路由到具有最低延迟的存储桶。有关多区域接入点及其使用方法的更多信息，请参阅 Amazon S3 中的多区域接入点。 | 2021 年 9 月 2 日 |

| | | |
|---|---|---|
| Amazon S3 on Outposts 为应用程序添加直接本地访问 | 从 Amazon Outposts Virtual Private Cloud（VPC）外部运行应用程序，并访问 S3 on Outposts 数据。您还可以直接从您的本地网络访问 S3 on Outposts 对象。有关使用客户拥有的 IP（CoIP）地址配置 S3 on Outposts 端点，以及通过从本地网络创建本地网关访问对象的详细信息，请参阅使用仅限 VPC 接入点访问 Amazon S3 on Outposts。 | 2021 年 7 月 29 日 |
| Amazon S3 接入点别名 | 当您创建接入点时，Amazon S3 会自动生成一个别名。您可以使用该别名来替代存储桶名称以进行数据访问。对于任何接入点数据层面操作，您都可以使用此接入点别名而不是 Amazon Resource Name（ARN）。有关更多信息，请参阅为您的接入点使用存储桶式别名。 | 2021 年 7 月 26 日 |
| Amazon S3 清单和 S3 批量操作支持 S3 存储桶密钥状态 | Amazon S3 清单和批量操作支持使用 S3 存储桶密钥识别和复制现有对象。S3 存储桶密钥可加快降低对现有对象进行服务器端加密的成本。有关更多信息，请参阅 Amazon S3 清单和批量操作复制对象。 | 2021 年 6 月 3 日 |

| | | |
|---|---|---|
| Amazon S3 Storage Lens 存储统计管理工具指标账户快照 | S3 Storage Lens 存储统计管理工具账户快照通过总结默认控制面板中的指标，在 S3 控制台主页（存储桶）上显示您的总存储空间、对象计数和平均对象大小。有关更多信息，请参阅 S3 Storage Lens 存储统计管理工具指标账户快照。 | 2021 年 5 月 5 日 |
| 增加了 Amazon S3 on Outposts 端点支持 | S3 on Outposts 现在支持在每个 Outposts 多达 100 个端点。有关更多信息，请参阅 S3 on Outposts 网络限制。 | 2021 年 4 月 29 日 |
| Amazon CloudWatch Events 中的 Amazon S3 on Outposts 事件通知 | 您现在可以使用 CloudWatch Events 捕获任意 S3 on Outposts API 事件，并通过所有受支持的 CloudWatch 目标获取通知。有关更多信息，请参阅使用 CloudWatch Events 接收 S3 on Outposts 事件通知。 | 2021 年 4 月 19 日 |
| S3 对象 Lambda | 借助 S3 对象 Lambda，您可以将自己的代码添加到 Amazon S3 GET 请求中，以便在数据返回到应用程序时修改和处理数据。您可以使用自定义代码来修改标准 S3 GET 请求返回的数据，以便执行筛选行、动态调整图像大小、隐去机密数据等操作。有关更多信息，请参阅转换对象。 | 2021 年 3 月 18 日 |

| | | |
|---|---|---|
| Amazon PrivateLink | 借助适用于 Amazon S3 的 Amazon PrivateLink，您可以使用虚拟私有云（VPC）中的接口端点直接连接到 S3，而不是通过互联网进行连接。接口端点可从本地或其他 Amazon Web Services 区域中的应用程序直接访问。有关更多信息，请参阅适用于 Amazon S3 的 Amazon PrivateLink。 | 2021 年 2 月 2 日 |
| 使用 Amazon CloudTrail 管理 Amazon S3 on Outposts 容量 | S3 on Outposts 管理事件可通过 CloudTrail 日志提供。有关更多信息，请参阅使用 CloudTrail 管理 S3 on Outposts 容量。 | 2020 年 12 月 21 日 |
| 强一致性 | Amazon S3 为针对所有 PUT的 S3 存储桶中对象的 DELETE 和 Amazon Web Services 区域 请求提供了强大的先写后读一致性。此外，针对 Amazon S3 Select、Amazon S3 访问控制列表、Amazon S3 对象标签和对象元数据（例如 HEAD 对象）的读取操作具有严格的一致性。有关更多信息，请参阅 Amazon S3 数据一致性模型。 | 2020 年 12 月 1 日 |
| Amazon S3 副本修改同步 | Amazon S3 副本修改同步使对象元数据（如标签、ACL 和对象锁定设置）在源对象和副本之间保持同步。启用此特征后，Amazon S3 会复制对源对象或副本所做的元数据更改。有关更多信息，请参阅使用副本修改同步复制元数据更改。 | 2020 年 12 月 1 日 |

| | | |
|---|---|---|
| Amazon S3 存储桶密钥 | Amazon S3 存储桶密钥降低了具有 Amazon Key Management Service 的 Amazon S3 服务器端加密（SSE-KMS）的成本。这一用于服务器端加密的存储桶级别密钥通过减少从 Amazon S3 到 Amazon KMS 的请求流量，将 Amazon KMS 请求成本降低多达 99%。有关更多信息，请参阅使用 S3 存储桶密钥降低 SSE-KMS 的成本。 | 2020 年 12 月 1 日 |
| Amazon S3 Storage Lens 存储统计管理工具 | S3 Storage Lens 存储统计管理工具聚合您的指标，并在 Amazon S3 控制台的 Buckets（存储桶）页上的 Account snapshot（账户快照）部分中显示此信息。S3 Storage Lens 存储统计管理工具还提供了一个交互式控制面板，您可以使用它来可视化见解和趋势，标记异常值，并接收有关优化存储成本和应用数据保护最佳实践的建议。控制面板提供深入分析选项，用于在组织、账户、Amazon Web Services 区域、存储类、存储桶、前缀或 Storage Lens 组级别生成和可视化见解。您还可以将采用 CSV 或 Parquet 格式的每日指标导出发送到 S3 存储桶。有关更多信息，请参阅使用 S3 Storage Lens 存储统计管理工具访问存储活动和使用情况。 | 2020 年 11 月 18 日 |

| | | |
|---|---|---|
| 使用 Amazon X-Ray 跟踪 S3 请求 | Amazon S3 与 X-Ray 集成，以传播跟踪上下文，并为您提供一个带有上游和下游节点的请求链。有关更多信息，请参阅使用 X-Ray 跟踪请求。 | 2020 年 11 月 16 日 |
| S3 复制指标 | S3 复制指标为复制配置中的复制规则提供了详细的指标。有关更多信息，请参阅复制指标和 Amazon S3 事件通知。 | 2020 年 11 月 9 日 |
| S3 Intelligent-Tiering 存档访问和深度存档访问 | S3 Intelligent-Tiering 存档访问和深度存档访问是 S3 Intelligent-Tiering 下的额外存储层。有关更多信息，请参阅可自动优化经常访问和不常访问对象的存储类。 | 2020 年 11 月 9 日 |
| 删除标记复制 | 通过删除标记复制，您可以确保将删除标记复制到复制规则的目标存储桶中。有关更多信息，请参阅使用删除标记复制。 | 2020 年 11 月 9 日 |
| S3 对象所有权 | 对象所有权是一个 S3 存储桶设置，您可以使用它来控制上传到存储桶的新对象的所有权。有关更多信息，请参阅使用 S3 对象所有权。 | 2020 年 10 月 2 日 |

| | | |
|---|---|---|
| Amazon S3 on Outposts | 通过使用 Amazon S3 on Outposts，您可以在 Amazon Outposts 资源上创建 S3 存储桶，并在本地为需要本地数据访问、本地数据处理和数据驻留的应用程序轻松地存储和检索对象。您可以通过 Amazon Web Services Management Console、Amazon CLI、Amazon SDK 或 REST API 使用 S3 on Outposts。有关更多信息，请参阅使用 Amazon S3 on Outposts。 | 2020 年 9 月 30 日 |
| 存储桶拥有者条件 | 您可以使用 Amazon S3 存储桶拥有者条件来确保您在 S3 操作中使用的存储桶属于您期望的 Amazon Web Services 账户。有关更多信息，请参阅存储桶拥有者条件。 | 2020 年 9 月 11 日 |
| S3 批量操作支持对象锁定保留 | 现在，您可以将批量操作与 S3 对象锁定一起使用，以便同时对许多 Amazon S3 对象应用保留设置。有关更多信息，请参阅使用 S3 批量操作设置 S3 对象锁定保留日期。 | 2020 年 5 月 4 日 |
| S3 批量操作支持对象锁定依法保留 | 现在，您可以将批量操作与 S3 对象锁定一起使用，以便同时为许多 Amazon S3 对象添加依法保留。有关更多信息，请参阅使用 S3 批量操作设置 S3 对象锁定依法保留。 | 2020 年 5 月 4 日 |

| | | |
|---|---|---|
| S3 批量操作的任务标签 | 您可以向 S3 批量操作作业添加标签以控制和标记这些作业。有关更多信息，请参阅 S3 批量操作任务的标签。 | 2020 年 3 月 16 日 |
| Amazon S3 接入点 | Amazon S3 接入点可简化对 S3 中的共享数据集的大规模数据访问管理。接入点是附加到存储桶的具名网络端点，您可以使用这些存储桶执行 S3 对象操作。有关更多信息，请参阅使用 Amazon S3 接入点管理数据访问。 | 2019 年 12 月 2 日 |
| Amazon S3 的访问分析器 | 如果存在已配置为允许 Internet 上的任何人或其他 Amazon Web Services 账户（包括组织外部的账户）访问的 S3 存储桶，Amazon S3 访问分析器会向您发出提醒。有关更多信息，请参阅使用 Amazon S3 的访问分析器。 | 2019 年 12 月 2 日 |
| S3 复制时间控制 (S3 RTC) | S3 复制时间控制 (S3 RTC) 可以在几秒钟内复制您上传到 Amazon S3 的大部分对象，其中 99.99% 的对象会在 15 分钟内完成复制。有关更多信息，请参阅使用 S3 Replication Time Control（S3 RTC）复制对象。 | 2019 年 11 月 20 日 |

| | | |
|---|---|---|
| 同区域复制 | 可以使用同区域复制（SRR）在同一 Amazon Web Services 区域中跨 Amazon S3 存储桶复制对象。有关跨区域复制（CRR）和同区域复制的信息，请参阅复制。 | 2019 年 9 月 18 日 |
| S3 对象锁定的跨区域复制支持 | 跨区域复制现在支持对象锁定。有关更多信息，请参阅 Amazon S3 会复制什么？ | 2019 年 5 月 28 日 |
| S3 批量操作 | 使用 S3 批量操作，您可以对 Amazon S3 对象执行大规模批量操作。S3 批量操作可以对您指定的对象列表运行单个操作。单个作业可对包含 EB 级数据的数十亿个对象执行指定操作。有关更多信息，请参阅执行 S3 批处理操作。 | 2019 年 4 月 30 日 |
| 亚太地区（香港）区域 | Amazon S3 现已在亚太地区（香港）区域中提供。有关 Amazon S3 区域和端点的更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。 | 2019 年 4 月 24 日 |
| 向服务器访问日志添加了新字段 | Amazon S3 向服务器访问日志添加了以下新字段：传输层安全性 (TLS) 版本。有关更多信息，请参阅服务器访问日志格式。 | 2019 年 3 月 28 日 |

| | | |
|---|---|---|
| 新归档存储类 | Amazon S3 现在提供了用于存储极少访问的对象的新归档存储类 S3 Glacier Deep Archive（DEEP_ARCHIVE ）。有关更多信息，请参阅存储类。 | 2019 年 3 月 27 日 |
| 向服务器访问日志添加了新字段 | Amazon S3 向服务器访问日志添加了以下新字段：主机 ID、签名版本、密码包、身份验证类型和主机标头。有关更多信息，请参阅服务器访问日志格式。 | 2019 年 3 月 5 日 |
| 支持 Parquet 格式的 Amazon S3 清单文件 | 除了 Apache optimized row columnar（ORC）和逗号分离值（CSV）文件格式之外，Amazon S3 现在还支持 Apache Parquet（Parquet）格式。有关更多信息，请参阅清单。 | 2018 年 12 月 4 日 |
| S3 对象锁定 | Amazon S3 现在提供可为 Amazon S3 对象提供一次写入、多次读取（WORM）保护的对象锁定功能。有关更多信息，请参阅锁定对象。 | 2018 年 11 月 26 日 |
| 还原速度升级 | 使用 Amazon S3 还原速度升级，您可以在从 S3 Glacier Flexible Retrieval 存储类进行还原的过程中将该还原的速度更改为更快的速度。有关更多信息，请参阅还原归档对象。 | 2018 年 11 月 26 日 |

| | | |
|---|---|---|
| 还原事件通知 | 现在，Amazon S3 事件通知支持在从 S3 Glacier Flexible Retrieval 存储类还原对象时的启动和完成事件。有关更多信息，请参阅事件通知。 | 2018 年 11 月 26 日 |
| 直接对 S3 Glacier Flexible Retrieval 存储类执行 PUT 操作 | 现在，Amazon S3 PUT 操作支持在创建对象时将 S3 Glacier Flexible Retrieval 指定为存储类。以前，您必须将对象从其他 Amazon S3 存储类转换为 S3 Glacier Flexible Retrieval 存储类。而且，在使用 S3 跨区域复制 (CRR) 时，现在您可以将 S3 Glacier Flexible Retrieval 指定为已复制对象的存储类。有关 S3 Glacier Flexible Retrieval 存储类的更多信息，请参阅存储类。有关为已复制的对象指定存储类的更多信息，请参阅复制配置概述。有关直接对 S3 Glacier Flexible Retrieval REST API 执行 PUT 操作这一更改的更多信息，请参阅文档历史记录：直接对 S3 Glacier Flexible Retrieval 执行 PUT 操作。 | 2018 年 11 月 26 日 |
| 新存储类 | Amazon S3 现在提供一种名为 S3 Intelligent-Tiering（`INTELLIGENT_TIERING`）的新存储类，这是专为不断变化或访问模式未知的长期数据设计的。有关更多信息，请参阅存储类。 | 2018 年 11 月 26 日 |

| | | |
|---|---|---|
| Amazon S3 屏蔽公共访问权限 | Amazon S3 现在包含按存储桶或账户对存储桶和对象屏蔽公共访问权限的功能。有关更多信息，请参阅使用 Amazon S3 屏蔽公共访问权限。 | 2018 年 11 月 15 日 |
| 跨区域复制 (CRR) 规则中的筛选增强功能 | 在 CRR 规则配置中，您可以指定对象筛选条件以选择要将向其应用规则的对象子级。以前，您只能按对象键前缀进行筛选。在本版本中，您可以按对象键前缀和/或一个或多个对象标签进行筛选。有关更多信息，请参阅 CRR 设置：复制配置概述。 | 2018 年 9 月 19 日 |
| 新的 Amazon S3 Select 特征 | Amazon S3 Select 现在支持 Apache Parquet 输入、对嵌套 JSON 对象的查询以及两个新的 Amazon CloudWatch 监控指标（`SelectScannedBytes` 和 `SelectReturnedBytes`）。 | 2018 年 9 月 5 日 |
| 现在可通过 RSS 更新 | 您现在可以订阅 RSS 源来接收有关《Amazon S3 用户指南》更新的通知。 | 2018 年 19 月 6 日 |

# 早期更新

下表描述了 2018 年 6 月 19 日之前每次发布 Amazon S3 用户指南时进行的重要更改。

| 更改 | 描述 | 日期 |
|---|---|---|
| 代码示例更新 | 更新了代码示例：<br>• | 2018 年 4 月 30 日 |

| 更改 | 描述 | 日期 |
| --- | --- | --- |
| | C# — 已将所有示例更新为使用基于任务的异步模式。有关更多信息，请参阅《适用于 .NET 的 Amazon SDK 开发人员指南》中的适用于 .NET 的 Amazon Web Services 异步 API。代码示例现在符合版本 3 的 适用于 .NET 的 Amazon SDK 的要求。<br>• Java — 已将所有示例更新为使用客户端生成器模型。有关客户端生成器模型的更多信息，请参阅创建服务客户端。<br>• PHP – 已将所有示例更新为使用 适用于 PHP 的 Amazon SDK 3.0。有关 适用于 PHP 的 Amazon SDK 3.0 的更多信息，请参阅 适用于 PHP 的 Amazon SDK。<br>• Ruby – 已更新示例代码，以便示例可以与 适用于 Ruby 的 Amazon SDK 版本 3 结合使用。 | |

| 更改 | 描述 | 日期 |
| --- | --- | --- |
| Amazon S3 现在将 S3 Glacier Flexible Retrieval 和 ONEZONE_IA 存储类报告给 Amazon CloudWatch Logs 存储指标 | 除了报告实际字节数之外，这些存储指标还包含合适的存储类（ONEZONE_IA 、STANDARD_IA 和 S3 Glacier Flexible Retrieval）的每对象开销字节数：<br>• 对于 ONEZONE_IA 和 STANDARD_IA 存储类对象，Amazon S3 将小于 128 KB 的对象报告为 128 KB。有关更多信息，请参阅 了解和管理 Amazon S3 存储类。<br>• 对于 S3 Glacier Flexible Retrieval 存储类对象，存储指标将报告以下开销：<br>  • 一个 32 KB 每对象开销，按 S3 Glacier Flexible Retrieval 存储类定价收费<br>  • 8KB 每对象开销，按 STANDARD 存储类定价收费<br>  有关更多信息，请参阅 使用 Amazon S3 生命周期转换对象。<br><br>有关存储指标的更多信息，请参阅 使用 Amazon CloudWatch 监控指标。 | 2018 年 30 月 4 日 |
| 新存储类 | Amazon S3 现在提供了用于存储对象的新存储类 STANDARD_IA （IA，适用于不频繁访问）。此存储类已针对长时间运行且不常访问的数据进行了优化。有关更多信息，请参阅 了解和管理 Amazon S3 存储类。 | 2018 年 4 月 4 日 |
| Amazon S3 Select | Amazon S3 现在支持根据 SQL 表达式检索对象内容。有关更多信息，请参阅 使用 Amazon S3 Select 就地查询数据。 | 2018 年 4 月 4 日 |

| 更改 | 描述 | 日期 |
| --- | --- | --- |
| 亚太区域 (大阪当地) | Amazon S3 现已在亚太地区（大阪本地）区域中提供。有关 Amazon S3 区域和端点的更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。<br><br>**Important**<br>您只能与亚太地区（东京）区域结合使用亚太地区（大阪本地）区域。要请求访问亚太地区（大阪本地）区域，请联系您的销售代表。 | 2018 年 2 月 12 日 |
| Amazon S3 清单创建时间戳 | Amazon S3 清单现在包括创建 Amazon S3 清单报告的日期和开始时间的时间戳。您可以使用此时间戳确定开始生成清单报告的时间之后 Amazon S3 存储中的变化。 | 2018 年 1 月 16 日 |
| 欧洲（巴黎）区域 | Amazon S3 现已在欧洲地区（巴黎）区域中提供。有关 Amazon S3 区域和端点的更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。 | 2017 年 12 月 18 日 |
| 中国 (宁夏) 区域 | Amazon S3 现已在中国（宁夏）区域中提供。有关 Amazon S3 区域和端点的更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。 | 2017 年 11 月 29 日 |
| 支持 ORC 格式 Amazon S3 清单文件 | 对于清单输出文件，除了逗号分隔值 (CSV) 文件格式之外，Amazon S3 现在还支持 Apache 优化行列式 (ORC) 格式。此外，现在您可以通过 Amazon Athena、Amazon Redshift Spectrum 以及其他工具（如 Presto、Apache Hive 和 Apache Spark）使用标准 SQL 语言查询 Amazon S3 清单。有关更多信息，请参阅 使用 S3 清单对数据进行编目和分析。 | 2017 年 11 月 17 日 |

| 更改 | 描述 | 日期 |
| --- | --- | --- |
| S3 存储桶的默认加密 | Amazon S3 默认加密提供了一种方法来设置 S3 存储桶的默认加密行为。您可以对存储桶设置默认加密，以便在存储桶中存储所有对象时对这些对象进行加密。这些对象使用具有 Amazon S3 托管式密钥（SSE-S3）或 Amazon 托管式密钥（SSE-KMS）的服务器端加密进行加密。有关更多信息，请参阅 为 Amazon S3 存储桶设置默认服务器端加密行为。 | 2017 年 11 月 06 日 |
| Amazon S3 清单中的加密状态 | Amazon S3 现在的支持包括 Amazon S3 清单中的加密状态，因此您查看对象在静态时如何加密，以用于合规性审计或其他用途。您还可以配置使用服务器端加密 (SSE) 或 SSE-KMS 来加密 Amazon S3 清单，从而相应地加密所有清单文件。有关更多信息，请参阅 使用 S3 清单对数据进行编目和分析。 | 2017 年 11 月 06 日 |
| 跨区域复制 (CRR) 增强功能 | 跨区域复制现在支持以下功能：<br>• 在跨账户方案中，您可以添加 CRR 配置，将副本所有权更改为拥有目标存储桶的 Amazon Web Services 账户。有关更多信息，请参阅 更改副本拥有者。<br>• 默认情况下，Amazon S3 不复制源存储桶中使用具有 Amazon KMS 中存储的密钥的服务器端加密创建的对象。在 CRR 配置中，您现在可以指示 Amazon S3 复制这些对象。有关更多信息，请参阅 复制加密对象（SSE-S3、SSE-KMS、DSSE-KMS、SSE-C）。 | 2017 年 11 月 06 日 |
| 欧洲（伦敦）区域 | Amazon S3 现已在欧洲地区（伦敦）区域中提供。有关 Amazon S3 区域和端点的更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。 | 2016 年 12 月 13 日 |
| 加拿大 (中部) 区域 | Amazon S3 现已在加拿大（中部）区域中提供。有关 Amazon S3 区域和端点的更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。 | 2016 年 12 月 8 日 |

| 更改 | 描述 | 日期 |
| --- | --- | --- |
| 对象标签 | Amazon S3 现在支持对象标签。利用对象标签，您可以对存储进行分类。对象键名前缀还可让您对存储进行分类，对象标签将向其添加另一个维度。<br><br>添加标签还可提供其他好处。包括：<br><br>• 对象标签支持权限的精细访问控制 (例如，您可以向 IAM 用户授予对具有特定标签的只读对象的权限)。<br>• 指定生命周期配置时的精细控制。您可以指定标签以选择生命周期规则应用于的对象子集。<br>• 如果您已配置跨区域复制 (CRR)，则 Amazon S3 可以复制标签。您必须向为 Amazon S3 创建且要代入的 IAM 角色授予代表您复制对象的权限。<br>• 您还可以自定义 CloudWatch 指标和 CloudTrail 事件，以便按特定标签筛选条件显示信息。<br><br>有关更多信息，请参阅 使用标签对存储进行分类。 | 2016 年 11 月 29 日 |
| Amazon S3 生命周期现在支持基于标签的筛选 | Amazon S3 现在支持生命周期配置中基于标签的筛选。您现在可以指定生命周期规则，在该规则下，您可以指定键前缀、一个或多个对象标签或二者的组合以选择生命周期规则将应用于的对象子集。有关更多信息，请参阅 管理对象的生命周期。 | 2016 年 11 月 29 日 |
| 存储桶的 CloudWatch 请求指标 | Amazon S3 现在支持在存储桶上发出的请求的 CloudWatch 指标。当您为存储桶启用这些指标时，指标每分钟报告一次。您还可以配置存储桶中的哪些对象将报告这些请求指标。有关更多信息，请参阅 使用 Amazon CloudWatch 监控指标。 | 2016 年 11 月 29 日 |

| 更改 | 描述 | 日期 |
| --- | --- | --- |
| Amazon S3 清单 | Amazon S3 现在支持存储清单。Amazon S3 清单每天或每周为 S3 存储桶或共享前缀（即，其名称以通用字符串开头的对象）提供对象及其对应元数据的平面文件输出。<br><br>有关更多信息，请参阅 使用 S3 清单对数据进行编目和分析。 | 2016 年 11 月 29 日 |
| Amazon S3 分析 - 存储类分析 | 新的 Amazon S3 分析 - 存储类分析特征可观察数据访问模式以帮助您确定何时将不常访问的 STANDARD 存储转换为 STANDARD_IA （IA 表示不频繁访问）存储类。在存储类分析在一段时间内观察到一组筛选出的数据的不常访问模式后，您可以使用分析结果来帮助改进您的生命周期配置。此特征还包括在指定的存储桶、前缀或标签级别对存储使用情况的详细日常分析，并且您可以将分析结果导出到 S3 存储桶。 | 2016 年 11 月 29 日 |
| 从 S3 Glacier 还原存档对象时新建加速和批量数据检索 | 在将存档对象还原至 S3 Glacier 时，Amazon S3 现在支持加速和批量数据检索以及标准检索。有关更多信息，请参阅恢复已归档的对象。 | 2016 年 11 月 21 日 |
| CloudTrail 对象日志记录 | CloudTrail 支持记录 Amazon S3 对象级别 API 操作，例如 GetObject 、PutObject 和 DeleteObject 。您可以将事件选择器配置为记录对象级别 API 操作。有关更多信息，请参阅 使用 Amazon CloudTrail 记录 Amazon S3 API 调用。 | 2016 年 11 月 21 日 |
| 美国东部（俄亥俄）区域 | Amazon S3 现已在美国东部（俄亥俄州）区域中提供。有关 Amazon S3 区域和端点的更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。 | 2016 年 10 月 17 日 |
| 对 Amazon S3 Transfer Acceleration 的 IPv6 支持 | Amazon S3 现在支持用于 Amazon S3 Transfer Acceleration 的 Internet 协议版本 6 (IPv6)。您可以使用全新的 Transfer Acceleration 双堆栈端点，通过 IPv6 连接到 Amazon S3。有关更多信息，请参阅 开始使用 Amazon S3 Transfer Acceleration。 | 2016 年 10 月 6 日 |

| 更改 | 描述 | 日期 |
| --- | --- | --- |
| IPv6 支持 | Amazon S3 现在支持 Internet 协议版本 6 (IPv6)。您可以使用双堆栈端点，通过 IPv6 访问 Amazon S3。有关更多信息，请参阅《Amazon S3 API 参考》中的 Making requests to Amazon S3 over IPv6。 | 2016 年 8 月 11 日 |
| 亚太地区 (孟买) 区域 | Amazon S3 现已在亚太地区（孟买）区域中提供。有关 Amazon S3 区域和端点的更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。 | 2016 年 6 月 27 日 |
| Amazon S3 Transfer Acceleration | Amazon S3 Transfer Acceleration 可在您的客户端和 S3 存储桶之间实现快速、轻松、安全的远距离文件传输。Transfer Acceleration 利用 Amazon CloudFront 的全球分布式边缘站点。<br><br>有关更多信息，请参阅 使用 Amazon S3 Transfer Acceleration 配置快速、安全的文件传输。 | 2016 年 4 月 19 日 |
| 生命周期支持移除过期对象删除标记 | 生命周期配置 `Expiration` 操作现在允许您指示 Amazon S3 移除受版本控制的存储桶中的过期对象删除标记。有关更多信息，请参阅 用于描述生命周期操作的元素。 | 2016 年 3 月 16 日 |

| 更改 | 描述 | 日期 |
| --- | --- | --- |
| 存储桶生命周期配置现在支持停止未完成的分段上传的操作 | 存储桶生命周期配置现在支持 AbortIncompleteMultipartUpload 操作，您可以使用该操作指示 Amazon S3 停止未在启动后的指定天数内完成的分段上传。当分段上传符合停止操作条件时，Amazon S3 将删除所有已上传的段并停止分段上传。<br><br>有关概念性信息，请参阅 Amazon S3 用户指南中的以下主题：<br><br>• 中止分段上传<br>• 用于描述生命周期操作的元素<br><br>以下 API 操作已更新为支持新操作：<br><br>• PUT 存储桶生命周期 – XML 配置现在允许您在生命周期配置规则中指定 AbortIncompleteMultipartUpload 操作。<br>• 列出段和启动分段上传 – 如果存储桶包含指定 AbortIncompleteMultipartUpload 操作的生命周期规则，则这两个 API 操作现在将返回两个额外的响应标头（x-amz-abort-date 和 x-amz-abort-rule-id ）。响应中的这些标头指示启动的分段上传何时符合停止操作的条件以及适用哪个生命周期规则。 | 2016 年 3 月 16 日 |
| 亚太区域（首尔） | Amazon S3 现已在亚太地区（首尔）区域中提供。有关 Amazon S3 区域和端点的更多信息，请参阅《Amazon Web Services 一般参考》中的区域和端点。 | 2016 年 1 月 6 日 |

| 更改 | 描述 | 日期 |
| --- | --- | --- |
| 新的条件键和分段上传变更 | IAM 策略现在支持 Amazon S3 `s3:x-amz-storage-class` 条件键。有关更多信息，请参阅 使用条件键的存储桶策略示例。<br><br>您不再需要作为分段上传的发起者就能上传分段和完成上传。有关更多信息，请参阅 分段上传 API 和权限。 | 2015 年 12 月 14 日 |
| 重命名美国标准区域 | 区域名称字符串从“美国标准”变更为“美国东部（弗吉尼亚北部）”。此次只更新了区域名称，功能上没有任何变化。 | 2015 年 12 月 11 日 |
| 新存储类 | Amazon S3 现在为存储对象提供了新存储类 STANDARD_IA（IA，适用于不频繁访问）。此存储类已针对长时间运行且不常访问的数据进行了优化。有关更多信息，请参阅 了解和管理 Amazon S3 存储类。<br><br>生命周期配置特征的更新现在可允许您将对象转换为 STANDARD_IA 存储类。有关更多信息，请参阅 管理对象的生命周期。<br><br>以前，跨区域复制特征对对象副本使用源对象的存储类。现在，当您配置跨区域复制时，您可以在目标存储桶中为创建的对象副本指定存储类。有关更多信息，请参阅 在区域内和跨区域复制对象。 | 2015 年 9 月 16 日 |
| Amazon CloudTrail 集成 | 新的 Amazon CloudTrail 集成能够记录您的 S3 存储桶中发生的 Amazon S3 API 活动。您可以使用 CloudTrail 来跟踪 S3 存储桶的创建或删除、访问控制修改或生命周期配置变更。有关更多信息，请参阅 使用 Amazon CloudTrail 记录 Amazon S3 API 调用。 | 2015 年 9 月 1 日 |

| 更改 | 描述 | 日期 |
| --- | --- | --- |
| 存储桶限额提升 | Amazon S3 现在支持存储桶限额提升。默认情况下，客户可在其 Amazon Web Services 账户中创建多达 100 个存储桶。需要更多存储桶的客户可通过提交服务限额提升来调高限制。有关如何提升存储桶限制的信息，请参阅《Amazon 一般参考》中的 Amazon Web Services 服务限额。有关更多信息，请参阅使用 Amazon 软件开发工具包和通用存储桶配额、限制和局限性。 | 2015 年 8 月 4 日 |
| 一致性模型更新 | Amazon S3 现在在美国东部（弗吉尼亚北部）区域对添加到 Amazon S3 的新对象支持先写后读一致性。在此更新之前，除美国东部（弗吉尼亚北部）区域之外的所有区域都对上传到 Amazon S3 的新对象支持先写后读一致性。利用此改进，Amazon S3 现在在所有区域对添加到 Amazon S3 的新对象都支持先写后读一致性。先写后读一致性允许您在 Amazon S3 中创建对象后立即检索对象。有关更多信息，请参阅 区域。 | 2015 年 8 月 4 日 |
| 事件通知 | Amazon S3 事件通知进行了更新，以添加在删除对象时发送的通知并添加通过前缀和后缀匹配进行对象名称筛选的功能。有关更多信息，请参阅 Amazon S3 事件通知。 | 2015 年 7 月 28 日 |
| Amazon CloudWatch 集成 | 借助新的 Amazon CloudWatch 集成，您可以通过适用于 Amazon S3 的 CloudWatch 指标监控和设置有关 Amazon S3 使用情况的警报。支持的指标包含 Standard 存储的总字节数、低冗余存储的总字节数以及给定 S3 存储桶的对象的总数。有关更多信息，请参阅 使用 Amazon CloudWatch 监控指标。 | 2015 年 7 月 28 日 |
| 支持删除和清空非空存储桶 | Amazon S3 现在支持删除和清空非空存储桶。有关更多信息，请参阅 清空通用存储桶。 | 2015 年 7 月 16 日 |

| 更改 | 描述 | 日期 |
| --- | --- | --- |
| Amazon VPC 端点的存储桶策略 | Amazon S3 添加了对 Virtual Private Cloud（VPC）端点的存储桶策略的支持。您可以使用 S3 存储桶策略控制从特定 VPC 端点或特定 VPC 对存储桶的访问。VPC 端点易于配置，高度可靠，并且提供到 Amazon S3 的安全连接而无需网关或 NAT 实例。有关更多信息，请参阅 使用存储桶策略控制从 VPC 端点的访问。 | 2015 年 4 月 29 日 |
| 事件通知 | 已更新 Amazon S3 事件通知，以支持切换到 Amazon Lambda 函数的基于资源的权限。有关更多信息，请参阅 Amazon S3 事件通知。 | 2015 年 4 月 9 日 |
| 跨区域复制 | Amazon S3 现在支持跨区域复制。跨区域复制是跨不同 Amazon Web Services 区域 中的存储桶自动、异步地复制对象。有关更多信息，请参阅 在区域内和跨区域复制对象。 | 2015 年 3 月 24 日 |
| 事件通知 | Amazon S3 现在支持存储桶通知配置中的新事件类型和目标。在此版本之前，Amazon S3 仅支持 s3:ReducedRedundancyLostObject 事件类型和 Amazon SNS 主题作为目标。有关新事件类型的更多信息，请参阅 Amazon S3 事件通知。 | 2014 年 11 月 13 日 |
| 使用客户提供的加密密钥的服务器端加密 | 具有 Amazon Key Management Service（Amazon KMS）密钥的服务器端加密（SSE-KMS）<br><br>Amazon S3 现已支持使用 Amazon KMS 的服务器端加密。此特征允许您通过 Amazon KMS 管理信封密钥，Amazon S3 调用 Amazon KMS 以在您设置的权限范围内访问信封密钥。<br><br>有关使用 Amazon KMS 的服务器端加密的更多信息，请参阅通过使用 Amazon Key Management Service 的服务器端加密保护数据。 | 2014 年 11 月 12 日 |
| 欧洲（法兰克福）区域 | Amazon S3 现已在欧洲（法兰克福）区域中提供。 | 2014 年 10 月 23 日 |

| 更改 | 描述 | 日期 |
| --- | --- | --- |
| 使用客户提供的加密密钥的服务器端加密 | Amazon S3 现在支持使用客户提供的加密密钥的服务器端加密 (SSE-C)。服务器端加密使您能够请求 Amazon S3 加密您的静态数据。在使用 SSE-C 时，Amazon S3 将使用您提供的自定义加密密钥加密您的对象。由于 Amazon S3 会自动执行加密，因此您可以使用自己的加密密钥，而无需编写或执行自己的加密代码。<br><br>有关 SSE-C 的更多信息，请参阅服务器端加密（使用客户提供的加密密钥）。 | 2014 年 6 月 12 日 |
| 版本控制的生命周期支持 | 在此版本之前，仅对不受版本控制的存储桶支持生命周期配置。现在您对不受版本控制和启用了版本控制的存储桶都可以配置生命周期。有关更多信息，请参阅 管理对象的生命周期。 | 2014 年 5 月 20 日 |
| 修订了访问控制主题 | 修订了 Amazon S3 访问控制文档。有关更多信息，请参阅 Amazon S3 的身份和访问管理。 | 2014 年 4 月 15 日 |
| 修订了服务器访问日志记录主题 | 修订了服务器访问日志记录文档。有关更多信息，请参阅 使用服务器访问日志记录来记录请求。 | 2013 年 11 月 26 日 |
| .NET SDK 示例已更新为版本 2.0 | 本指南中的 .NET SDK 示例现在符合版本 2.0 标准。 | 2013 年 11 月 26 日 |
| HTTP 上的 SOAP 支持已弃用 | HTTP 上的 SOAP 支持已弃用，但是仍可在 HTTPS 上使用。不支持将新 Amazon S3 特征用于 SOAP。我们建议您使用 REST API 或 Amazon SDK。 | 2013 年 9 月 20 日 |

| 更改 | 描述 | 日期 |
| --- | --- | --- |
| IAM 策略变量支持 | IAM 策略语言现在支持变量。在评估策略时，任何策略变量都会替换为来自经身份验证的用户会话的上下文相关信息提供的值。您可以使用策略变量来定义通用策略，无需显式列出策略的所有部分。有关策略变量的更多信息，请参阅《IAM 用户指南》中的 IAM 策略变量概述。<br><br>有关 Amazon S3 中策略变量的示例，请参阅Amazon S3 基于身份的策略示例。 | 2013 年 4 月 3 日 |
| 对申请方付款的控制台支持 | 现在，您可以使用 Amazon S3 控制台为申请方付款配置存储段。有关更多信息，请参阅 使用申请方付款通用存储桶进行存储传输和使用。 | 2012 年 12 月 31 日 |
| 对网站托管的根域支持 | Amazon S3 现已支持在根域中托管静态网站。网站访问者在其浏览器中访问网站时，无需在 Web 地址中指定 www（例如，他们可以使用 example.com，而不是 www.example.com）。许多客户已在 Amazon S3 上托管了静态网站，访问者可通过 www 子域（例如 www.example.com）进行访问。此前，要支持根域访问，您必须在运行自己的 Web 服务器时将根域请求从浏览器以代理的方式转至您在 Amazon S3 上的网站。运行 Web 服务器对请求进行代理会导致出现额外成本、运转负荷和其他潜在的故障点。现在，对于 www 和根域地址，您都可以充分利用 Amazon S3 的高可用性和耐用性了。有关更多信息，请参阅 使用 Amazon S3 托管静态网站。 | 2012 年 12 月 27 日 |
| 控制台修改 | 对 Amazon S3 控制台进行了更新。并对与控制台相关的文档主题做出了相应修改。 | 2012 年 12 月 14 日 |

| 更改 | 描述 | 日期 |
| --- | --- | --- |
| 支持将数据存档到 S3 Glacier | Amazon S3 现已支持的存储选项可让您使用 S3 Glacier 的低成本存储服务来归档数据。要将对象归档，您需要定义归档规则来确定对象以及您希望 Amazon S3 据之将这些对象归档到 S3 Glacier 的时间范围。通过使用 Amazon S3 控制台，或以编程方式使用 Amazon S3 API 或 Amazon SDK，您可以轻松地在存储桶上设置规则。<br><br>有关更多信息，请参阅 管理对象的生命周期。 | 2012 年 11 月 13 日 |
| 对网页重定向的支持 | 对于配置为网站的存储段，Amazon S3 现已支持将对象的请求重定向到相同存储段中的另一个对象或外部 URL。有关更多信息，请参阅 （可选）配置网页重定向。<br><br>有关托管网站的信息，请参阅使用 Amazon S3 托管静态网站。 | 2012 年 10 月 4 日 |
| 对跨域资源共享 (CORS) 的支持 | Amazon S3 现已支持跨域资源共享 (CORS) 功能。一个域中加载的客户端 Web 应用程序可借助 CORS 定义的方式与不同域中的资源进行交互，或访问这些资源。借助 Amazon S3 中的 CORS 支持，您可以基于 Amazon S3 构建各种富客户端 Web 应用程序，并选择性地允许跨域访问您的 Amazon S3 资源。有关更多信息，请参阅 使用跨源资源共享 (CORS)。 | 2012 年 8 月 31 日 |
| 对成本分配标记的支持 | Amazon S3 现已支持成本分配标记，这允许您为 S3 存储桶加标签，从而可以更轻松地根据项目或其他条件跟踪其成本。有关将标记用于存储桶的更多信息，请参阅 使用成本分配 S3 存储桶标签。 | 2012 年 8 月 21 日 |

| 更改 | 描述 | 日期 |
| --- | --- | --- |
| 对存储桶策略中受 MFA 保护的 API 访问的支持 | Amazon S3 现已支持受 MFA 保护的 API 访问，这项特征在访问 Amazon S3 资源时可强制执行 Amazon Multi-Factor Authentication 以提供更高级别的安全性。它是一项安全特征，要求用户通过提供有效 MFA 代码来证明实际拥有 MFA 设备。有关更多信息，请参阅 Amazon Multi-Factor Authentication。现在，您可以对任何访问 Amazon S3 资源的请求要求进行 MFA 身份验证。<br><br>为了强制执行 MFA 身份验证，Amazon S3 现已支持存储桶策略中的 `aws:MultiFactorAuthAge` 密钥。有关存储桶策略示例，请参阅 需要 MFA。 | 2012 年 7 月 10 日 |
| 对象到期支持 | 借助“对象到期”功能，您可以设定在已配置时间段后自动删除数据。通过向存储桶添加生命周期配置，可以设置对象到期规则。 | 2011 年 12 月 27 日 |
| 增加了新的支持区域 | Amazon S3 现已支持南美洲（圣保罗）区域。有关更多信息，请参阅 访问 Amazon S3 通用存储桶。 | 2011 年 12 月 14 日 |
| 多对象删除 | Amazon S3 现已支持多对象删除 API，使您能够删除单个请求中的多个对象。借助此特征，您可以比使用多个单独的 DELETE 请求更快地从 Amazon S3 删除大量对象。有关更多信息，请参阅 删除 Amazon S3 对象。 | 2011 年 12 月 7 日 |
| 增加了新的支持区域 | Amazon S3 现已支持美国西部（俄勒冈）地区。有关更多信息，请参阅存储桶和区域。 | 2011 年 11 月 8 日 |
| 文档更新 | 文档错误修复。 | 2011 年 11 月 8 日 |
| 文档更新 | 除了文档错误修复，本版本还包括以下增强功能：<br><br>• 使用 适用于 PHP 的 Amazon SDK 和 适用于 Ruby 的 Amazon SDK（请参阅指定具有 Amazon S3 托管式密钥的服务器端加密（SSE-S3））的新服务器端加密部分。 | 2011 年 10 月 17 日 |

| 更改 | 描述 | 日期 |
| --- | --- | --- |
| 服务器端加密支持 | Amazon S3 现已支持服务器端加密。它使您能够请求 Amazon S3 静态加密数据，即，当 Amazon S3 将数据写入其数据中心内的磁盘时，加密您的对象数据。除了 REST API 更新，适用于 Java 的 Amazon SDK 和 .NET 可提供必要的功能来请求服务器端加密。当使用 Amazon Web Services Management Console 上传对象时，还可以请求服务器端加密。要了解有关数据加密的更多信息，请转至使用数据加密。 | 2011 年 10 月 4 日 |
| 文档更新 | 除了文档错误修复，本版本还包括以下增强功能：<br>• 在《Amazon S3 API 参考》部分的 Making requests 中添加了 Ruby 和 PHP 示例。<br>• 添加了介绍如何生成和使用预签名 URL 的部分。有关更多信息，请参阅使用预签名 URL 共享对象和使用预签名 URL 共享对象。<br>• 更新了介绍 Amazon Explorer for Eclipse 和 Visual Studio 的部分。有关更多信息，请参阅《Amazon S3 API 参考》中的 Developing with Amazon S3 using the Amazon SDKs。 | 2011 年 9 月 22 日 |

| 更改 | 描述 | 日期 |
| --- | --- | --- |
| 对使用临时安全凭证发送请求的支持 | 除了使用您的 Amazon Web Services 账户和 IAM 用户安全凭证将经身份验证的请求发送到 Amazon S3，您现在还可以使用从 Amazon Identity and Access Management（IAM）获取的临时安全凭证发送请求。您可以使用 Amazon Security Token Service API 或 Amazon SDK 包装程序库从 IAM 请求这些临时凭证。您可以请求这些临时安全凭证以供自己使用，也可以提供给联合身份用户和应用程序使用。此特征使您能够管理Amazon之外的用户，并为他们提供临时安全凭证来访问Amazon资源。<br><br>有关更多信息，请参阅《Amazon S3 API 参考》中的 Making requests。<br><br>有关 IAM 对临时安全凭证的支持的更多信息，请参阅《IAM 用户指南》中的临时安全凭证。 | 2011 年 8 月 3 日 |
| 扩展了分段上传 API 以支持复制多达 5 TB 的对象 | 在此版本之前，Amazon S3 API 支持复制的对象最大为 5 GB。为了支持复制大于 5 GB 的对象，Amazon S3 现已通过新的操作 `Upload Part (Copy)` 扩展了分段上传 API。您可以使用该分段上传操作来复制多达 5 TB 的对象。有关更多信息，请参阅 复制、移动和重命名对象。<br><br>有关分段上传 API 的概念性信息，请参阅在 Amazon S3 中使用分段上传来上传和复制对象。 | 2011 年 21 月 6 日 |
| 已禁用通过 HTTP 的 SOAP API 调用 | 为了提高安全性，已禁用通过 HTTP 的 SOAP API 调用。经身份验证的和匿名的 SOAP 请求必须使用 SSL 发送到 Amazon S3。 | 2011 年 6 月 6 日 |

| 更改 | 描述 | 日期 |
| --- | --- | --- |
| IAM 支持跨账户的委派 | 以前，要访问 Amazon S3 资源，IAM 用户需要从父 Amazon Web Services 账户和 Amazon S3 资源拥有者这两者处获得许可。借助跨账户访问，IAM 用户现在仅需要从所有者账户获得许可。也即，如果资源拥有者向 Amazon Web Services 账户授予访问权限，则 Amazon Web Services 账户现在可以向其 IAM 用户授予对这些资源的访问权限。<br><br>有关更多信息，请参阅《IAM 用户指南》中的创建向 IAM 用户委派权限的角色。<br><br>有关在存储桶策略中指定主体的更多信息，请参阅 存储桶策略的主体。 | 2011 年 6 月 6 日 |
| 新链接 | 此服务的端点信息现在位于《Amazon 一般参考》中。有关更多信息，请参阅《Amazon 一般参考》https://docs.amazonaws.cn/general/latest/gr/rande.html中的“区域和端点”。 | 2011 年 3 月 1 日 |
| 支持在 Amazon S3 中托管静态网站 | Amazon S3 增强了对托管静态网站的支持。其中包括支持索引文档和自定义错误文档。使用这些特征时，访问存储桶的根目录或子文件夹（例如 `http://mywebsite.com/subfolder` ）的请求会返回索引文档，而不是存储桶中对象的列表。遇到错误时，Amazon S3 会返回用户自定义的错误消息，而不是 Amazon S3 错误消息。有关更多信息，请参阅 使用 Amazon S3 托管静态网站。 | 2011 年 6 月 6 日 |
| 此服务的端点信息现在位于《Amazon 一般参考》中。有关更多信息，请参阅《Amazon 一般参考》https://docs.amazonaws.cn/general/latest/gr/rande.html中的“区域和端点”。 | 2011 年 3 月 1 日 | |

| 更改 | 描述 | 日期 |
| --- | --- | --- |
| 支持在 Amazon S3 中托管静态网站 | Amazon S3 增强了对托管静态网站的支持。其中包括支持索引文档和自定义错误文档。使用这些特征时，访问存储桶的根目录或子文件夹（例如 `http://mywebsite.com/subfolder` ）的请求会返回索引文档，而不是存储桶中对象的列表。遇到错误时，Amazon S3 会返回用户自定义的错误消息，而不是 Amazon S3 错误消息。有关更多信息，请参阅 使用 Amazon S3 托管静态网站。 | 2011 年 2 月 17 日 |
| 支持响应标头 API | GET Object REST API 现在允许您为每个请求更改 REST GET Object 请求的响应标头。即，您可以改变响应中的对象元数据，无需改变对象本身。有关更多信息，请参阅 下载对象。 | 2011 年 1 月 14 日 |
| 支持大型对象 | Amazon S3 已将 S3 存储桶中可存储对象的最大大小从 5 GB 提高到 5 TB。如果您使用 REST API，则可以在单个 PUT 操作中上传最多 5GB 的对象。对于大型对象，必须使用分段上传 REST API 来分段上传对象。有关更多信息，请参阅 在 Amazon S3 中使用分段上传来上传和复制对象。 | 2010 年 12 月 9 日 |
| 分段上传 | 分段上传可以更快、更灵活地上传到 Amazon S3。它允许您上传单个对象作为一组分段。有关更多信息，请参阅 在 Amazon S3 中使用分段上传来上传和复制对象。 | 2010 年 11 月 10 日 |
| 支持存储桶策略中的规范 ID | 现在您可以在存储桶策略中指定规范 ID。有关更多信息，请参阅存储桶策略的主体。 | 2010 年 9 月 17 日 |
| Amazon S3 与 IAM 结合使用 | 该服务现已集成 Amazon Identity and Access Management（IAM）。有关更多信息，请转到《IAM 用户指南》中的与 IAM 结合使用的 Amazon Web Services 服务。 | 2010 年 9 月 2 日 |
| 通知 | Amazon S3 通知特征使您能够配置存储桶，以便当 Amazon S3 在存储桶上检测到关键事件时，Amazon S3 可向 Amazon Simple Notification Service（Amazon SNS）主题发布消息。有关更多信息，请参阅设置存储桶事件的通知。 | 2010 年 7 月 14 日 |

| 更改 | 描述 | 日期 |
| --- | --- | --- |
| 存储桶策略 | 存储桶策略是用来跨存储桶、对象和对象集设置访问权限的访问管理系统。此功能可补充（在许多情况下，可替代）访问控制列表。有关更多信息，请参阅 Amazon S3 的存储桶策略。 | 2010 年 7 月 6 日 |
| 在所有区域中可用的路径类型语法 | 在美国传统区域，或者如果存储桶与请求的端点位于相同区域，Amazon S3 现在支持任何存储桶的路径类型语法。有关更多信息，请参阅虚拟托管。 | 2010 年 6 月 9 日 |
| 欧洲（爱尔兰）的新端点 | Amazon S3 现在为欧洲（爱尔兰）提供端点：`http://s3-eu-west-1.amazonaws.com` 。 | 2010 年 6 月 9 日 |
| 控制台 | 您现在可以通过Amazon Web Services Management Console使用 Amazon S3。您可以在《Amazon Simple Storage Service 用户指南》中阅读有关控制台中所有 Amazon S3 功能的信息。 | 2010 年 6 月 9 日 |
| 去冗余 | Amazon S3 现在使您能够通过在去冗余的 Amazon S3 中存储对象，来降低存储成本。有关更多信息，请参阅低冗余存储。 | 2010 年 5 月 12 日 |
| 增加了新的支持区域 | Amazon S3 现已支持亚太地区（新加坡）区域。有关更多信息，请参阅存储桶和区域。 | 2010 年 4 月 28 日 |
| 对象版本控制 | 本版本引入了对象版本控制。所有对象现在都有键和版本。如果您启用对存储段的版本控制，则 Amazon S3 将为所有添加到存储段的对象提供唯一的版本 ID。此特征使您能够从意外覆盖和删除中恢复。有关更多信息，请参阅版本控制和使用版本控制。 | 2010 年 2 月 8 日 |
| 增加了新的支持区域 | Amazon S3 现在支持美国西部（北加利福尼亚）区域。对此区域的请求的新端点为 `s3-us-west-1.amazonaws.com` 。有关更多信息，请参阅存储桶和区域。 | 2009 年 12 月 2 日 |

| 更改 | 描述 | 日期 |
| --- | --- | --- |
| 适用于 .NET 的 Amazon SDK | 对于更喜欢使用 .NET 语言特定的 API 操作而不是使用 REST 或 SOAP 来构建应用程序的软件开发人员，Amazon 现在为他们提供了库、示例代码、教程和其他资源。这些库提供了一些基本功能 (未包括在 REST 或 SOAP API 中)，比如请求身份验证、请求重试和错误处置，以便您轻松地开始工作。有关语言特定的库和资源的更多信息，请参阅《Amazon S3 API 参考》中的 Developing with Amazon S3 using the Amazon SDKs。 | 2009 年 11 月 11 日 |