亚马逊云科技

用户指南

Amazon EBS

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

Amazon EBS: 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 EBS？ 1
Amazon EBS 的功能 1
相关服务 2
访问 Amazon EBS 2
定价 3
为 Amazon EBS 进行设置 4
注册获取 Amazon Web Services 账户 4
保护 IAM 用户 4
（可选）创建和使用用于 Amazon EBS 加密的客户托管密钥 5
（可选）启用阻止公开访问 Amazon EBS 快照 5
EBS 卷 7
功能和优势 8
数据可用性 8
数据持久性 8
数据加密 9
数据安全性 9
快照 9
弹性 10
EBS 卷类型 10
固态硬盘（SSD）卷 11
硬盘驱动器（HDD）卷 12
上一代卷 13
通用型 SSD 卷 14
预置 IOPS SSD 卷 18
吞吐量优化型 HDD 和 Cold HDD 卷 21
EBS 卷限制 31
存储容量 31
服务限制 32
分区方案 33
数据块大小 34
EBS 交易量和 NVMe 36
将卷映射到设备名称 37
I/O 操作超时 40
Abort 命令 40

卷生命周期 41
创建卷 42
将卷挂载到实例 46
将卷挂载到多个实例 47
使卷可用 55
查看卷详细信息 68
修改卷 74
从实例分离卷 96
删除卷 100
替换卷 101
状态检查 104
卷事件 106
使用受损的卷 108
自动启用 I/O 111
故障测试 113
EBS 快照 115
快照的工作原理 116
快照生命周期 119
创建 快照 120
查看快照信息 126
复制快照 129
共享快照 140
归档快照 147
删除快照 179
快速快照还原 182
注意事项 183
定价和计费 183
卷创建积分 184
配置快速快照还原 185
检查快速快照还原状态 187
查看使用快速快照还原功能还原的卷 189
快照锁定 190
概念 191
注意事项 193
控制 访问 194
锁定快照 196

解锁快照 199
更新快照锁定设置 200
监控快照锁定 201
阻止公开访问快照 204
IAM 权限 205
配置阻止公有访问 206
查看阻止公开访问设置 209
禁用屏蔽公共访问权限 212
监控阻止公开访问 215
开启本地快照 Outposts 216
常见问题 217
先决条件 218
注意事项 48
使用 IAM 控制访问 219
使用本地快照 221
Local Zones 中的本地快照 226
常见问题 217
注意事项 48
使用 IAM 控制访问 228
EBS 加密 232
EBS 加密的工作原理 232
快照加密时 EBS 加密的工作原理 233
快照未加密时 EBS 加密的工作原理 233
不可用的 KMS 密钥如何影响数据密钥 234
要求 234
支持的卷类型 235
支持的实例类型 235
用户的权限 235
实例的权限 236
默认启用加密 237
加密 EBS 资源 241
在创建时加密空卷 241
加密未加密的资源 242
轮换 KMS 密钥 242
示例 243
还原未加密的卷（未启用默认加密） 243

还原未加密的卷（启用了默认加密） 244
复制未加密的快照（未启用默认加密） 244
复制未加密的快照（启用了默认加密） 245
重新加密已加密卷 245
重新加密已加密快照 245
在加密卷与未加密卷之间迁移数据 246
加密结果 246
EBS 性能 249
Amazon EBS 性能提示 249
使用 EBS 优化的实例 249
配置实例带宽 249
了解如何计算性能 250
了解工作负载 250
请注意，从快照中初始化卷时，性能将会下降 250
可能导致 HDD 性能下降的因素 250
为 st1 和 sc1 上的高吞吐量读取密集型工作负载增加预读值（仅限 Linux 实例） 251
使用现代 Linux 内核（仅限 Linux 实例） 251
使用 RAID 0 以最大限度利用实例资源 252
监控 Amazon EBS 卷性能 252
EBS 优化 252
初始化 卷 253
使用 Amazon EBS 预配置速率进行卷初始化 253
使用已启用的快照进行快速快照恢复 256
手动初始化卷 256
可配置的实例带宽权重 260
I/O 特性和监控 261
IOPS 261
卷队列长度和延迟 263
I/O 大小和卷吞吐量限制 263
使用监控 I/O 特性 CloudWatch 264
监控实时 I/O 性能统计信息 265
相关资源 265
RAID 配置 265
RAID 配置选项 266
创建 RAID 0 阵列 266
创建 RAID 阵列中卷的快照 275

对 EBS 卷进行基准测试 275
设置实例 275
安装基准测试工具 277
选择卷队列长度 278
禁用 C 状态 279
执行基准测试 280
Amazon Data Lifecycle Manager 284
限额 285
工作方式 285
策略 286
政策计划 287
定位资源标签 287
快照 287
EBS 支持 AMIs 288
Amazon Data Lifecycle Manager 标签 288
默认策略与自定义策略 288
EBS 快照策略比较 289
EBS 支持的 AMI 策略比较 290
创建默认策略 292
默认策略注意事项 292
创建 Amazon EBS 快照的默认策略 293
为 EBS 支持的创建默认策略 AMIs 296
跨账户和区域启用默认策略 299
为快照创建自定义策略 304
创建快照生命周期策略 304
快照生命周期策略的注意事项 318
其他资源 322
自动生成应用程序一致性快照 322
前置和后置脚本的其他用例 356
前置和后置脚本的工作方式 364
识别使用前置和后置脚本创建的快照 367
监控前置和后置脚本 368
为创建自定义策略 AMIs 368
创建 AMI 生命周期策略 369
AMI 生命周期策略的注意事项 375
其他资源 378

自动执行跨账户快照副本 378
创建跨账户快照复制策略 378
指定快照描述筛选条件 388
跨账户快照复制策略的注意事项 388
其他资源 389
修改策略 389
删除策略 391
控制 访问 393
Amazon 托管策略 395
IAM 服务角色 402
监控策略 407
控制台和 Amazon CLI 408
Amazon CloudTrail 408
使用监控策略 EventBridge 408
使用监控策略 CloudWatch 410
服务端点 423
IPv4 端点 423
双栈（IPv4 和 IPv6）端点 424
指定端点 424
接口 VPC 端点 424
亚马逊 EBS VPC 终端节点的注意事项 425
为 Amazon EBS 创建接口 VPC 终端节点 426
故障排除 426
错误：Role with name already exists 426
亚马逊 EBS direct APIs 428
定价 429
的定价 APIs 429
联网成本 429
概念 429
快照 430
数据块 430
数据块索引 430
数据块令牌 430
校验和 430
加密 430
API 操作 431

签名版本 4 签名 431
控制 访问 431
读取快照 437
列出快照中的数据块 438
列出两个快照之间存在不同的数据块 441
从快照获取数据块数据 444
写入快照 445
启动快照 446
将数据放入快照 448
完成快照 450
加密结果 451
加密结果：未加密父快照 451
加密结果：已加密父快照 452
加密结果：无父快照 453
验证快照数据 454
确保幂等性 455
错误重试 456
优化性能 458
服务端点 458
IPv4 端点 459
双栈（IPv4 和 IPv6）端点 459
指定端点 460
SDK 代码示例 461
StartSnapshot 462
PutSnapshotBlock 462
CompleteSnapshot 463
接口 VPC 端点 464
亚马逊 EBS VPC 终端节点的注意事项 465
为 Amazon EBS 创建接口 VPC 终端节点 466
CloudTrail 日志 466
中的 Amazon EBS 数据事件 CloudTrail 467
中的 Amazon EBS 管理事件 CloudTrail 468
亚马逊 EBS 事件示例 468
FAQs 474
回收站 477
支持的资源 478

如何工作？ 478
注意事项 479
限额 481
相关服务 482
定价 482
控制 访问 483
使用回收站和保留规则的权限 483
使用回收站中的资源的权限 484
回收站的条件键 485
创建保留规则 487
更新保留规则 491
锁定保留规则 492
解锁保留规则 494
标签保留规则 495
查看保留规则标签 496
从保留规则中删除标签 497
删除保留规则 498
恢复已删除的快照 498
使用回收站中的快照的权限 499
在回收站中查看快照 500
从回收站中还原快照 501
恢复已删除 AMIs 502
在回收站 AMIs 中使用的权限 503
AMIs 在回收站中查看 504
AMIs 从回收站恢复 506
监视器使用 EventBridge 507
RuleLocked 507
RuleChangeAttempted 508
RuleUnlockScheduled 508
RuleUnlockingNotice 509
RuleUnlocked 510
监视器使用 CloudTrail 510
中的回收站信息 CloudTrail 510
了解回收站日志文件条目 512
服务端点 525
IPv4 端点 459

双栈（IPv4 和 IPv6）端点 526
指定端点 526
使用接口 VPC 端点 526
为回收站创建接口 VPC 端点 527
为回收站创建 VPC 端点策略 527
安全性 529
数据保护 529
Amazon EBS 数据安全 530
静态和动态加密 530
KMS 密钥管理 531
身份和访问管理 531
受众 532
使用身份进行身份验证 532
使用策略管理访问 534
EBS 如何与 IAM 配合使用 536
示例 IAM policies 542
故障排除 560
合规性验证 562
数据弹性 562
监控 564
Amazon CloudWatch 564
Amazon EBS 卷的指标 565
亚马逊 EBS 快照的指标 578
Nitro 实例的指标 579
快速快照还原的指标 582
Amazon EC2 控制台图表 583
Amazon EventBridge 584
EBS 卷事件 585
EBS 卷初始化事件 591
EBS 卷修改事件 591
EBS 快照事件 592
EBS 快照归档事件 600
EBS 快速快照还原事件 600
Amazon Lambda 用于处理 EventBridge 事件 601
EBS 详细的性能统计数据 604
统计信息 605

访问统计数据 607
Amazon GuardDuty 608
限额 610
文档历史记录 624
..... dcxxxii

什么是 Amazon Elastic Block Store？

Amazon Elastic Block Store (Amazon EBS) 提供可扩展、高性能的块存储资源，可用于亚马逊弹性计算云 (Amazon) 实例。 EC2使用 Amazon Elastic Block Store 时，您可以创建和管理以下数据块存储资源：

- Amazon EBS 卷 — 这些是您附加到亚马逊 EC2 实例的存储卷。将卷挂载到实例后，您可以像使用挂载到计算机上的本地硬盘一样使用卷，例如用于存储文件或安装应用程序。
- Amazon EBS 快照 — 这些是 Amazon EBS 卷的 point-in-time备份，它们独立于卷本身而持续存在。您可以通过创建快照来备份 Amazon EBS 卷上的数据。而后可以随时从这些快照还原新卷。

主题

- Amazon EBS 的功能
- 相关服务
- 访问 Amazon EBS
- 定价

Amazon EBS 的功能

Amazon EBS 提供以下功能和优势：

- 多种卷类型 – Amazon EBS 提供多种卷类型，可优化各种应用程序的存储性能和成本。卷类型分为两大类：用于交易工作负载的 SSD 支持型存储，以及用于吞吐量密集型工作负载的 HDD 支持型存储。
- 可扩展性 – 您可以创建容量和性能规范都满足需求的 Amazon EBS 卷。随着需求的变化，您可以在不必停机的情况下使用弹性卷操作来动态增加容量或调整性能。
- 备份和恢复 – 使用 Amazon EBS 快照来备份存储在卷上的数据。然后，您可以使用这些快照立即恢复卷或跨 Amazon 账户、 Amazon 区域或可用区迁移数据。
- 数据保护 – 使用 Amazon EBS 加密来加密 Amazon EBS 卷和 Amazon EBS 快照。加密操作发生在托管 Amazon EC2 实例的服务器上，从而确保两者的安全， data-at-rest以及实例 data-in-transit与其附加卷和后续快照之间的安全。
- 数据可用性和持久性 – io2 Block Express 卷持久性为 99.999%，年故障率为 0.001%。其他卷类型持久性为 99.8% 到 99.9%，年故障率为 0.1% 到 0.2%。另外，卷的数据可在可用区内多个服务器间进行自动复制，以防任何单个组件故障导致数据丢失。

- 数据存档 — EBS Snapshots Archive 提供了一个低成本的存储层，用于存档完整的 EBS 快照 point-in-time副本，出于监管和合规原因或将来的项目发布，您必须保留 90 天或更长时间。

相关服务

Amazon EBS 适用于以下服务：

- Amazon Elastic Compute Cloud — 一项允许您在 Amazon 云中启动和管理虚拟机（亚马逊 EC2 实例）的服务。您可以将 EBS 卷挂载到这些实例，并像使用本地硬盘一样使用 EBS 卷，例如用于存储文件或安装应用程序。有关更多信息，请参阅什么是亚马逊 EC2？
- Amazon Key Management Service – 此为允许您创建和管理加密密钥的托管服务。您可以使用 Amazon KMS 加密密钥对存储在 Amazon EBS 卷和亚马逊 EBS 快照中的数据进行加密。有关更多信息，请参阅 Amazon EBS 的使用 Amazon KMS方式。
- Amazon Data Lifecycle Manager — 一项托管服务，可自动创建、保留和删除 EBS 快照和 EBS 支持的快照。 AMIs您可以使用 Amazon Data Lifecycle Manager 自动备份您的亚马逊 EBS 卷和亚马逊 EC2 实例。有关更多信息，请参阅 使用 Amazon Data Lifecycle Manager 自动备份。
- EBS dire ct APIs — 一项服务，使您能够创建 EBS 快照、将数据直接写入快照、从快照中读取数据以及识别两个快照之间的差异或变化。有关更多信息，请参阅 使用 EBS 直接 APIs 访问快照的内容。
- 回收站 — 一种数据恢复服务，可让您恢复意外删除的 EBS 快照和 E AMIs BS 支持的快照。有关更多信息，请参阅回收站。

访问 Amazon EBS

您可以使用以下界面创建和管理 Amazon EBS 资源：

亚马逊 EC2 控制台

此为用于创建和管理卷与快照的 Web 界面。如果您已注册 Amazon 账户，则可以在以下网址访问亚马逊 EC2 控制台 https://console.aws.amazon.com/ec2/。

Amazon Command Line Interface

此为命令行工具，允许您在命令行 Shell 中使用命令管理 Amazon EBS 资源。它在 Windows、Mac 和 Linux 上受支持。有关更多信息，请参阅Amazon Command Line Interface 用户指南和 ec2 命令。

Amazon Tools for PowerShell

一组 PowerShell 模块，可让您通过 PowerShell 命令行编写对 Amazon EBS 资源的操作脚本。有关更多信息，请参阅 Amazon Tools for Windows PowerShell 用户指南和 Amazon Tools for PowerShell Cmdlet 参考。

Amazon CloudFormation

一项完全托管的 Amazon 服务，允许您创建可重复使用的 JSON 或 YAML 模板来描述您的 Amazon 资源，然后为您预置和配置这些资源。有关更多信息，请参阅 用户指南。Amazon CloudFormation

亚马逊 EC2 查询 API

Amazon EC2 查询 API 提供使用 HTTP 动词或POST和名为的查询参数的 HTTP GET 或 HTTPS 请求Action。有关更多信息，请参阅 Amazon EC2 API 参考。

Amazon SDKs

特定语言 APIs ，使您能够构建与 Amazon 服务集成的应用程序。 Amazon SDKs 适用于许多流行的编程语言。有关更多信息，请参阅构建工具 Amazon。

定价

使用 Amazon EBS，您可以按实际预置量付费。有关更多信息，请参阅 Amazon EBS 定价。

为 Amazon EBS 进行设置

完成本部分中的任务，为使用 Amazon EBS 资源做好准备。

任务

- 注册获取 Amazon Web Services 账户
- 保护 IAM 用户
- （可选）创建和使用用于 Amazon EBS 加密的客户托管密钥
- （可选）启用阻止公开访问 Amazon EBS 快照

注册获取 Amazon Web Services 账户

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

报名参加 Amazon Web Services 账户

1. 打开https://portal.aws.amazon.com/billing/注册。
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。

   当您注册时 Amazon Web Services 账户，就会创建Amazon Web Services 账户根用户一个。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。

Amazon 注册过程完成后会向您发送一封确认电子邮件。您可以随时前往 https://aws.amazon.com/并选择 “我的账户”，查看您当前的账户活动并管理您的账户。

保护 IAM 用户

注册后 Amazon Web Services 账户，开启多重身份验证 (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）。

要允许其他用户访问您的 Amazon Web Services 账户 资源，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：

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

（可选）创建和使用用于 Amazon EBS 加密的客户托管密钥

Amazon EBS 加密是一种加密解决方案，它使用 Amazon KMS 加密密钥来加密您的亚马逊 EBS 卷和亚马逊 EBS 快照。Amazon EBS 会自动为每个地区的亚马逊 EBS 加密创建唯一的 Amazon 托管 KMS 密钥。此 KMS 密钥具有 aws/ebs 别名。您无法轮换默认 KMS 密钥或管理其权限。为了提高灵活性和更好地控制用于 Amazon EBS 加密的 KMS 密钥，您可考虑创建和使用客户托管密钥。

创建和使用用于 Amazon EBS 加密的客户托管密钥

1. 创建对称加密 KMS 密钥。
2. 选择将 KMS 密钥作为用于 Amazon EBS 加密的默认 KMS 密钥。
3. 授予用户使用用于 Amazon EBS 加密的 KMS 密钥的权限。

（可选）启用阻止公开访问 Amazon EBS 快照

要防止公开共享您的快照，您可以启用阻止公开访问快照。在为一个区域阻止公开访问快照之后，将自动阻止任何尝试在此区域公开共享快照的行为。这样可以帮助您提高快照的安全性，并保护您的快照数据免遭未经授权的访问或意外访问。

有关更多信息，请参阅 阻止 Amazon EBS 快照的公开访问。

Console

启用阻止公开访问快照

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 “EC2 控制面板”，然后在 “帐户属性”（右侧）中，选择 “数据保护和安全”。
3. 在阻止公开访问 EBS 快照部分中，选择管理。
4. 选择阻止公开访问，然后选择以下选项之一：

   - 阻止所有公开访问 – 阻止所有公开共享快照的行为。此账户中的用户无法请求新的公开共享。此外，已公开共享的快照将被视为私有快照，且不可公开访问。

- 阻止新的公开共享 – 仅阻止公开共享快照的新行为。此账户中的用户无法请求新的公开共享。不过，已经公开共享的快照仍可公开访问。

5. 选择更新。

Amazon CLI

启用快照的屏蔽公共访问权限

使用 enable-snapshot-block-public-access 命令。对于 `--state`，请指定下列值之一：

- `block-all-sharing` – 阻止所有公开共享快照的行为。此账户中的用户无法请求新的公开共享。此外，已公开共享的快照将被视为私有快照，且不可公开访问。
- `block-new-sharing` – 仅阻止公开共享快照的新行为。此账户中的用户无法请求新的公开共享。不过，已经公开共享的快照仍可公开访问。

```
aws ec2 enable-snapshot-block-public-access --state block-new-sharing
```

PowerShell

启用快照的屏蔽公共访问权限

使用 Enable-EC2SnapshotBlockPublicAccess cmdlet。对于 `-State`，请指定下列值之一：

- `block-all-sharing` – 阻止所有公开共享快照的行为。此账户中的用户无法请求新的公开共享。此外，已公开共享的快照将被视为私有快照，且不可公开访问。
- `block-new-sharing` – 仅阻止公开共享快照的新行为。此账户中的用户无法请求新的公开共享。不过，已经公开共享的快照仍可公开访问。

```
Enable-EC2SnapshotBlockPublicAccess -State block-new-sharing
```

Amazon EBS 卷

Amazon EBS 卷是一种耐用的数据块级存储设备，您可以将其附加到您的实例。将卷附加到实例后，您可以像使用其他物理硬盘一样使用它。EBS 卷非常灵活。对于附加到当前一代实例类型的当前一代卷，您可以动态增加大小、修改预配置 IOPS 容量以及更改实际生产卷上的卷类型。

可以将 EBS 卷用作需要频繁更新的数据的主存储（例如实例的系统驱动器或数据库应用程序的存储）。还可以将其用于执行连续磁盘扫描的吞吐量密集型应用程序。EBS 卷的持续时间与 EC2 实例的运行寿命无关。

您可以将多个 EBS 卷附加到单个实例。该卷与实例必须位于同一可用区。根据卷和实例类型，您可以使用多重挂载将卷同时挂载到多个实例。

Amazon EBS 提供以下卷类型：通用型 SSD（gp2 和 gp3）、预调配 IOPS SSD（io1 和 io2）、吞吐量优化型 HDD（st1）、Cold HDD（sc1）以及磁介质卷（standard）。它们的性能特点和价格不同，您可根据应用程序要求定制您所需的存储性能和相应费用。有关更多信息，请参阅 Amazon EBS 卷类型。

您的账户对可用的总存储空间有限制。有关这些限制以及如何请求提高限制的更多信息，请参阅 Amazon EBS 端点和限额。

托管 EBS 卷是指由服务提供商（例如 Amazon EKS 自动模式）管理的卷。您不能直接修改托管 EBS 卷的设置。托管 EBS 卷由托管字段中的 true 值标识。有关更多信息，请参阅 Amazon EC2 托管实例。

有关定价的更多信息，请参阅 Amazon EBS 定价。

内容

- Amazon EBS 卷的特性和优势
- Amazon EBS 卷类型
- Amazon EBS 卷限制
- 亚马逊 EBS 交易量和 NVMe
- Amazon EBS 卷的生命周期
- 使用快照替换 Amazon EBS 卷
- Amazon EBS 卷状态检查
- 在 Amazon EBS 上进行故障测试

Amazon EBS 卷的特性和优势

EBS 卷具有实例存储卷不具备的优势。

优势

- 数据可用性
- 数据持久性
- 数据加密
- 数据安全性
- 快照
- 弹性

数据可用性

当您创建 EBS 卷时，系统会在其可用区内自动复制该卷，以防止因任何一个硬件组件出现故障而导致数据丢失。您可以将 EBS 卷连接到同一可用区中的任何 EC2 实例。附加后，该卷显示为类似于硬盘或其他物理设备的本机块储存设备。这时，实例就像与本地驱动器交互一样与该卷交互。您可以连接到实例并使用文件系统 [例如 Ext4（Linux 实例）或 NTFS（Windows 实例）] 格式化 EBS 卷，然后安装应用程序。

如果您将多个卷附加到您指定的一个设备，则可以在卷内将数据条带化，以增强 I/O 性能和吞吐量。

您可以获取针对 EBS 卷（包括 EBS 支持的实例的根设备卷）的监控数据，而无需额外付费。有关监控指标的更多信息，请参阅亚马逊 EBS 的亚马逊 CloudWatch 指标。有关跟踪卷状态的信息，请参阅亚马逊 EBS 的亚马逊 EventBridge 活动。

数据持久性

EBS 卷是一种实例外存储，其数据的保存期限不受实例使用寿命的影响。只要数据存在，您就要继续支付卷的使用费用。

如果您在控制台上为实例配置 EBS 卷时取消选中 “终止时删除” 复选框，则挂载到正在运行的实例的 EBS 卷可以在实例终止时自动与实例分离，且其数据完好无损。 EC2 然后，可将卷重新附加到新的实例，从而快速恢复数据。如果选中 “终止时删除” 复选框，则该卷将在 EC2 实例终止时删除。如果您使用的是 EBS 支持的实例，则可以停止并重启该实例，而不会影响与其附加的卷中保存储的数据。在从停止到启动的整个周期中，该卷均为已附加状态。这使您能够无限期地在卷上处理和存储数据，并只在需要时使用处理和存储资源。数据将一直保存在该卷上，直至将其显式删除。已删除的 EBS 卷所使用

的物理块存储将在分配给新卷之前被零或加密伪随机数据覆盖。如果要处理敏感数据，应考虑手动加密数据或将数据存储在由 Amazon EBS 加密 保护的卷上。有关更多信息，请参阅 Amazon EBS 加密。

默认情况下，当一个实例终止时，将删除在启动时创建并附加到该实例的根 EBS 卷。您可以修改此操作，方法是在启动实例时，将此标记的值从 `DeleteOnTermination` 改为 `false`。修改值后，即使实例终止，也可将该卷保留下来并附加到其他实例。

默认情况下，当一个实例终止时，不会删除在启动时创建并附加到该实例的额外 EBS 卷。您可以修改此操作，方法是在启动实例时，将此标记的值从 `DeleteOnTermination` 改为 `true`。此修改的值会导致在实例终止时删除卷。

数据加密

为简化数据加密，您可以使用 Amazon EBS 加密功能创建加密 EBS 卷。所有 EBS 卷类型都支持加密。您可以使用加密的 EBS 卷来满足监管/审计的数据和应用程序的各种 data-at-rest加密要求。Amazon EBS 加密使用 256 位高级加密标准算法（AES-256）和 Amazon 托管密钥基础设施。加密发生在托管实例的服务器上，从而提供 data-in-transit从 EC2 EC2 实例到 Amazon EBS 存储的加密。有关更多信息，请参阅 Amazon EBS 加密。

Amazon EBS 加密 Amazon KMS keys 在创建加密卷以及从您的加密卷创建的任何快照时使用。首次在区域中创建加密 EBS 卷时，系统会自动为您创建默认的 Amazon 托管 KMS 密钥。此密钥用于 Amazon EBS 加密，除非您创建和使用客户自主管理型密钥。创建您自己的客户自主管理型密钥可为您提供更大灵活性，包括创建、轮换、禁用、定义访问控制，以及审核用于保护数据的加密密钥等功能。有关更多信息，请参见Amazon Key Management Service 开发人员指南。

数据安全性

Amazon EBS 卷作为未格式化的原始块储存设备呈现。这些设备是在 EBS 基础设施上创建的逻辑设备；Amazon EBS 服务可确保在客户使用或重复使用之前，这些设备为逻辑空白（即，原始数据块被归零或包含加密伪随机数据）。

如果您有要求在使用后和/或使用前使用特定方法擦除所有数据的程序，例如 DoD 5220.22-M（美国《国家工业安全计划操作手册》）或 NIST 800-88（《存储介质清理指南》）中详细说明的程序，您可以在 Amazon EBS 上执行此操作。该数据块级活动将反映到 Amazon EBS 服务的底层存储介质中。

快照

Amazon EBS 提供为任何 EBS 卷创建快照（备份）并将卷中数据的副本写入 Amazon S3（其中数据以冗余方式存储在多个可用区中）的功能。不必将该卷附加到运行中的实例，也可以制作快照。因为您

不断向卷写入数据，则可定期创建该卷的快照，以用作创建新卷的基准。也可利用这些快照创建多个新的 EBS 卷或在可用区间移动卷的位置。加密 EBS 卷的快照会自动加密。

从快照创建新卷时，新卷是制作快照时的原始卷的精确副本。通过加密快照创建的 EBS 卷会自动加密。通过指定不同的可用区（可选），您可以使用此功能在该区域中创建重复的卷。快照可以与特定 Amazon 账户共享或公开。创建快照时，会根据备份数据的大小（而不是源卷的大小）收取 Amazon S3 费用。同一卷的后续快照为增量快照。这些快照仅包含自上次创建快照以来写入卷的已更改数据和新数据，您只需为这些已更改数据和新数据付费。

快照是增量备份，这意味着仅保存卷上在最新快照之后更改的数据块。如果您的卷中有 100 GiB 的数据，但自上次快照以来只更改了 5 GiB 的数据，则只有这 5 GiB 经过修改的数据会写入 Amazon S3。尽管快照是以增量方式保存的，但快照删除过程仅要求保留最新的快照。

为了便于对卷和快照进行分类和管理，您可以使用选择的元数据对它们加以标记。

要自动备份卷，您可以使用 Amazon Data Lifecycle Manager 或 Amazon Backup。

弹性

EBS 卷支持生产期间的实时配置更改。您可以在不中断服务的情况下修改卷类型、卷大小和 IOPS 容量。有关更多信息，请参阅 使用弹性卷操作修改 Amazon EBS 卷。

Amazon EBS 卷类型

Amazon EBS 提供以下卷类型，各种类型性能特点和价格不同，因此您可根据应用程序要求定制您所需的存储性能和相应成本。

> **Important**
>
> 有多种因素会影响 EBS 卷的性能，如实例配置、I/O 特性和工作负载需求。为了充分利用 EBS 卷上预调配的 IOPS，请使用 EBS 优化实例。有关充分利用 EBS 卷的更多信息，请参阅 Amazon EBS 卷性能。

有关定价的更多信息，请参阅 Amazon EBS 定价。

卷类型

- 固态硬盘（SSD）卷

- 硬盘驱动器（HDD）卷
- 上一代卷

固态硬盘（SSD）卷

SSD 支持的卷针对涉及频繁read/write operations with small I/O大小的事务性工作负载进行了优化，其中主要的性能属性是 IOPS。由 SSD 支持的卷类型包括通用型 SSD 和预调配 IOPS SSD。下面是 SSD 支持的卷的使用案例和特征摘要。

	Amazon EBS 通用型 SSD 卷		Amazon EBS 预调配 IOPS SSD 卷	
卷类型	gp3	gp2	io2方块快车	io1
持久性	99.8% - 99.9% 耐用性（0.1% - 0.2% 的年故障率）		99.999% 的耐用性（0.001% 的年故障率）	99.8% - 99.9% 耐用性（0.1% - 0.2% 的年故障率）
使用案例	• 事务性工作负载 • 虚拟桌面 • 中型单实例数据库 • 低延迟交互式应用程序 • 引导卷 • 开发和测试环境		需要以下工作负载： • 亚毫秒级延迟 • 持续 IOPS 绩效 • 超过 64,000 IOPS 或 1,000 MiB/s 吞吐量	• 需要持续 IOPS 性能或超过 16,000 IOPS 性能的工作负载 • I/O 密集型数据库工作负载
卷大小	1 GiB - 16 TiB		4 GiB-64 TiB 3	4 GiB - 16 TiB
最大 IOPS	16,000 (64 KiB I/O 4)	16,000 (16 kiB I/O 4)	256,000 [3] (16 kiB I/O 5)	64,000 (16 kiB I/O 4)
最大吞吐量	1,000 MiB/s	250MiB/s [1]	4,000 MiB/s	1000MiB/s [2]
Amazon EBS 多重挂载	不支持		支持	

	Amazon EBS 通用型 SSD 卷	Amazon EBS 预调配 IOPS SSD 卷	
NVMe 保留	不支持	支持	不支持
引导卷	支持		

[1] 吞吐量限制介于 128 之间MiB/s and 250 MiB/s，具体取决于卷大小。有关更多信息，请参阅 gp2 卷性能。除非您修改卷，否则在 2018 年 12 月 3 日之前创建并且自创建以来未经修改的卷可能无法实现完全性能。

[2] 要实现 1,000 MiB/s 的最大吞吐量，必须为该卷配置 64,000 IOPS，并且必须将其连接到基于 Nitro的实例。除非修改卷，否则在 2017 年 12 月 6 日之前创建且自创建以来未经修改的卷可能无法实现完全性能。

[3] 基于 Nitro 的实例支持配置高达 256,000 IOPS 的卷。其他实例类型可以挂载到预置了最多 64000IOPS 的卷，但可以实现最多 32000IOPS。

[4] 表示在卷的吞吐量限制内达到最大 IOPS 所需的 I/O 大小。

有关 SSD 支持的卷类型的更多信息，请参阅以下文件：

- Amazon EBS 通用型 SSD 卷
- Amazon EBS 预调配 IOPS SSD 卷

硬盘驱动器（HDD）卷

HDD 支持的卷针对大型流式处理工作负载进行了优化，其中主要的性能属性是吞吐量。HDD 容量类型包括吞吐量优化型 HDD 和冷 HDD。下面是 HDD 支持的卷的使用案例和特征摘要。

	吞吐量优化型 HDD 卷	Cold HDD 卷
卷类型	`st1`	`sc1`
持久性	99.8% - 99.9% 耐用性（0.1% - 0.2% 的年故障率）	
使用案例	• 大数据 • 数据仓库	• 适用于访问频率较低的数据的高吞吐量存储

	吞吐量优化型 HDD 卷	Cold HDD 卷
	• 日志处理	• 最低存储成本至关重要的情形
卷大小	125 GiB - 16 TiB	
每个卷的最大 IOPS（1 MiB I/O）	500	250
每个卷的最大吞吐量	500 MiB/s	250 MiB/s
Amazon EBS 多重挂载	不支持	
引导卷	不支持	

有关硬盘驱动器（HDD）卷的更多信息，请参阅 Amazon EBS 吞吐量优化型 HDD 和冷 HDD 卷。

上一代卷

磁性（`standard`）卷是采用磁性驱动器的上一代卷。它们适用于具有较小数据集的工作负载，在这些工作负载中，数据访问不频繁，性能不是最重要的。这些卷平均提供大约 100 IOPS，突增能力最大可达数百 IOPS，大小范围是 1 GiB 到 1 TiB。

> **Tip**
>
> 磁介质卷是上一代卷类型。如果您需要比上一代卷更高的性能或性能一致性，建议您考虑使用一种更新的卷类型。

下表列出了上一代 EBS 卷类型。

	磁介质
卷类型	`standard`
使用案例	数据不常访问的工作负载

	磁介质
卷大小	1 GiB - 1 TiB
每个卷的最大 IOPS	40–200
每个卷的最大吞吐量	40–90 MiB/s
引导卷	支持

有关更多信息，请参阅上一代卷。

Amazon EBS 通用型 SSD 卷

通用固态硬盘（gp2 和 gp3）卷由固态硬盘（ ）提供支持。SSDs通用型 SSD 卷在各种事务性工作负载的价格和性能之间实现平衡。其中包括虚拟桌面、中型单实例数据库、延迟敏感型交互式应用程序、开发和测试环境以及启动卷。建议为大多数工作负载使用这种卷。

Amazon EBS 提供以下类型的通用型 SSD 卷：

类型

- 通用型 SSD（gp3）卷
- 通用型 SSD（gp2）卷

通用型 SSD（gp3）卷

通用型 SSD（gp3）卷是最新一代通用型 SSD 卷，也是 Amazon EBS 提供的成本最低的 SSD 卷。这种卷类型有助于为大多数应用程序提供合理得当的价格和性能。其还可以帮助您独立于卷大小扩展卷的性能。这意味着您可以预置所需性能，而无需预置额外的块存储容量。此外，gp3 卷每 GiB 价格比通用型 SSD（gp2）卷低了 20%。

gp3 卷提供个位数的毫秒延迟和 99.8% 至 99.9% 的卷持久性，年故障率 (AFR) 不高于 0.2%，这意味着在一年内每 1,000 个运行卷中最多有两次卷故障。 Amazon 设计 gp3 卷以在 99% 的时间内提供其预配置的性能。

内容

- gp3 卷性能
- gp3 卷大小

- 从 gp2 迁移到 gp3

gp3 卷性能

> **Tip**
>
> gp3 卷不使用突增性能。其可以无限期地维持其完全预调配 IOPS 和吞吐量性能。

IOPS 性能

gp3 卷提供 3000 IOPS 的一致基准 IOPS 性能，这包含在存储价格中。您可以按每 GiB 卷大小 500 IOPS 的比例预置额外的 IOPS（最大 16000 IOPS），但需支付额外费用。可为 32 GiB 或更大的卷预置最大 IOPS（每 GiB 500 IOPS × 32 GiB = 16000 IOPS）。

吞吐量性能

gp3 卷提供一致的基准吞吐量性能（为 125MiB/s, which is included with the price of storage. You can provision additional throughput (up to a maximum of 1,000 MiB/s) for an additional cost at a ratio of 0.25 MiB/s per provisioned IOPS. Maximum throughput can be provisioned at 4,000 IOPS or higher and 8 GiB or larger (4,000 IOPS × 0.25 MiB/s per IOPS = 1,000 MiB/s）。

gp3 卷大小

gp3 卷的大小范围为 1 GiB 到 16 TiB。

从 gp2 迁移到 gp3

如果您当前正在使用 gp2 卷，则可以使用 使用弹性卷操作修改 Amazon EBS 卷 操作将卷迁移到 gp3。您可以使用 Amazon EBS Elastic Volumes 操作修改现有卷的卷类型、IOPS 和吞吐量，而无需中断您的 Amazon 实例。 EC2 当使用控制台创建卷或从快照中创建 AMI 时，卷类型的默认选择是“通用型 SSD gp3”。在其他情况下，默认选择是 gp2。在这些情况下，可以选择 gp3 作为卷类型而不是使用 gp2。

若要了解将 gp2 卷迁移到 gp3 可以节省多少费用，请使用 Amazon EBS gp2 至 gp3 迁移成本节省计算器。

通用型 SSD（gp2）卷

这种卷类型可提供经济实惠的存储，是广泛事务性工作负载的理想选择。使用 gp2 卷，性能随卷大小而扩展。

> **Tip**
>
> gp3 卷是最新一代通用型 SSD 卷。其提供更加可预测的性能扩展，而且价格比 gp2 卷低 20%。有关更多信息，请参阅 通用型 SSD（gp3）卷。
> 若要了解将 gp2 卷迁移到 gp3 可以节省多少费用，请使用 Amazon EBS gp2 至 gp3 迁移成本节省计算器。

gp2卷提供个位数的毫秒延迟和 99.8% 至 99.9% 的卷持久性，年故障率 (AFR) 不高于 0.2%，这意味着在一年内每 1,000 个运行卷中最多有两次卷故障。 Amazon 设计gp2卷以在 99% 的时间内提供其预配置的性能。

内容

- gp2 卷性能
- gp2 卷大小

gp2 卷性能

IOPS 性能

基准 IOPS 性能以每 GiB 卷大小 3 IOPS 的速度，在最小 100 IOPS 和最大 16000 IOPS 之间进行线性扩缩。IOPS 性能预置如下：

- 33.33 GiB 及更小的卷预置至少 100 IOPS。
- 大于 33.33GiB 的卷预置每 GiB 卷大小 3IOPS，最高可达 16000IOPS，达到 5334GiB（3 X 5334）。
- 5334 GiB 及更大的卷预置 16000 IOPS。

小于 1 TiB 的 gp2 卷（且预置的 IOPS 低于 3000）可在需要较长时间时突增至 3000 IOPS。卷的突增能力受 I/O 积分的控制。I/O 需求大于基准性能时，卷花费 I/O 积分以突增至所需的性能级别（最多 3000 IOPS）。突增时，I/O 积分不会累积，而是按照高于基准 IOPS 的 IOPS 速率进行消费（费用率 = 突增 IOPS - 基准 IOPS）。卷累积的 I/O 积分越多，其维持突增性能的时间就越长。您可以按如下方式计算突增持续时间：

$$\text{Burst duration} = \frac{\text{(I/O credit balance)}}{\text{(Burst IOPS) - (Baseline IOPS)}}$$

I/O 需求降至基准性能水平或更低时，卷开始以每 GiB 卷大小每秒 3 个 I/O 积分的速率获得 I/O 积分。每个卷都有 540 万 I/O 积分的 I/O 积分累积限制，这足以在至少 30 分钟内维持 3000 IOPS 的最大突增性能。

> **Note**
>
> 每个卷都有 540 万 I/O 积分的初始 I/O 积分余额，这为启动卷提供了快速初始启动循环，并为其他应用程序提供良好的引导过程。

下表列出了示例卷大小和卷的相关基准性能、突增持续时间（从 540 万 I/O 积分开始时）以及重填空 I/O 积分余额所需的时间。

卷大小（GiB）	基准性能（IOPS）	3000 IOPS 时的最大突增持续时间（秒）	重填空 I/O 积分余额所需的时间（秒）
1 至 33.33	100	1862	54000
100	300	2000	18000
334（最大吞吐量的最小大小）	1,002	2,703	5,389
750	2250	7200	2400
1000	3000	不适用*	不适用*
5334（最大 IOPS 的最小大小）及更大	16000	不适用*	不适用*

*卷的基准性能超过了最大突发性能。

您可以使用亚马逊中的 Amazon EBS `BurstBalance` 指标监控卷的 I/O 积分余额。 CloudWatch 此指标显示 gp2 剩余的 I/O 积分百分比。有关更多信息，请参阅 Amazon EBS I/O 特性和监控。您可以设置警报，以便在 `BurstBalance` 值降到特定水平时获取通知。有关更多信息，请参阅创建 CloudWatch 警报。

吞吐量性能

gp2卷提供的吞吐量介于 128 之间MiB/s and 250 MiB/s，具体取决于卷大小。吞吐量性能预置如下：

- 170 GiB 或更小的卷提供最大 128 MiB/s 的吞吐量。
- 大于 170 GiB 但小于 334 GiB 的卷可以突增至 250 MiB/s 的最大吞吐量。
- 334 GiB 及更大的卷提供 250 MiB/s 的吞吐量。

gp2 卷的吞吐量可以使用以下公式计算，吞吐量上限为 250 MiB/s：

```
Throughput in MiB/s = IOPS performance × I/O size in KiB / 1,024
```

gp2 卷大小

gp2 卷的大小范围为 1 GiB 到 16 TiB。请记住，卷性能随卷大小呈线性扩缩。

Amazon EBS 预调配 IOPS SSD 卷

预配置的 IOPS SSD 卷由固态硬盘（ ）提供支持。SSDs这种卷是性能最高的 Amazon EBS 存储卷，专为需要低延迟的 IOPS 密集型和吞吐量密集型关键工作负载而设计。预调配 IOPS SSD 卷在 99.9% 的时间里可提供预置 IOPS 性能。

Amazon EBS 提供了两种类型的预调配 IOPS SSD 卷：

- 预调配 IOPS SSD（io2）Block Express 卷
- 预调配 IOPS SSD（io1）卷

预调配 IOPS SSD（**io2**）Block Express 卷

io2 Block Express 卷基于下一代 Amazon EBS 存储服务器架构而构建。它旨在满足基于 Nitro 系统构建的实例上运行的最苛刻 I/O 密集型应用程序的性能要求。Block Express 具有最高耐用性和最低延迟，非常适合运行性能密集、任务关键型工作负载，例如 Oracle、SAP HANA、Microsoft SQL Server 和 SAS Analytics。

Block Express 架构提高了 io2 卷的性能和规模。Block Express 服务器使用可扩展可靠数据报 (SRD) 网络协议与基于 Nitro 的实例进行通信。此接口在专用于实例主机硬件上 Amazon EBS I/O 功能的 Nitro Card 中实现。它最大限度地减少 I/O 延迟和延迟变化（网络抖动），从而为应用程序提供更快、更一致的性能。

io2 Block Express 卷可提供 99.999% 的卷耐用性，年故障率（AFR）不超过 0.001%，这意味着在一年时间内，每 10 万个正在运行的卷最多发生一次卷故障。io2Block Express 卷非常适合可以从达到亚毫秒级延迟的单个卷受益的工作负载，并支持比 gp3 卷更多的 IOPS、更高的吞吐量和更大的容量。

预调配 IOPS SSD（io2）Block Express 卷在 99.9% 的时间里可提供预调配的 IOPS 性能。

主题

- 注意事项
- 性能

注意事项

- io2 Block Express 卷已在以下区域提供：美国东部（俄亥俄州）|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（香港）|亚太地区（孟买）|亚太地区（首尔）|亚太地区（新加坡）|亚太地区（悉尼）|亚太地区（东京）|加拿大（中部）|欧洲地区（法兰克福）|欧洲地区（爱尔兰）|欧洲地区（伦敦）|欧洲地区（斯德哥尔摩）|中东（巴林）。
- 截至 2025年4月30日，所有新增和之前创建的io2卷均为 io2 Block Express卷。
- 基于 Nitro 的实例支持配置高达 256,000 IOPS 的卷。其他实例类型可以挂载到预置了最多 64000IOPS 的卷，但可以实现最多 32000IOPS。
- 要使用未加密的快照或共享的加密快照创建大小大于 16 TiB 或 IOPS 大于 64,000 的加密 B io2 lock Express 卷，您必须：
  1. 在您的账户中，创建此快照的加密副本
  2. 使用此快照副本创建卷

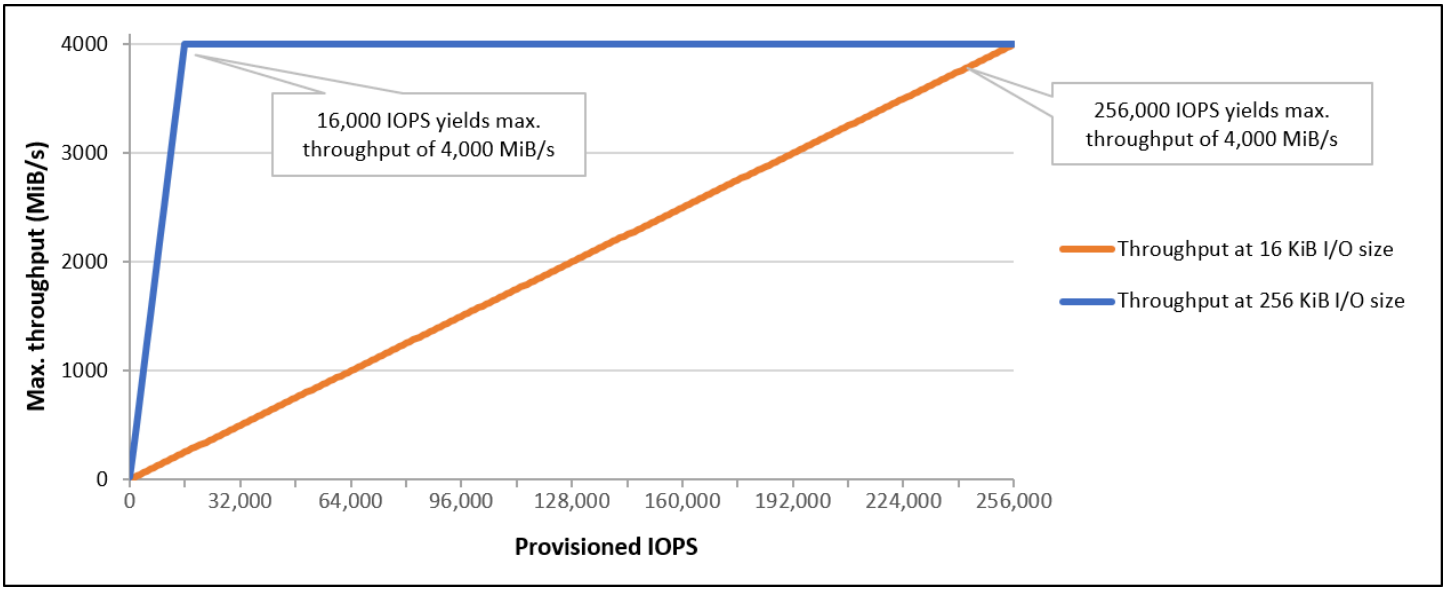
性能

借助 io2 Block Express 卷，您可以通过以下方式预置卷：

- 亚毫秒级平均延迟
- 存储容量高达 64TiB（65536GiB）
- 预置 IOPS 高达 256,000，IOPS:GiB 比率为 1,000:1。可以为 256GiB 和更大的卷预置最多 IOPS（1000IOPS x 256GiB = 256000IOPS）。

> **Note**
>
> 使用基于 Nitro 的实例，您最多可以实现 256,000 个 IOPS。在其他实例上，您最多可以实现 32,000 IOPS。

- MiB/s. Throughput scales proportionally at a rate of 0.256 MiB/s每个预配置 IOPS 的容量吞吐量高达 4,000。最大吞吐量可在 16,000 IOPS 或更高的情况下实现。



预调配 IOPS SSD（**io1**）卷

预调配 IOPS SSD（io1）卷旨在满足 I/O 密集型工作负载（尤其是数据库工作负载）的需求，这些工作负载对存储性能和一致性非常敏感。预置 IOPS SSD 卷使用一致的 IOPS 速率（在创建卷时指定），而 Amazon EBS 在 99.9% 的时间里可提供预置性能。

io1 卷可提供 99.8% 到 99.9% 的卷耐用性，年故障率（AFR）不超过 0.2%，这意味着在一年时间内，每 1000 个正在运行的卷最多发生两次卷故障。

io1卷适用于所有 Amazon EC2 实例类型。

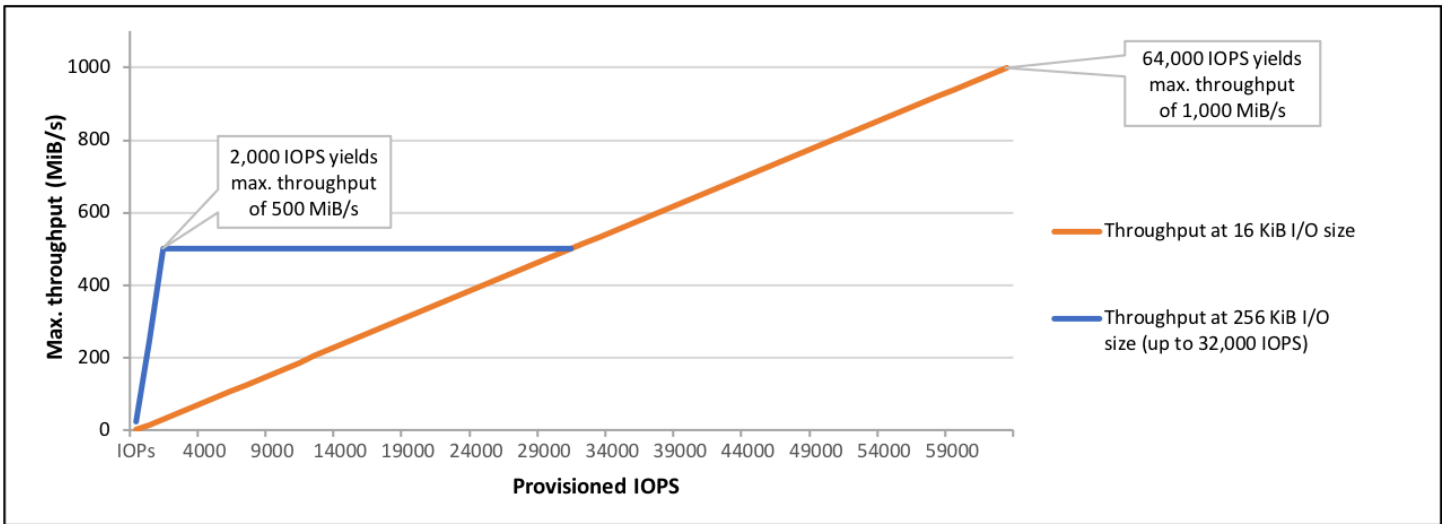
性能

io1 卷的大小介于 4GiB 到 16TiB 不等，可以为每个卷预置 100IOPS 到最多 64000IOPS。预调配 IOPS 与请求的卷大小（以 GiB 为单位）的最大比率为 50:1。例如，可以为一个 100GiB io1 卷预置最多 5000IOPS。

可以为 1280GiB 或更大的卷预置最多的 IOPS（50 × 1280GiB = 64000IOPS）。

- io1配置了高达 32,000 IOPS 的卷支持的最大 I/O 大小为 256 KiB，最大可产生高达 500 个MiB/s of throughput. With the I/O大小，在 2,000 IOPS 时达到峰值吞吐量。
- 预调配超过 32000IOPS（最高可达 64000IOPS）的 io1 卷以每个预调配 IOPS 16KiB 的速率线性增大吞吐量。例如，预置了 48,000 IOPS 的卷最多可以支持 750 个）。MiB/s of throughput (16 KiB per provisioned IOPS × 48,000 provisioned IOPS = 750 MiB/s
- 达到最大吞吐量MiB/s, a volume must be provisioned with 64,000 IOPS (16 KiB per provisioned IOPS × 64,000 provisioned IOPS = 1,000 MiB/s（1,000）。
- 只有在基于 Nitro 的实例上，您最多可以实现 64,000 个 IOPS。在其他实例上，您最多可以实现 32,000 IOPS。

下图说明了这些性能特性：



您的每 I/O 延迟体验取决于预置 IOPS 以及您的工作负载模式。要获得最佳 I/O 延迟体验，请确保您预配置 IOPS 以满足工作负载的 I/O 配置文件。

Amazon EBS 吞吐量优化型 HDD 和冷 HDD 卷

Amazon EBS 提供的 HDD 卷分为以下几个类别：

- 吞吐量优化型 HDD – 适用于访问频率较高的吞吐量密集型工作负载的低成本 HDD。
- 冷硬盘 — 成本最低的硬盘，专为访问频率较低的工作负载而设计。

主题

- 每实例吞吐量限制
- 吞吐量优化型 HDD 卷
- Cold HDD 卷
- 使用 HDD 卷时的性能注意事项
- 监控卷的突发存储桶余额

每实例吞吐量限制

st1 和 sc1 卷的吞吐量始终由以下限制中较小的决定：

- 卷的吞吐量限制
- 实例的吞吐量限制

对于所有 Amazon EBS 卷，我们建议您选择适当的 EBS 优化 EC2 实例，以避免网络瓶颈。

吞吐量优化型 HDD 卷

吞吐量优化型 HDD（st1）卷提供低成本的磁性存储，该存储以吞吐量而不是 IOPS 定义性能。该卷类型是大型顺序工作负载（例如 Amazon EMR、ETL、数据仓库和日志处理）的理想之选。不支持可启动的 st1 卷。

吞吐量优化型 HDD（st1）卷虽然与 Cold HDD（sc1）卷类似，但其旨在支持频繁访问的数据。

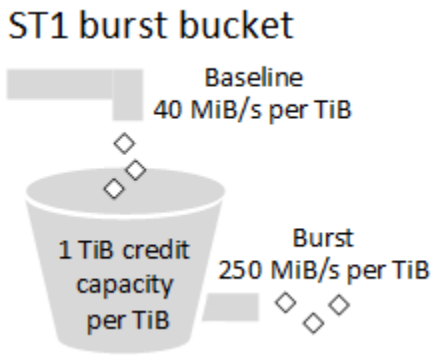
> **Note**
>
> 该卷类型针对涉及大型顺序 I/O 的工作负载进行了优化，建议具有执行少量随机 I/O 工作负载的客户使用 Amazon EBS 通用型 SSD 卷 或 Amazon EBS 预调配 IOPS SSD 卷。有关更多信息，请参阅 HDD 上的小型读/写效率低下问题。

附加到 EBS 优化型实例的吞吐量优化型 HDD（st1）卷旨在提供一致的性能，在给定年度的 99% 时间内交付至少 90% 的预期吞吐量性能。

吞吐量积分和突增性能

与 gp2 类似，st1 使用突增存储桶模型提高性能。卷大小决定卷的基准吞吐量，即卷积累吞吐量积分的速度。卷大小还决定卷的突增吞吐量，即有积分可用时消耗积分的速度。较大的卷有较高的基准吞吐量和突增吞吐量。卷的积分越多，它以突增水平驱动 I/O 的时间就越长。

下图显示 st1 的突增存储桶行为。



st1 卷的可用吞吐量受吞吐量和吞吐量积分上限的限制，由以下公式表示：

```
(Volume size) × (Credit accumulation rate per TiB) = Throughput
```

对于 1 TiB 的st1卷，突发吞吐量限制为 250MiB/s, the bucket fills with credits at 40 MiB/s，并且最多可以容纳 1 TiB 的积分。

体积越大，这些限制就会线性扩展，吞吐量上限为每 MiB/s. After the bucket is depleted, throughput is limited to the baseline rate of 40 MiB/s TiB 500。

对于介于 0.125 TiB 到 16 TiB 之间的卷大小，基准吞吐量从 MiB/s to a cap of 500 MiB/s 5 到达 12.5 TiB 不等，如下所示：

```
            40 MiB/s
12.5 TiB × ---------- = 500 MiB/s
             1 TiB
```

突发吞吐量从 31 不等MiB/s to a cap of 500 MiB/s，在 2 TiB 时达到，如下所示：

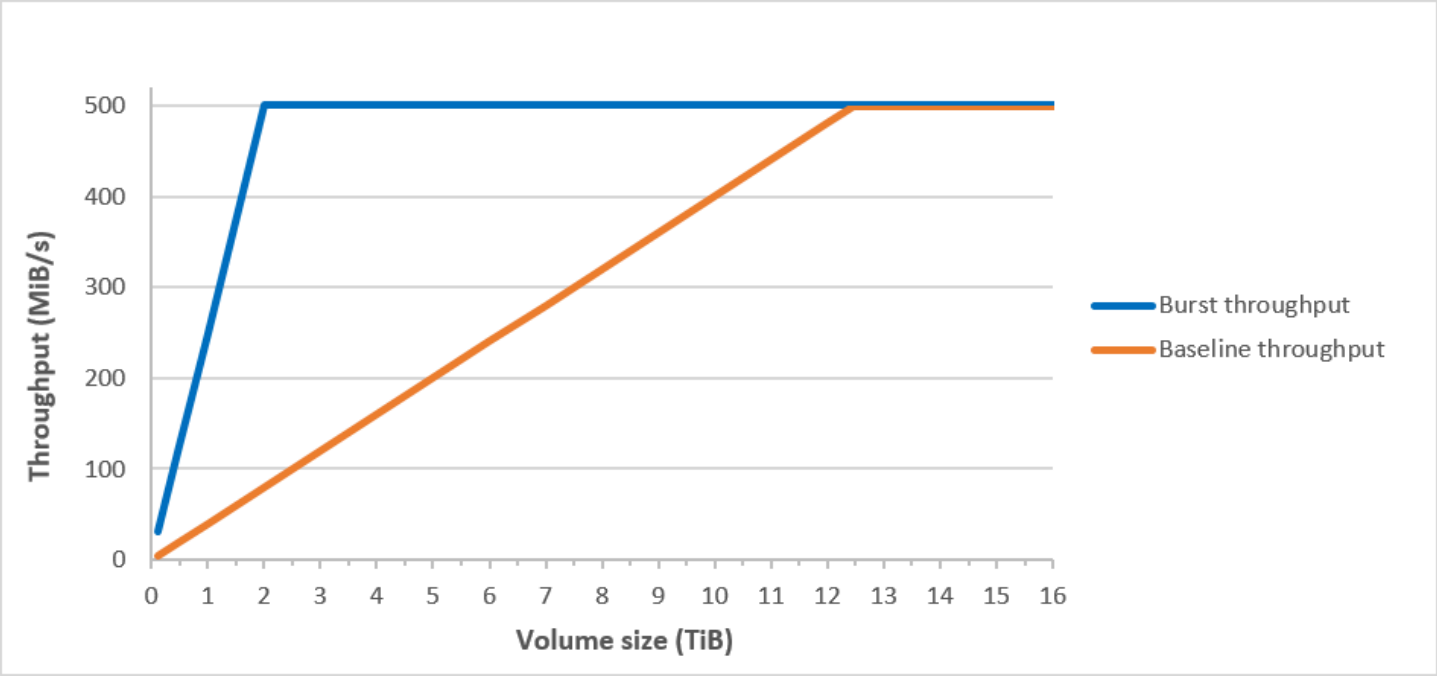
```
         250 MiB/s
2 TiB × ---------- = 500 MiB/s
          1 TiB
```

下表列出了 st1 基准和突增吞吐量值的完整范围。

卷大小（TiB）	ST1 基本吞吐量 (MiB/s)	ST1 突发吞吐量 (MiB/s)
0.125	5	31

卷大小（TiB）	ST1 基本吞吐量 (MiB/s)	ST1 突发吞吐量 (MiB/s)
0.5	20	125
1	40	250
2	80	500
3	120	500
4	160	500
5	200	500
6	240	500
7	280	500
8	320	500
9	360	500
10	400	500
11	440	500
12	480	500
12.5	500	500
13	500	500
14	500	500
15	500	500
16	500	500

下图绘制了表值：



> **Note**
>
> 如果创建吞吐量优化型 HDD（st1）卷的快照，则在快照处理过程中，性能可能会降低，最坏情况下会降低到卷的基准值。

有关使用 CloudWatch 指标和警报监控突发存储桶余额的信息，请参阅监控卷的突发存储桶余额。

Cold HDD 卷

Cold HDD（sc1）卷提供低成本的磁性存储，该存储以吞吐量而不是 IOPS 定义性能。st1 的吞吐量限制比 sc1 更低，是大型顺序冷数据工作负载的绝佳选择。如果您需要频繁访问数据并且希望节约成本，sc1 提供价格低廉的块存储。不支持可启动的 sc1 卷。

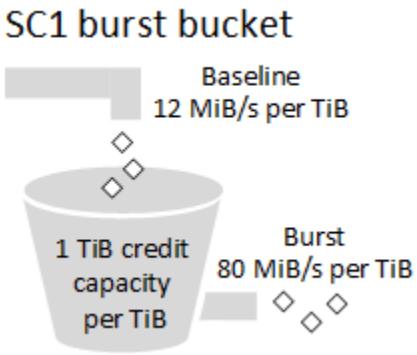
Cold HDD（sc1）卷虽然与吞吐量优化型 HDD（st1）卷类似，但其旨在支持不频繁访问的数据。

> **Note**
>
> 该卷类型针对涉及大型顺序 I/O 的工作负载进行了优化，建议具有执行少量随机 I/O 工作负载的客户使用 Amazon EBS 通用型 SSD 卷 或 Amazon EBS 预调配 IOPS SSD 卷。有关更多信息，请参阅 HDD 上的小型读/写效率低下问题。

附加到 EBS 优化型实例的 Cold HDD（sc1）卷旨在提供一致的性能，在给定年度的 99% 时间内交付至少 90% 的预期吞吐量性能。

吞吐量积分和突增性能

与 gp2 类似，sc1 使用突增存储桶模型提高性能。卷大小决定卷的基准吞吐量，即卷积累吞吐量积分的速度。卷大小还决定卷的突增吞吐量，即有积分可用时消耗积分的速度。较大的卷有较高的基准吞吐量和突增吞吐量。卷的积分越多，它以突增水平驱动 I/O 的时间就越长。



sc1 卷的可用吞吐量受吞吐量和吞吐量积分上限的限制，由以下公式表示：

```
(Volume size) × (Credit accumulation rate per TiB) = Throughput
```

对于 1 TiB 的sc1卷，突发吞吐量限制为 80MiB/s, the bucket fills with credits at 12 MiB/s，并且最多可以容纳 1 TiB 的积分。

体积越大，这些限制就会线性扩展，吞吐量上限为每 MiB/s. After the bucket is depleted, throughput is limited to the baseline rate of 12 MiB/s TiB 最大 250。

对于介于 0.125 TiB 到 16 TiB 之间的卷大小，基准吞吐量从 MiB/s to a maximum of 192 MiB/s 1.5 不等，在 16 TiB 时达到，如下所示：

```
           12 MiB/s
16 TiB × ---------- = 192 MiB/s
            1 TiB
```

突发吞吐量从 10 不等MiB/s to a cap of 250 MiB/s，在 3.125 TiB 时达到，如下所示：

```
             80 MiB/s
3.125 TiB × ----------- = 250 MiB/s
```

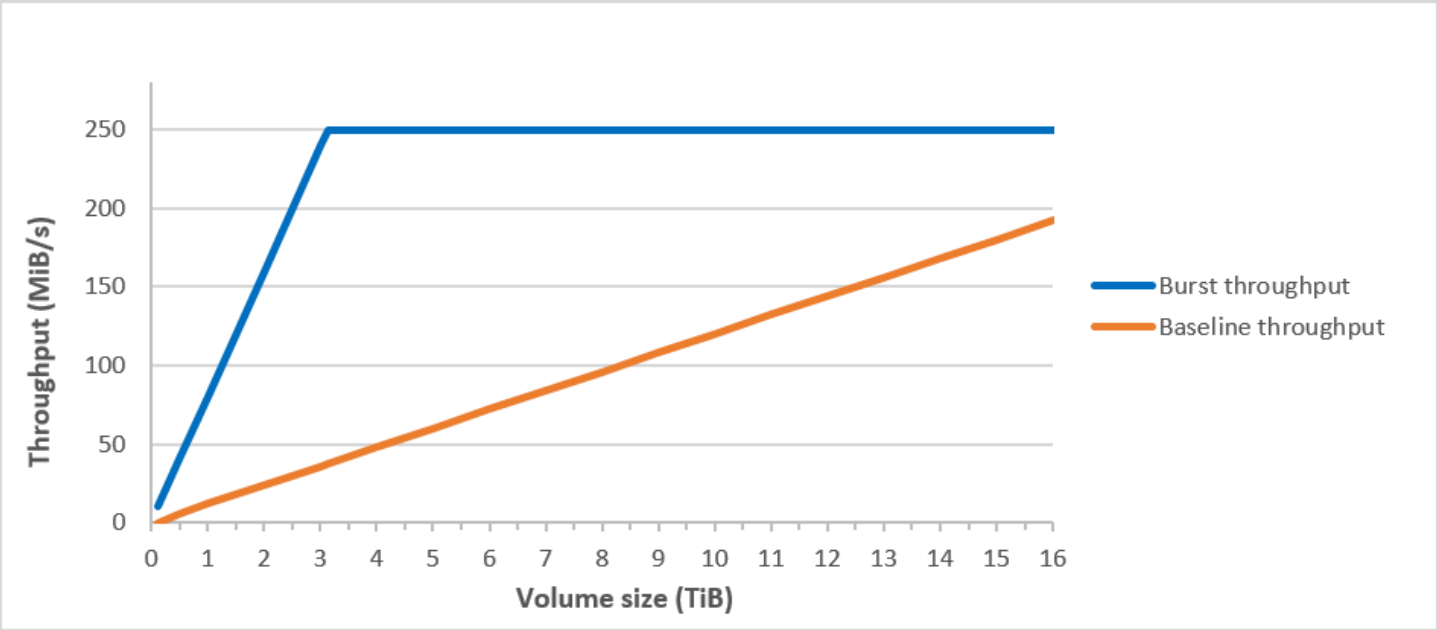
```
                1 TiB
```

下表列出了 sc1 基准和突增吞吐量值的完整范围：

卷大小（TiB）	SC1 基本吞吐量 (MiB/s)	SC1 突发吞吐量 (MiB/s)
0.125	1.5	10
0.5	6	40
1	12	80
2	24	160
3	36	240
3.125	37.5	250
4	48	250
5	60	250
6	72	250
7	84	250
8	96	250
9	108	250
10	120	250
11	132	250
12	144	250
13	156	250
14	168	250
15	180	250

卷大小（TiB）	SC1 基本吞吐量 (MiB/s)	SC1 突发吞吐量 (MiB/s)
16	192	250

下图绘制了表值：



> **Note**
>
> 如果创建 Cold HDD（sc1）卷的快照，则在快照处理过程中，性能可能会降低，最坏情况下会降低到卷的基准值。

有关使用 CloudWatch 指标和警报监控突发存储桶余额的信息，请参阅监控卷的突发存储桶余额。

使用 HDD 卷时的性能注意事项

为了使用 HDD 卷获得最优的吞吐量结果，请根据以下注意事项计划您的工作负载。

比较吞吐量优化型 HDD 和 Cold HDD

st1 和 sc1 存储桶大小因卷大小而异，满的存储桶包含充足的令牌用于完整卷扫描。不过，因为每实例和每卷的吞吐量限制，更大的 st1 和 sc1 卷需要更长的时间完成卷扫描。附加到较小实例的卷被限制在每实例吞吐量上，而不是 st1 或 sc1 吞吐量限制。

st1 和 sc1 专为在 99% 的时间内实现 90% 的突增吞吐量性能一致性而设计。不合规时间段大致均匀分布，目标是达到 99% 的每小时预计总吞吐量。

一般来说，扫描时间可由此公式表示：

```
 Volume size
------------ = Scan time
 Throughput
```

例如，考虑到性能一致性保证和其他优化，拥有 5 TiB 卷的 st1 客户预计在 2.91 到 3.27 小时内完成整卷扫描。

- 最佳扫描时间

```
   5 TiB             5 TiB
----------- = ------------------ = 10,486 seconds = 2.91 hours
 500 MiB/s     0.00047684 TiB/s
```

- 最长扫描时间

```
  2.91 hours
-------------- = 3.27 hours
 (0.90)(0.99) <-- From expected performance of 90% of burst 99% of the time
```

同样，拥有 5 TiB 卷的 sc1 客户预计在 5.83 到 6.54 小时内完成整卷扫描。

- 最佳扫描时间

```
   5 TiB              5 TiB
----------- = ------------------- = 20972 seconds = 5.83 hours
 250 MiB/s     0.000238418 TiB/s
```

- 最长扫描时间

```
  5.83 hours
-------------- = 6.54 hours
 (0.90)(0.99)
```

下表列出了不同大小卷的理想扫描时间，假设存储桶是满的并且有充足的实例吞吐量。

卷大小（TiB）	ST1 连拍扫描时间（小时）*	SC1 连拍扫描时间（小时）*
1	1.17	3.64
2	1.17	3.64
3	1.75	3.64
4	2.33	4.66
5	2.91	5.83
6	3.50	6.99
7	4.08	8.16
8	4.66	9.32
9	5.24	10.49
10	5.83	11.65
11	6.41	12.82
12	6.99	13.98
13	7.57	15.15
14	8.16	16.31
15	8.74	17.48
16	9.32	18.64

* 这些扫描时间在执行 1 MiB 顺序 I/O 时采取平均队列深度（四舍五入到最近的整数）四或更多。

因此，如果您有面向吞吐量的工作负载需要快速完成扫描（最快 500MiB/s）或一天查询几个整卷，请使用 `st1`。如果您针对成本进行了优化，数据访问相对不频繁，而且不需要超过 250 MiB/s 的扫描性能，请使用 `sc1`。

HDD 上的小型读/写效率低下问题

st1 和 sc1 卷的性能模型针对顺序 I/O 进行了优化，支持高吞吐量工作负载，对具有混合 IOPS 和吞吐量的工作负载提供可接受的性能，不建议使用具有小型随机 I/O 的工作负载。

例如，1 MiB 或更小的 I/O 请求计为 1 MiB I/O 积分。但是，如果是顺序 I/O，则会合并为 1 MiB I/O 数据块，并且只计为 1 MiB I/O 积分。

监控卷的突发存储桶余额

您可以使用亚马逊上提供的 Amazon EBS BurstBalance 指标监控st1和sc1卷的突发存储桶级别。CloudWatch此指标显示 st1 和 sc1 在突增存储桶中剩余的吞吐量积分。有关指标和其他与 I/O 相关的指标的更多信息，请参阅Amazon EBS I/O 特性和监控。BurstBalance CloudWatch 还允许您设置警报，当该BurstBalance值降至一定水平时会通知您。有关更多信息，请参阅创建 CloudWatch 警报。

Amazon EBS 卷限制

Amazon EBS 卷的大小受块数据存储的物理和算术以及操作系统 (OS) 和文件系统设计者的实施决策的限制。 Amazon 对卷大小施加了额外的限制，以保障其服务的可靠性。

以下部分介绍了限制 EBS 卷的可用大小并提供配置 EBS 卷的建议的最重要因素。

目录

- 存储容量
- 服务限制
- 分区方案
- 数据块大小

存储容量

下表总结了 Amazon EBS 上的最常用文件系统的理论和实现存储容量（假定 4096 字节块大小）。

分区方案	最大可寻址块数	理论最大大小（块数 x 块大小）	Ext4 实现的最大大小*	XFS 实现的最大大小**	NTFS 实现的最大大小	EBS 支持的最大大小
MBR	2^{32}	2 TiB	2 TiB	2 TiB	2 TiB	2 TiB

分区方案	最大可寻址块数	理论最大大小（块数 x 块大小）	Ext4 实现的最大大小*	XFS 实现的最大大小**	NTFS 实现的最大大小	EBS 支持的最大大小
GPT	2^{64}	64 ZiB	1 EiB = 242 [1]0TiB （已通过 50 TiB 认证） RHEL7	500 TiB （已通过认证 RHEL7）	256 TiB	64 TiB †

* Ext4 How to 以及红帽企业 Linux 的文件和系统大小限制是多少？

** 红帽企业 Linux 的文件和系统大小限制是多少？

† io2 Block Express 卷最高支持 64TiB 的 GPT 分区。有关更多信息，请参阅 预调配 IOPS SSD（io2）Block Express 卷。

服务限制

Amazon EBS 将数据中心的大规模分布式存储提取到虚拟硬盘中。对于安装在 EC2 实例上的操作系统，连接的 EBS 卷看起来像是包含 512 字节磁盘扇区的物理硬盘驱动器。操作系统通过其存储管理实用程序对数据块（或集群）分配到这些虚拟扇区进行管理。分配与卷分区方案（例如主启动记录 [MBR] 或 GUID 分区表 [GPT]）一致，并且属于已安装文件系统（ext4、NTFS 等）的功能。

EBS 不知道其虚拟磁盘扇区中包含的数据；它只会确保扇区的完整性。这意味着 Amazon 操作和操作系统操作是相互独立的。在您选择卷大小时，请注意二者的功能和限制，如以下情况中所示：

- EBS 当前支持最大卷大小 64 TiB。这意味着您可以创建一个大小为 64 TiB 的 EBS 卷，但操作系统是否能够识别该容量的全部取决于其自身的设计特征以及该卷的分区方式。
- 启动卷必须使用 MBR 或 GPT 分区方案。您从中启动实例的 AMI 决定了启动模式以及随后用于启动卷的分区方案。

  使用 MBR 时，启动卷的大小限制为 2 TiB。

  使用 GPT，与 (Linux) 或 UEFI 启动模式 (Windows) GRUB2 一起使用时，启动卷的大小可以高达 64 TiB。

有关更多信息，请参阅 使 Amazon EBS 卷可供使用。

- 2 TiB（2048 GiB）或更大的非启动卷必须使用 GPT 分区表才能访问整个卷。

分区方案

除其他影响之外，分区方案还确定了可以在单个卷中唯一寻址的逻辑数据块的数量。有关更多信息，请参阅数据块大小。正在使用的常见分区方案是主启动记录（MBR）和 GUID 分区表（GPT）。这两个方案之间的重要差别可归纳如下。

MBR

MBR 使用 32 位数据结构来存储块地址。这意味着，每个数据块会映射到 2^{32} 个可能整数之一。卷的最大可寻址大小由以下公式给出：

$$2^{32} \times \text{Block size}$$

MBR 卷的块大小通常限制为 512 字节。因此：

$$2^{32} \times 512 \text{ bytes} = 2 \text{ TiB}$$

工程解决办法是提高 MBR 卷的这个 2 TiB 限制，但还没有被行业广泛采用。因此，Linux 和 Windows 永远不会检测到 MBR 体积大于 2 TiB， Amazon 即使显示其大小更大。

GPT

GPT 使用 64 位数据结构来存储块地址。这意味着，每个数据块会映射到 2^{64} 个可能整数之一。卷的最大可寻址大小由以下公式给出：

$$2^{64} \times \text{Block size}$$

GPT 卷的块大小通常限制为 4,096 字节。因此：

$$\begin{aligned} & 2^{64} \times 4{,}096 \text{ bytes} \\ &= 2^{64} \times 2^{12} \text{ bytes} \\ &= 2^{70} \times 2^{6} \text{ bytes} \\ &= 64 \text{ ZiB} \end{aligned}$$

现实世界中的计算机系统不支持任何接近这个理论最大值的值。实施的文件系统大小目前上限为 50TiB（对于 ext4）和 256TiB（对于 NTFS）。

数据块大小

现代硬盘驱动器上的数据存储是通过逻辑块寻址 来管理的，逻辑块寻址是一个抽象层，它允许操作系统在逻辑块中读取和写入数据，而无需详细了解底层硬件。操作系统依靠存储设备将块映射到其物理扇区，并使用是扇区大小数倍的数据块将数据读写到磁盘。

Amazon EBS 向操作系统公布 512 字节或 4,096 字节（4 KiB）的物理扇区。只有在 Amazon EC2 实例类型、操作系统和驱动程序支持的情况下，Amazon EBS 才会宣传 4 KiB 的 Amazon NVMe 物理扇区。如果实例类型、操作系统或 Amazon NVMe 驱动程序不支持 4 KiB 的物理扇区，Amazon EBS 将改用 512 字节的物理扇区。

Amazon EC2 实例类型支持

下表显示了 Amazon EBS 针对不同的 Amazon EC2 实例类型宣传的扇区大小。

公布的物理扇区大小	实例类型
512 字节	所有基于 Xen 的实例以及以下基于 Nitro 的实例： • 通用型：A1 | M5 | M5a | M5ad | M5d | M5dn | M5n | M5zn | M6g | M6gd | Mac1 | Mac2 | T3 | T3a | T4g • 计算优化型：C5 | C5a | C5ad | C5d | C5n | C6g | C6gd • 内存优化型：R5 | R5a | R5ad | R5d | R5dn | R5n | R6g | R6gd | U-12tb1 | U-18tb1 | U-24tb1 | U-3tb1 | U-6tb1 | U-9tb1 | X2gd | X2iezn | Z1d • 存储优化：D3 | D3en | I3en • 加速计算：Dl1 | g4ad | g4dn | G5 | g5g | Inf1 | p3dn | p4d | p4de | p4de | VT1
4 KiB	所有其他基于 Nitro 的实例

操作系统支持

下表显示了 Amazon EBS 针对某些常见操作系统公布的扇区大小。

> **Note**
>
> 该列表并不完整。我们建议您在操作系统中验证 Amazon EBS 公布的物理扇区大小。

公布的物理扇区大小	操作系统
512 字节	• 内核版本 4.14 及更早版本的 Amazon Linux • RHEL 7.9 及更早版本 • Ubuntu 20.04 及更早版本 • Windows 7 或更早版本 • Windows Server 2008 及更早版本
4 KiB	• 内核版本 5.3 及更高版本的 Amazon Linux • RHEL8.8 及更高版本 • Ubuntu 22.04 及更高版本 • Windows 8 及更高版本 • Windows Server 2012 及更高版本

Amazon NVMe 驱动程序支持

亚马逊 EBS 宣传 4 KiB 物理扇区， Amazon NVMe 驱动程序版本为 1.5.1 及更高版本。请务必确保您使用的是最新版本的Amazon NVMe 驱动程序。

非默认块大小

逻辑数据块的行业默认大小当前为 4 KiB。由于某些工作负载受益于较小或较大的块大小，因此文件系统支持可在格式化期间指定的非默认块大小。应使用非默认块大小的情况（如优化）不在本文档的范围内，但块大小的选择会对卷的存储容量产生影响。下表显示了理论存储容量随不同块大小的变化。但是，请记住，EBS 对卷大小的限制（io2 Block Express 为 64 TiB）当前等于 16 KiB 数据块支持的最大大小。

块大小	最大卷大小
4KiB（默认）	16 TiB

块大小	最大卷大小
8 KiB	32 TiB
16 KiB	64 TiB
32 KiB	128 TiB
64KiB（最大）	256 TiB

亚马逊 EBS 交易量和 NVMe

Amazon EBS 卷作为 NVMe 区块设备暴露在基于 Amazon Nitro 系统的亚马逊 EC2 实例上。要充分利用作为 NVMe 块设备公开的 Amazon EBS 卷的性能和功能，该 EC2 实例必须安装 Amazon NVMe 驱动程序。默认情况下，所有最新一代的 Amazon Windows 和 Linux AMIs 都安装了 Amazon NVMe 驱动程序。

如果您使用的 AMI 没有 Amazon NVMe 驱动程序，则可以手动安装该驱动程序。有关更多信息，请参阅 Amazon EC2 用户指南中的Amazon NVMe 驱动程序。

Linux 实例

设备名称为 `/dev/nvme0n1`、`/dev/nvme1n1`，以此类推。使用设备名称 (`/dev/nvme[0-26]n1`) 重命名您在块储存设备映射中指定的 NVMe 设备名称。块储存设备驱动程序可以按照与您在块储存 NVMe 设备映射中为卷指定的顺序不同的顺序分配设备名称。

Windows 实例

当您将卷附加到实例时，需要为卷提供设备名称。此设备名称由 Amazon 使用 EC2。实例的块储存设备驱动程序在装入卷时会分配实际的卷名，分配的名称可以与 Amazon EC2 使用的名称不同。

内容

- 将 Amazon EBS 卷映射到 NVMe 设备名称
- NVMe 亚马逊 EBS 卷的 I/O 操作超时
- NVMe Abort 适用于 Amazon EBS 卷的命令

将 Amazon EBS 卷映射到 NVMe 设备名称

EBS 使用单根 I/O 虚拟化 (SR-IOV)，根据该规范在基于 Nitro 的实例上提供卷附件。 NVMe 这些设备依赖于操作系统上的标准 NVMe驱动程序。这些驱动程序通常在实例启动期间发现附加的设备，然后根据设备响应的顺序创建设备节点，而不是按照在块设备映射中指定设备的顺序。

Linux 实例

在 Linux 中， NVMe 设备名称遵循模式/dev/nvme<x>n<y>，其中<x>是枚举顺序，对于 EBS，<y>则为 1。有时候，在接下来的实例启动时，设备会以不同顺序响应发现过程，这会导致设备名称更改。此外，块储存设备驱动程序分配的设备名称可以不同于块储存设备映射中指定的名称。

建议您在实例中为 EBS 卷使用静态标识符，例如以下之一：

- 对于基于 Nitro 的实例，将在 EC2 控制器标识的供应商特定数据字段中捕获您在连接 EBS 卷时或在`AttachVolume`或 `RunInstances` API 调用期间在 Amazon 控制台中指定的块储存设备映射。NVMe 对于 AMIs 高于 2017.09.01 版本的 Amazon Linux，我们提供了一`udev`条规则，用于读取这些数据并创建指向区块设备映射的符号链接。
- EBS 卷 ID 和挂载点在实例状态更改之间保持稳定。 NVMe 设备名称可以根据设备在实例启动期间的响应顺序而变化。我们建议使用 EBS 卷 ID 和挂载点以实现一致的设备标识。
- NVMe EBS 卷将 EBS 卷 ID 设置为设备标识中的序列号。使用 `lsblk -o +SERIAL` 命令列出序列号。
- NVMe 设备名称格式可能有所不同，具体取决于 EBS 卷是在实例启动期间还是之后连接的。 NVMe 实例启动后连接的卷的 NVMe设备名称包含/dev/前缀，而实例启动期间连接的卷的设备名称不包含/dev/前缀。
  - 对于 Amazon Linux 或 FreeBSD AMI，`sudo ebsnvme-id /dev/nvme0n1 -u`使用命令获得一致 NVMe 的设备名称。
  - 对于其他发行版，请使用`sudo nvme id-ctrl -v /dev/nvme0n1`命令来确定 NVMe 设备名称。您可能需要包含 `--vendor-specific` 命令选项。
- 格式化设备时，将生成在文件系统的使用寿命内保持的 UUID。此时可指定设备标签。有关更多信息，请参阅使 Amazon EBS 卷可供使用和从错误的卷启动。

亚马逊 Linux AMIs

在 Amazon Linux AMI 2017.09.01 或更高版本（包括亚马逊 Linux 2）中，您可以按如下方式运行ebsnvme-id命令将 NVMe 设备名称映射到卷 ID 和设备名称：

以下示例显示实例启动期间附上的卷的命令和输出。请注意， NVMe 设备名称不包含前/dev/缀。

```
[ec2-user ~]$ sudo /sbin/ebsnvme-id /dev/nvme0n1
Volume ID: vol-01324f611e2463981
sda
```

以下示例显示实例启动后附上的卷的命令和输出。请注意，NVMe 设备名称包含前/dev/缀。

```
[ec2-user ~]$ sudo /sbin/ebsnvme-id /dev/nvme1n1
Volume ID: vol-064784f1011136656
/dev/sdf
```

Amazon Linux 还会创建从块储存设备映射中的设备名称（例如/dev/sdf）到 NVMe 设备名称的符号链接。

FreeBSD AMIs

从 FreeBSD 12.2-RELEASE 开始，您可以运行如上所示的 ebsnvme-id 命令。传递 NVMe 设备的名称（例如，nvme0）或磁盘设备的名称（例如nvd0或nda0）。FreeBSD 还会创建指向磁盘设备的符号链接（例如，）。/dev/aws/disk/ebs/ *volume_id*

其他Linux AMIs

如果内核版本为 4.2 或更高版本，则可以按如下方式运行nvme id-ctrl命令将 NVMe 设备映射到卷 ID。首先，使用适用于 Linux 发行版的软件包管理工具安装 NVMe 命令行软件包。nvme-cli有关其他发行版的下载和安装说明，请参阅特定于您的发行版的文档。

以下示例获取在实例启动期间连接的卷的卷 ID 和 NVMe 设备名称。请注意，NVMe 设备名称不包含前/dev/缀。设备名称可通过 NVMe控制器供应商特定的扩展名获得（控制器标识的 384:4095 字节）：

```
[ec2-user ~]$ sudo nvme id-ctrl -v /dev/nvme0n1
NVME Identify Controller:
vid     : 0x1d0f
ssvid   : 0x1d0f
sn      : vol01234567890abcdef
mn      : Amazon Elastic Block Store
...
0000: 2f 64 65 76 2f 73 64 6a 20 20 20 20 20 20 20 20 "sda..."
```

以下示例获取实例启动后连接的卷的卷 ID 和 NVMe 设备名称。请注意，NVMe 设备名称包含前/dev/缀。

```
[ec2-user ~]$ sudo nvme id-ctrl -v /dev/nvme1n1
NVME Identify Controller:
vid     : 0x1d0f
ssvid   : 0x1d0f
sn      : volabcdef01234567890
mn      : Amazon Elastic Block Store
...
0000: 2f 64 65 76 2f 73 64 6a 20 20 20 20 20 20 20 20 "/dev/sdf..."
```

lsblk 命令可列出可用设备及其挂载点（如果适用）。这有助于确定要使用的正确设备名称。在本示例中，/dev/nvme0n1p1 作为根设备挂载，/dev/nvme1n1 会附加但不会挂载。

```
[ec2-user ~]$ lsblk
NAME          MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
nvme1n1       259:3   0  100G  0 disk
nvme0n1       259:0   0    8G  0 disk
  nvme0n1p1   259:1   0    8G  0 part /
  nvme0n1p128 259:2   0    1M  0 part
```

Windows 实例

您可以运行**ebsnvme-id**命令将 NVMe 设备磁盘号映射到 EBS 卷 ID 和设备名称。默认情况下，会枚举所有 EBS NVMe 设备。您可以传递磁盘编号以枚举特定设备的信息。该ebsnvme-id工具包含在最新 Amazon 提供的 Windows 服务器中， AMIs 位于C:\PROGRAMDATA\AMAZON\Tools。

```
PS C:\Users\Administrator\Desktop> ebsnvme-id.exe
Disk Number: 0
Volume ID: vol-0d6d7ee9f6e471a7f
Device Name: sda1

Disk Number: 1
Volume ID: vol-03a26248ff39b57cf
Device Name: xvdd

Disk Number: 2
Volume ID: vol-038bd1c629aa125e6
Device Name: xvde

Disk Number: 3
Volume ID: vol-034f9d29ec0b64c89
Device Name: xvdb
```

```
Disk Number: 4
Volume ID: vol-03e2dbe464b66f0a1
Device Name: xvdc
PS C:\Users\Administrator\Desktop> ebsnvme-id.exe 4
Disk Number: 4
Volume ID: vol-03e2dbe464b66f0a1
Device Name: xvdc
```

NVMe 亚马逊 EBS 卷的 I/O 操作超时

大多数操作系统都为提交给 NVMe 设备的 I/O 操作指定超时时间。

Linux 实例

在 Linux 上，连接到基于 Nitro的实例的 EBS 卷使用操作系统提供的默认 NVMe 驱动程序。大多数操作系统都为提交给 NVMe 设备的 I/O 操作指定超时时间。默认超时为 30 秒，可以使用 `nvme_core.io_timeout` 引导参数更改该超时。对于 4.6 版之前的大多数 Linux 内核版本，此参数为 `nvme.io_timeout`。

如果 I/O 延迟超过此超时参数的值，Linux NVMe 驱动程序将 I/O 失败并向文件系统或应用程序返回错误。根据 I/O 操作，您的文件系统或应用程序可以重试错误。在某些情况下，您的文件系统可能会通过只读方式重新挂载。

为了获得与附加到 Xen 实例的 EBS 卷类似的体验，我们建议将 `nvme_core.io_timeout` 设置为可能的最大值。对于当前内核，最大值为 4294967295，而对于较早的内核，最大值为 255。根据 Linux 版本的不同，超时时间可能已设置为支持的最大值。例如，对于 Amazon Linux AMI 2017.09.01 以及更高的版本，超时时间默认设置为 4294967295。

您可以通过将高于建议最大值的值写入 `/sys/module/nvme_core/parameters/io_timeout` 并在尝试保存文件时检查数值结果超出范围错误，以此来验证您的 Linux 发行版的最大值。

Windows 实例

在 Windows 上，默认超时为 60 秒，最大超时为 255 秒。您可以使用 SCSI 微端口驱动程序的注册表项中所述的步骤修改 `TimeoutValue` 磁盘类注册表设置。

NVMe Abort 适用于 Amazon EBS 卷的命令

该`Abort`命令是一个 NVMe 管理员命令，用于结束先前提交给控制器的特定命令。此命令通常由设备驱动程序向超过输入/输出操作超时阈值的存储设备发出。

默认情况下支持该Abort命令的 Amazon EC2 实例类型将结束之前在向连接的 Amazon EBS 卷发出Abort命令时提交给控制器的特定命令。向连接的 Amazon EBS 卷发出Abort命令时，不支持该Abort命令的 Amazon EC2 实例不会执行任何操作。

以下对象支持 Abort 命令：

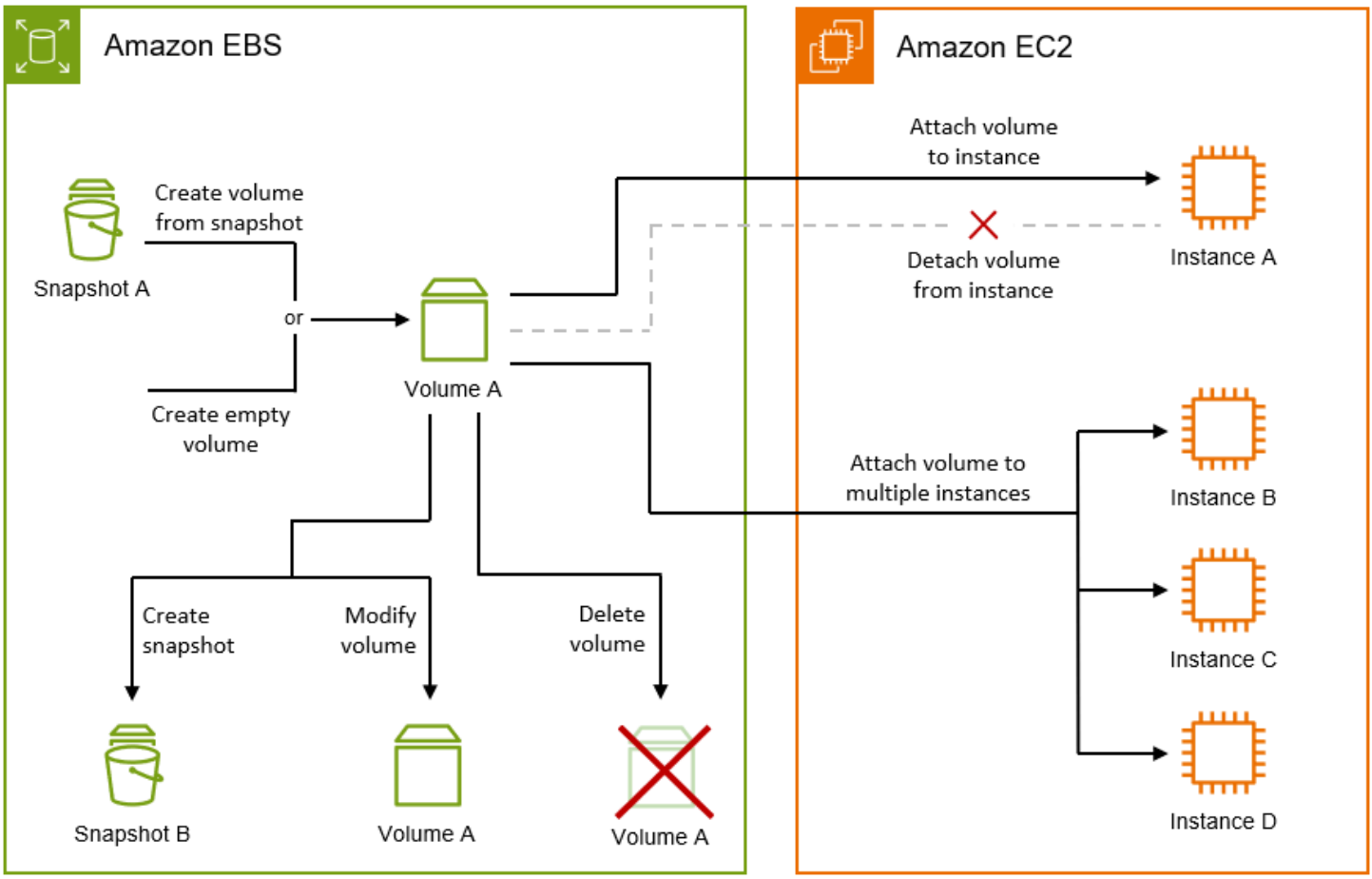
- 设备版本为 1.4 或更高版本的 Amazon EBS NVMe 设备。
- 所有 Amazon EC2 实例，但基于 Xen 的实例类型和以下基于 Nitro 的实例类型除外：
  - 通用型：A1 | M5 | M5a | M5ad | M5d | M5dn | M5n | M5zn | M6g | M6gd | Mac1 | Mac2 | T3 | T3a | T4g
  - 计算优化型：C5 | c5a | C5ad | C5d | C5n | C6g | C6gd
  - 内存优化型：R5 | R5a | R5ad | R5d | R5dn | R5n | R6g | R6gd | U-12tb1 | U-18tb1 | U-24tb1 | U-3tb1 | U-6tb1 | U-9tb1 | X2gd | X2iezn | Z1d
  - 存储优化：D3 | D3en | I3en
  - 加速计算： DL1 | g4ad | g4dn | G5 | g5g | Inf1 | p3dn | p4d | p4de | p4de | VT1

有关更多信息，请参阅第 5.1 节 Abort NVM Express 基本规范的命令。

Amazon EBS 卷的生命周期

Amazon EBS 卷的生命周期始于创建过程。您可以通过 Amazon EBS 快照创建卷，也可以创建空卷。在使用您的卷之前，您必须将其连接到与该卷位于同一可用区的一个或多个 Amazon EC2 实例。您可以将多个卷挂载到一个实例。如有需要，您也可以将卷从实例中分离，随后将其挂载到另一个实例。如果存储需求发生变化，则可以随时修改卷的大小或性能。您可以通过创建 Amazon EBS 快照来创建卷的 point-in-time备份。如果不再需要卷，则可将其删除，以免产生相关存储成本。

下图显示了可以在卷生命周期中对卷执行的操作。您还可以通过连接到实例并运行操作系统命令来执行某些任务。例如，格式化卷、挂载卷、管理分区和查看可用磁盘空间。



任务

- 创建 Amazon EBS 卷
- 将 Amazon EBS 卷附加到亚马逊 EC2 实例
- 使用多重连接将 EBS 卷连接到多个 EC2 实例
- 使 Amazon EBS 卷可供使用
- 查看关于 Amazon EBS 卷的信息
- 使用弹性卷操作修改 Amazon EBS 卷
- 将 Amazon EBS 卷与亚马逊实例分离 EC2
- 删除 Amazon EBS 卷

创建 Amazon EBS 卷

您可以创建 Amazon EBS 卷，然后将其连接到同一可用区中的任何 EC2 实例。

您可以创建空卷，也可以从 Amazon EBS 快照创建卷。如果从快照创建卷，则该卷将开始作为用于创建该快照的卷的精确副本。

卷初始化

当您从快照创建卷时，必须从 Amazon S3 下载快照中的存储块并将其写入卷，然后您才能访问它们。此过程称为卷初始化。在此期间，卷的 I/O 延迟将增加。只有将所有存储块下载并写入卷后，才能实现全卷性能。

默认的卷初始化率在整个初始化过程中会波动，这可能会使完成时间变得不可预测。

为了最大限度地减少与卷初始化相关的性能影响，您可以使用 Amazon EBS 预配置速率进行卷初始化（卷初始化率）或快速快照恢复。有关更多信息，请参阅 初始化 Amazon EBS 卷。

卷加密

卷的加密状态取决于您的账户是否启用了默认加密，以及快照的加密状态（如果您选择使用快照）。下表汇总了可能的加密结果。

默认加密	是否使用了快照？	卷加密结果	注意
已禁用	否	可选加密	如果启用加密，则可以指定要使用的 KMS 密钥。如果您启用加密但未指定 KMS 密钥，则使用 Amazon 托管式密钥 (aws/ebs)。
已禁用	是，未加密	可选加密	如果启用加密，则可以指定要使用的 KMS 密钥。如果您启用加密但未指定 KMS 密钥，则使用 Amazon 托管式密钥 (aws/ebs)。
已禁用	是，已加密	自动加密	您可以指定要使用的 KMS 密钥。如果未指定 KMS 密钥，则将使用与源快照相同的 KMS 密钥对卷进行加密。
已启用	否	自动加密	您可以指定要使用的 KMS 密钥。如果未指定 KMS 密钥，则默认使用指定用于加密的密钥。

默认加密	是否使用了快照？	卷加密结果	注意
已启用	是，未加密	自动加密	您可以指定要使用的 KMS 密钥。如果未指定 KMS 密钥，则默认使用指定用于加密的密钥。
已启用	是，已加密	自动加密	您可以指定要使用的 KMS 密钥。如果未指定 KMS 密钥，则使用与源快照（控制台）相同的密钥或默认指定用于加密的密钥（CLI/API）对卷进行加密。

额外注意事项

- 卷必须连接到同一可用区中的实例。
- 卷只有在进入`available`状态后才可以使用。
- 使用控制台创建卷时，gp3 是默认卷类型。对于命令行工具、API 和 SDK，默认卷类型是 gp2。
- 要对在 Outpost 上运行的实例使用某个卷，您必须在与该实例相同的 Outpost 上创建该卷。
- 如果创建了一个用于 Windows 实例的卷，并且该卷大于 2048 GiB，请确保将该卷配置为使用 GPT 分区表。有关更多信息，请参阅 Amazon EBS 卷限制 和 Windows support for disks larger than 2 TB。
- 也可以通过启动 Amazon EC2 实例间接创建卷。用于启动实例的 AMI 或实例启动请求本身可以包含 Amazon EBS 卷的块设备映射。有关更多信息，请参阅块设备映射。

Console

创建卷

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择卷，然后选择创建卷。
3. （仅限Outpost客户）对于 OutpostARN，请输入要在其Amazon Outpost上创建卷的 ARN。
4. 对于 Volume Type（卷类型），选择需要创建的卷类型。有关可用卷类型的更多信息，请参阅 Amazon EBS 卷类型。
5. 对于大小，以 GiB 为单位输入卷的大小。有关更多信息，请参阅 Amazon EBS 卷限制。

6. （仅限于 *io1*、*io2* 和 *gp3*）对于 IOPS，输入该卷应提供的每秒进行读写操作的次数（IOPS）的最大值。
7. （仅限于 *gp3*）对于吞吐量，以 MiB/s 为单位输入卷应提供的吞吐量。
8. 对于 Availability Zone，选择要在其中创建卷的可用区。
9. 对于快照 ID，执行以下任一操作：
   - 要创建空卷，保留默认值（不要从快照创建卷）。
   - 要从快照创建卷，请选择要使用的快照。
10. 如果您选择了快照，则可以选择为卷初始化速率指定卷初始化速率（以 MiB/s 为单位），即快照块在创建后从 Amazon S3 下载到卷的速率。有关更多信息，请参阅 使用 Amazon EBS 预配置速率进行卷初始化。要使用默认初始化速率或快速快照还原功能（如果已为所选快照启用此功能），请不要指定速率。
11. 设置卷的加密状态。
    - 如果您的账户启用了默认加密，则加密是自动的并且无法禁用。
    - 如果您选择了加密快照，则加密是自动的并且无法禁用。
    - 如果您的账户未启用默认加密，并且您选择未加密的快照或未选择快照，则加密是可选的。
12. （可选）要为卷分配自定义标签，请在标签部分中选择添加标签，然后输入标签键和值对。
13. 选择创建卷。
14. 要使用该卷，请等待其达到`available`状态，然后将其连接到同一可用区中的 Amazon EC2 实例。有关更多信息，请参阅 将 Amazon EBS 卷附加到亚马逊 EC2 实例。

Amazon CLI

创建卷

使用 create-volume 命令。以下示例在指定的可用区中创建一个大小为 100 GiB 的空 gp3 卷。

```
aws ec2 create-volume \
    --volume-type gp3 \
    --size 100 \
    --availability-zone us-east-1a
```

PowerShell

创建卷

使用 New-EC2Volume cmdlet。以下示例在指定的可用区中创建一个大小为 100 GiB 的空 gp3 卷。

```
New-EC2Volume `
    -VolumeType gp3 `
    -Size 100 `
    -AvailabilityZone us-east-1a
```

将 Amazon EBS 卷附加到亚马逊 EC2 实例

您可以将可用的 EBS 卷附加到与该卷处于同一可用区中的一个或多个实例。

有关在启动时向实例添加 EBS 卷的信息，请参阅实例块设备映射.。

注意事项

- 您可以连接到实例的 Amazon EBS 卷的最大数量取决于实例类型。如果您超过了某个实例类型的卷连接限制，则连接请求将失败并AttachmentLimitExceeded显示错误。有关更多信息，请参阅实例卷限制。
- 您只能将卷连接到位于同一可用区的实例。
- 如果卷上有 Amazon Web Services Marketplace 产品代码：
  - 您只能将其附加到已停止的实例。
  - 您必须订阅卷上的 Amazon Web Services Marketplace 代码。
  - 实例的配置（例如其类型和操作系统）必须支持该特定 Amazon Web Services Marketplace 代码。例如，您不能从 Windows 实例取用卷，然后将其附加到 Linux 实例。
  - Amazon Web Services Marketplace 代码从卷复制到实例。
- 您指定的设备名称由 Amazon 使用 EC2。块储存设备驱动程序可以用与您指定的名称不同的设备名称来装载设备。有关更多信息，请参阅 Amazon EC2 实例上卷的设备名称。
- 在某些情况下，与实例连接的卷以外的卷/dev/xvda或/dev/sda可能成为该实例的根卷。如果您将另一个实例的根卷或根据根卷的快照创建的卷连接到具有现有根卷的实例，则可能会发生这种情况。有关更多信息，请参阅从错误的音量启动。

Console

将 EBS 卷连接到实例

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。

2. 在导航窗格中，选择 Volumes。
3. 选择需要附加的卷，然后选择 Actions（操作）、Attach volume（附加卷）。
4. 对于 Instance（实例），输入实例的 ID 或从选项列表中选择实例。
5. 对于设备名称，执行以下操作之一：
   - 对于根卷，从列表的为根卷预留部分选择所需的设备名称。对于 Linux 实例通常为 `/dev/sda1` 或 `/dev/xvda`（具体取决于 AMI），或者对于 Windows 实例 为 `/dev/sda1`。
   - 对于数据卷，请从列表的建议用于数据卷部分中选择一个可用的设备名称。
   - 要使用自定义设备名称，请选择指定自定义设备名称，然后输入要使用的设备名称。
6. 选择附加卷。
7. 连接到实例并挂载卷。有关更多信息，请参阅 使 Amazon EBS 卷可供使用。

Amazon CLI

将 EBS 卷连接到实例

使用 attach-volume 命令。以下示例使用指定的设备名称将指定的卷连接到指定的实例。

```
aws ec2 attach-volume \
    --volume-id vol-01234567890abcdef \
    --instance-id i-1234567890abcdef0 \
    --device /dev/sdf
```

PowerShell

将 EBS 卷连接到实例

使用 Add-EC2Volume cmdlet。以下示例使用指定的设备名称将指定的卷连接到指定的实例。

```
Add-EC2Volume `
    -VolumeId vol-01234567890abcdef `
    -InstanceId i-1234567890abcdef0 `
    -Device /dev/sdf
```

使用多重连接将 EBS 卷连接到多个 EC2 实例

通过 Amazon EBS 多重挂载，您可以将单个预置 IOPS SSD（io1 或 io2）卷挂载到位于同一可用区中的多个实例。您可以将多个启用多重挂载的卷附加到一个实例或一组实例。卷附加到的每个实例都对

共享卷拥有完全读取和写入权限。通过多重挂载，您可以更轻松地在管理并发写入操作的应用程序中实现更高的应用程序可用性。

定价和计费

使用 Amazon EBS 多重挂载不会产生额外费用。您需要按照适用于预置 IOPS SSD（io1 和 io2）卷的标准计费。有关更多信息，请参阅 Amazon EBS 定价。

内容

- 注意事项和限制
- 多重挂载 Amazon EBS 卷的性能
- 为 Amazon EBS 卷启用多重挂载
- 为 Amazon EBS 卷禁用多重挂载
- 使用支持多重连接的 Amazon EBS 卷的 NVMe 预留

注意事项和限制

- 启用多重挂载的卷最多可以挂载到位于相同可用区内的基于 Nitro 系统构建的 16 个实例。
- Linux 实例支持启用多重挂载的 io1 和 io2 卷。Windows 实例仅支持启用多重挂载的 io2 卷。
- 您可以挂载到实例的最大 Amazon EBS 卷数取决于实例类型和实例规模。有关更多信息，请参阅实例卷限制。
- 仅在预调配 IOPS SSD（io1 和 io2）卷上才支持多重挂载。
- io1 卷的多重挂载仅在以下区域可用：美国东部（弗吉尼亚州北部）、美国西部（俄勒冈州）和亚太地区（首尔）。

  适用于 io2 的多重挂载功能已在所有支持 io2 的区域中提供。

  > **Note**
  >
  > 为了以更低的成本获得更好的性能、一致性和耐用性，我们建议您使用 io2 卷。

- 当基于 Nitro System 而构建的实例仅支持可扩展的可靠数据报（SRD）网络协议时，将不支持启用了多重挂载的 io1 卷。要对这些实例类型使用多重连接，必须使用io2。
- 标准文件系统（例如 XFS 和 EXT4）不适合多台服务器（例如 EC2 实例）同时访问。您应使用集群文件系统来确保生产工作负载的数据恢复能力和可靠性。

- 启用多重挂载的 io2 卷支持 I/O 隔离栏。I/O 隔离栏协议控制共享存储环境中的写入访问，以保持数据一致性。您的应用程序必须为附加的实例提供写入顺序，以保持数据一致性。有关更多信息，请参阅 使用支持多重连接的 Amazon EBS 卷的 NVMe 预留。

  启用多重挂载的 io1 卷不支持 I/O 隔离栏。
- 无法将启用多重挂载的卷创建为引导卷。
- 可以将启用多重挂载的卷附加到每个实例的一个块储存设备映射。
- 在实例启动期间，无法使用 Amazon EC2 控制台或 RunInstances API 启用多重连接。
- 在 Amazon EBS 基础结构层存在问题的启用多重挂载的卷对于所有附加的实例都不可用。Amazon EC2 或网络层的问题可能只会影响部分连接的实例。
- 下表显示了创建后对启用多重挂载的 io1 和 io2 卷的卷修改支持。

	io2 卷	**io1 卷**
修改卷类型	✗	✗
修改卷大小	✓	✗
修改预置 IOPS	✓	✗
启用多重挂载	✓ *	✗
禁用多重挂载	✓ *	✗

*当卷挂载到实例时，您无法启用或禁用多重挂载。

- 如果最后一个附加的实例终止，并且该实例配置为在终止时删除卷，则启用多重挂载的卷将在实例终止时被删除。如果卷附加到多个实例，而这些实例在其卷块储存设备映射中具有不同的终止时删除设置，则最后一个附加的实例的块储存设备映射设置决定终止时删除行为。

  要确保对终止行为进行可预测删除，为卷挂载到的所有实例启用或禁用“终止时删除”。有关更多信息，请参阅实例终止时保留数据。
- 您可以使用 Amazon EBS 卷的 CloudWatch 指标监控启用了多重连接的卷。在所有附加的实例之间聚合数据。您无法监控单个附加的实例的指标。有关更多信息，请参阅 亚马逊 EBS 的亚马逊 CloudWatch 指标。

多重挂载 Amazon EBS 卷的性能

每个附加的实例都能够将其最大 IOPS 性能提升到卷的最大预置性能。但是，所有附加的实例的总体性能不能超过卷的最大预置性能。如果附加实例的 IOPS 需求高于卷的预置 IOPS，则卷不会超过其预置性能。

例如，假设您使用 `io2` 预置 IOPS 创建 `80,000` 启用了多重挂载的卷，然后将其挂载到最高支持 `40,000` IOPS 的 `m7g.large` 实例和最高支持 `60,000` IOPS 的 `r7g.12xlarge` 实例。每个实例都可以提升其最大 IOPS，因为它小于卷的预置 IOPS `80,000`。但是，如果两个实例同时提升对卷的 I/O，则其组合 IOPS 不能超过卷的预置性能 `80,000` IOPS。

为了实现一致的性能，最佳做法是在启用多重挂载的卷的扇区间平衡由附加实例提升的 I/O。

有关亚马逊 EC2 实例类型的 IOPS 性能的更多信息，请参阅亚马逊 EC2 用户指南中的亚马逊 EBS 优化实例类型。

为 Amazon EBS 卷启用多重挂载

启用了多重挂载的卷的管理方式与管理任何其他 Amazon EBS 卷的方式大致相同。但是，为了使用多重挂载功能，您必须为卷启用它。

当您创建新卷时，默认情况下，多重挂载处于禁用状态。您可以在创建卷时启用多重连接。

您还可以在创建 `io2` 卷之后，仅在这些卷没有挂载到任何实例的情况下，为其启用多重挂载。在创建之后，您不能为 `io1` 卷启用多重挂载。

为卷启用多重连接后，您可以像连接任何其他 EBS 卷一样将该卷连接到实例。有关更多信息，请参阅将 Amazon EBS 卷附加到亚马逊 EC2 实例。

Console

在卷创建过程中启用多重挂载

1. 打开亚马逊 EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Volumes。
3. 选择创建卷。
4. 对于卷类型，选择预调配 IOPS SSD（**io1**）或预调配 IOPS SSD（**io2**）。
5. 对于大小和 IOPS，选择所需的卷大小和要预置的 IOPS 数。
6. 对于可用区，请选择实例所在的相同可用区。

7. 对于 Amazon EBS Multi-Attach（Amazon EBS 多重挂载），选择 Enable Multi-Attach（启用多重挂载）。
8. （可选）对于快照 ID，选择快照并从中创建卷。
9. 设置卷的加密状态。

   如果选定的快照已加密，或者您的账户已启用默认加密，则加密会自动启用，而且您无法禁用它。您可以选择用于加密卷的 KMS 密钥。

   如果选定的快照未加密，且默认情况下账户未启用加密，则加密是可选的。要加密卷，请为 Encryption（加密）选择 Encrypt this volume（加密此卷），然后选择要用于加密卷的 KMS 密钥。

   加密卷只能附加到支持 Amazon EBS 加密的实例上。有关更多信息，请参阅 Amazon EBS 加密。
10. （可选）要为卷分配自定义标签，请在标签部分中选择添加标签，然后输入标签键和值对。
11. 选择创建卷。

在创建后启用多重挂载

1. 打开亚马逊 EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Volumes。
3. 选择所需卷，然后选择 Actions（操作）、Modify Volume（修改卷）。
4. 对于 Amazon EBS Multi-Attach（Amazon EBS 多重挂载），选择 Enable Multi-Attach（启用多重挂载）。
5. 选择 Modify(修改)。

Amazon CLI

在卷创建过程中启用多重挂载

使用带选项的 create-vol ume 命令。`--multi-attach-enabled`

```
aws ec2 create-volume \
    --volume-type io2 \
    --multi-attach-enabled \
    --size 100 \
```

```
    --iops 2000 \
    --region us-west-2 \
    --availability-zone us-west-2b
```

在创建后启用多重挂载

使用带有选项的 m odify-vol ume 命令。`--multi-attach-enabled`

```
aws ec2 modify-volume \
    --volume-id vol-01234567890abcdef \
    --multi-attach-enabled
```

PowerShell

在卷创建过程中启用多重挂载

使用带有参数的 New-EC2Volumecmdlet。`-MultiAttachEnabled`

```
New-EC2Volume `
    -VolumeType io2 `
    -MultiAttachEnabled $true `
    -Size 100 `
    -Iops 2000 `
    -Region us-west-2 `
    -AvailabilityZone us-west-2b
```

在创建后启用多重挂载

使用带有参数的 Edit-EC2Volumecmdlet。`-MultiAttachEnabled`

```
Edit-EC2Volume `
    -VolumeId vol-01234567890abcdef `
    -MultiAttachEnabled $true
```

为 Amazon EBS 卷禁用多重挂载

只有当 io2 卷挂载到不超过一个实例时，您才能对其禁用多重挂载。

在创建之后，您不能为 io1 卷禁用多重挂载。

Console

在创建后禁用多重挂载

1. 打开亚马逊 EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Volumes。
3. 选择所需卷，然后选择 Actions（操作）、Modify Volume（修改卷）。
4. 对于 Amazon EBS 多重挂载，清除 Enable Multi-Attach（启用多重挂载）。
5. 选择修改。

Amazon CLI

在创建后禁用多重挂载

使用带有选项的 m odify-vol ume 命令。`-no-multi-attach-enabled`

```
aws ec2 modify-volume \
    --volume-id vol-01234567890abcdef \
    --no-multi-attach-enabled
```

PowerShell

在创建后禁用多重挂载

使用带有参数的 Edit-EC2Volumecmdlet。`-MultiAttachEnabled`

```
Edit-EC2Volume `
    -VolumeId vol-01234567890abcdef `
    -MultiAttachEnabled $false
```

使用支持多重连接的 Amazon EBS 卷的 NVMe 预留

支持多重连接的io2卷支持 NVMe 预留，这是一组行业标准的存储屏蔽协议。这些协议可让您创建和管理预留，以控制和协调多个实例对共享卷的访问。共享存储应用程序使用预留来确保数据一致性。

内容

- 要求
- 启用对 NVMe 预订的支持

- 支持的 NVMe 预留命令
- 定价

要求

NVMe 只有启用了多重连接的io2卷才支持预留。启用多重挂载的卷仅可以连接到基于 Nitro 系统构建的实例。

NVMe 以下操作系统支持预订：

- SUSE Linux 企业版 12 SP3 及更高版本
- RHEL 8.3 和更高版本
- Amazon Linux 2 和更高版本
- Windows Server 2016 及更高版本

> **Note**
>
> 对于 AMIs 日期为 2023.09.13 及更高版本的 Windows 服务器，包括所需的NVMe 驱动程序。对于更早版本 AMIs，您必须更新到 NVMe 驱动程序版本 1.5.0 或更高版本。有关更多信息，请参阅Amazon NVMe 驱动程序。

如果您使用 La EC2 unch v2 初始化磁盘，则必须升级到 2.0.1521 或更高版本。有关更多信息，请参阅使用 La EC2 unch v2 代理。

启用对 NVMe 预订的支持

2023 年 9 月 18 日之后创建的所有支持多重连接的io2卷默认启用 NVMe 预留支持。

要启用对在 2023 年 9 月 18 日之前创建的现有io2卷的 NVMe 预留支持，您必须将所有实例与该卷分离，然后重新连接所需的实例。在分离所有实例后创建的所有附件都将启用 NVMe 预留。

支持的 NVMe 预留命令

Amazon EBS 支持以下 NVMe 预留命令：

Reservation Register

注册、取消注册或替换预留密钥。注册密钥用于识别和验证实例。向卷注册预留密钥会在实例和卷之间建立关联。您必须先向卷注册实例，然后该实例才能获得预留。

Reservation Acquire

获取卷上的预留，抢占命名空间上保存的预留，以及中止在卷上保存的预留。可以获取以下预留类型：

- 写专属预留
- 专属访问预留
- 写专属 - 仅限注册者预留
- 专属访问 - 仅限注册者预留
- 写专属 - 所有注册者预留
- 专属访问 - 所有注册者预留

Reservation Release

释放或清除卷上保存的预留。

Reservation Report

描述卷的注册和预留状态。

定价

启用和使用多重挂载不会产生额外费用。

使 Amazon EBS 卷可供使用

将某个 Amazon EBS 卷挂载到实例后，该卷将显示为块设备。您可以使用任何文件系统将卷格式化，然后进行挂载。在使 EBS 卷可供使用后，您可以像访问其他所有卷一样访问该卷。任何写入此文件系统的数据均写入 EBS 卷，并且对使用该设备的应用程序是透明的。

您可以制作 EBS 卷的快照以进行备份或在您创建其他卷时作为基准。有关更多信息，请参阅 Amazon EBS 快照。

如果您准备使用的 EBS 卷大于 2TiB，则必须使用 GPT 分区方案才能访问整个卷。有关更多信息，请参阅 Amazon EBS 卷限制。

Linux 实例

格式化并挂载附加的卷

假设您有一个带有根设备的 EBS 卷的 EC2 实例`/dev/xvda`，并且您刚刚使用将一个空的 EBS 卷连接到该实例。`/dev/sdf`按照以下过程使新附加的卷可用。

在 Linux 上格式化并挂载 EBS 卷

1. 使用 SSH 连接到实例。有关更多信息，请参阅连接到您的 Linux 实例。
2. 设备可附加到设备名称与您在块储存设备映射中指定的设备名称不同的实例。有关更多信息，请参阅 Linux 实例上的设备名称。使用 lsblk 命令可查看可用磁盘设备及其挂载点（如果适用），以帮助您确定要使用的正确设备名称。lsblk 的输出从完整的设备路径中去掉了 /dev/ 前缀。

   以下是基于 Nitro System 构建的实例的输出示例，该系统将 EBS 卷作为 NVMe区块设备公开。根设备为 /dev/nvme0n1，它有两个名为 nvme0n1p1 和 nvme0n1p128。如果没有分区且尚未附加，则附加卷为 /dev/nvme1n1。

   ```
   [ec2-user ~]$ lsblk
   NAME          MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
   nvme1n1       259:0    0  10G  0 disk
   nvme0n1       259:1    0   8G  0 disk
   -nvme0n1p1    259:2    0   8G  0 part /
   -nvme0n1p128  259:3    0   1M  0 part
   ```

   以下是 T2 实例的示例输出。根设备为 /dev/xvda，它有名为 xvda1 的一个分区。如果没有分区且尚未附加，则附加卷为 /dev/xvdf。

   ```
   [ec2-user ~]$ lsblk
   NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
   xvda    202:0    0    8G  0 disk
   -xvda1  202:1    0    8G  0 part /
   xvdf    202:80   0   10G  0 disk
   ```

3. 确定卷上是否存在文件系统。新卷为原始的块储存设备，您必须先在这种设备上创建文件系统，然后才能够挂载并使用它们。从快照创建的卷可能已经含有文件系统；如果您在现有的文件系统上创建新的文件系统，则该操作将覆盖您的数据。

   使用以下一种或两种方法来确定卷上是否有文件系统：

   - 使用 file -s 命令获取有关特定设备的信息，例如其文件系统类型。如果输出仅显示 data（如以下示例输出所示），则说明设备上没有文件系统。

     ```
     [ec2-user ~]$ sudo file -s /dev/xvdf
     /dev/xvdf: data
     ```

如果设备有文件系统，该命令会显示有关文件系统类型的信息。例如，以下示例输出显示具有 XFS 文件系统的根设备。

```
[ec2-user ~]$ sudo file -s /dev/xvda1
/dev/xvda1: SGI XFS filesystem data (blksz 4096, inosz 512, v2 dirs)
```

- 使用 lsblk -f 命令获取有关连接到实例的所有设备的信息。

```
[ec2-user ~]$ sudo lsblk -f
```

例如，以下输出显示有三个设备连接到实例 – nvme1n1、nvme0n1 和 nvme2n1。第一列列出了设备及其分区。FSTYPE 列显示每个设备的文件系统类型。如果该列对于特定设备为空，则表示该设备没有文件系统。在这种情况下，设备 nvme1n1 和设备 nvme0n1 上的分区 nvme0n1p1 都使用 XFS 文件系统进行格式化，而设备 nvme2n1 和设备 nvme0n1 上的分区 nvme0n1p128 没有文件系统。

```
NAME  FSTYPE LABEL UUID      MOUNTPOINT
nvme1n1         xfs  7f939f28-6dcc-4315-8c42-6806080b94dd
nvme0n1
##nvme0n1p1 xfs     / 90e29211-2de8-4967-b0fb-16f51a6e464c         /
##nvme0n1p128
nvme2n1
```

如果这些命令的输出显示设备上没有文件系统，则必须创建一个文件系统。

4. （有条件）如果您在上一步中发现设备上存在文件系统，请跳过此步骤。如果您有一个空卷，请使用 mkfs -t 命令在该卷上创建一个文件系统。

> **Warning**
>
> 如果要挂载已具有数据的卷（例如，从快照创建的卷），请勿使用此命令。否则，您会格式化卷并删除现有数据。

```
[ec2-user ~]$ sudo mkfs -t xfs /dev/xvdf
```

如果出现“找不到 mkfs.xfs”错误，请使用以下命令安装 XFS 工具，然后重复上一命令：

```
[ec2-user ~]$ sudo yum install xfsprogs
```

5. 使用 mkdir 命令创建卷的挂载点目录。挂载点是卷在文件系统树中的位置，以及您在安装卷之后读写文件的位置。下面的示例创建一个名为 /data 的目录。

```
[ec2-user ~]$ sudo mkdir /data
```

6. 在您于上一步创建的挂载点目录中挂载卷或分区。

   如果该卷没有分区，请使用以下命令并指定设备名称来挂载完整的卷。

```
[ec2-user ~]$ sudo mount /dev/xvdf /data
```

   如果该卷有分区，请使用以下命令并指定分区名称来挂载分区。

```
[ec2-user ~]$ sudo mount /dev/xvdf1 /data
```

7. 检查新卷挂载的文件权限，确保您的用户和应用程序可以向该卷写入数据。有关文件权限的更多信息，请参阅 Linux 文档项目 文件安全性。
8. 重启实例后，挂载点不会自动保留。要在重启后自动挂载此 EBS 卷，请按照下一个过程进行操作。

重启后自动挂载附加的卷

要在每次系统重启时附加附加的 EBS 卷，可在 /etc/fstab 文件中为该设备添加一个条目。

您可以在 /dev/xvdf 中使用设备名称（例如 /etc/fstab），但建议改为使用设备的 128 位通用唯一标识符（UUID）。设备名称可以更改，但 UUID 会在整个分区的使用寿命期间保留。通过使用 UUID，您可以减少系统在硬件重新配置后无法启动的机会。有关更多信息，请参阅将 Amazon EBS 卷映射到 NVMe 设备名称。

重启后自动附加附加卷

1. （可选）创建 /etc/fstab 文件的备份，以便在编辑时误损坏或删除此文件时使用。

```
[ec2-user ~]$ sudo cp /etc/fstab /etc/fstab.orig
```

2. 使用 blkid 命令查找设备的 UUID。记下要在重新启动后挂载的设备的 UUID。在下一步中您将需要用到它。

例如，以下命令显示实例上装载了两台设备，并显示了这两台设备 UUIDs 的。

```
[ec2-user ~]$ sudo blkid
/dev/xvda1: LABEL="/" UUID="ca774df7-756d-4261-a3f1-76038323e572" TYPE="xfs"
 PARTLABEL="Linux" PARTUUID="02dcd367-e87c-4f2e-9a72-a3cf8f299c10"
/dev/xvdf: UUID="aebf131c-6957-451e-8d34-ec978d9581ae" TYPE="xfs"
```

对于 Ubuntu 18.04，请使用 lsblk 命令。

```
[ec2-user ~]$ sudo lsblk -o +UUID
```

3. 使用任何文本编辑器（如 /etc/fstab 和 nano）打开 vim 文件。

```
[ec2-user ~]$ sudo vim /etc/fstab
```

4. 将以下条目添加到 /etc/fstab 以在指定的挂载点挂载设备。这些字段是 blkid（或用于 Ubuntu 18.04 的 lsblk）返回的 UUID 值、挂载点、文件系统以及建议的文件系统挂载选项。有关必填字段的更多信息，请运行 man fstab 以打开 fstab 手册。

   在以下示例中，我们将 UUID 为 aebf131c-6957-451e-8d34-ec978d9581ae 的设备挂载到挂载点 /data，然后我们使用 xfs 文件系统。我们还使用 defaults 和 nofail 标志。我们指定 0 以防止文件系统被转储，并且我们指定 2 以指示它是非根设备。

```
UUID=aebf131c-6957-451e-8d34-ec978d9581ae  /data  xfs  defaults,nofail  0  2
```

> **Note**
>
> 如果您要在未附加此卷的情况下启动实例（例如，将卷移动到另一个实例之后），nofail 附加选项允许该实例即使在卷附加过程中出现错误时也可启动。Debian 衍生物（包括早于 16.04 的 Ubuntu 版本）还必须添加 nobootwait 挂载选项。

5. 要检查条目是否有效，请在 /etc/fstab 中运行以下命令以卸载设备，然后挂载所有文件系统。如果未产生错误，则说明 /etc/fstab 文件正常，您的文件系统会在重启后自动挂载。

```
[ec2-user ~]$ sudo umount /data
[ec2-user ~]$ sudo mount -a
```

   如果收到错误消息，请解决文件中的错误。

> **Warning**
>
> /etc/fstab 文件中的错误可能显示系统无法启动。请勿关闭 /etc/fstab 文件中有错误的系统。

如果您无法确定如何更正 /etc/fstab 中的错误并且您在此过程的第一步中创建了一个备份文件，则可以使用以下命令从您的备份文件还原。

```
[ec2-user ~]$ sudo mv /etc/fstab.orig /etc/fstab
```

Windows 实例

使用以下任一方法在 Windows 实例上启用卷。

PowerShell

使所有带有原始分区的 EBS 卷都可用于 Windows PowerShell

1. 使用远程桌面登录 Windows 实例。有关更多信息，请参阅连接到 Windows 实例。
2. 在任务栏上，打开 “开始” 菜单，然后选择 “Windows PowerShell”。
3. 在打开的 PowerShell 提示符下使用提供的一系列 Windows PowerShell 命令。此脚本会默认执行以下操作：
   1. 停止命令行管理程序HWDetection 服务。
   2. 枚举分区样式为原始的磁盘。
   3. 创建一个涵盖磁盘和分区类型将支持的最大大小的新分区。
   4. 分配一个可用的驱动器盘符。
   5. 使用指定的文件系统标注将文件系统格式化为 NTFS。
   6. 再次启动命令行管理程序HWDetection 服务。

```
Stop-Service -Name ShellHWDetection
Get-Disk | Where PartitionStyle -eq 'raw' | Initialize-Disk -PartitionStyle MBR
 -PassThru | New-Partition -AssignDriveLetter -UseMaximumSize | Format-Volume -
FileSystem NTFS -NewFileSystemLabel "Volume Label" -Confirm:$false
```

```
Start-Service -Name ShellHWDetection
```

DiskPart command line tool

使 EBS 卷可用于 DiskPart 命令行工具

1. 使用远程桌面登录 Windows 实例。有关更多信息，请参阅连接到 Windows 实例。
2. 确定要开放使用的磁盘编号：
   1. 打开 “开始” 菜单，然后选择 “窗口” PowerShell。
   2. 使用 `Get-Disk` Cmdlet 来检索可用磁盘列表。
   3. 在命令输出中，记下您开放使用的磁盘对应的 Number（编号）。
3. 创建脚本文件来执行 DiskPart 命令：
   1. 打开 Start（开始）菜单，然后选择 File Explorer（文件管理器）。
   2. 导航到某个目录（例如 C:\）以存储脚本文件。
   3. 选择或右键单击文件夹中的空白区域以打开对话框，将光标置于 New（新建）上方以访问上下文菜单，然后选择 Text Document（文本文档）。
   4. 命名文本文件 `diskpart.txt`。
4. 将下列命令添加到脚本文件中。您可能需要修改磁盘编号、分区类型、卷标和驱动器盘符。此脚本会默认执行以下操作：
   1. 选择磁盘 1 进行修改。
   2. 将卷配置为使用主引导记录（MBR）分区结构。
   3. 将卷格式化为 NTFS 卷。
   4. 设置卷标。
   5. 为卷分配一个驱动器盘符。

> **Warning**
>
> 如果您挂载其中已有数据的卷，请不要格式化卷，否则会删除现有数据。

```
select disk 1
attributes disk clear readonly
```

```
online disk noerr
convert mbr
create partition primary
format quick fs=ntfs label="volume_label"
assign letter="drive_letter"
```

有关更多信息，请参阅DiskPart 语法和参数。

5. 打开命令提示符，导航到脚本所在的文件夹，然后运行以下命令以使该卷可用于指定的磁盘：

```
C:\> diskpart /s diskpart.txt
```

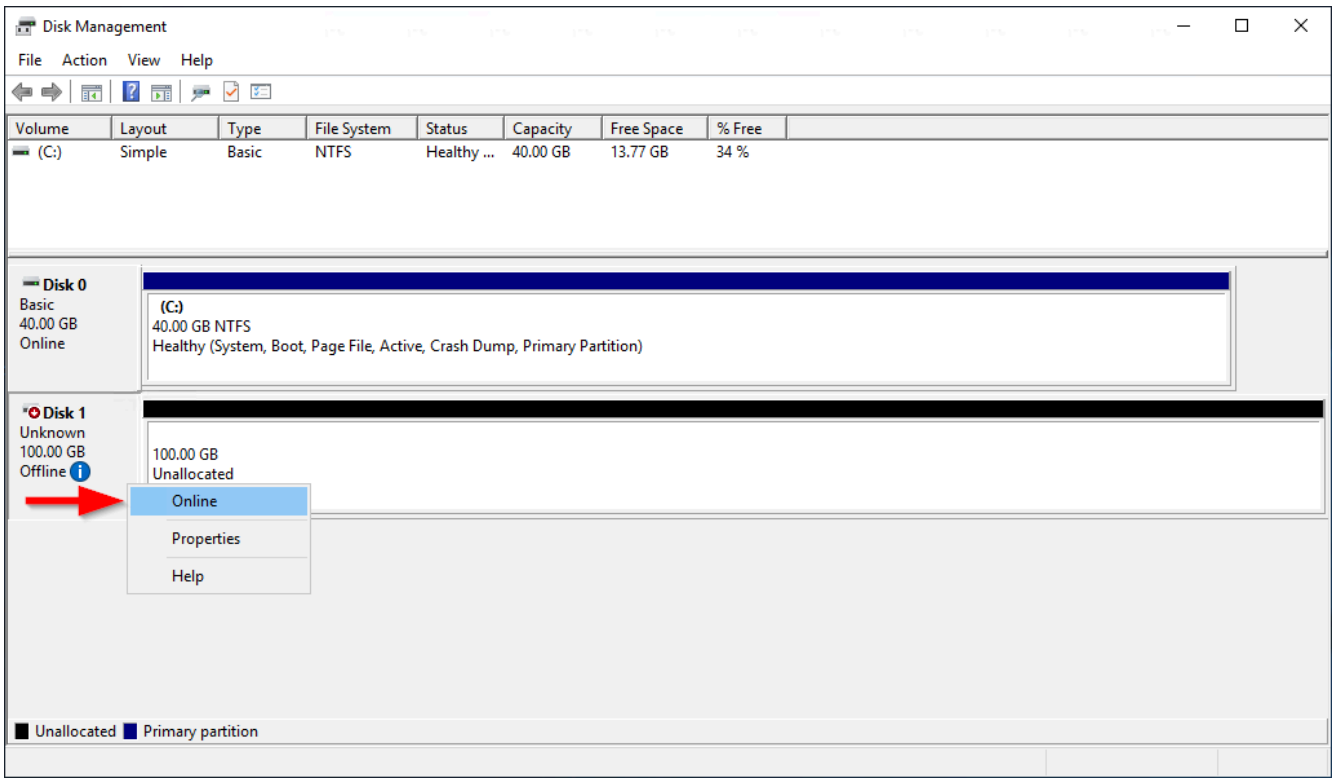
Disk Management utility

借助磁盘管理实用工具使 EBS 卷可供使用

1. 使用远程桌面登录 Windows 实例。有关更多信息，请参阅连接到 Windows 实例。
2. 开启磁盘管理实用工具。在任务栏上，打开 Windows 徽标的上下文（右键单击）菜单，然后选择磁盘管理。

> **Note**
>
> 在 Windows Server 2008 中，依次选择 Start（开始）、Administrative Tools（管理工具）、Computer Management（计算机管理）和 Disk Management（磁盘管理）。

3. 将卷联机。在下面的窗格中，在左侧面板中打开 EBS 卷磁盘的上下文（右键单击）菜单。选择联机。

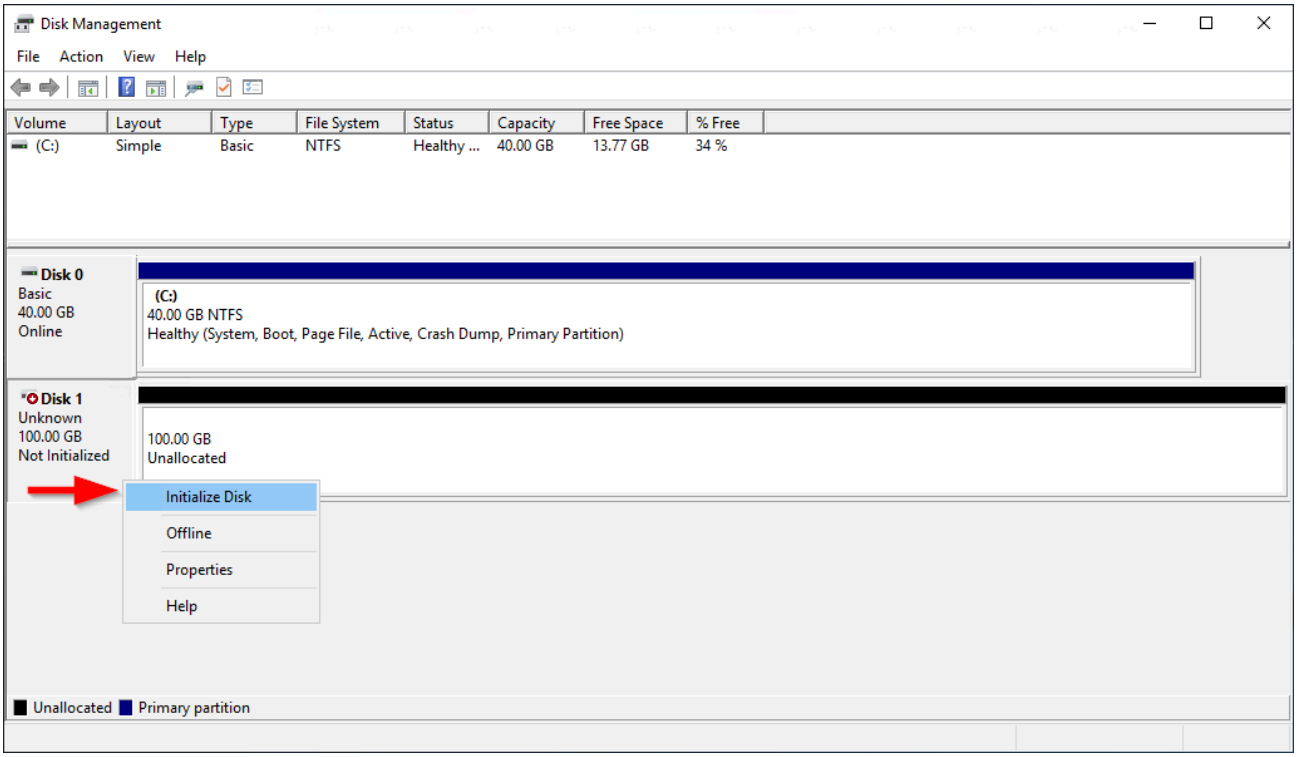


4. （视情况而定）若未初始化磁盘，您必须初始化磁盘然后才能使用。如果磁盘已初始化，请跳过此步骤。

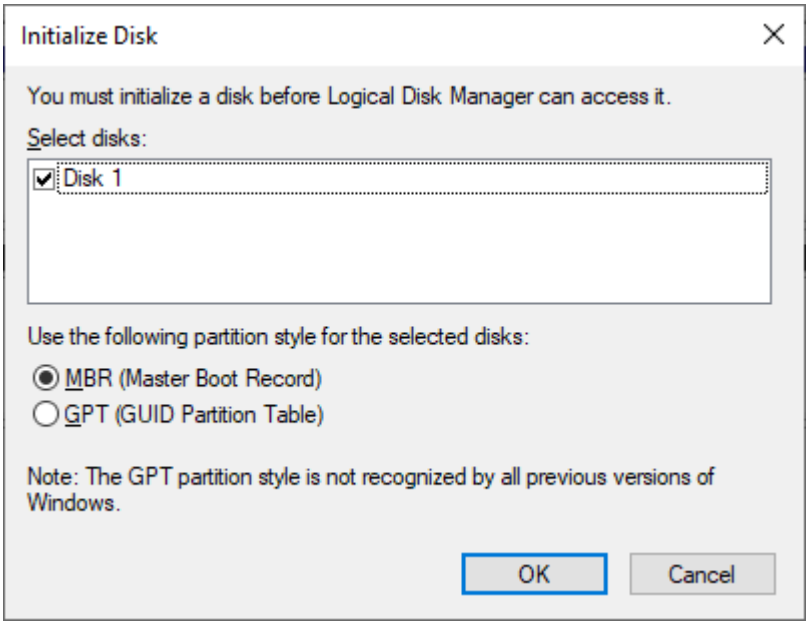
> **Warning**
>
> 如果在挂载的卷上已包含数据（例如，公用数据集或通过快照创建的卷），请不要重新格式化卷，否则，将删除现有的数据。

如果未初始化磁盘，请按以下方式将其初始化：

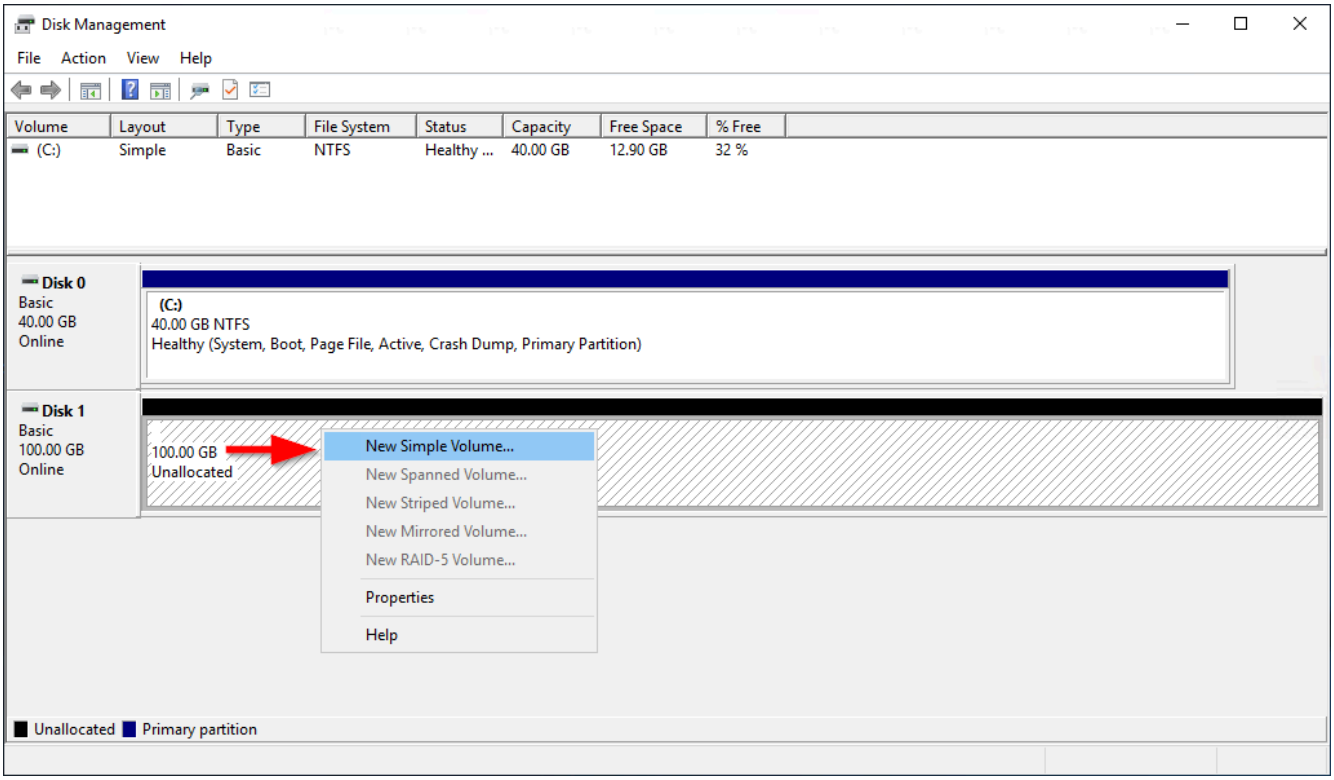
1. 在左侧面板中打开磁盘的上下文（右键单击）菜单，然后选择初始化磁盘。



2. 在 Initialize Disk（初始化磁盘）对话框中，选择一种分区格式，然后选择 OK（确定）。

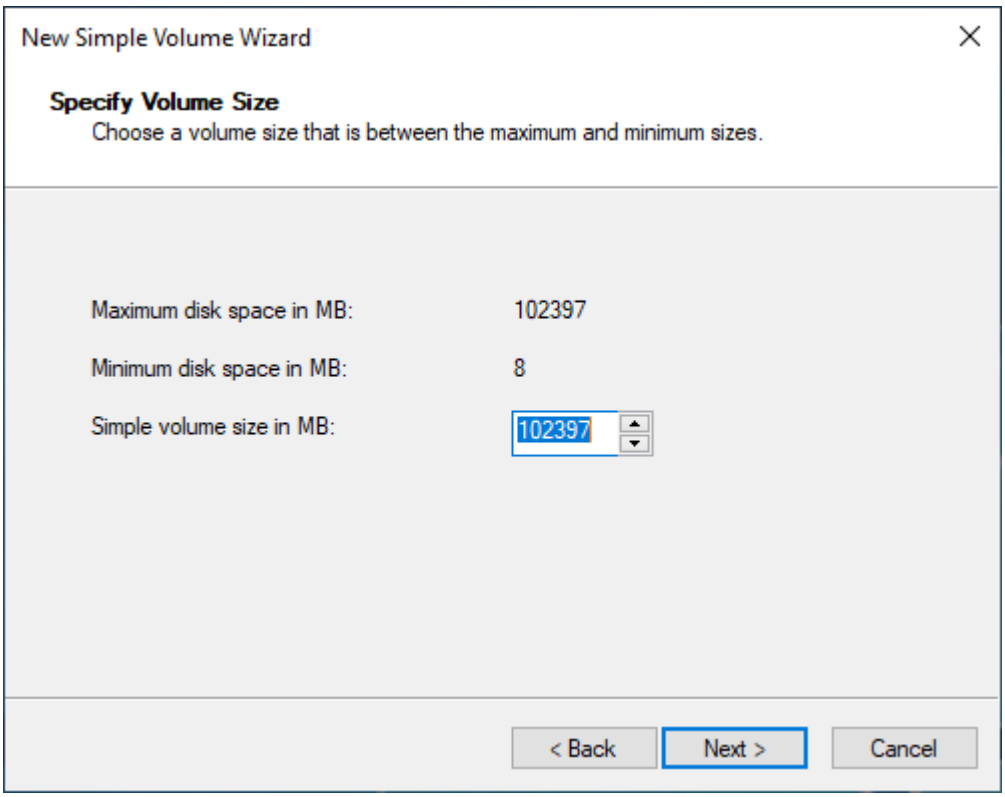


5. 在右侧面板中打开磁盘的上下文（右键单击）菜单，然后选择新建简单卷。

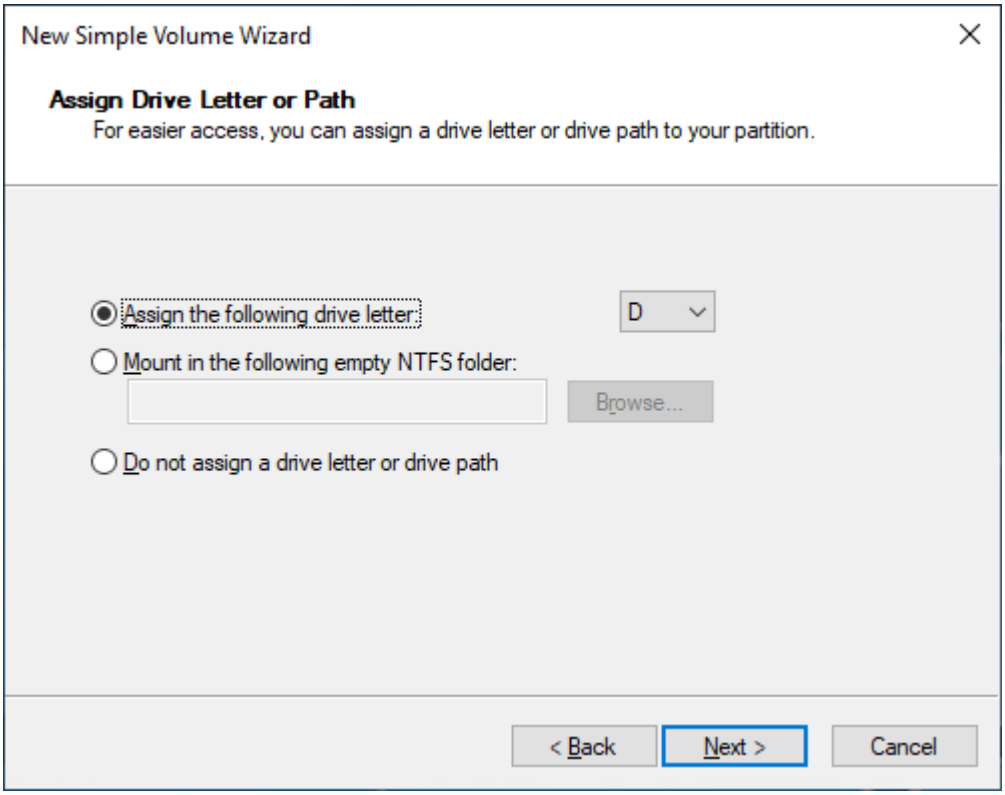


6. 在 New Simple Volume Wizard（新建简单卷向导）中，选择 Next（下一步）。

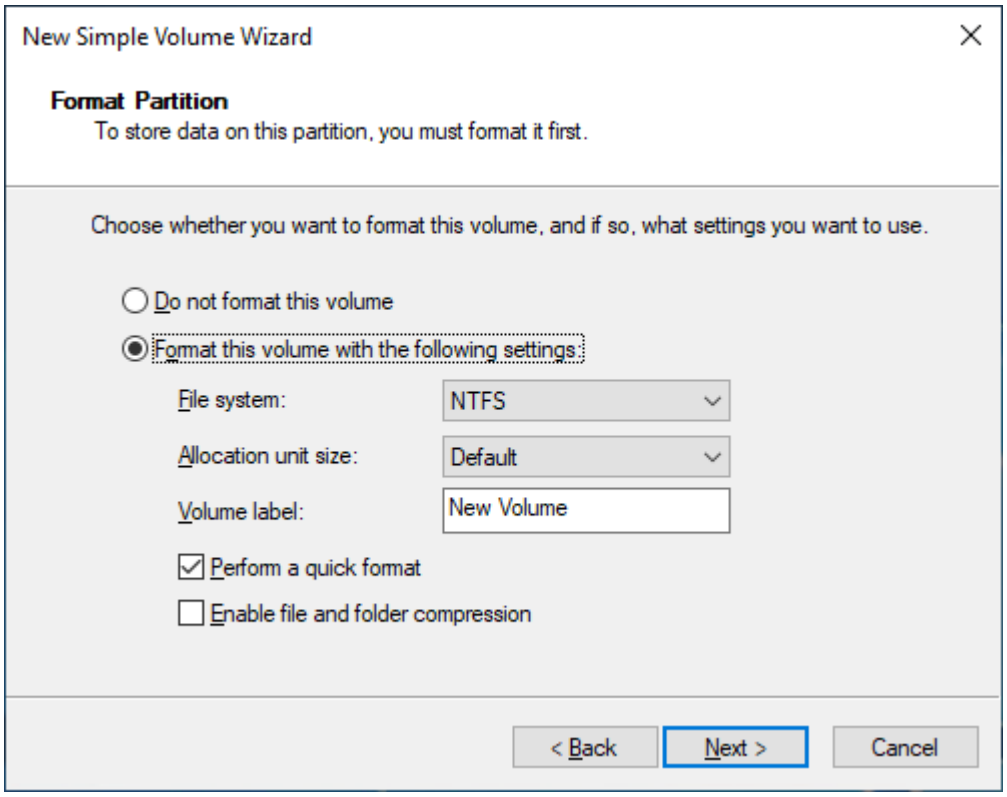
7. 如果要原定设置的最大值，请指定Simple volume size in MB [简单卷大小（MB）]，然后选择 Next（下一步）。



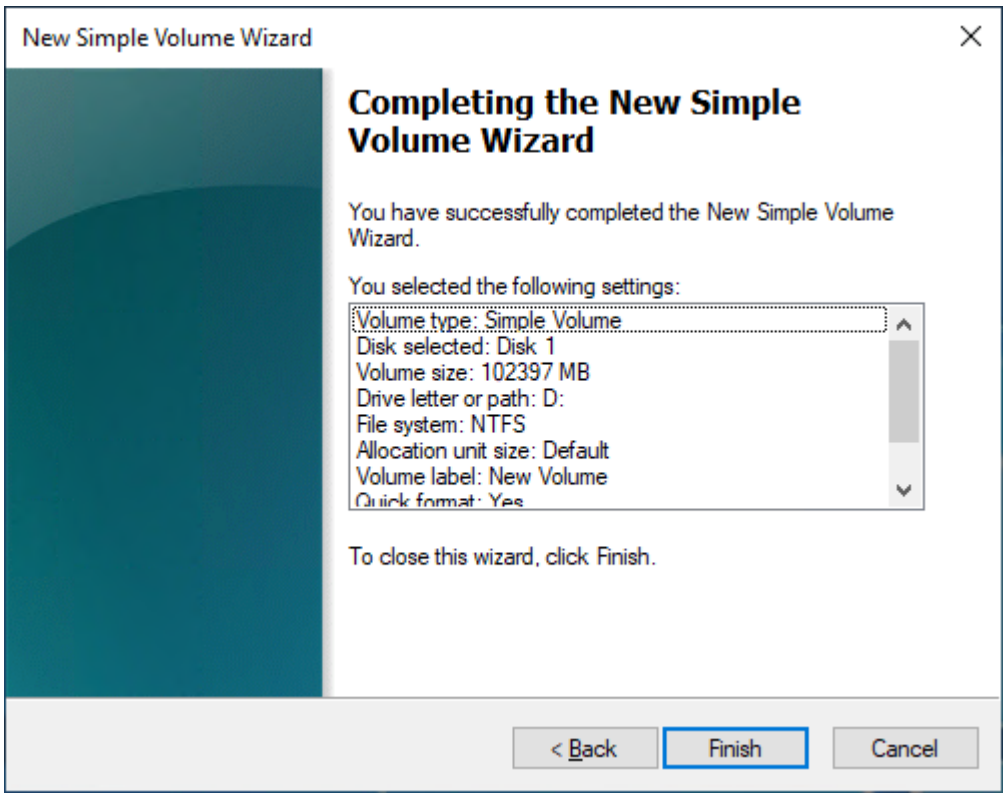
8. 如有必要，在 Assign the following drive letter（分配以下驱动器盘符）下拉菜单中指定一个您偏好的驱动器盘符，然后选择 Next（下一步）。



9. 指定 Volume Label（卷标）并根据需要调整原定设置，然后选择 Next（下一步）。



10. 检查设置，然后选择 Finish（完成）以应用修改并关闭新建简单卷向导。



查看关于 Amazon EBS 卷的信息

您可以查看有关您的 EBS 卷的描述信息。例如，您可以查看有关特定区域中所有卷的信息，或者查看有关单个卷的详细信息，包括其大小、卷类型、卷是否加密、加密卷所用的 KMS 密钥以及卷附加到的特定实例。

您可以获得有关您的 EBS 卷的其他信息，例如该实例的操作系统上有多少空间磁盘可用。

内容

- 查看卷信息
- 卷状态
- 查看卷指标
- 查看可用磁盘空间

查看卷信息

您可以查看有关您的 EBS 卷的信息。

Console

查看有关卷的信息

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Volumes。
3. 要减少列表，您可以使用标签和卷属性来筛选卷。选择筛选条件字段，选择标签或卷属性，然后选择筛选条件值。
4. 要查看有关卷的更多信息，请选择其 ID。

查看已附加到实例的 EBS 卷

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Instances (实例)。
3. 选择实例。
4. 在 Storage（存储）选项卡上，Block devices（块储存设备）部分列出了已附加到实例的卷。要查看有关特定卷的信息，请在 Volume ID（卷 ID）列中选择卷 ID。

Amazon EC2 Global View

您可以使用 Amazon EC2 Global View 查看您的 Amazon 账户已启用的所有地区的交易量。

获取所有地区的 EBS 交易量摘要

1. 在https://console.aws.amazon.com/ec2globalview/家中打开 Amazon EC2 Global View 控制台。
2. 在区域资源管理器选项卡的摘要下，检查卷的资源计数，其中包括卷的数量和区域的数量。点击带下划线的文本，查看卷数在各区域的分布情况。
3. 在 “全局搜索” 选项卡上，选择客户端筛选器资源类型 = 卷。您可以通过指定区域或标签来进一步筛选结果。

Amazon CLI

查看有关 EBS 卷的信息

使用 describe-volumes 命令。以下示例计算了当前区域的音量。

```
aws ec2 describe-volumes --query "length(Volumes[*])"
```

以下示例列出了连接到指定实例的卷。

```
aws ec2 describe-volumes \
    --filters "Name=attachment.instance-id,Values=i-1234567890abcdef0" \
    --query Volumes[*].VolumeId \
    --output text
```

以下示例描述了指定的音量。

```
aws ec2 describe-volumes --volume-ids vol-01234567890abcdef
```

下面是示例输出。

```
{
    "Volumes": [
        {
            "Iops": 3000,
            "VolumeType": "gp3",
```

```
            "MultiAttachEnabled": false,
            "Throughput": 125,
            "Operator": {
                "Managed": false
            },
            "VolumeId": "vol-01234567890abcdef",
            "Size": 8,
            "SnapshotId": "snap-0abcdef1234567890",
            "AvailabilityZone": "us-west-2b",
            "State": "in-use",
            "CreateTime": "2024-05-17T23:23:00.400000+00:00",
            "Attachments": [
                {
                    "DeleteOnTermination": true,
                    "VolumeId": "vol-01234567890abcdef",
                    "InstanceId": "i-1234567890abcdef0",
                    "Device": "/dev/xvda",
                    "State": "attached",
                    "AttachTime": "2024-05-17T23:23:00+00:00"
                }
            ],
            "Encrypted": false
        }
    ]
}
```

PowerShell

查看有关 EBS 卷的信息

使用 Get-EC2Volume cmdlet。以下示例计算了当前区域的音量。

```
(Get-EC2Volume).Count
```

以下示例列出了连接到指定实例的卷。

```
(Get-EC2Volume `
    -Filters @{Name="attachment.instance-id";Values="i-1234567890abcdef0"}).VolumeId
```

以下示例描述了指定的音量。

```
Get-EC2Volume -VolumeId vol-01234567890abcdef
```

下面是示例输出。

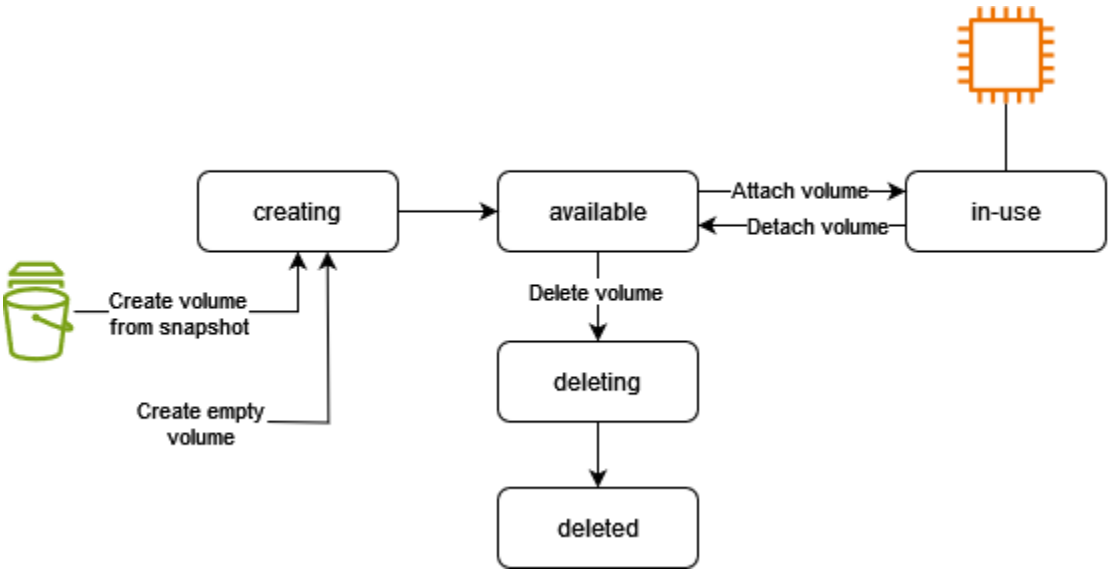
```
Attachments        : {i-1234567890abcdef0}
AvailabilityZone   : us-west-2b
CreateTime         : 5/17/2024 11:23:00 PM
Encrypted          : False
FastRestored       : False
Iops               : 3000
KmsKeyId           :
MultiAttachEnabled : False
Operator           : Amazon.EC2.Model.OperatorResponse
OutpostArn         :
Size               : 8
SnapshotId         : snap-0abcdef1234567890
SseType            :
State              : in-use
Tags               : {}
Throughput         : 125
VolumeId           : vol-01234567890abcdef
VolumeType         : gp3
```

卷状态

卷状态描述 Amazon EBS 卷的可用性。您可以在控制台的 “卷” 页面上的 “状态” 列中查看卷状态，也可以使用 desc ribe- Amazon CLI volumes 命令查看卷状态。

从创建直至删除，Amazon EBS 卷会历经不同状态的转换。

下图阐释了卷状态之间的转换。您可以通过 Amazon EBS 快照创建卷，也可以创建空卷。创建卷时，其进入 `creating` 状态。当卷准备就绪后，其进入 `available` 状态。您可以将可用的卷挂载到与该卷位于相同可用区中的实例。必须先分离该卷，才能将其删除或挂载到其他实例。如果您不再需要某个卷，可以将其删除。



下表汇总了卷状态。

状态	描述
creating	正在创建卷。
available	卷未连接到实例。
in-use	卷已连接到实例。
deleting	正在删除卷。
deleted	卷被删除。
error	与 EBS 卷有关的底层硬件出现故障，与卷关联的数据不可恢复。有关如何恢复卷或恢复卷上的数据的信息，请参阅为什么我的 EBS 卷的状态为 “错误”？ 。

查看卷指标

您可以从 Amazon CloudWatch 获取有关您的 EBS 卷的更多信息。有关更多信息，请参阅 亚马逊 EBS 的亚马逊 CloudWatch 指标。

查看可用磁盘空间

您可以获得有关您的 EBS 卷的其他信息，例如该实例的操作系统上有多少空间磁盘可用。

Linux 实例

使用以下命令：

```
[ec2-user ~]$ df -hT /dev/xvda1
Filesystem     Type      Size  Used Avail Use% Mounted on
/dev/xvda1     xfs       8.0G  1.2G  6.9G  15% /
```

Windows 实例

您可以通过打开文件资源管理器并选择这台电脑来查看可用磁盘空间。

您还可以使用以下 dir 命令并检查输出的最后一行来查看可用磁盘空间：

```
C:\> dir C:
 Volume in drive C has no label.
 Volume Serial Number is 68C3-8081

 Directory of C:\

03/25/2018  02:10 AM    <DIR>          .
03/25/2018  02:10 AM    <DIR>          ..
03/25/2018  03:47 AM    <DIR>          Contacts
03/25/2018  03:47 AM    <DIR>          Desktop
03/25/2018  03:47 AM    <DIR>          Documents
03/25/2018  03:47 AM    <DIR>          Downloads
03/25/2018  03:47 AM    <DIR>          Favorites
03/25/2018  03:47 AM    <DIR>          Links
03/25/2018  03:47 AM    <DIR>          Music
03/25/2018  03:47 AM    <DIR>          Pictures
03/25/2018  03:47 AM    <DIR>          Saved Games
03/25/2018  03:47 AM    <DIR>          Searches
03/25/2018  03:47 AM    <DIR>          Videos
               0 File(s)              0 bytes
              13 Dir(s)  18,113,662,976 bytes free
```

您还可以使用以下 fsutil 命令查看可用磁盘空间：

```
C:\> fsutil volume diskfree C:
Total # of free bytes        : 18113204224
Total # of bytes             : 32210153472
Total # of avail free bytes  : 18113204224
```

> **Tip**
>
> 您也可以使用 CloudWatch 代理从 Amazon EC2 实例收集磁盘空间使用率指标，而无需连接到该实例。有关更多信息，请参阅 Amazon CloudWatch 用户指南中的创建 CloudWatch CloudWatch 代理配置文件和安装代理。如果您需要监控多个实例的磁盘空间使用情况，则可以使用 Systems Manager 在这些实例上安装和配置 CloudWatch 代理。有关更多信息，请参阅使用 Systems Manager 安装 CloudWatch 代理。

使用弹性卷操作修改 Amazon EBS 卷

通过使用 Amazon EBS 弹性卷，您可以增加卷大小，更改卷类型或调整 EBS 卷的性能。如果您的实例支持弹性卷，您可以执行这些操作，而无需分离卷或重新启动实例。这样，您就可以在更改生效时继续使用应用程序。

修改卷配置是免费的。卷修改开始后，您需要支付新卷配置的费用。有关更多信息，请参阅Amazon EBS 定价页面。

内容

- 注意事项
- 限制
- Amazon EBS 卷修改要求
- 申请 Amazon EBS 卷修改
- 监控 Amazon EBS 卷修改的进度
- 调整 Amazon EBS 卷大小后扩展文件系统

注意事项

- 修改卷后，必须等待至少六个小时并确保卷处于 `in-use` 或 `available` 状态，然后再对同一个卷进行其他修改。
- 修改 EBS 卷可能需要几分钟到几小时才能完成，具体视应用的配置更改而定。大小为 1TiB 的 EBS 卷通常最多可能需要六个小时即可得到修改。但是，在其他情况下，相同的卷可能需要 24 小时或更长时间。修改卷所需的时间并不总是线性扩展。因此，较大的卷可能需要较短时间，而较小的卷却可能需要较长时间。
- 尚未完全初始化的卷的修改时间会增加。有关更多信息，请参阅创建后手动初始化卷。

- 如果您将卷类型从 gp2 更改为 gp3，并且您未指定 IOPS 或吞吐量性能，则 Amazon EBS 将自动预调配与源 gp2 卷的性能或基准 gp3 性能相当的性能（以二者中较高者为准）。

  例如，如果您将具有 250 MiB/s 吞吐量和 1500 IOPS 的 500 GiB gp2 卷修改为 gp3，但未指定 IOPS 或吞吐量性能，Amazon EBS 会自动预调配具有 3000 IOPS（基准gp3 IOPS）和 250 MiB/s（用于匹配源 gp2 卷吞吐量）的 gp3 卷。
- 如果在尝试修改 EBS 卷时遇到错误消息，或者要修改附加到上一代实例类型的 EBS 卷，请执行以下步骤之一：
  - 对于非根卷，将卷与实例分离，应用修改，然后重新附加卷。
  - 对于根卷，停止实例，应用修改，然后重新启动实例。

限制

- 提交卷修改请求后，您将无法取消该请求。
- 必须增加卷大小。您无法减小音量大小。但是，您可以创建较小的卷，然后使用应用程序级工具 [如 rsync（Linux 实例）或 robocopy（Windows 实例）] 将数据迁移到该卷。
- 卷修改过程中可以请求的最大聚合存储空间存在限制。有关更多信息，请参阅 Amazon Web Services 一般参考 中 Amazon EBS 服务限额。
- 新卷大小不能超过其文件系统和分区方案所支持的容量。有关更多信息，请参阅 Amazon EBS 卷限制。
- 如果您没有修改卷类型，则卷的大小和性能修改必须在当前卷类型的限制范围内。如果您修改卷类型，则卷的大小和性能修改必须在目标卷类型的限制范围内。有关更多信息，请参阅 Amazon EBS 卷类型。
- 基于 Nitro 的实例支持配置高达 256,000 IOPS 的卷。其他实例类型可以挂载到预置了最多 64000IOPS 的卷，但可以实现最多 32000IOPS。
- 您无法修改启用多重连接的卷的io2卷类型。
- 您无法修改启用了多重挂载的 io1 卷的卷类型、大小或预置 IOPS。
- 无法将类型 io1、io2、gp2、gp3 或 standard 的根卷修改为 st1 或 sc1 卷，即使已将它与实例分离也是如此。
- 如果卷是在 UTC 时间 2016 年 11 月 3 日 23:40 之前附加的，您必须初始化弹性卷支持。有关更多信息，请参阅初始化弹性卷支持。
- 虽然 m3.medium 实例完全支持卷修改，但 m3.large、m3.xlarge 和 m3.2xlarge 实例可能不支持所有卷修改功能。

Amazon EBS 卷修改要求

您修改 Amazon EBS 卷时存在以下要求和限制。若要了解有关 EBS 卷的常规要求的更多信息，请参阅 Amazon EBS 卷限制。

主题

- 支持的实例类型
- 操作系统

支持的实例类型

以下实例上支持弹性卷：

- 所有当前一代实例
- 下面这些上一代的实例：C1、C3、C4、G2、I2、M1、M3、M4、R3 和 R4

如果您的实例类型不支持弹性卷，请参阅在不支持弹性卷的情况下修改 EBS 卷。

操作系统

以下操作系统要求适用：

Linux

对于大于 2 TiB（2,048 GiB）的启动卷，Linux AMIs 需要 GUID 分区表 (GPT) 和 GRUB 2。 AMIs 如今，许多 Linux 仍在使用 MBR 分区方案，该方案仅支持最大 2 TiB 的启动卷大小。如果您的实例不通过大于 2 TiB 的引导卷启动，您要使用的 AMI 可能限制为小于 2 TiB 的引导卷大小。非引导卷对 Linux 实例没有这种限制。

在尝试调整超过 2 TiB 的引导卷大小之前，您可以通过在您的实例上运行以下命令来决定该卷是使用 MBR 分区还是使用 GPT 分区：

```
[ec2-user ~]$ sudo gdisk -l /dev/xvda
```

使用 GPT 分区的 Amazon Linux 实例返回以下信息：

```
GPT fdisk (gdisk) version 0.8.10

  Partition table scan:
```

```
    MBR: protective
    BSD: not present
    APM: not present
    GPT: present

  Found valid GPT with protective MBR; using GPT.
```

使用 MBR 分区的 SUSE 实例返回以下信息：

```
GPT fdisk (gdisk) version 0.8.8

  Partition table scan:
    MBR: MBR only
    BSD: not present
    APM: not present
    GPT: not present
```

Windows

默认情况下，Windows 使用主启动记录（MBR）分区表来初始化卷。由于 MBR 只支持小于 2TiB（2048GiB）的卷，Windows 会阻止您将 MBR 卷大小调整为超过此限制。在这种情况下，Windows 磁盘管理实用程序中的磁盘管理选项会禁用。如果您使用 Amazon Web Services Management Console 或 Amazon CLI 创建超出大小限制的 MBR 分区卷，Windows 将无法检测或使用额外的空间。

要克服此限制，您可以使用 GUID 分区表（GPT）创建新的较大的卷并从原始 MBR 卷复制数据。

创建 GPT 卷

1. 在 EC2实例的可用区中创建所需大小的新空卷，并将其连接到您的实例。

   > **Note**
   >
   > 新卷不能是从快照恢复的卷。

2. 登录到您的 Windows 系统并打开磁盘管理（diskmgmt.exe）。
3. 打开新磁盘的上下文（右键单击）菜单并选择在线。
4. 在初始化磁盘窗口中，选择新磁盘，并依次选择 GPT（GUID 分区表）、确定。
5. 初始化完成后，使用 robocopy 或 teracopy 等工具将数据从原始卷复制到新卷。
6. 在 Disk Management 中，将盘符更改为适当的值，并使旧卷脱机。

7. 在 Amazon EC2 控制台中，将旧卷与实例分离，重启实例以验证其是否正常运行，然后删除旧卷。

申请 Amazon EBS 卷修改

对于弹性卷，您可以在不分离 Amazon EBS 卷的情况下动态增加卷的大小或降低其性能，以及修改卷类型。

过程概述

1. （可选）在修改包含有用数据的卷之前，最佳实践是创建卷的快照（如果您需要回滚您的更改）。有关更多信息，请参阅创建 Amazon EBS 快照。
2. 请求卷修改。
3. 监控卷修改进度。有关更多信息，请参阅监控 Amazon EBS 卷修改的进度。
4. 如果修改了卷的大小，请扩展卷的文件系统以利用增加的存储容量。有关更多信息，请参阅 调整 Amazon EBS 卷大小后扩展文件系统。

目录

- 使用弹性卷修改 EBS 卷
- 在不支持弹性卷的情况下修改 EBS 卷
- 初始化弹性卷支持（如果需要）

使用弹性卷修改 EBS 卷

在开始之前，请查看以下内容：

- 注意事项
- 限制
- 要求

Console

修改 EBS 卷

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Volumes。

3. 选择要修改的卷，然后选择 Actions（操作）、Modify Volume（修改卷）。
4. Modify Volume（修改卷）窗口显示卷 ID 和卷的当前配置，包括类型、大小、IOPS 和吞吐量。设置新的配置值，如下所述：
   - 要修改类型，请为 Volume type（卷类型）选择一个值。
   - 要修改大小，请为大小输入新值。
   - （仅限于 gp3、io1 和 io2）要修改 IOPS，为 IOPS 输入新值。
   - （仅限于 gp3）要修改吞吐量，为 Throughput（吞吐量）输入新值。
5. 完成更改卷设置后，请选择修改。当系统提示您确认时，选择 Modify（修改）。
6. 如果您增加了卷的大小，则还必须扩展卷的分区来使用额外的存储容量。有关更多信息，请参阅 调整 Amazon EBS 卷大小后扩展文件系统。
7. （仅限 Windows 实例）如果您在没有 Amazon NVMe 驱动程序的实例上增加 NVMe 卷的大小，则必须重启该实例才能让 Windows 看到新的卷大小。有关安装 Amazon NVMe 驱动程序的更多信息，请参阅Amazon NVMe 驱动程序。

Amazon CLI

修改 EBS 卷

使用 m odify- volume 命令。例如，如果您的卷类型gp2为 100 GiB，则以下示例将其配置更改为类型为 10,000 IOPS、大小为 io1 200 GiB 的卷。

```
aws ec2 modify-volume \
    --volume-id vol-01234567890abcdef \
    --volume-type io1 \
    --iops 10000 \
    --size 200
```

下面是示例输出。

```
{
    "VolumeModification": {
        "TargetSize": 200,
        "TargetVolumeType": "io1",
        "ModificationState": "modifying",
        "VolumeId": "vol-01234567890abcdef",
        "TargetIops": 10000,
        "StartTime": "2022-01-19T22:21:02.959Z",
        "Progress": 0,
```

```
        "OriginalVolumeType": "gp2",
        "OriginalIops": 300,
        "OriginalSize": 100
    }
}
```

如果您增加了卷的大小，则还必须扩展卷的分区来使用额外的存储容量。有关更多信息，请参阅 调整 Amazon EBS 卷大小后扩展文件系统。

PowerShell

修改 EBS 卷

使用 Edit-EC2Volume cmdlet。例如，如果您的卷类型gp2为 100 GiB，则以下示例将其配置更改为类型为 10,000 IOPS、大小为 io1 200 GiB 的卷。

```
Edit-EC2Volume `
    -VolumeId vol-01234567890abcdef `
    -VolumeType io1 `
    -Iops 10000 `
    -Size 200
```

如果您增加了卷的大小，则还必须扩展卷的分区来使用额外的存储容量。有关更多信息，请参阅 调整 Amazon EBS 卷大小后扩展文件系统。

在不支持弹性卷的情况下修改 EBS 卷

如果您使用的是支持的实例类型，则可以使用弹性卷来在不分离 Amazon EBS 卷的情况下动态修改卷的大小、性能和卷类型。

如果您无法使用弹性卷但需要修改根（启动）卷，则必须停止实例，修改卷，然后重新启动实例。

实例启动之后，可以检查文件系统大小，看实例是否识别这个更大的卷空间。在 Linux 上，请使用 df -h 命令检查文件系统大小。

```
[ec2-user ~]$ df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/xvda1            7.9G  943M  6.9G  12% /
tmpfs                 1.9G     0  1.9G   0% /dev/shm
```

如果大小没有反映新扩展的卷，则必须扩展设备的文件系统，以便实例可以使用新的空间。有关更多信息，请参阅 调整 Amazon EBS 卷大小后扩展文件系统。

您可能需要将卷联机才能使用 Windows 实例。有关更多信息，请参阅 使 Amazon EBS 卷可供使用。您无需重新格式化卷。

初始化弹性卷支持（如果需要）

您必须先使用以下操作之一初始化卷修改支持，然后才能修改在 UTC 时间 2016 年 11 月 3 日 23:40 前附加到实例的卷：

- 分离和附加卷
- 停止和启动实例

Console

确定您的实例是否准备就绪

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择实例。
3. 选择显示/隐藏列图标（齿轮）。选择启动时间属性列，然后选择确认。
4. 按 Launch Time 列对实例列表进行排序。对于在截止日期之前启动的每个实例，选择存储选项卡，并检查连接时间列以查看其卷附加的时间。

Amazon CLI

确定您的实例是否准备就绪

使用以下 describe-instances 命令确定卷是否是在 UTC 时间 2016 年 11 月 3 日 23:40 之前附加的。

```
aws ec2 describe-instances \
    --query "Reservations[*].Instances[*].
[InstanceId,LaunchTime<='2016-11-01',BlockDeviceMappings[*]
[Ebs.AttachTime<='2016-11-01']]" \
    --output text
```

每个实例的输出的第一行都将显示其 ID，无论实例是否在截止日期前启动（True 或 False）。第一行后跟一行或多行，以显示是否在截止日期前已附加每个 EBS 卷（True 或 False）。在以下示例输出中，您必须为第一个实例初始化卷修改，因为该实例是在截止日期前启动的，并且其根卷是在截止日期前附加的。其他实例已准备就绪，因为它们是在截止日期后启动的。

```
i-e905622e              True
True
i-719f99a8              False
True
i-006b02c1b78381e57     False
False
False
i-e3d172ed              False
True
```

PowerShell

确定实例是否准备就绪

使用 Get-EC2Instancecmdlet 来确定是否在世界标准时间 2016 年 11 月 3 日 23:40 之前附加了卷。

```
(Get-EC2Instance `
    -InstanceId i-1234567890abcdef0).Instances.BlockDeviceMappings | `
     Format-Table @{Name="VolumeId";Expression={$_.Ebs.VolumeId}}, `
                  @{Name="AttachTime";Expression={$_.Ebs.AttachTime}}
```

下面是示例输出。

```
VolumeId              AttachTime
--------              ----------
vol-0b243c8d927752d2b 3/23/2020 12:21:14 AM
vol-043eadbeb4a8387c3 9/5/2020 7:39:22 PM
vol-0c3f0c4e55c082753 4/23/2019 4:07:40 PM
```

监控 Amazon EBS 卷修改的进度

当您修改 EBS 卷时，它将经历一系列状态。卷将依次进入 modifying 状态、optimizing 状态和 completed 状态。此时，卷已准备好做进一步的修改。

当卷处于 optimizing 状态时，卷性能介于源配置规范和目标配置规范之间。过渡卷的性能将不会低于源卷的性能。如果您降级 IOPS，则过渡卷的性能不会低于目标卷的性能。

卷修改更改将生效，如下所示：

- 大小更改通常需要几秒钟才能完成，并在卷转为 Optimizing 状态后生效。
- 性能（IOPS）更改可能需要几分钟到几小时才能完成，具体视所做的配置更改而定。
- 在某些情况下，新配置生效最长需要 24 个小时，例如卷未完全初始化时。通常，完全使用的 1 TiB 卷需要约 6 个小时才能迁移到新的性能配置。

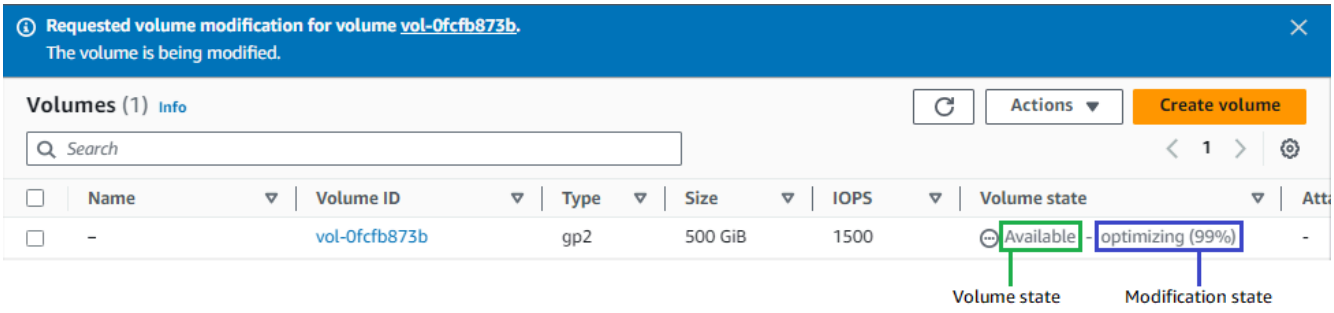
可能的卷状态包括 creating、available、in-use、deleting、deleted 和 error。

可能的修改状态为 modifying、optimizing 和 completed。

Console

监控修改进度

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Volumes。
3. 选择该卷。
4. “详细信息” 选项卡中的 “卷状态” 列和 “卷状态” 字段包含以下格式的信息：***Volume state-Modification state*** (***Modification progress***%)。下图显示了卷和卷修改状态。



修改完成后，仅显示卷状态。不再显示修改状态和进度。

或者，您可以使用 Amazon EventBridge 为批量修改事件创建通知规则。有关更多信息，请参阅 Amazon 入门 EventBridge。

Amazon CLI

监控修改进度

使用describe-volumes-modifications命令查看一个或多个卷修改的进度。以下示例描述了两个卷的卷修改。

```
aws ec2 describe-volumes-modifications \
    --volume-ids vol-1111111111111111 vol-22222222222222222
```

在以下示例输出中，卷修改仍处于 modifying 状态。以百分比形式报告进展情况。

```
{
    "VolumesModifications": [
        {
            "TargetSize": 200,
            "TargetVolumeType": "io1",
            "ModificationState": "modifying",
            "VolumeId": "vol-11111111111111111",
            "TargetIops": 10000,
            "StartTime": "2017-01-19T22:21:02.959Z",
            "Progress": 0,
            "OriginalVolumeType": "gp2",
            "OriginalIops": 300,
            "OriginalSize": 100
        },
        {
            "TargetSize": 2000,
            "TargetVolumeType": "sc1",
            "ModificationState": "modifying",
            "VolumeId": "vol-22222222222222222",
            "StartTime": "2017-01-19T22:23:22.158Z",
            "Progress": 0,
            "OriginalVolumeType": "gp2",
            "OriginalIops": 300,
            "OriginalSize": 1000
        }
    ]
}
```

下一个示例描述了修改状态为 optimizing 或 completed 的所有卷，然后筛选和格式化结果以只显示于 2017 年 2 月 1 日及之后做出的修改：

```
aws ec2 describe-volumes-modifications \
    --filters Name=modification-state,Values="optimizing","completed" \
    --query "VolumesModifications[?StartTime>='2017-02-01'].
{ID:VolumeId,STATE:ModificationState}"
```

以下是包含有关两个卷的信息的示例输出：

```
[
    {
        "STATE": "optimizing",
        "ID": "vol-06397e7a0eEXAMPLE"
    },
    {
        "STATE": "completed",
        "ID": "vol-ba74e18c2aEXAMPLE"
    }
]
```

PowerShell

监控修改进度

使用 Get-EC2VolumeModification cmdlet。以下示例描述了两个卷的卷修改。

```
Get-EC2VolumeModification `
    -VolumeId vol-1111111111111111 vol-2222222222222222
```

> **Note**
>
> 在极少数情况下，瞬态 Amazon 故障会导致`failed`状态。这并不指示卷的运行状况；它仅指示卷修改失败。如果发生这种情况，请重试卷修改。

调整 Amazon EBS 卷大小后扩展文件系统

增加 EBS 卷的大小后，您必须将分区和文件系统扩展到新的较大大小。您可以在卷进入 `optimizing` 状态后立即执行此操作。

开始前的准备工作

- 如果需要回滚更改，则创建卷的快照。有关更多信息，请参阅 创建 Amazon EBS 快照。
- 确认卷修改成功并且其处于 `optimizing` 或 `completed` 状态。有关更多信息，请参阅 监控 Amazon EBS 卷修改的进度。
- 确保卷已附加到实例，并且已格式化和挂载。有关更多信息，请参阅 格式化并挂载附加的卷。

- （仅限 Linux 实例）如果在 Amazon EBS 卷上使用逻辑卷，则必须使用逻辑卷管理器（LVM）来扩展逻辑卷。有关如何执行此操作的说明，请参阅 “如何使用 LVM 在 EBS 卷的分区上创建逻辑卷？” 一文中的 “扩展 L V” 部分 。

Linux 实例

> **Note**
>
> 以下说明将引导您完成为 Linux 扩展 XFS 和 Ext4 文件系统的过程。有关扩展其他文件系统的信息，请参阅相关文档。

如果卷有分区，则必须先扩展分区，才能在 Linux 上扩展文件系统。

扩展 EBS 卷的文件系统

按照以下过程扩展调整大小后的卷的文件系统。

请注意，Xen 实例和基于 Nitro 系统构建的实例的设备和分区命名有所不同。要确定您的实例是基于 Xen还是基于 Nitro的，请参阅 A mazon EC2 虚拟机管理程序类型。

扩展 EBS 卷的文件系统

1. 连接到您的 实例。
2. 如果需要，调整分区的大小。为此，请执行以下操作：

   a. 检查卷是否有分区。使用 lsblk 命令。

      Nitro instance example

      在以下示例输出中，根卷（nvme0n1）有两个分区（nvme0n1p1 和 nvme0n1p128），而额外的卷（nvme1n1）没有分区。

```
[ec2-user ~]$ sudo lsblk
NAME          MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
nvme1n1       259:0    0  30G  0 disk /data
nvme0n1       259:1    0  16G  0 disk
##nvme0n1p1   259:2    0   8G  0 part /
##nvme0n1p128 259:3    0   1M  0 part
```

Xen instance example

在以下示例输出中，根卷（xvda）有一个分区（xvda1），而额外的卷（xvdf）没有分区。

```
[ec2-user ~]$ sudo lsblk
NAME    MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
xvda    202:0    0  16G  0 disk
##xvda1 202:1    0   8G  0 part /
xvdf    202:80   0  24G  0 disk
```

- 如果该卷有分区，请继续执行下一步 (2b)。
- 如果该卷没有分区，请跳过步骤 2b、2c 和 2d，然后继续执行步骤 3。

> **故障排除技巧**
>
> 如果没有在命令输出中看到该卷，请确保该卷已附加到实例并且已格式化和挂载。

b. 检查是否需要扩展分区。在上一步的 lsblk 命令输出中，比较分区大小和卷大小。

- 如果分区大小小于卷大小，请继续执行下一步 (2c)。
- 如果分区大小等于卷大小，则无需扩展分区-跳过步骤 2c 和 2d，继续步骤 3。

> **故障排除技巧**
>
> 如果卷仍然反映原始大小，则请确认卷修改成功。

c. 扩展分区。使用 growpart 命令并指定设备名称和分区编号。

Nitro instance example

分区编号是 p 后面的数字。例如，对于 nvme0n1p1，分区编号为 1。对于 nvme0n1p128，分区编号为 128。

要扩展名为 nvme0n1p1 的分区，请使用以下命令。

> **Important**
>
> 请注意，设备名称（nvme0n1）和分区编号（1）之间有空格。

```
[ec2-user ~]$ sudo growpart /dev/nvme0n1 1
```

Xen instance example

分区编号是设备名称后面的数字。例如，对于 xvda1，分区编号为 1。对于 xvda128，分区编号为 128。

要扩展名为 xvda1 的分区，请使用以下命令。

> **Important**
>
> 请注意，设备名称 (xvda) 和分区编号 (1) 之间有空格。

```
[ec2-user ~]$ sudo growpart /dev/xvda 1
```

> **问题排查技巧**
>
> - `mkdir: cannot create directory ‘/tmp/growpart.31171’: No space left on device FAILED: failed to make temp dir`：表示卷上没有足够的可用磁盘空间供 growpart 创建执行调整大小所需的临时目录。请释放一些磁盘空间并重试。
> - `must supply partition-number`：表示您指定的分区不正确。使用 lsblk 命令以确认分区名称，并确保在设备名称和分区编号之间输入空格。
> - `NOCHANGE: partition 1 is size 16773087. it cannot be grown`：表示分区已经扩展了整个卷，无法再扩展。确认卷修改成功。

d. 验证是否已扩展分区。使用 lsblk 命令。分区大小现在应等于卷大小。

Nitro instance example

以下示例输出显示卷（nvme0n1）和分区（nvme0n1p1）的大小相同（16 GB）。

```
[ec2-user ~]$ sudo lsblk
NAME          MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
nvme1n1       259:0    0  30G  0 disk /data
nvme0n1       259:1    0  16G  0 disk
##nvme0n1p1   259:2    0  16G  0 part /
##nvme0n1p128 259:3    0   1M  0 part
```

Xen instance example

以下示例输出显示卷 (xvda) 和分区 (xvda1) 的大小相同 (16 GB)。

```
[ec2-user ~]$ sudo lsblk
NAME    MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
xvda    202:0    0  16G  0 disk
##xvda1 202:1    0  16G  0 part /
xvdf    202:80   0  24G  0 disk
```

3. 扩展文件系统。

a. 获取需要扩展的文件系统的名称、大小、类型和挂载点。使用 df -hT 命令。

Nitro instance example

以下示例输出显示了 /dev/nvme0n1p1 文件系统的大小为 8 GB，其类型为 xfs，其挂载点是 /。

```
[ec2-user ~]$ df -hT
Filesystem      Type  Size  Used Avail Use% Mounted on
/dev/nvme0n1p1  xfs   8.0G  1.6G  6.5G  20% /
/dev/nvme1n1    xfs   8.0G   33M  8.0G   1% /data
...
```

Xen instance example

以下示例输出显示了 /dev/xvda1 文件系统的大小为 8 GB，其类型为 ext4，其挂载点是 /。

```
[ec2-user ~]$ df -hT
Filesystem      Type   Size    Used   Avail   Use%   Mounted on
/dev/xvda1      ext4   8.0G    1.9G   6.2G    24%    /
/dev/xvdf1      xfs    24.0G   45M    8.0G    1%     /data
...
```

- 如果文件系统大小小于卷大小，请继续执行下一步 (3b)。
- 如果文件系统大小等于卷大小，则无需对其进行扩展。在这种情况下，请跳过剩下的步骤-分区和文件系统已扩展到新的卷大小。

b. 扩展文件系统的命令因文件系统类型而异。根据您在上一步中记录的文件系统类型选择以下正确命令。

- [XFS 文件系统] 使用 xfs_growfs 命令并指定您在上一步中记录的文件系统的挂载点。

  Nitro and Xen instance example

  例如，若要扩展挂载在 / 上的文件系统，请使用以下命令。

  ```
  [ec2-user ~]$ sudo xfs_growfs -d /
  ```

  问题排查技巧

  - `xfs_growfs: /data is not a mounted XFS filesystem`：表示指定的挂载点不正确，或者文件系统不是 XFS。若要验证挂载点和文件系统类型，请使用 df -hT 命令。
  - `data size unchanged, skipping`：表示文件系统已经扩展了整个卷。如果卷没有分区，则请确认卷修改成功。如果卷有分区，则请确保该分区已按照步骤 2 中的说明进行扩展。

- [Ext4 文件系统] 使用 resize2fs 命令并指定您在上一步中记录的文件系统的名称。

  Nitro instance example

  例如，若要扩展名为 /dev/nvme0n1p1 的挂载文件系统，请使用以下命令。

  ```
  [ec2-user ~]$ sudo resize2fs /dev/nvme0n1p1
  ```

Xen instance example

例如，若要扩展名为 /dev/xvda1 的挂载文件系统，请使用以下命令。

```
[ec2-user ~]$ sudo resize2fs /dev/xvda1
```

问题排查技巧

- resize2fs: Bad magic number in super-block while trying to open /dev/xvda1：表示文件系统不是 Ext4。若要验证文件系统类型，请使用 df -hT 命令。
- open: No such file or directory while opening /dev/xvdb1：表示您指定的分区不正确。若要验证分区，请使用 df -hT 命令。
- The filesystem is already 3932160 blocks long. Nothing to do!：表示文件系统已经扩展了整个卷。如果卷没有分区，则请确认卷修改成功。如果卷有分区，则请确保该分区已按照步骤 2 中的说明进行扩展。

- [其他文件系统]，请参阅文件系统的文档，了解相关说明。

c. 验证是否已扩展文件系统。使用 df -hT 命令并确认文件系统大小等于卷大小。

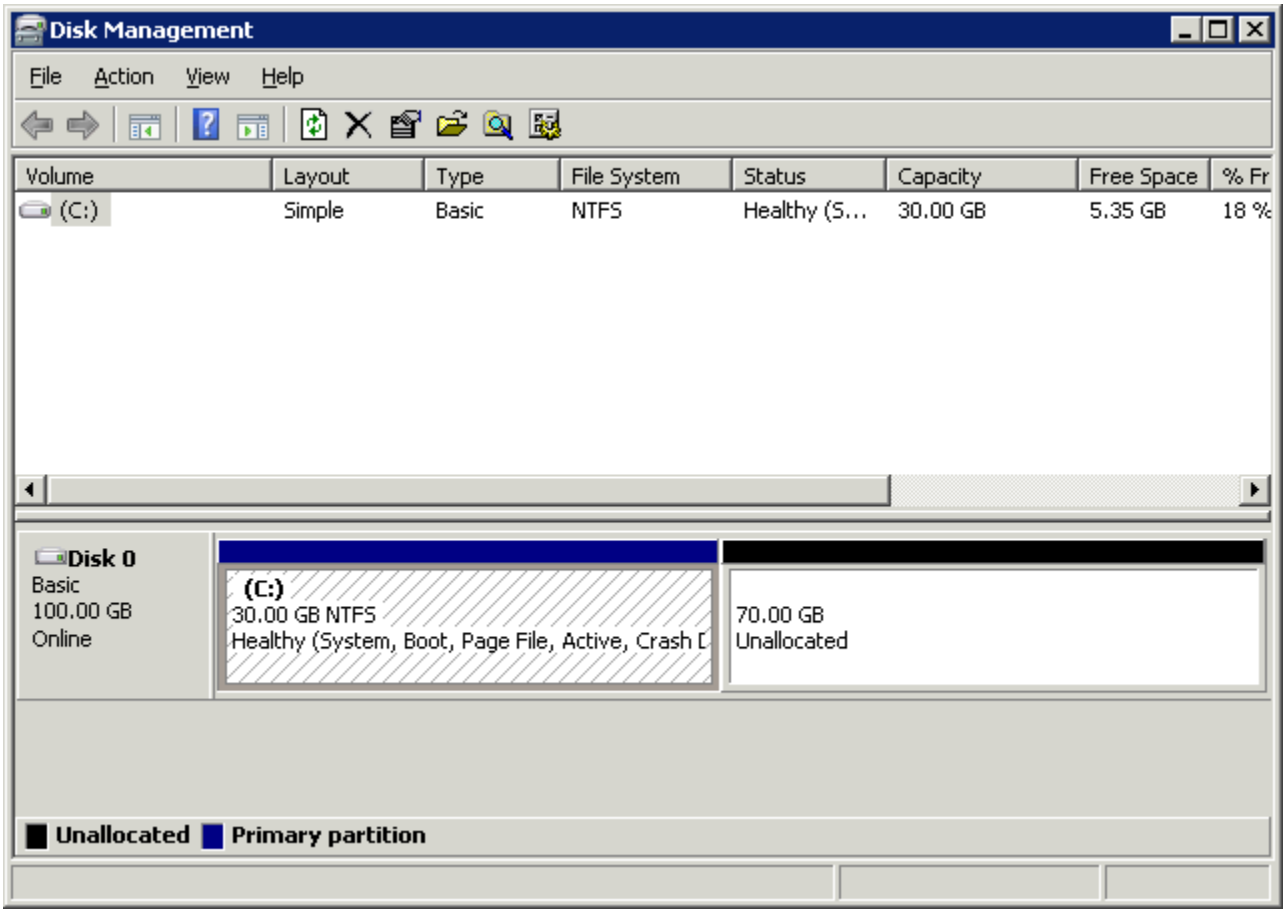
Windows 实例

使用以下任一方法在 Windows 实例上扩展文件系统。

Disk Management utility

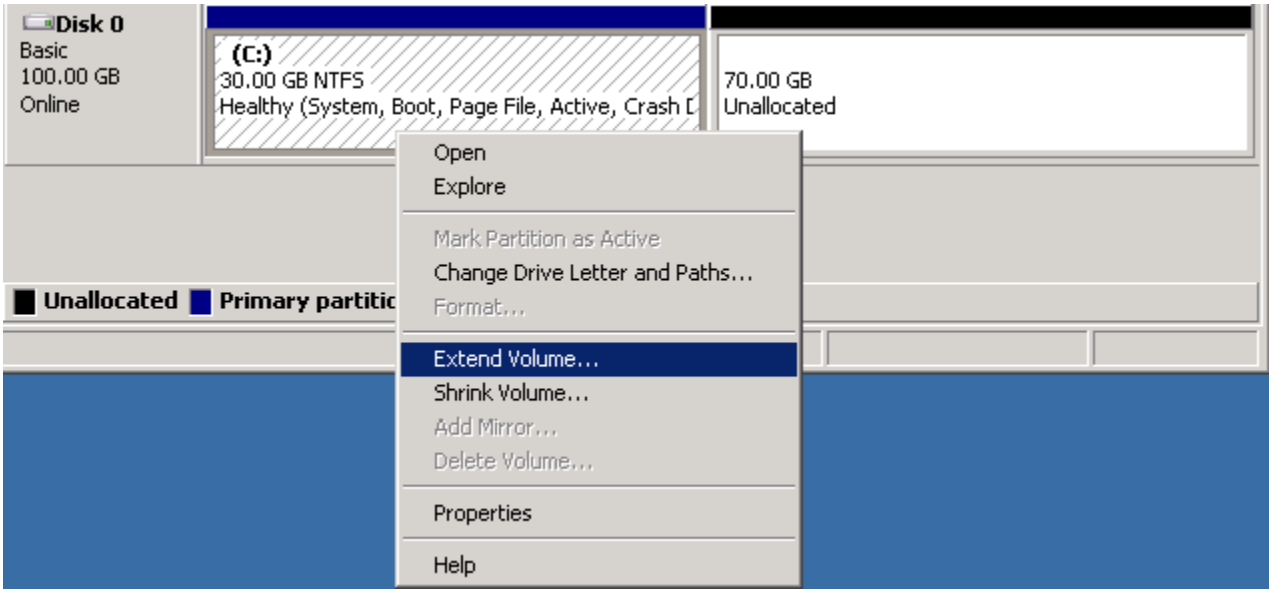
使用磁盘管理扩展文件系统

1. 在扩展包含有用数据的文件系统之前，最佳实践是创建包含它的卷的快照 (如果您需要回滚您的更改)。有关更多信息，请参阅创建 Amazon EBS 快照。
2. 使用远程桌面登录 Windows 实例。
3. 在运行对话框中，输入 diskmgmt.msc 并按 Enter。然后，磁盘管理实例程序随之打开。

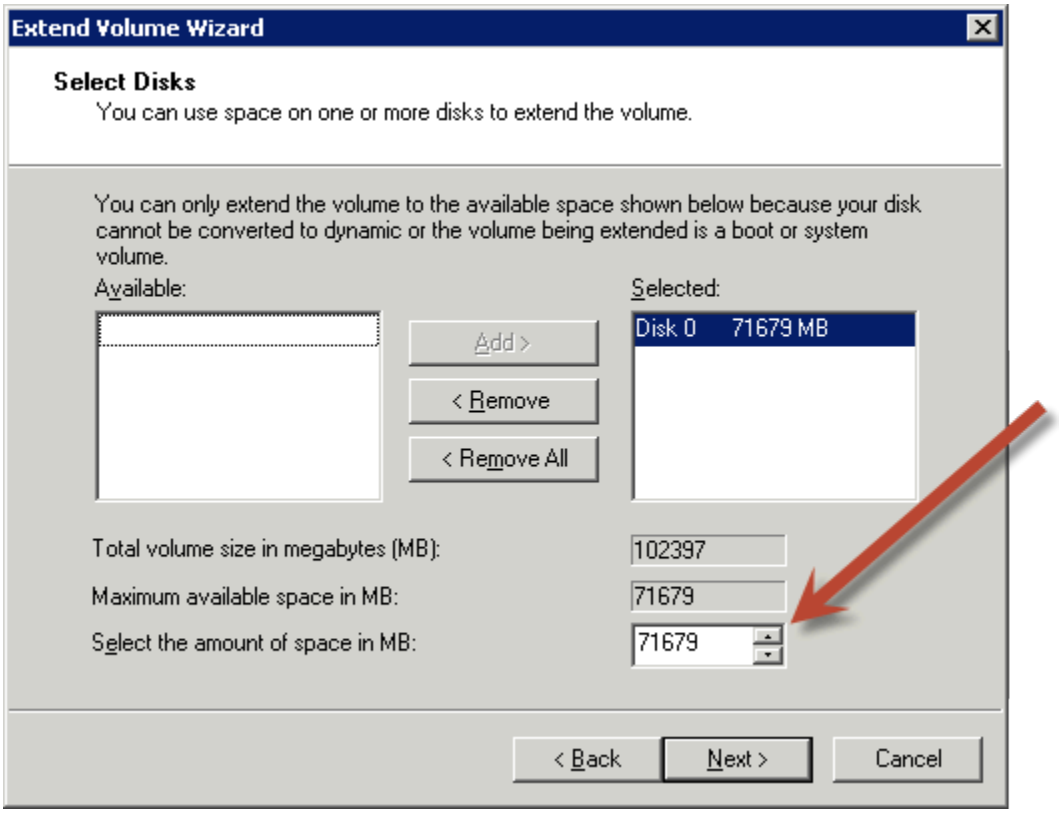


4. 在 Disk Management 菜单上，选择 Action、Rescan Disks。
5. 打开扩展驱动器的上下文（右键单击）菜单，然后选择扩展卷。

> **Note**
>
> 如果出现以下情况，说明扩展卷可能已被禁用（灰显）：
>
> - 未分配的空间不在驱动器旁边。未分配的空间必须与要扩展的驱动器的右侧相邻。
> - 卷使用主引导记录（MBR）分区样式，大小已经为 2TB。使用 MBR 的卷的大小不能超过 2TB。



6. 在扩展卷向导中，选择下一步。对于 Select the amount of space in MB，输入扩展卷的兆字节数。通常，您可指定最大可用空间。Selected 下突出显示的文本是将添加的空间量，而不是卷最终将具有的大小。完成向导。



7. 如果您在没有 Amazon NVMe 驱动程序的实例上增加 NVMe 卷的大小，则必须重启该实例才能让 Windows 看到新的卷大小。有关安装 Amazon NVMe 驱动程序的更多信息，请参阅Amazon NVMe 驱动程序。

PowerShell

使用以下步骤使用扩展 Windows 文件系统 PowerShell。

使用扩展文件系统 PowerShell

1. 在扩展包含有用数据的文件系统之前，最佳实践是创建包含它的卷的快照（如果您需要回滚您的更改）。有关更多信息，请参阅创建 Amazon EBS 快照。
2. 使用远程桌面登录 Windows 实例。
3. 以管理员 PowerShell 身份运行。
4. 运行`Get-Partition`命令。 PowerShell 返回每个分区的相应分区号、驱动器号、偏移量、大小和类型。请注意要扩展的分区的盘符。
5. 运行以下命令重新扫描磁盘。

```
"rescan" | diskpart
```

6. 运行以下命令，使用您在步骤 4 中记下的驱动器号代替**<drive-letter>**。 PowerShell 返回允许的分区的最小和最大大小（以字节为单位）。

```
Get-PartitionSupportedSize -DriveLetter <drive-letter>
```

7. 要将分区扩展到指定的量，请运行以下命令，并在 **<size>** 的位置输入卷的新大小。您可以输入以 KB、MB 和 GB 为单位的大小，例如 50GB。

```
Resize-Partition -DriveLetter <drive-letter> -Size <size>
```

要将分区扩展到最大可用大小，请运行以下命令。

```
Resize-Partition -DriveLetter <drive-letter> -Size $(Get-PartitionSupportedSize
 -DriveLetter <drive-letter>).SizeMax
```

以下 PowerShell 命令显示了将文件系统扩展到特定大小的完整命令和响应流。

```
PS C:\> Get-Partition


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&26a12046&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                C           1048576                                     30 GB IFS


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&3476342 3&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                D           1048576                                     8 MB IFS


PS C:\> "rescan" | diskpart

Microsoft DiskPart version 10.0.17763.1911

Copyright (C) Microsoft Corporation.
On computer:

DISKPART>
Please wait while DiskPart scans your configuration...

DiskPart has finished scanning your configuration.

DISKPART>
PS C:\> Get-PartitionSupportedSize -DriveLetter D

SizeMin      SizeMax
-------      -------
8388608 107372085248


PS C:\> Resize-Partition -DriveLetter D -Size 50GB
PS C:\> Get-Partition


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&26a12046&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                C           1048576                                     30 GB IFS


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&3476342 3&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                D           1048576                                     50 GB IFS
```

以下 PowerShell 命令显示了将文件系统扩展到最大可用大小的完整命令和响应流。

```
PS C:\> Get-Partition


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&26a12046&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                C           1048576                                     30 GB IFS


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&34763423&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                D           1048576                                     50 GB IFS


PS C:\> "rescan" | diskpart

Microsoft DiskPart version 10.0.17763.1911

Copyright (C) Microsoft Corporation.
On computer:

DISKPART>
Please wait while DiskPart scans your configuration...

DiskPart has finished scanning your configuration.

DISKPART>
PS C:\> Get-PartitionSupportedSize -DriveLetter D

 SizeMin      SizeMax
 -------      -------
59047936 107372085248


PS C:\> Resize-Partition -DriveLetter D -Size $(Get-PartitionSupportedSize -DriveLetter D).SizeMax
PS C:\> Get-Partition


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&26a12046&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                C           1048576                                     30 GB IFS


   DiskPath: \\?\scsi#disk&ven_nvme&prod_amazon_elastic_b#4&34763423&0&000000#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
1                D           1048576                                    100 GB IFS
```

将 Amazon EBS 卷与亚马逊实例分离 EC2

您需要将 Amazon Elastic Block Store（Amazon EBS）卷与实例分离，然后才能将其挂载到其他实例或删除该卷。分离卷不会影响卷上的数据。

主题

- 注意事项
- 卸载并分离卷
- 故障排除

注意事项

- 您可以明确地将 Amazon EBS 卷与实例分离，或终止实例。但是，如果实例正在运行，您首先必须从实例卸载卷。
- 如果 EBS 卷是实例的根设备，则在分离卷之前必须停止该实例。
- 您可以重新附加分离的卷（无需卸载），但可能不能获得相同挂载点。如果分离时正在写入卷，那么卷上的数据可能不同步。
- 分离卷后，只要存储量超过 Amazon 免费套餐的限制，您仍需要支付卷存储费用。您必须删除卷以避免产生更多费用。有关更多信息，请参阅删除 Amazon EBS 卷。

卸载并分离卷

使用以下程序从实例卸载并分离卷。当您需要将卷挂载到不同实例时或当您需要删除卷时，此操作非常有用。

步骤

- 第 1 步：卸载卷
- 第 2 步：从实例分离卷
- 第 3 步：（仅限 Windows 实例）卸载离线设备位置

第 1 步：卸载卷

Linux 实例

从 Linux 实例中，使用以下命令卸载 /dev/sdh 设备。

```
[ec2-user ~]$ sudo umount -d /dev/sdh
```

Windows 实例

按照以下步骤从 Windows 实例中卸载卷。

1. 启动磁盘管理实用工具。
   - （Windows Server 2012 及更高版本）在任务栏上，右键单击 Windows 徽标，然后选择磁盘管理。
   - （Windows Server 2008）依次选择开始、管理工具、计算机管理和磁盘管理。

2. 右键单击磁盘（例如，右键单击磁盘 1），然后选择脱机。等待磁盘状态变为“离线”，然后再打开 Amazon EC2 控制台。

第 2 步：从实例分离卷

要将卷与实例分离，请使用以下方法之一：

Console

要断开 EBS 卷

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Volumes。
3. 选择该卷。
4. 选择“操作”、“分离音量”。
5. 当系统提示进行确认时，选择分离。

Amazon CLI

将 EBS 卷与实例分离

卸载卷之后，使用 detach-volume 命令。

```
aws ec2 detach-volume --volume-id vol-01234567890abcdef
```

PowerShell

将 EBS 卷与实例分离

卸载卷后，使用 Dismount-EC2Volumecmdlet。

```
Dismount-EC2Volume -VolumeId vol-01234567890abcdef
```

第 3 步：（仅限 Windows 实例）卸载离线设备位置

从实例卸载和分离卷时，Windows 会将该设备位置标记为脱机。重新启动后以及停止并重新启动实例后，设备位置将保持脱机状态。重启实例时，Windows 可能会将其余卷之一挂载到脱机设备位置。这会导致卷在 Windows 中不可用。为了防止这种情况发生，并确保下次启动 Windows 时所有卷都附加到在线设备位置，请执行以下步骤：

1. 在实例上，打开设备管理器。
2. 在设备管理器中，依次选择查看、显示隐藏的设备。
3. 在设备列表中，展开存储控制器节点。

   已分离卷挂载到的设备位置命名为 AWS NVMe Elastic Block Storage Adapter，且应显示为灰色。
4. 右键单击每个命名为 AWS NVMe Elastic Block Storage Adapter 的灰显设备位置，选择 Uninstall device（卸载设备），然后选择 Uninstall（卸载）。

   > **Important**
   >
   > 不要选中删除此设备的驱动程序软件复选框。

故障排除

以下内容介绍在分离卷时遇到的常见问题并以及如何解决这些问题。

> **Note**
>
> 要防止出现数据丢失的可能性，请在尝试卸载之前为您的卷制作快照。强制分离一个状态卡住的卷可能对文件系统或其中包含的数据造成破坏，或者除非重启实例，否则无法使用同样的设备名称附加新卷。

- 如果您在通过 Amazon EC2 控制台分离卷时遇到问题，使用 describe-volumes CLI 命令诊断问题可能会有所帮助。有关更多信息，请参阅 describe-volumes。
- 如果您的卷处于 detaching 状态，您可以通过选择 Force Detach 强制执行分离操作。请将该选项仅用作在不得已的情况下从故障实例分离卷的方法，或是在要删除卷的情况下分离卷时使用。此实例没有机会来冲击文件系统缓存或文件系统元数据。如果您使用该选项，则必须执行文件系统检查和修复流程。
- 如果在几分钟内多次尝试强制分离卷，并且该卷处于 detaching 状态，则可以向 Amazon re:Post 发布帮助请求。为了帮助加快解决问题，请提供卷 ID 并描述已采取的步骤。
- 如果尝试分离仍挂载的卷，该卷可能在尝试分离时卡在 busy 状态。describe-volumes 的以下输出说明了这种情况：

```
"Volumes": [
```

```
    {
        "AvailabilityZone": "us-west-2b",
        "Attachments": [
            {
                "AttachTime": "2022-07-21T23:44:52.000Z",
                "InstanceId": "i-1234567890abcdef0",
                "VolumeId": "vol-01234567890abcdef",
                "State": "busy",
                "DeleteOnTermination": false,
                "Device": "/dev/sdf"
            }
        ...
    }
]
```

如果遇到这种状态，可能无限期延迟分离，直到您卸载卷，强制分离，重启实例，或者执行前述全部三项操作。

删除 Amazon EBS 卷

如果您不再需要某个 Amazon EBS 卷，可以将其删除。删除后，卷上的数据都不复存在，并且再也不能附加到任何实例。然而，您可在删除之前保存卷的快照，以便以后可以使用该快照重新创建卷。

无法删除连接到实例的卷。要删除卷，必须先将其与实例分离。有关更多信息，请参阅 将 Amazon EBS 卷与亚马逊实例分离 EC2 。

Console

删除 EBS 卷

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Volumes。
3. 选择该卷。验证卷是否处于 “可用” 状态。
4. 选择操作，删除音量。

   如果禁用此选项，则该卷将连接到实例，并且无法删除。
5. 提示进行确认时，输入 **delete**，然后选择 Delete（删除）。

Amazon CLI

检查 EBS 卷是否正在使用中

使用 describe-volumes 命令。如果该卷正在使用中，则状态为in-use。否则为 available。

```
aws ec2 describe-volumes \
    --volume-id vol-01234567890abcdef \
    --query Volumes[*].State \
    --output text
```

删除 EBS 卷

使用 delete-volume 命令。

```
aws ec2 delete-volume --volume-id vol-01234567890abcdef
```

PowerShell

检查 EBS 卷是否正在使用中

使用 Get-EC2Volume cmdlet。如果该卷正在使用中，则状态为in-use。否则为 available。

```
(Get-EC2Volume `
    -VolumeId vol-01234567890abcdef).State.Value
```

删除 EBS 卷

使用 Remove-EC2Volume cmdlet。

```
Remove-EC2Volume -VolumeId vol-01234567890abcdef
```

使用快照替换 Amazon EBS 卷

Amazon EBS 快照 EC2 因其速度、便利性和成本而成为亚马逊的首选备份工具。当从快照中创建卷时，您重新创建了它在过去特定时间点的状态，并且所有数据完整无缺。通过将从快照中创建的卷附加到实例，您可以在不同的区域之间复制数据，创建测试环境，完全替换受损或损坏的生产卷，或检索特定文件和目录并将其传输到另一个附加的卷。有关更多信息，请参阅 Amazon EBS 快照。

可以使用以下过程之一将 Amazon EBS 卷替换为从此卷的上一个快照创建的另一个卷。

要求

您必须在实例所在的可用区中创建卷。卷必须连接到同一可用区中的实例。

Console

替换卷

1. 从快照中创建一个卷，并记下新卷的 ID。有关更多信息，请参阅 创建 Amazon EBS 卷。
2. 在 Instances（实例）页面上，选择要替换卷的实例，然后记下实例 ID。

   在实例处于选中状态时，选择 Storage（存储）选项卡。在 Block devices（块储存设备）部分中，找到要替换的卷并记下该卷的设备名称，例如 `/dev/sda1`。
3. 在存储选项卡上，选择卷 ID，然后卸载该卷并将其与实例分离。
4. 选择在步骤 1 中创建的新卷，然后选择 Actions（操作）、Attach volume（附加卷）。

   对于 Instance（实例）和 Device name（设备名称），输入您在步骤 2 中记下的实例 ID 和设备名称，然后选择 Attach volume（附加卷）。
5. 连接到您的实例并安装卷。有关更多信息，请参阅 使 Amazon EBS 卷可供使用。

Amazon CLI

替换卷

1. 从快照创建一个新卷。使用带选项的 create-vol ume 命令。`--snapshot-id`对于 `--availability-zone`，指定与实例相同的可用区。在输出中记下新卷的 ID。

```
aws ec2 create-volume \
    --volume-type gp3 \
    --snapshot-id snap-0abcdef1234567890 \
    --availability-zone us-east-1a
```

2. 获取要替换的卷的设备名称。可以使用 describe-instances 命令。对于 `--instance-ids`，指定要在其上替换卷的实例的 ID。记下要替换的卷的设备名称和卷 ID。

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0 \
    --query Reservations[].Instances[].BlockDeviceMappings
```

3. 从实例中分离要替换的卷。使用 detach-volume 命令。

```
aws ec2 detach-volume --volume-id vol-xxxxxxxxxxxxxxxxx
```

4. 将替换卷挂载到实例。使用 attach-volume 命令。对于 `--volume-id`，指定替换卷的 ID。对于`--instance-id`，请指定要连接卷的实例的 ID。对于 `--device`，指定此前记下的设备名称。

```
aws ec2 attach-volume \
    --volume-id vol-01234567890abcdef \
    --instance-id i-1234567890abcdef0 \
    --device /dev/sdf
```

5. 连接到您的实例并安装卷。有关更多信息，请参阅 使 Amazon EBS 卷可供使用。

PowerShell

替换卷

1. 从快照创建一个新卷。使用带有选项的 New-EC2Volumecmdlet。`-SnapshotId`对于 `-AvailabilityZone`，指定与实例相同的可用区。在输出中记下新卷的 ID。

```
New-EC2Volume `
    -VolumeType gp3 `
    -SnapshotId snap-0abcdef1234567890 `
    -AvailabilityZone us-east-1a
```

2. 获取要替换的卷的设备名称。使用 Get-EC2Instance cmdlet。对于 `-InstanceId`，指定要在其上替换卷的实例的 ID。记下要替换的卷的设备名称和卷 ID。

```
(Get-EC2Instance `
    -InstanceId i-1234567890abcdef0).Instances.BlockDeviceMappings | `
     Format-Table DeviceName, @{Name="VolumeId";Expression={$_.Ebs.VolumeId}}
```

3. 从实例中分离要替换的卷。使用 Dismount-EC2Volume cmdlet。

```
DismountEC2Volume -VolumeId vol-xxxxxxxxxxxxxxxxx
```

4. 将替换卷挂载到实例。使用 Add-EC2Volume cmdlet。对于 `-VolumeId`，指定替换卷的 ID。对于`-InstanceId`，请指定要连接卷的实例的 ID。对于 `-Device`，指定此前记下的设备名称。

```
Add-EC2Volume`
    -VolumeId vol-01234567890abcdef `
    -InstanceId i-1234567890abcdef0 `
    -Device /dev/sdf
```

5. 连接到您的实例并安装卷。有关更多信息，请参阅 使 Amazon EBS 卷可供使用。

Amazon EBS 卷状态检查

通过卷状态检查，您可以更好地了解、追踪和管理 Amazon EBS 卷上数据的潜在不一致性。它们的作用是在您需要确定 Amazon EBS 卷是否损坏的时候为您提供信息，帮助您控制处理潜在不一致卷的方式。

卷状态检查为自动执行的测试，该测试每隔 5 分钟运行一次并返回通过或故障状态。如果所有的检查都通过，则卷的状态为ok。如果一个检查返回故障，则卷的状态为impaired。如果状态为insufficient-data，那么该检查将在该卷上继续进行。您可以查看卷状态检查的结果来识别任意受损卷并进行所需操作。

当 Amazon EBS 确定卷的数据可能不一致时，默认情况下会禁用任何连接的 EC2 实例对该卷的 I/O，这有助于防止数据损坏。禁用 I/O 后，下一个卷状态检查故障，并且卷状态为impaired。此外，您还会看到一个通知您 I/O 被禁用的事件，并且您可以通过使能到该卷的 I/O 来解决卷的损坏状态。我们将等待您启用 I/O，期间您有机会决定是继续让实例使用该卷，还是在使用该卷之前先使用命令 [如 fsck（Linux 实例）或 chkdsk（Windows 实例）] 运行一致性检查。

> **Note**
>
> 卷状况以卷状况检查为依据，并不反映卷状态。因此，卷状态并不表示卷处于 error 状态（例如，卷无法接受 I/O 时）。有关卷状态的信息，请参阅 卷状态。

如果某个卷的一致性无关重要，您可以立即使该卷可用，如果该卷状态是“受损”，您可以配置该卷为自动启用 I/O 来覆盖默认操作。如果您启用自动启用 IO 卷属性（API 中的 autoEnableIO），则卷状态检查会继续通过。此外，您将会看到一个通知您该卷具有潜在不一致性的事件，但它的 I/O 不会自动启用。这使您能够检查卷的一致性或随后替换它。

I/O 性能状态检查将实际卷性能与卷的预期性能进行比较。如果卷的表现低于预期，它会提醒您。此状态检查仅适用于挂载到实例的预调配 IOPS SSD（io1 和 io2）和通用型 SSD（gp3）卷。状态检查对于通用型 SSD（gp2）、吞吐量优化型 HDD（st1）、Cold HDD（sc1）或磁介质（standard）

卷无效。I/O 性能状态检查每分钟执行一次，并每 5 分钟 CloudWatch 收集一次此数据。从您将 io1 或 io2 卷挂载到实例的那一刻起，可能需要 5 分钟来进行状态检查，以报告 I/O 性能状态。

> **Important**
>
> 在初始化已从快照还原的 Provisioned IOPS SSD 卷时，该卷的性能可能会下降到预期水平的 50% 以下，这会导致该卷在 I/O 性能状态检查中显示 warning 状态。这是预期行为，并且您可在初始化 Provisioned IOPS SSD 卷时忽略该卷上的 warning 状态。有关更多信息，请参阅 创建后手动初始化卷。

下表列出了 Amazon EBS 卷的状态。

卷状态	I/O 使能状态	I/O 性能状态（仅限 **io1**、**io2** 和 **gp3** 卷）
ok	使能（I/O 使能或 I/O 自动使能）	正常（卷的期望性能）
warning	使能 (I/O 使能或 I/O 自动使能)	降级（卷的性能低于期望性能） 严重降级（卷的性能大大低于期望性能）
impaired	使能 (I/O 使能或 I/O 自动使能) 禁用（卷脱机和挂起恢复，或等待用户使能 I/O）	停滞（卷性能受到严重影响） 不可用（由于 I/O 被禁用，所以不能确定 I/O 性能）
insufficient-data	使能 (I/O 使能或 I/O 自动使能) 数据不足	数据不足

Console

查看状态检查，需要进行以下操作

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。

2. 在导航窗格中，选择 Volumes。

   卷状态列显示每个卷的运行状态。

3. 要查看特定卷的详细状态信息，请在网格中选择该卷，然后选择 Status checks（状态检查）选项卡。

4. 如果您的卷状态检查返回故障（状态是 `impaired`），请参阅 使用受损的 Amazon EBS 卷。

另外，您还可以在导航器中选择事件来查看实例和卷所有的事件。有关更多信息，请参阅Amazon EBS 卷事件。

Amazon CLI

查看卷状态信息

使用 describe-volume-status 命令。

```
aws ec2 describe-volume-status --volume-ids vol-01234567890abcdef
```

使用以下示例来识别受损的卷。

```
aws ec2 describe-volume-status --filters Name=volume-status.status,Values=impaired
```

PowerShell

查看卷状态信息

使用 Get-EC2VolumeStatus cmdlet。

```
Get-EC2VolumeStatus -VolumeId vol-01234567890abcdef
```

使用以下示例来识别受损的卷。

```
Get-EC2VolumeStatus -Filter @{Name="volume-status.status"; Values="impaired"}
```

Amazon EBS 卷事件

当 Amazon EBS 确定某个卷的数据可能不一致时，它会默认禁用任何连接的 EC2 实例对该卷的 I/O。这将导致卷状态检查故障，并新建一个卷状态事件来指明故障的原因。

想要自动使能具有潜在不一致性卷上的 I/O，您可以改变自动启用 IO 卷属性（在 API 中为 autoEnableIO）的设置。更多关于改变这些属性的信息，请参阅使用受损的 Amazon EBS 卷。

每一个事件都包括一个开始时间，该时间指明事件发生的时间，和一个持续时间，该时间会指明该卷 I/O 会被禁用多久。当该卷的 I/O 被使能时，将会为该事件添加结束时间。

卷状态事件

`Awaiting Action: Enable IO`

卷数据具有潜在一致性。在您明确的使能它之前，将一直禁用 I/O。当您明确启用 I/O 后，事件描述变为 IO Enabled。

`IO Enabled`

明确地使能这些卷的 I/O 操作。

`IO Auto-Enabled`

事件发生后，自动使能这些卷上的 I/O 操作。我们建议您在继续使用数据前，先检查数据的不一致性。

`Normal`

仅适用于 io1、io2 和 gp3 卷。卷执行其期望性能。

`Degraded`

仅适用于 io1、io2 和 gp3 卷。卷性能低于期望性能。

`Severely Degraded`

仅适用于 io1、io2 和 gp3 卷。卷性能大大地低于期望性能。

`Stalled`

仅适用于 io1、io2 和 gp3 卷。卷的性能受到严重影响。

如果您的卷 I/O 被禁用，请参阅使用受损的 Amazon EBS 卷。如果您的卷 I/O 性能低于正常值，这可能是因为您之前的操作（例如，在使用高峰期间创建卷快照、在无法支持所需 I/O 带宽的实例上运行卷、第一次访问卷上的数据，等等）而造成的暂时状况。

Console

想要查看您的卷事件，需要执行以下操作

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Events。列出具有事件的所有实例和卷。
3. 可以按卷进行筛选以便仅查看卷状态。您也可以筛选指定的状态类型。
4. 选择一个卷以查看其特定事件。

Amazon CLI

想要查看您的卷事件，需要执行以下操作

使用 describe-volume-status 命令。

```
aws ec2 describe-volume-status --volume-ids vol-01234567890abcdef
```

PowerShell

想要查看您的卷事件，需要执行以下操作

使用 Get-EC2VolumeStatus cmdlet。

```
Get-EC2VolumeStatus -VolumeId vol-01234567890abcdef
```

使用受损的 Amazon EBS 卷

如果卷受损，请使用以下选项，因为卷的数据可能不一致。

选项

- 选项 1：对附加到其实例的卷执行一致性检查
- 选项 2：使用其他实例对该卷执行一致性检查
- 选项 3：如果您不再需要卷，请将其删除

选项 1：对附加到其实例的卷执行一致性检查

最简单的选择是启用 I/O，然后在卷仍连接到其 Amazon EC2 实例时对该卷执行数据一致性检查。

想要在一个附加的卷上进行一次一致性检查，需要执行以下操作

1. 停止所有使用该卷的应用程序。
2. 在该卷上使能 I/O。使用以下方法之一。

   Console

   为卷启用 I/O

   1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
   2. 在导航窗格中，选择 Events（事件）。
   3. 选择该卷。
   4. 选择 Actions（操作）、Enable I/O（启用输入/输出）。

   Amazon CLI

   为卷启用 I/O

   使用 enable-volume-io 命令。

   ```
   aws ec2 enable-volume-io --volume-id vol-01234567890abcdef
   ```

   PowerShell

   为卷启用 I/O

   使用 Enable-EC2VolumeIO cmdlet。

   ```
   Enable-EC2VolumeIO -VolumeId vol-01234567890abcdef
   ```

3. 检查卷上数据。

   a. 运行 fsck（Linux 实例）或 chkdsk（Windows 实例）命令。

   b. （可选）查看所有适用的应用程序或系统日志以了解相关错误消息。

   c. 如果音量受损超过 20 分钟，则可以联系 Su Amazon pport Center。选择问题排查，然后在状态检查故障排除对话框上选择联系客户服务提交一个支持案例。

选项 2：使用其他实例对该卷执行一致性检查

按照以下程序在您的产品环境外检查该卷。

> **Important**
>
> 当卷 I/O 被禁用时，这些程序可能会导致挂起的写入 I/O 丢失。

想要在一个隔离环境中在一个卷上进行一次一致性检查，需要执行以下操作

1. 停止所有使用该卷的应用程序。
2. 将该卷从实例中分离。有关更多信息，请参阅将 Amazon EBS 卷与亚马逊实例分离 EC2 。
3. 在该卷上使能 I/O。使用以下方法之一。

Console

为卷启用 I/O

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Events（事件）。
3. 选择您在之前的步骤中分离的卷。
4. 选择 Actions（操作）、Enable I/O（启用输入/输出）。

Amazon CLI

为卷启用 I/O

使用 enable-volume-io 命令。

```
aws ec2 enable-volume-io --volume-id vol-01234567890abcdef
```

PowerShell

为卷启用 I/O

使用 Enable-EC2VolumeIO cmdlet。

```
Enable-EC2VolumeIO -VolumeId vol-01234567890abcdef
```

4. 将该卷附加到另一个实例。有关更多信息，请参阅启动实例和将 Amazon EBS 卷附加到亚马逊 EC2 实例。
5. 检查卷上数据。
   a. 运行 fsck（Linux 实例）或 chkdsk（Windows 实例）命令。
   b. （可选）查看所有适用的应用程序或系统日志以了解相关错误消息。
   c. 如果音量受损超过 20 分钟，则可以联系 Su Amazon pport Center。选择 Troubleshoot，然后在故障排除对话框中选择 Contact Support 以提交支持案例。

选项 3：如果您不再需要卷，请将其删除

如果您想将该卷从您的环境中去除，只需删除它即可。关于删除一个卷的信息，请查阅删除 Amazon EBS 卷。

如果您有在该卷上备份的近期快照，那么您可以从快照中创建一个新卷。有关更多信息，请参阅 创建 Amazon EBS 卷。

为受损的 Amazon EBS 卷自动启用 I/O

当 Amazon EBS 确定某个卷的数据可能不一致时，它会默认禁用任何连接的 EC2 实例对该卷的 I/O。这将导致卷状态检查故障，并新建一个卷状态事件来指明故障的原因。如果某个卷的一致性无关重要，您可以立即使该卷可用，如果该卷状态是受损，您可以配置该卷为自动启用 I/O 来覆盖默认操作。如果您启用自动启用 IO 卷属性（API 中的 `autoEnableIO`），则卷和实例之间的 I/O 会自动重新启用，并且卷将通过状态检查。此外，您将会看到一个通知您该卷具有潜在不一致状态的事件，但它的 I/O 不会自动启用。如果发生此事件，您应该检查该卷的一致性，如有必要，可对其进行更换。有关更多信息，请参阅 Amazon EBS 卷事件。

Console

查看卷的“自动启用 IO”属性

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Volumes。
3. 选择卷，然后选择 Status checks（状态检查）选项卡。

   Auto-enabled I/O（自动启用输入/输出）字段为所选择的卷显示当前设置：已启用或已禁用。

修改卷的“自动启用 IO”属性

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Volumes。
3. 选择所需卷，然后选择 Actions（操作）、Manage auto-enabled I/O（管理自动启用的输入/输出）。
4. 选中 Auto-enable I/O for impaired volumes（为受损卷自动启用输入/输出）复选框，以便为受损卷自动启用输入/输出。想要禁用该功能，请清除复选框。
5. 选择更新。

Amazon CLI

查看卷的 autoEnableIO 属性

使用 describe-volume-attribute 命令。

```
aws ec2 describe-volume-attribute \
    --attribute autoEnableIO \
    --volume-id vol-01234567890abcdef
```

下面是示例输出。

```
{
    "AutoEnableIO": {
        "Value": true
    },
    "VolumeId": "vol-01234567890abcdef"
}
```

要修改一个卷的 autoEnableIO 属性

使用 modify-volume-attribute 命令。

```
aws ec2 modify-volume-attribute \
    --auto-enable-io \
    --volume-id vol-01234567890abcdef
```

PowerShell

查看卷的 autoEnableIO 属性

使用 Get-EC2VolumeAttribute cmdlet。

```
(Get-EC2VolumeAttribute `
    -Attribute autoEnableIO `
    -VolumeId vol-01234567890abcdef).AutoEnableIO
```

下面是示例输出。

```
True
```

要修改一个卷的 autoEnableIO 属性

使用 Edit-EC2VolumeAttribute cmdlet。

```
Edit-EC2VolumeAttribute `
    -AutoEnableIO $true `
    -VolumeId vol-01234567890abcdef
```

在 Amazon EBS 上进行故障测试

使用 Amazon Fault Injection Service 和 “暂停 I/O” 操作可暂时停止 Amazon EBS 卷与其连接的实例之间的 I/O，以测试您的工作负载如何处理 I/O 中断。借 Amazon FIS助，您可以使用对照实验来测试您的架构和监控，例如 Amazon CloudWatch 警报和操作系统超时配置，并提高应对存储故障的弹性。

有关的更多信息 Amazon FIS，请参阅《Amazon Fault Injection Service 用户指南》。

注意事项

暂停卷 I/O 时请注意以下事项：

- 可以为挂载到基于 Nitro 系统构建的实例的所有 Amazon EBS 卷类型暂停 I/O。
- 可以为根卷暂停 I/O。
- 可以为启用多重挂载的卷暂停 I/O。如果为已启用多重挂载的卷暂停 I/O，则该卷及其所有附加实例之间将暂停 I/O。
- 要测试操作系统超时配置，请将实验持续时间设置为等于或大于为 `nvme_core.io_timeout` 指定的值。有关更多信息，请参阅 NVMe 亚马逊 EBS 卷的 I/O 操作超时。
- 如果提升对已暂停 I/O 卷的 I/O，会发生以下情况：
  - 卷的状态将在 120 秒内转换为 `impaired`。有关更多信息，请参阅 Amazon EBS 卷状态检查。

- 队列长度 (`VolumeQueueLength`) 的 CloudWatch 指标将为非零。任何告警或监控都应监控非零队列深度。有关更多信息，请参阅 Amazon EBS 卷的指标。
- `VolumeReadOps`或的 CloudWatch 指标`VolumeWriteOps`将是`0`，这表示该卷不再处理 I/O。

限制

暂停卷 I/O 时请注意以下限制：

- 不支持实例存储卷。
- 不支持基于 Xen 的实例类型。
- 您无法暂停在Outpost、区域或本地 Amazon Wavelength 区域中创建的卷的 I/O。

您可以从 Amazon EC2 控制台执行基本实验，也可以使用控制 Amazon FIS 台进行更高级的实验。有关使用 Amazon FIS 控制台执行高级实验的更多信息，请参阅《Amazon Fault Injection Service 用户指南》 Amazon FIS中的教程。

使用 Amazon EC2 控制台执行基本实验

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Volumes。
3. 选择要为其暂停 I/O 的卷，然后选择操作、错误注入、暂停卷 I/O。
4. 对于持续时间，输入要在卷和实例之间暂停 I/O 的持续时间。“持续时间”下拉列表旁边的字段将以 ISO 8601 格式显示持续时间。
5. 在服务访问权限部分，选择要代入的 IAM 服务角色 Amazon FIS 来执行实验。您可以使用默认角色，也可以使用您创建的现有角色。有关更多信息，请参阅为 Amazon FIS 创建 IAM 角色。
6. 选择暂停卷 I/O。系统提示时，在确认字段中输入 `start` 并选择开始实验。
7. 监控实验的进度和影响。有关更多信息，请参阅《Amazon FIS 用户指南》中的监控 Amazon FIS。

Amazon EBS 快照

您可以通过制作 point-in-time副本（称为 Amazon EBS 快照）来备份 Amazon EBS 卷上的数据。快照是增量备份，这意味着我们仅保存卷上自最新快照之后发生更改的块。由于无需复制数据，这将最大限度缩短创建快照所需的时间和增加存储成本节省。

> **Important**
>
> Amazon 不会自动备份存储在 EBS 卷上的数据。为满足数据恢复能力和灾难恢复的需要，您应定期创建 EBS 快照，或者使用 使用 Amazon Data Lifecycle Manager 自动备份 或 Amazon Backup 设置自动快照创建。

快照存储在 Amazon S3 中您无法直接访问的 S3 存储桶中。您可以使用亚马逊 EC2 控制台或亚马逊 EC2 API 创建和管理您的快照。您无法使用 Amazon S3 控制台或 Amazon S3 API 访问您的快照。

快照数据会自动复制到该区域的所有可用区。这为快照数据提供了高可用性和持久性，并使您能够恢复该区域中任何可用区的卷。

每个快照都包含将数据（拍摄快照时存在的数据）还原到新 EBS 卷所需的所有信息。当您从快照创建 EBS 卷时，新卷将开始作为用于创建快照的卷的精确副本。

有关更多信息，请参阅 Amazon EBS 快照产品页面。

快照事件

您可以通过 “ CloudWatch 事件” 跟踪 EBS 快照的状态。有关更多信息，请参阅 EBS 快照事件。

快照定价

快照的费用取决于存储的数据量。由于快照是增量的，因此删除快照可能不会降低您的数据存储成本。删除快照时，专由某个快照引用的数据将被删除，但保留其他快照引用的数据。有关更多信息，请参阅 Amazon Billing 用户指南中的 Amazon Elastic Block Store 卷和快照。

内容

- Amazon EBS 快照的工作原理
- Amazon EBS 快照生命周期
- Amazon EBS 快速快照还原
- Amazon EBS 快照锁

- 阻止 Amazon EBS 快照的公开访问
- Amazon EBS local snapshots on Outposts
- Local Zones 中的本地快照

Amazon EBS 快照的工作原理

您从卷创建的第一个快照始终是完整快照。它包括创建快照时写入卷的所有数据块。同一卷的后续快照为增量快照。这些快照仅包括自上次创建快照以来写入卷的已更改数据块和新数据块

完整快照的大小取决于备份数据的大小，而非源卷的大小。同样地，与完整快照相关的存储成本取决于快照的大小，而非源卷的大小。例如，您创建了仅包含 50 GiB 数据的 200 GiB Amazon EBS 卷的第一个快照。这会生成大小为 50 GiB 的完整快照，并且您需要为 50 GiB 快照存储付费。

同样，增量快照的大小和存储成本取决于自上次快照创建以来写入卷的任何数据的大小。继续前面的示例，如果您在更改数据和添加10 GiB数据后创建了同一200 GiB卷20 GiB的第二个快照，则增量快照的大小就是30 GiB这样。然后，您需要为额外的 30 GiB 快照存储付费。

有关快照定价的更多信息，请参阅 Amazon EBS 定价。

> **Important**
>
> 归档增量快照时，增量快照将转换为完整快照，其中包括创建快照时写入卷的所有块。然后，快照将移动到 Amazon EBS 快照归档层。归档层中的快照费率与标准层中的快照费率不同。有关更多信息，请参阅 归档 Amazon EBS 快照的定价和计费。

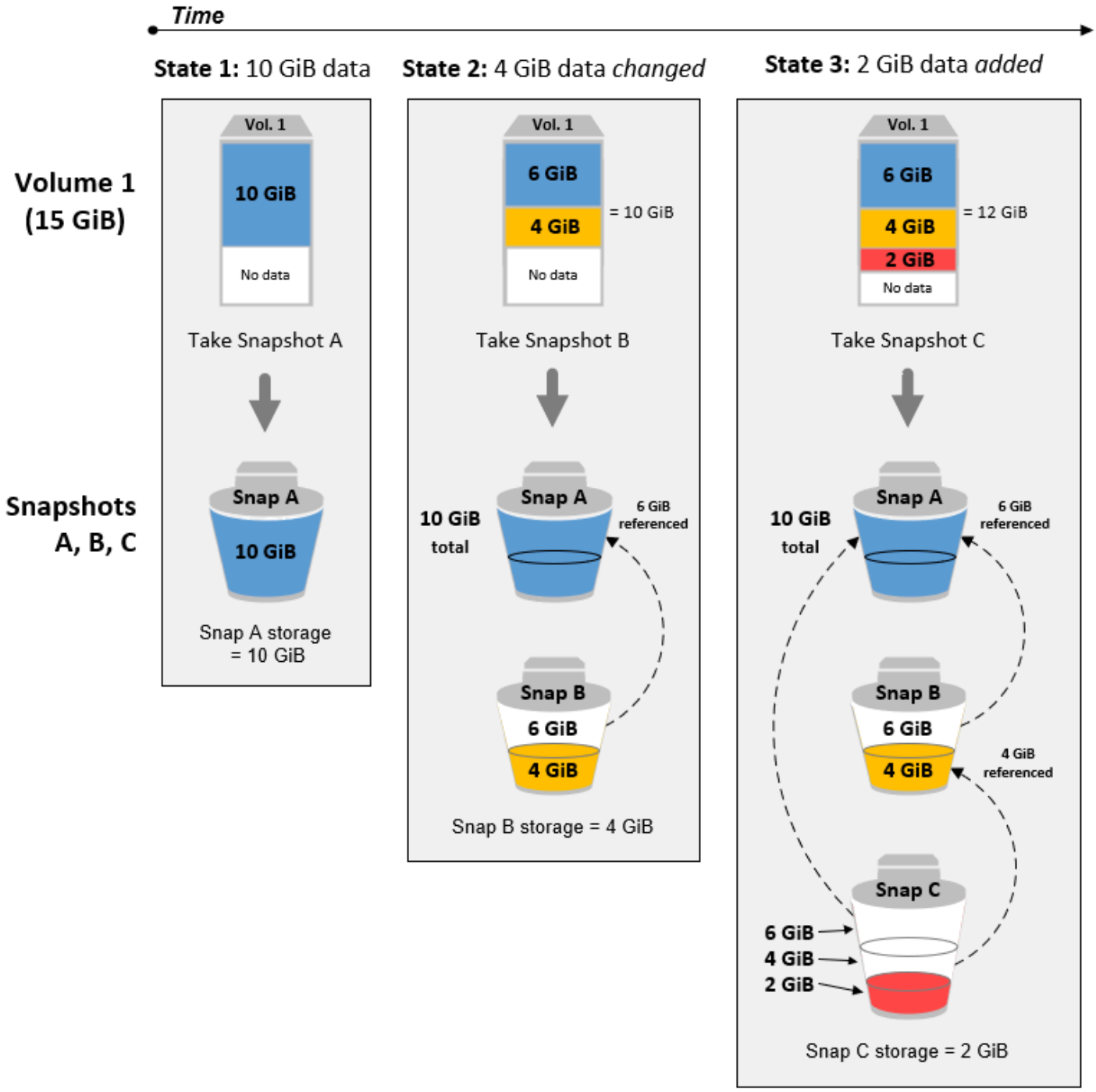
以下部分阐述了 EBS 快照如何捕获卷在某一时间点的状态，以及正在更改的卷的后续快照如何创建这些更改的历史记录。

同一卷的多个快照

在本部分的图表中，大小为 15 GiB 的卷 1 在 3 个时间点上显示。为这三个卷状态分别制作快照。该图表明确显示以下内容：

- 在状态 1 中，该卷具有 10 GiB 数据。快照 A 是为该卷制作的第一个快照。快照 A 是完整快照，所有 10 GiB 数据均已备份。
- 在状态 2 中，该卷仍包含 10 GiB 数据，但是，捕获快照 A 后仅 4 GiB 数据发生更改。快照 B 是增量快照。只需要备份已更改的 4 GiB 数据。未更改的其他 6 GiB 数据（已在快照 A 中备份）将由快照 B 引用，而不会再次备份。这通过虚线箭头指示。

- 在状态 3 中，捕获快照 B 后，2 GiB 数据已添加到该卷中，共计 12 GiB 数据。快照 C 是增量快照。只需要对捕获快照 B 之后添加的 2 GiB 数据进行备份。如虚线箭头所示，快照 C 还引用了存储在快照 B 中的 4 GiB 数据和存储在快照 A 中的 6 GiB 数据。
- 三个快照共需 16 GiB 存储空间。这相当于快照 A 需要 10 GiB，快照 B 需要 4 GiB，快照 C 需要 2 GiB。



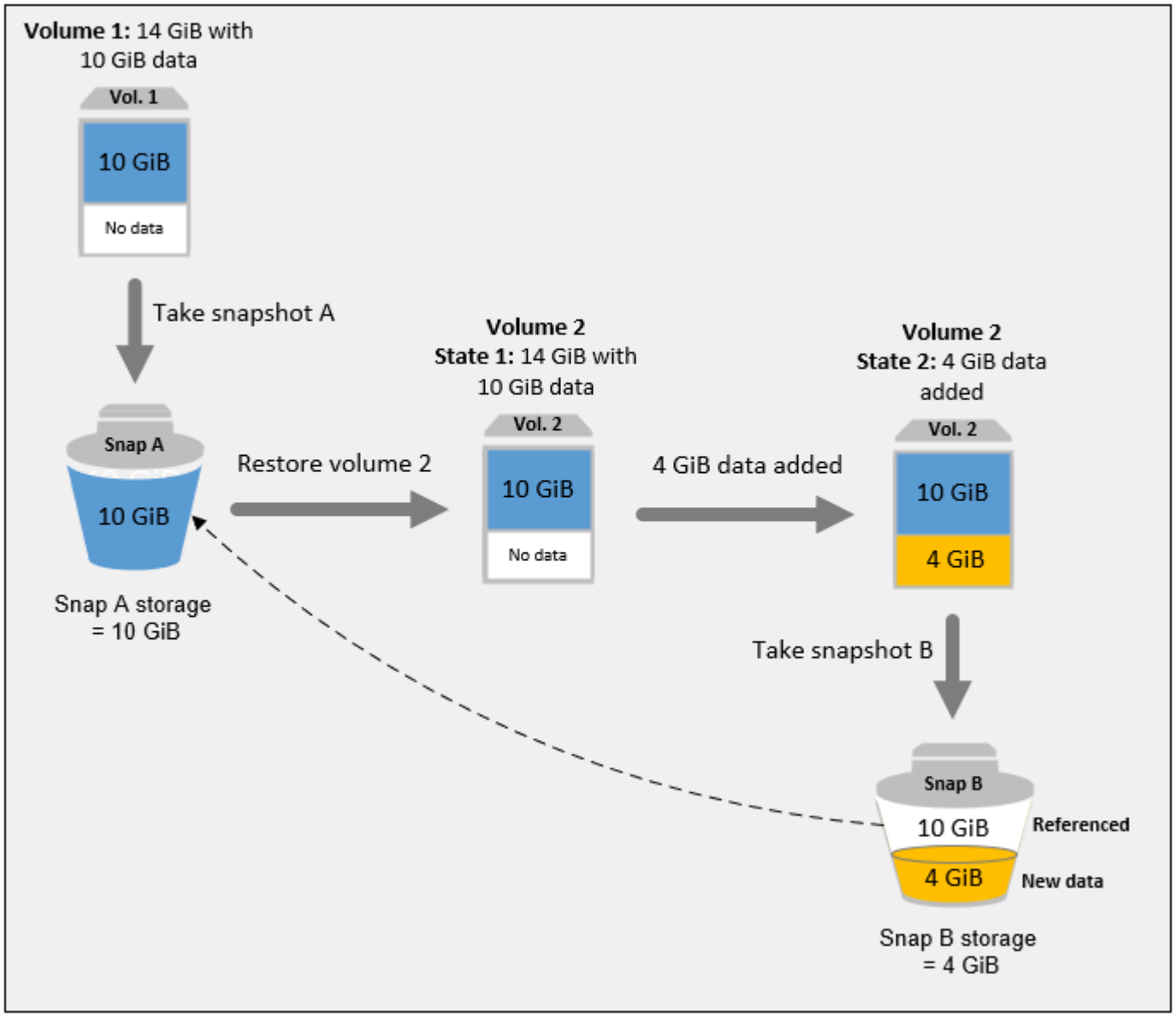
不同卷的增量快照

本节中的图表显示了如何从不同卷获取增量快照。

1. 大小为 14 GiB 的卷 1 包含 10 GiB 数据。因为快照 A 是为该卷捕获的首个快照，是完整快照，因此会备份所有 10 GiB 数据。
2. 卷 2 是从快照 A 创建的，所以它是卷 1 在拍摄快照时的精准副本。
3. 随着时间的推移，4 GiB 的数据将添加到卷 2，并且其数据总大小为 14 GiB。
4. 快照 B 是基于卷 2 制作的。对于快照 B，仅备份从快照 A 创建卷后添加的 4 GiB 数据。未更改的其他 10 GiB 数据（已存储在快照 A 中）将由快照 B 引用，而不会再次备份。

   快照 B 是快照 A 的增量快照，即使它是从不同的卷创建的。

> **Important**
>
> 该图表假定您拥有卷 1 和快照 A，并且卷 2 使用与卷 1 相同的 KMS 密钥进行加密。如果 Vol 1 归另一个 Amazon 账户所有，并且该账户使用了 Snap A 并与你共享，那么 Snap B 将是完整快照。或者，如果卷 2 使用与卷 1 不同的 KMS 密钥进行加密，则快照 B 将是完整快照。

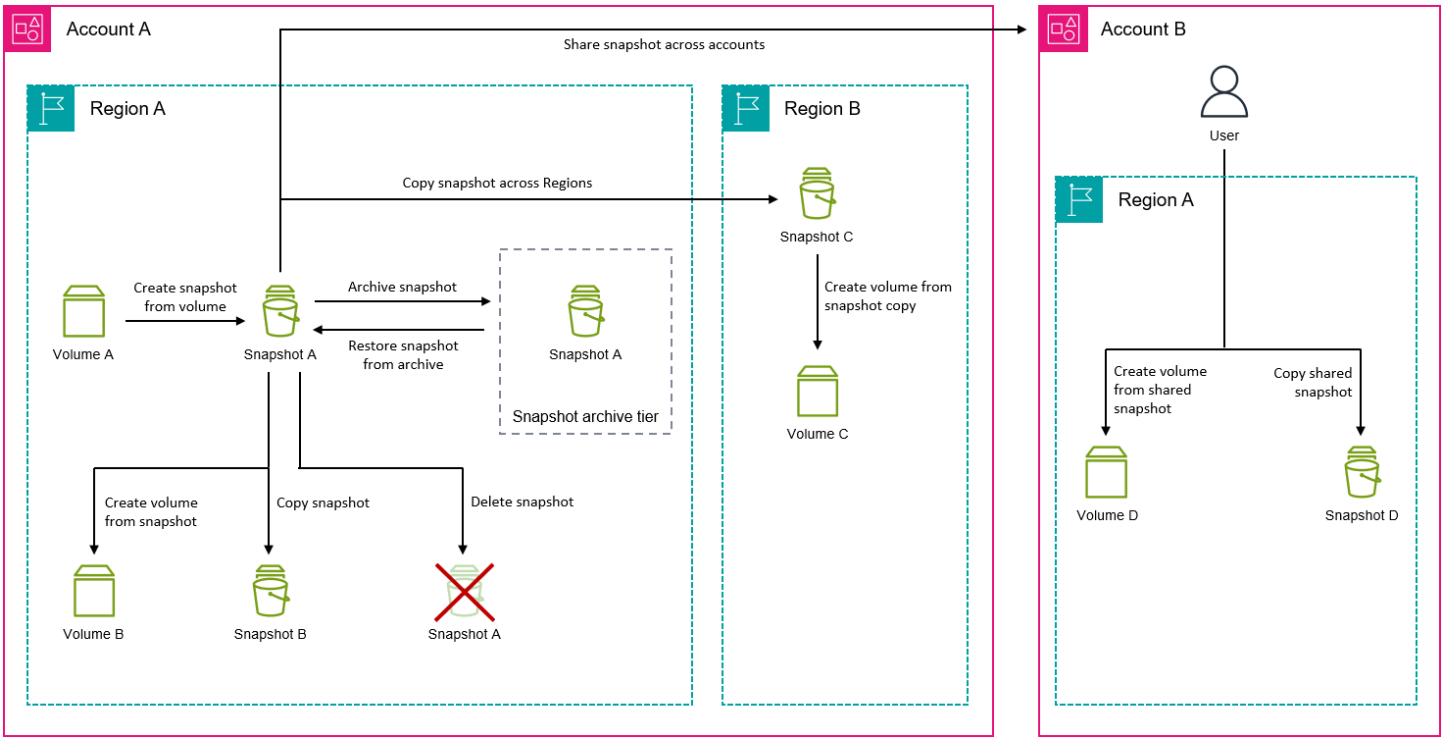


有关删除快照后如何管理数据的更多信息，请参阅删除 Amazon EBS 快照。

Amazon EBS 快照生命周期

Amazon EBS 快照的生命周期始于创建过程。从 Amazon EBS 卷创建快照。可以使用快照还原新的 Amazon EBS 卷。可以在相同区域或不同区域创建快照副本。您可以公开或私下与其他 Amazon Web Services 账户人共享快照。这些账户可以从共享快照还原卷，也可以在自有账户中创建共享快照的副本。如果不需要立即访问快照，则可以将其存档以节省存储成本。

下图显示了可以在快照生命周期中对快照执行的操作。



任务

- 创建 Amazon EBS 快照
- 查看 Amazon EBS 快照信息
- 复制 Amazon EBS 快照
- 与其他账户共享 Amazon EBS 快照 Amazon
- 归档 Amazon EBS 快照
- 删除 Amazon EBS 快照

创建 Amazon EBS 快照

您可以创建 Amazon EBS 卷的 Amazon EBS 快照来创建该卷的 point-in-time备份。您可以创建单个 Amazon EBS 卷的快照，也可以为附加到 Ama EC2 zon 实例的全部卷或部分卷创建多卷快照。

快照创建是异步进行的。快照会立即创建，但在所有数据都传输到 Amazon S3 之前，它会一直保持 `pending` 状态。这可能需要几个小时才能完成，具体取决于卷上已修改的数据块数量。在此期间，您可以继续使用卷，而不会影响快照。快照仅包含请求快照时写入卷的数据。它不包括应用程序或操作系统缓存的数据。

> **Tip**
>
> 为确保快照的一致性和完整性，我们建议在创建快照之前暂停对卷的写入。如果无法暂停对卷的写入，我们建议在创建快照之前从实例中卸载该卷。快照进入 pending 状态后，您可以重新挂载并恢复写入。
> 如果您为充当 Amazon EC2 实例根设备的卷创建快照，我们建议您在拍摄快照之前停止该实例。

内容

- 快照加密
- 快照目标
- 自动化快照
- 创建快照的注意事项
- 创建 EBS 卷的快照
- 从实例创建多卷 EBS 快照 EC2

快照加密

快照会自动获得与其创建时所在的卷相同的加密状态。从未加密的卷创建的快照不会进行加密。从已加密的卷创建的快照将自动使用与卷相同的 KMS 密钥进行加密。

> **Tip**
>
> 如果需要从未加密的卷创建已加密的快照，请首先创建该卷的未加密快照，然后创建该快照的加密副本。

快照目标

源资源（卷或实例）的位置决定了您可以在何处创建快照。

- 如果源资源位于某个区域，则必须在与源资源相同的区域中创建快照。
- 如果源资源位于本地区域中，则可以在同一个本地区域或其父区域中创建快照。有关更多信息，请参阅 Local Zones 中的本地快照。

- 如果源资源位于 Outpost，你可以在同一个上面创建快照 Outpost 或在其父区域。有关更多信息，请参阅 Amazon EBS local snapshots on Outposts。

自动化快照

您可以使用 Amazon Data Lifecycle Manager 和 Amazon Backup 自动创建快照。

创建快照的注意事项

- 我们建议您不要为挂载到处于休眠状态或已启用休眠状态的 Amazon EC2 实例的卷创建快照。有关更多信息，请参阅 Amazon EC2 实例休眠的工作原理。
- 尽管您可以在某个卷的前一个快照处于 pending 状态时拍摄该卷的快照，但如果同一个卷的多个快照处于 pending 状态，则可能会导致该卷的性能降低，直至这些快照完成。
- 处于 pending 状态的快照数量以及对于每个卷类型可以请求的并发快照数量均有限制。有关更多信息，请参阅 Quotas for Amazon EBS。如果超出其中一个配额，请等待当前快照完成，然后重试。

创建 EBS 卷的快照

您可以为单个卷创建单个快照。或者，要自动创建快照，请使用 Amazon Data Lifecycle Manager 或Amazon Backup。要为 EC2 实例创建所有卷的快照，请使用多卷快照。

Console

创建快照

1. 打开亚马逊 EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Snapshots（快照）、Create snapshot（创建快照）。
3. 对于资源类型，选择卷。
4. 对于 Volume ID（卷 ID），选择需要从其创建快照的卷。加密字段指示卷和生成的快照的加密状态。不可修改。
5. （可选）对于描述，输入快照的简短描述。
6. 如果音量开启 Outpost 或者在本地区域中，将出现 “快照目标” 字段。请执行以下操作之一：
   - 如果卷位于本地区域中，请选择本地区域在同一个本地区域中创建快照，或者选择Amazon 区域在本地区域的父区域中创建快照。
   - 如果音量开启 Outpost，选择 Amazon Outpost，在同一个上创建快照 Outpost，或者选择 Amazon Re gion 在的父区域中创建快照 Outpost.

> **Note**
>
> 如果卷位于某个区域中，则不会显示快照目标。快照将在与卷相同的区域中自动创建。

7. （可选）要为快照分配自定义标签，请在标签部分中选择添加标签，然后输入键值对。最多可以添加 50 个标签。
8. 选择创建快照。

Amazon CLI

创建快照

使用 create-snapshot 命令。

```
aws ec2 create-snapshot  \
    --volume-id vol-01234567890abcdef \
    --description "Snapshot of the root volume for i-1234567890abcdef0"
```

PowerShell

创建快照

使用 New-EC2Snapshot cmdlet。

```
New-EC2Snapshot `
    -VolumeId vol-01234567890abcdef `
    -Description "Snapshot of the root volume for i-1234567890abcdef0"
```

从实例创建多卷 EBS 快照 EC2

默认情况下，当您从亚马逊实例创建多卷快照时，Amazon EBS 会创建附加到该 EC2 实例的所有 Amazon EBS 卷的快照。但是，如果需要，您可以选择排除根卷或特定数据卷。

> **Tip**
>
> 我们建议您为多卷快照添加标签，以便轻松地识别和集中管理它们。您还可以将标签从源卷复制到相应的快照，以设置快照元数据（例如访问策略、挂载信息和成本分配），从而匹配源卷。

多卷快照的注意事项

- 如果所有快照都成功完成，则会向您的 Amazon 账户发送一个结果为`createSnapshots` CloudWatch 的事件。`succeeded`如果多卷快照集中的任何一个快照失败，则所有其他快照都将进入`error`状态，结果为`createSnapshots` CloudWatch 的事件将发送到您的账户。`failed`有关更多信息，请参阅 创建多个快照（createSnapshots）。
- 多卷快照支持最多 128 个 Amazon EBS 卷挂载到实例，包括根卷和最多 127 个数据卷。
- 多卷快照集中的每个快照都是一个单独的快照，可以相同的方式使用，并且支持与单独快照相同的功能。
- 您可以使用命令文档为附加到亚马逊 EC2 Windows 实例的所有 Amazon EBS 卷拍摄应用程序一致的快照。Amazon Systems Manager

Console

创建多卷快照

1. 打开亚马逊 EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Snapshots（快照）、Create snapshot（创建快照）。
3. 对于资源类型，选择实例。
4. 对于 Description （描述），输入快照的简短描述。此描述适用于所有快照。
5. 如果实例在 Outpost 或者在本地区域中，将出现 “快照目标” 字段。请执行以下操作之一：
   - 如果实例位于本地区域中，请选择本地区域在同一个本地区域中创建快照，或者选择Amazon 区域在本地区域的父区域中创建快照。
   - 如果实例在 Outpost，选择 Amazon Outpost，在同一个上面创建快照 Outpost，或者选择Amazon 区域在的父区域中创建快照 Outpost.

> **Note**
>
> 如果实例位于某个区域中，则不会显示快照目标。快照将在与实例相同的区域中自动创建。

6. （可选）要排除实例的根卷，请选择排除根卷。
7. （可选）要排除数据卷，请选择排除特定的数据卷。Attached data volumes（附加的数据卷）部分列出了当前附加到所选实例的所有数据卷。

   选择要排除的数据卷。只有未选中的卷才会包含在多卷快照集中。
8. （可选）若要自动将标签从源卷复制到相应快照，对于从源卷复制标签，选择复制标签。
9. （可选）若要为快照分配其他自定义标签，请在标签部分选择添加标签，然后输入键值对。最多可以添加 50 个标签。
10. 选择创建快照。

Amazon CLI

创建多卷快照

使用 create-snapshots 命令。

```
aws ec2 create-snapshots \
    --instance-specification InstanceId=i-1234567890abcdef0 \
    --description "from a multi-volume snapshot of i-1234567890abcdef0"
```

要排除根卷，请在`--instance-specification`选项中添加以下内容。

```
ExcludeBootVolume=true
```

要排除数据量，请在`--instance-specification`选项中添加以下内容。

```
ExcludeDataVolumeIds=vol-01234567890abcdef
```

PowerShell

创建多卷快照

使用 New-EC2SnapshotBatch cmdlet。

```
New-EC2SnapshotBatch `
    -InstanceSpecification_InstanceId i-1234567890abcdef0 `
    -Description "from a multi-volume snapshot of i-1234567890abcdef0"
```

要排除根卷，请添加以下参数。

```
-InstanceSpecification_ExcludeBootVolume $true
```

要排除数据量，请添加以下参数。

```
-InstanceSpecification_ExcludeDataVolumes "vol-01234567890abcdef"
```

查看 Amazon EBS 快照信息

您可以查看有关您的快照的详细信息。

Console

查看快照信息

1. 打开亚马逊 EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择快照。
3. 要仅查看您拥有的快照，请在屏幕左上角选择 Owned by me（我拥有的）。您还可以使用标签和快照属性筛选快照列表。在 Filter（筛选条件）字段中，选择属性字段，然后选择或输入属性值。例如，要仅查看加密的快照，请选择 Encryption（加密），然后输入 `true`。
4. 要查看有关特定快照的更多信息，请在列表中选择其 ID。

> **Note**
>
> “完整快照大小” 字段显示快照的完整大小（以字节为单位）。这不是快照的增量大小。相反，它表示创建快照时写入源卷的所有块的大小。
> 如果未指定其他大小，则卷大小字段显示将从快照创建的 EBS 卷的大小。

Amazon CLI

查看快照信息

可以使用 describe-hosts 命令。

Example 示例 1：基于标签进行筛选

以下示例描述了标签为 stack=Production 的快照。

```
aws ec2 describe-snapshots --filters Name=tag:Stack,Values=production
```

Example 示例 2：基于卷进行筛选

以下示例描述了从指定卷创建的快照。

```
aws ec2 describe-snapshots --filters Name=volume-id,Values=vol-049df61146c4d7901
```

Example 示例 3：基于快照期限进行筛选

您可以使用 JMESPath 表达式筛选结果。例如，以下命令显示您的账户在指定日期之前创建的所有快照。 IDs 如果未指定所有者，则结果将包括所有公有快照。

```
aws ec2 describe-snapshots \
    --filters Name=owner-id,Values=123456789012 \
    --query "Snapshots[?(StartTime<='2024-03-31')].[SnapshotId]" \
    --output text
```

以下命令显示在 IDs 指定日期范围内创建的所有快照。

```
aws ec2 describe-snapshots \
    --filters Name=owner-id,Values=123456789012 \
    --query "Snapshots[?(StartTime>='2024-01-01') && (StartTime<='2024-12-31')].
[SnapshotId]" \
    --output text
```

PowerShell

查看快照信息

使用 Get-EC2Snapshot cmdlet。

示例 1：描述快照

以下 示例描述了指定的快照。

```
Get-EC2Snapshot -SnapshotId snap-0abcdef1234567890
```

示例 2：基于卷进行筛选

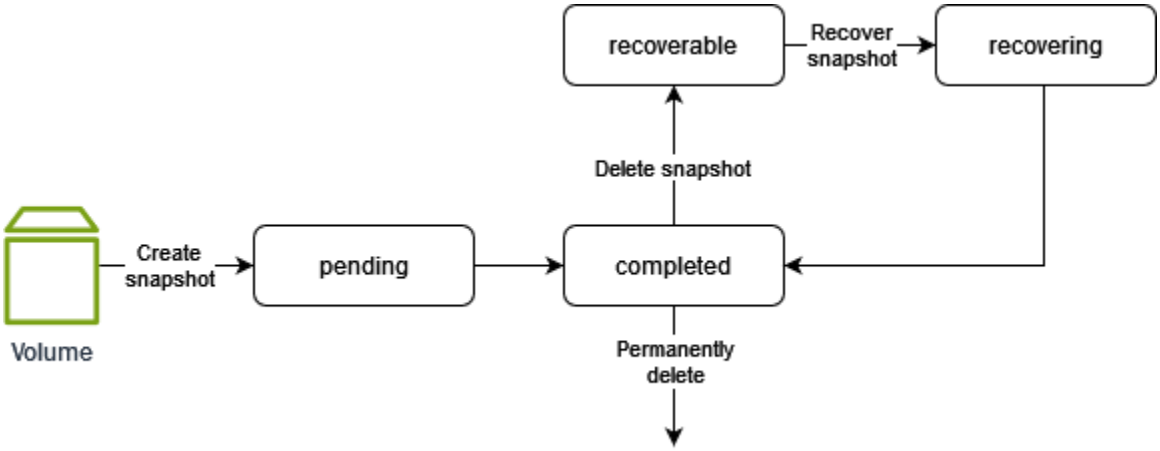
以下示例描述了从指定卷创建的快照。

```
Get-EC2Snapshot`
    -Filter @{Name="volume-id"; Values="vol-01234567890abcdef"}
```

快照状态

从创建直至永久删除，Amazon EBS 快照会历经不同状态的转换。

下图阐释了快照状态之间的转换。创建快照时，其进入 pending 状态。当快照准备就绪后，其进入 completed 状态。若决定不再需要某个快照，可以删除该快照。如果删除与回收站保留规则匹配的快照，该快照会保留在回收站中并进入 recoverable 状态。如果从回收站还原快照，该快照会进入 recovering 状态，然后进入 completed 状态。否则，将永久删除此快照。



下表汇总了快照状态。

状态	描述
pending	快照创建过程仍在进行中。处于 pending 状态时，快照无法使用。
completed	快照创建过程已完成，快照可供使用。

状态	描述
recoverable	快照目前在回收站中。要使用快照，您必须首先从回收站中还原快照。
recovering	正在从回收站中还原快照。快照还原后会转换到 completed 状态并且可供使用。
error	快照创建过程已失败。处于 error 状态时，快照无法使用。

复制 Amazon EBS 快照

创建快照并达到completed状态后，您可以将其从一个 Amazon 区域复制到另一个区域，或者复制到同一区域内。快照副本是原始副本的精确副本，但它具有唯一的资源 ID。您可以复制您拥有的快照以及私下或公开与您共享的快照。您可能需要为以下使用场景复制快照：

- 地理扩展 — 您需要在新区域中启动您的应用程序。
- 迁移 — 您需要将应用程序迁移到新区域，以实现更好的可用性或最大限度地降低成本。
- 灾难恢复 — 您需要将数据和日志备份到辅助区域，以实现数据冗余。
- 加密 — 您需要加密以前未加密的快照或使用其他 KMS 密钥重新加密已加密的快照。
- 复制共享快照 — 您需要复制与您共享的快照。
- 数据保留和审计要求 — 您需要将加密快照从一个 Amazon 账户复制到另一个账户，以保留用于审计或数据保留的数据。如果您的主账户遭到入侵，使用其他 Amazon 账户可以保护您。

要将多卷快照复制到另一个 Amazon 区域，请使用您在创建时分配的标签识别属于该快照集的所有快照，然后将快照单独复制到所需的区域。

有关复制 Amazon RDS 快照的信息，请参阅 Amazon RDS 用户指南 中的复制数据库快照。

定价

有关跨 Amazon 区域和账户复制快照的定价信息，请参阅 Amazon EBS 定价。

内容

- 复制快照的注意事项

- 快照副本的目的地
- 增量快照复制
- Amazon EBS 快照和 EBS 支持的基于时间的副本 AMIs
- 加密和快照复制
- 复制快照

复制快照的注意事项

- 您可以复制 Amazon Web Services Marketplace、虚拟机导入/导出和 Storage Gateway 快照，但必须验证目标区域是否支持该快照。
- 每个目标区域限制并发快照复制请求不得超过 20 个。如果您超出此配额，会收到 `ResourceLimitExceeded` 错误。如果收到此错误，请等待一个或多个复制请求完成，然后再发出新的快照复制请求。
- 用户定义的标签不会从源快照复制到快照副本。您可以在复制操作期间或之后添加用户定义的标签。
- 由快照复制操作创建的快照具有任意性的卷 ID，例如 `vol-ffff` 或 `vol-ffffffff`。这些任意音量 IDs 不应用于任何目的。
- 为快照复制操作指定的资源级权限可以应用于快照副本和源快照。有关示例，请参阅示例：复制快照。
- 如果复制已启用快速快照还原的快照，则快照副本不会自动启用快速快照还原。您必须为快照副本明确启用快速快照还原。
- 如果将快照复制到新 KMS 密钥并将其加密，则会创建完整（非增量）副本。这会产生额外的存储成本。
- 如果将快照复制到新区域，则会创建完整（非增量）副本。这会产生额外的存储成本。同一快照的后续副本是增量副本。
- 如果您使用外部或跨区域数据传输，则将收取额外EC2 的数据传输费用。如果在启动后删除任何快照，仍需要为已传输的数据付费。

快照副本的目的地

源快照的位置决定了您是否可以复制它。

- 如果源快照位于某个区域中，则可以将其复制到该区域内、另一个区域或一个 Outpost 与该地区相关联。
- 如果源快照位于本地区域中，则无法对其进行复制。

- 如果源快照在 Outpost，你无法复制。

增量快照复制

同一账户和区域内使用相同 KMS 密钥的快照复制操作始终是增量复制。但是，如果您使用不同的 KMS 密钥加密快照副本，则该副本是完整副本。

在跨区域或账户复制快照时，如果满足以下条件，则副本为增量副本：

- 快照以前已复制到目标区域或账户。
- 最新的快照副本仍位于目标区域或账户中。
- 最新的快照副本尚未归档。
- 目标区域或账户中的所有快照副本均未加密，或者是使用同一 KMS 密钥加密的。

> **Tip**
>
> 我们建议您使用卷 ID 和创建时间来标记快照副本，以便在目标区域或账户中跟踪卷的最新快照副本。

要查看您的快照副本是否为增量副本，请查看 CopySn apshot 事件 CloudWatch 。

Amazon EBS 快照和 EBS 支持的基于时间的副本 AMIs

基于时间的副本可以确保在指定的时间范围内在区域内和跨 Amazon 区域复制 EBS 快照和 EBS 支持的 AMIs 副本，从而帮助您满足数据复制的合规性或业务要求。基于时间的副本还可以帮助备份管理员满足严格的灾难恢复要求（恢复点目标和恢复时间目标），并通过确保快照和EB AMIs S支持的复制时间可预测来提高开发灵活性。

使用基于时间的快照和 EBS 支持的 AMI 复制操作，您可以指定完成复制的完成持续时间，介于 15 分钟到 48 小时之间。必须以 15 分钟为增量指定完成持续时间。

主题

- 限额
- 确定您的完成时长
- 注意事项
- 监控

- 定价和计费

限额

以下配额适用于基于时间的快照和 EBS 支持的 AMI 复制操作：

配额	描述	配额值	可调整
快照复制操作吞吐量配额	单次基于时间的快照复制操作可实现的最大吞吐量。 Note 对于 AMI 复制操作，配额适用于与 AMI 关联的每个快照。	500 MiB/s	否
累积快照副本吞吐量配额	源和目标区域之间基于时间的并发快照复制操作可以实现的最大累积吞吐量。 Note 对于 AMI 复制操作，与 AMI 关联的每个快照都计入配额。	2,000 miB/s	是

启动基于时间的快照复制操作时，需要指定完成持续时间。请求使用的吞吐量由快照数据的大小和请求的完成持续时间决定。例如，如果您复制一个包含 225,000 MiB（0.214 TiB）数据的快照，并且您请求的完成持续时间为 15 分钟，则吞吐量为 250）。MiB/s (225,000 MiB ÷ 15 minutes = 250 MiB/s

当您启动基于时间的 AMI 复制操作时，您指定的完成持续时间适用于与 AMI 关联的每个快照。由于每个快照的大小可能不同，因此每个快照都以不同的吞吐量进行复制，以确保在完成时间内复制所有快照。例如，假设您有一个 AMI，其中包含以下关联快照：

- 快照 1：200,000 MiB
- 快照 2：500,000 MiB
- 快照 3：450,000 MiB

如果您为此 AMI 启动基于时间的副本，并将完成持续时间指定为 60 分钟，则该请求将使用以下吞吐量：

- 快照 1：55.56MiB/s (200,000 MiB ÷ 60 minutes = 55.56 MiB/s)
- 快照 2：138.89MiB/s (500,000 MiB ÷ 60 minutes = 138.89 MiB/s)
- 快照 3：125MiB/s (450,000 MiB ÷ 60 minutes = 125 MiB/s)

这意味着该请求使用累积快照副本吞吐量配额的 319.45 MiB/s 来确保复制在 60 分钟内完成。

如果您发起基于时间的快照或 EBS 支持的 AMI 复制请求，并且您的可用累积快照副本吞吐量配额为：

- 大于或等于所需的吞吐速率，则复制将在请求的完成持续时间内完成。
- 小于所需的吞吐率但大于零，则请求成功，但所需的时间将比您请求的要长。使用您的可用吞吐量配额完成复制。
- 零（已达到配额），则请求失败。

确定您的完成时长

对于基于时间的快照或 EBS 支持的 AMI 复制操作，您可以请求的最短完成时间为 15 分钟，您可以请求的最长完成时间为 48 小时。必须以 15 分钟为增量指定完成持续时间。

基于时间的并发快照复制操作

只要所有并发操作的总吞吐量不超过您的累积快照副本吞吐量配额（默认为 2,000 MiB/s），您就可以在同一源区域和目标区域之间执行基于时间的并发快照复制操作。

要确定现有快照能否达到所需的完成时长，请将所有快照的总大小除以所需的完成时长，以确定所需的吞吐量。

> **Tip**
>
> 如果您不知道快照中数据的确切大小，则可以改用完整快照大小作为代理。要获取完整的快照大小，请使用 desc ribe- Amazon CLI snapshots 命令。

```
required throughput rate = combined snapshot size ÷ required completion duration
```

如果所需的吞吐率小于您的累积快照副本吞吐量配额，则可以达到所需的完成持续时间。如果所需的吞吐率大于您的累积快照副本吞吐量配额，我们建议您请求将配额提高到比所需吞吐率至少高 10%。

> **Tip**
>
> Amazon EC2 控制台提供了一个计算器，您可以使用该计算器根据特定的累积快照副本吞吐量配额来检查您在特定时间段内在两个区域之间复制了多少快照数据，以及针对该数据量可以实现的最短完成时间。计算器使用该SnapshotCopyBytesTransferred CloudWatch 指标来计算一段时间内在两个区域之间复制的数据。要打开计算器，请在 Amazon EC2 控制台导航面板中选择 “快照”，然后选择 “操作”、“启动复制时长计算器”。

单个基于时间的快照复制操作

您可以通过将快照数据大小除以快照复制操作吞吐量配额 (500 MiB/s) 来计算单个基于时间的快照复制操作的最小完成持续时间。

> **Tip**
>
> 如果您不知道快照中数据的确切大小，则可以改用完整快照大小作为代理。要获取完整的快照大小，请使用 desc ribe- Amazon CLI snapshots 命令。

```
minimum completion duration = Max(15 minutes, (snapshot data size ÷ 500 MiB/s)
```

例如，包含 900,000 MiB 数据的快照的最短完成时间为 30 分钟。

```
minimum completion duration = Max(15 minutes, (900,000 MiB ÷ 500 MiB/s)
```

```
= Max(15 minutes, 30 minutes)
= 30 minutes
```

基于时间的 AMI 复制操作

当您为具有单个关联快照的 EBS 支持的 AMI 启动基于时间的 AMI 复制操作时，其行为方式将与单个基于时间的快照复制操作相同，并且具有相同的吞吐量限制。

当您为具有多个关联快照的 EBS 支持的 AMI 启动基于时间的 AMI 复制操作时，其行为方式与基于时间的并发快照复制操作相同，并且适用相同的吞吐量限制。每个关联的快照都会导致一个单独的快照复制请求，并且每个请求都会占用您的累积快照复制吞吐量配额。您指定的完成期限将应用于每个关联的快照。

注意事项

- 在同一区域内复制快照或跨区域复制快照时，您可以启动基于时间的快照和 EBS 支持的 AMI 复制操作。
- 如果您为同一个快照或 AMI 启动了两个基于时间的复制操作，则第二个复制操作的完成持续时间仅在第一个复制操作完成后开始。
- Local Zones 和 Wavelength Zones 不支持基于时间的复制操作。 Amazon Outposts

监控

您可以使用 A EC2 mazon 控制台和，监控基于时间的快照和 EBS 支持的 AMI 复制操作的进度。Amazon CLI在控制台中，选择快照，然后在详细信息选项卡中检查进度字段。使用 Amazon CLI，检查 desc ribe-snapshots 命令响应中的`Progress`输出元素。

您可以通过检查控制台或响应中的 “已启动” 和 “已完成” 时间之间的差异，来检查基于时间的快照**`StartTime`**或 **`CompletionTime`** EBS 支持的 AMI 复制操作是否在请求的完成时间内完成。`describe-snapshots`

您还可以使用 `copySnapshot` Amazon EventBridge 事件来监控基于时间的复制操作的结果。该事件表示操作是否已完成以及是否满足了请求的完成持续时间。如果未达到完成持续时间，则该事件将包含有关原因的更多信息。有关更多信息，请参阅 EBS 快照事件。

定价和计费

> **Note**
>
> 与标准快照复制操作类似，如果您将快照复制到新区域，则会创建完整（非增量）副本，这会导致额外的存储成本。同一快照的后续副本是增量副本。此外，如果您使用外部或跨区域数据传输，则将收取额外的 Amazon EC2 数据传输费用。

基于时间的快照和 EBS 支持的 AMI 复制操作需要支付额外费用。基于时间的复制操作按每复制的 GiB 快照数据按请求的完成时长收费。固定利率如下：

> **Note**
>
> 必须以 15 分钟为增量指定完成持续时间。最短完成时间为 15 分钟，最长为 48 小时。

- 15 分钟 — 每 GiB 数据 0.14036 元人民币
- 30 分钟 45 分钟 — 每 GiB 数据 0.12633 元人民币
- 1 小时到 1 小时 45 分钟 — 每 GiB 数据 0.11229 元人民币
- 2 小时到 3 小时 45 分钟 — 每 GiB 数据 0.09825 元人民币
- 4 小时到 7 小时 45 分钟 — 每 GiB 数据 0.08422 元人民币
- 8 小时到 15 小时 45 分钟 — 每 GiB 数据 0.07018 元人民币
- 16 小时或更长时间 — 每 GiB 数据 0.03509 元人民币

例如，如果您复制一个包含 3,000 GiB 数据的快照，完成时间为 8 小时，则需要支付 210.54 元人民币（0.07018 元人民币 x 3,000 GiB）的费用。

如果您启动了基于时间的复制操作，但由于超出配额而无法满足请求的完成持续时间，则系统将根据实际完成持续时间而不是请求的完成持续时间向您计费。例如，如果您请求的完成持续时间为 1 小时，但操作在 2 小时后完成，则将按照 2 小时完成时长的费率进行计费。

如果 Amazon EBS 无法达到所请求的完成时长，或者由于服务端问题而取消了请求，则不会向您收取基于时间的快照复制操作的额外费用。

如果您在基于时间的快照复制操作仍在进行时删除快照副本，则按与指定完成时长对应的速率对应于该时间点的复制数据计费。

加密和快照复制

> **Note**
>
> Amazon S3 服务器端加密（256 位 AES）可在复制操作期间保护传输中的快照数据。

您可以创建未加密的源快照的已加密快照副本。并且，您可以使用与源快照不同的 KMS 密钥加密快照副本。但是，在复制操作过程中更改快照副本的加密状态可能会生成完整（非增量）副本，这可能产生更多的数据传输和存储费用。

> **Tip**
>
> 使用与您共享的已加密快照时，我们建议您通过复制快照并使用您拥有的 KMS 密钥来重新加密该快照。如果原始 KMS 密钥泄露或拥有者撤销您的访问权限（可能会导致您无法访问快照以及从中创建的任何加密卷），这可以保护您。

复制加密快照的权限

要复制加密快照，您的用户必须具有以下权限才能使用 Amazon EBS 加密。

- • `kms:DescribeKey`
  - `kms:CreateGrant`
  - `kms:GenerateDataKey`
  - `kms:GenerateDataKeyWithoutPlaintext`
  - `kms:ReEncrypt`
  - `kms:Decrypt`
- 要复制从其他 Amazon 账户共享的加密快照，您必须有权使用用于加密该快照的客户托管密钥。有关更多信息，请参阅 共享用于加密共享的 Amazon EBS 快照的 KMS 密钥。

快照副本的加密结果

下表描述了在复制您拥有的快照以及与您共享的快照时的加密结果。

目标区域的默认加密	源快照	快照副本加密结果	注意
已禁用	未加密	可选加密	如果加密副本，则可以指定要使用的 KMS 密钥。如果您加密副本但未指定 KMS 密钥，则使用 Amazon 托管式密钥 (aws/ebs)。
已禁用	已加密	自动加密	您可以指定要使用的 KMS 密钥。如果未指定 KMS 密钥，则使用 Amazon 托管式密钥（aws/ebs）。
已启用	未加密	自动加密	您可以指定要使用的 KMS 密钥。如果未指定 KMS 密钥，则默认使用指定用于加密的密钥。
已启用	已加密	自动加密	您可以指定要使用的 KMS 密钥。如果未指定 KMS 密钥，则默认使用指定用于加密的密钥。

复制快照

您可以将快照从一个区域复制到另一个区域。您可以将未加密的快照复制到加密的快照。但是，如果您在无权使用加密密钥的情况下尝试复制加密快照，则操作会以静默方式失败，并且快照副本会收到 “给定密钥 ID 不可访问” 的状态消息。

Console

复制快照

1. 打开亚马逊 EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择快照。
3. 选择要复制的快照，然后选择 Actions（操作）、Copy snapshot（复制快照）。
4. （可选）在 Description （描述）中，输入快照副本的简短描述。

   在默认情况下，描述包括源快照的相关信息，以便您能区别副本和原始内容。
5. 指定快照副本的目标。

   - 要将快照复制到同一区域或其他区域，请选择Amazon 区域，然后选择目标区域。

- (Outpost 仅限客户）将快照复制到 Outpost，选择 Amazon Outpost然后输入目的地的 ARN Outpost.

6. 如果您需要在特定时间范围内完成快照复制，请选择 “启用基于时间的复制”。在完成期限中，以 15 分钟为增量输入所需的完成期限。有关更多信息，请参阅 Amazon EBS 快照和 EBS 支持的基于时间的副本 AMIs。

   如果您不需要在特定的时间范围内完成快照副本，请不要启用基于时间的复制。在这种情况下，快照复制会尽快完成。

7. (Outpost 仅限客户）在上创建快照副本 Outpost 在所选区域中，为快照目标选择 Amazon Outpost，然后是目的地 Outpost ARN，输入 ARN 的 ARN Outpost 将快照复制到其中。只有当你有并时，才会显示快照目标字段 Outpost 在所选区域中。

8. 指定快照副本的加密状态。

   如果源快照已加密，或者您的账户已启用默认加密，则快照副本会自动加密。如果源快照未加密，并且在默认情况下未为您的账户启用加密，则您可以选择启用或禁用加密。

9. 选择复制快照。

Amazon CLI

将快照复制到另一个区域

使用 copy-snapshot 命令。以下示例将指定的快照从源区域复制到当前区域，该区域由--region选项指定。

```
aws ec2 copy-snapshot \
    --source-snapshot-id snap-0abcdef1234567890 \
    --source-region us-east-1 \
    --region us-west-2
```

将未加密的快照复制到加密的快照

使用 copy-snapshot 命令。以下示例将指定的未加密快照从源区域复制到当前区域，使用指定的 KMS 密钥对新快照进行加密。

```
aws ec2 copy-snapshot \
    --source-snapshot-id snap-0abcdef1234567890 \
    --source-region us-east-1 \
    --encrypted \
```

```
    --kms-key-id alias/my-kms-key
```

PowerShell

将快照复制到另一个区域

使用 Copy-EC2Snapshot cmdlet。以下示例将指定的快照从源区域复制到当前区域，该区域由--region选项指定。

```
Copy-EC2Snapshot `
    -SourceSnapshotId snap-0abcdef1234567890 `
    -SourceRegion us-east-1 `
    -Region us-west-2
```

将未加密的快照复制到加密的快照

使用 Copy-EC2Snapshot cmdlet。以下示例将指定的未加密快照从源区域复制到当前区域，使用指定的 KMS 密钥对新快照进行加密。

```
Copy-EC2Snapshot `
    -SourceSnapshotId snap-0abcdef1234567890 `
    -SourceRegion us-east-1 `
    -Encrypted $true `
    -KmsKeyId alias/my-kms-key
```

与其他账户共享 Amazon EBS 快照 Amazon

如果您想与其他 Amazon 账户共享快照，可以修改快照的权限。您可以与所有其他 Amazon 账户公开共享快照，也可以与您指定的个人 Amazon 账户私下共享快照。您已授权的用户可以使用您共享的快照来创建自己的 EBS 卷，同时您的原始快照不受影响。

> **Important**
>
> 共享快照时，您可以让其他人访问快照上的所有数据。仅与您信任的人共享所有快照数据的快照。

要防止公开共享快照，您可以启用 阻止 Amazon EBS 快照的公开访问。

主题

- 共享快照之前
- 共享快照
- 共享用于加密共享的 Amazon EBS 快照的 KMS 密钥
- 使用与您共享的 Amazon EBS 快照
- 确定共享快照的用途

共享快照之前

共享快照时需考虑以下事项：

- 如果为此区域阻止公开访问快照，将阻止尝试公开共享快照的行为。仍然可以私下共享快照。
- 快照受限于在其中创建它们的区域。要与其他区域共享快照，请将快照复制到该区域，然后分享副本。有关更多信息，请参阅 复制 Amazon EBS 快照。
- 您无法共享使用默认 Amazon 托管式密钥加密的快照。您只能共享使用客户托管密钥加密的快照。有关更多信息，请参阅 Amazon Key Management Service 开发人员指南中的创建密钥。
- 您只能公开共享未加密的快照。
- 共享加密快照时，还必须共享用于加密快照的客户托管密钥。有关更多信息，请参阅共享用于加密共享的 Amazon EBS 快照的 KMS 密钥。

共享快照

您可以公开共享快照，也可以与特定 Amazon 账户共享快照。

Console

共享快照

1. 打开亚马逊 EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择快照。
3. 选择快照，然后依次选择 Actions（操作）、Modify Permissions（修改权限）。
4. 请指定快照的权限。Current setting（当前设置）表示快照的当前共享权限。
   - 要与所有 Amazon 账户公开共享快照，请选择公开。
   - 要与特定 Amazon 账户私下共享快照，请选择 “私人”。然后，在共享账户部分中，选择添加账户，接着输入要与之共享的账户的 12 位账户 ID（不带连字符）。

5. 选择保存更改。

Amazon CLI

使用快照的 `createVolumePermission` 属性指定快照的权限。要使快照公开可用，请将组设置为 `all`。要与特定 Amazon 账户共享快照，请将用户设置为该 Amazon 账户的 ID。

公开共享快照

使用 modify-snapshot-attribute 命令。

对于 `--attribute`，请指定 `createVolumePermission`。对于 `--operation-type`，请指定 `add`。对于 `--group-names`，请指定 `all`。

```
aws ec2 modify-snapshot-attribute \
    --snapshot-id snap-0abcdef1234567890 \
    --attribute createVolumePermission \
    --operation-type add \
    --group-names all
```

私密共享快照

使用 modify-snapshot-attribute 命令。

对于 `--attribute`，请指定 `createVolumePermission`。对于 `--operation-type`，请指定 `add`。对于`--user-ids`，请指定要与 IDs 之共享快照的 Amazon 账户的 12 位数。

```
aws ec2 modify-snapshot-attribute \
    --snapshot-id snap-0abcdef1234567890 \
    --attribute createVolumePermission \
    --operation-type add \
    --user-ids 123456789012 111122223333
```

PowerShell

使用快照的 `createVolumePermission` 属性指定快照的权限。要使快照公开可用，请将组设置为 `all`。要与特定 Amazon 账户共享快照，请将用户设置为该 Amazon 账户的 ID。

公开共享快照

使用 Edit-EC2SnapshotAttribute cmdlet。

对于 -Attribute，请指定 CreateVolumePermission。对于 -OperationType，请指定 Add。对于 -GroupName，请指定 all。

```
Edit-EC2SnapshotAttribute `
    -SnapshotId snap-0abcdef1234567890 `
    -Attribute CreateVolumePermission `
    -OperationType Add `
    -GroupName all
```

私密共享快照

使用 Edit-EC2SnapshotAttribute cmdlet。

对于 -Attribute，请指定 CreateVolumePermission。对于 -OperationType，请指定 Add。对于UserId，请指定要与 IDs 之共享快照的 Amazon 账户的 12 位数。

```
Edit-EC2SnapshotAttribute `
    -SnapshotId snap-0abcdef1234567890 `
    -Attribute CreateVolumePermission `
    -OperationType Add `
    -UserId 123456789012 111122223333
```

共享用于加密共享的 Amazon EBS 快照的 KMS 密钥

共享加密快照时，还必须共享用于加密快照的客户托管密钥。您可以在创建客户托管密钥时或以后的某个时间向客户托管密钥应用跨账户权限。

必须为正在访问加密快照的共享客户托管密钥用户授予对密钥执行以下操作的权限：

- kms:DescribeKey
- kms:CreateGrant
- kms:GenerateDataKey
- kms:GenerateDataKeyWithoutPlaintext
- kms:ReEncrypt
- kms:Decrypt

> **Tip**
>
> 为遵循最小特权原则，请不要允许对 `kms:CreateGrant` 拥有完全访问权限。相反，使用`kms:GrantIsForAWSResource`条件密钥允许用户仅在 Amazon 服务代表用户创建授权时才允许用户在 KMS 密钥上创建授权。

有关如何控制对客户托管密钥的访问权限的更多信息，请参阅 Amazon Key Management Service 开发人员指南中的使用 Amazon KMS中的密钥策略。

使用 Amazon KMS 控制台共享客户托管密钥

1. 在 https://console.aws.amazon.com/km Amazon KMS s 处打开控制台。
2. 要更改 Amazon Web Services 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择客户托管密钥。
4. 在别名列中，选择用于加密快照的客户托管密钥的别名（文本链接）。密钥详细信息将在新页面中打开。
5. 在密钥政策部分中，您会看到政策视图或默认视图。策略视图显示密钥策略文档。默认视图显示密钥管理员、密钥删除、密钥使用和其他 Amazon 账户几个部分。如果您在控制台中创建了策略，但尚未对其进行自定义，则会显示默认视图。如果默认视图不可用，则需要在策略视图中手动编辑策略。有关更多信息，请参阅 Amazon Key Management Service 开发人员指南中的查看密钥策略（控制台）。

   根据您可以访问的视图，使用策略视图或默认视图向策略中添加一个或多个 Amazon 账户 IDs ，如下所示：

   - （策略视图）选择编辑。在以下 IDs 对 Amazon 账单中添加一个或多个账户："Allow use of the key"和"Allow attachment of persistent resources"。选择保存更改。在以下示例中， Amazon 账户 ID 444455556666 已添加到策略中。

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {"AWS": [
    "arn:aws:iam::111122223333:user/KeyUser",
    "arn:aws:iam::444455556666:root"
  ]},
  "Action": [
    "kms:Encrypt",
```

```
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*"
},
{
  "Sid": "Allow attachment of persistent resources",
  "Effect": "Allow",
  "Principal": {"AWS": [
    "arn:aws:iam::111122223333:user/KeyUser",
    "arn:aws:iam::444455556666:root"
  ]},
  "Action": [
    "kms:CreateGrant",
    "kms:ListGrants",
    "kms:RevokeGrant"
  ],
  "Resource": "*",
  "Condition": {"Bool": {"kms:GrantIsForAWSResource": true}}
}
```

- （默认视图）向下滚动到“其他 Amazon 账户”。选择“添加其他 Amazon 账户”，然后根据提示输入 Amazon 账户 ID。要添加其他账户，请选择添加其他 Amazon 账户并输入 Amazon 账户 ID。添加完所有 Amazon 账户后，选择 Save changes（保存更改）。

使用与您共享的 Amazon EBS 快照

使用共享的未加密快照

按 ID 或描述查找共享快照。您可以像使用账户中拥有的任何其他快照一样使用此快照。例如，您可以从快照中创建卷或将卷复制到其他区域。

使用共享的已加密快照

按 ID 或描述查找共享快照。在您的账户中创建共享快照的副本，并使用您拥有的 KMS 密钥对副本进行加密。然后，您可以使用副本创建卷，也可以将其复制到不同的区域。

Console

查看快照权限

1. 打开亚马逊 EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择快照。
3. 选择快照。
4. 如果筛选条件为 “我所有”，则快照归该账户所有。如果筛选条件为 “私有快照”，则快照要么归该账户所有，要么专门与该账户共享。选择一个快照，然后在详细信息选项卡上，检查所有者是指定了此帐户还是其他帐户。

Amazon CLI

查看快照权限

使用describe-snapshot-attribute命令获取指定快照的快照权限。

```
aws ec2 describe-snapshot-attribute \
    --snapshot-id snap-0abcdef1234567890 \
    --attribute createVolumePermission
```

下面是示例输出。

```
{
    "SnapshotId": "snap-0abcdef1234567890",
    "CreateVolumePermissions": [
        {
            "UserId": "111122223333"
        }
    ]
}
```

PowerShell

查看快照权限

使用 Get-EC2SnapshotAttribute cmdlet。

```
(Get-EC2SnapshotAttribute `
```

```
    -SnapshotId snap-0abcdef1234567890 `
    -Attribute createVolumePermission).CreateVolumePermissions
```

下面是示例输出。

```
Group UserId
----- ------
      111122223333
```

确定共享快照的用途

您可以使用 Amazon CloudTrail 来监控您与他人共享的快照是否被复制或用于创建卷。对您共享的快照执行操作 CloudTrail 时，会记录以下事件：

- SharedSnapshotCopyInitiated— 正在复制共享快照。
- SharedSnapshotVolumeCreated— 正在使用共享快照来创建卷。

有关使用的更多信息 CloudTrail，请参阅使用记录亚马逊 EC2 和亚马逊 EBS API 调用 Amazon CloudTrail。

归档 Amazon EBS 快照

Amazon EBS 快照归档是一个存储层，可用于长期低成本地存储很少访问且不需要频繁或快速检索的快照。

默认情况下，快照在创建时将存储在 Amazon EBS 快照标准层中（标准层）。存储在标准层中的快照可递增。这意味着只在卷上保存在最新快照之后发生更改的数据块。

归档快照时，增量快照将转换为完整快照，然后从标准层移动到 Amazon EBS 快照归档层（归档层）。完整快照包括创建快照时写入卷的所有数据块。

当您需要访问归档的快照时，可以将其从归档层还原到标准层，然后像使用账户中任何其它快照一样使用它。

Amazon EBS 快照归档为您存储极少需要访问的快照达 90 天或更长时间，同时存储成本降低 75%。

一些典型的使用案例包括：

- 存档卷的唯一快照，例如 end-of-project快照

- 出于合规性考虑，存档完整的 point-in-time增量快照。
- 归档月度、季度或每年的增量快照。

主题

- 限额
- 归档 Amazon EBS 快照的注意事项和限制
- 归档 Amazon EBS 快照的定价和计费
- 归档 Amazon EBS 快照的准则和最佳实践
- 归档 Amazon EBS 快照所需的 IAM 权限
- 归档 Amazon EBS 快照
- 还原已归档的 Amazon EBS 快照
- 修改临时还原的 Amazon EBS 快照的还原期
- 查看已归档的 Amazon EBS 快照
- 使用 CloudWatch 事件监控 Amazon EBS 快照存档

限额

本部分介绍了归档快照和正在进行的快照的默认配额。

配额	默认配额			
每卷的已归档快照	25			
每个账户的正在并发进行的快照归档	25			
每个账户的正	5			

配额	默认配额			
在并发进行的快照还原				

如果您需要的数量超过默认限制，请填写 Cent Amazon Web Services 支持 er C reate cas e 表单以申请提高限额。

归档 Amazon EBS 快照的注意事项和限制

归档 Amazon EBS 快照时请记住以下事项。

注意事项

- 最短归档期为 90 天。如果您在最短 90 天的归档期限到来之前删除或永久还原已归档的快照，则需要为归档层的剩余天数付费（四舍五入到最接近的小时数）。有关更多信息，请参阅 归档 Amazon EBS 快照的定价和计费。
- 将归档快照从归档层还原到标准层最长可能需要 72 小时，具体时间取决于快照的大小。
- 归档的快照始终是完整的快照。完整快照包含创建快照时写入卷的所有块。完整快照可能会大于它赖以创建的增量快照。但是，如果您在标准层上只有一个卷的快照，则存档层中完整快照的大小将与标准层中的快照大小相同。这是因为卷的第一个快照始终是完整快照。要获取完整的快照大小，请使用 desc ribe- Amazon CLI snapshots 命令。
- 建议将月度、季度或每年快照存档。与将单个卷的每日增量快照保存在标准层中相比，将单个卷的每日增量快照存档可能会导致成本增加。
- 在归档快照时，快照谱系中其它快照引用的快照数据将保留在标准层中。与保留在标准层中的引用数据相关的数据和存储成本将分配给谱系中的下一个快照。这可以确保谱系中的后续快照不会受到归档的影响。
- 如果删除与回收站保留规则匹配的归档快照，则归档的快照将在保留规则定义的保留期内保留在回收站中。要使用快照，您必须首先从回收站中恢复快照，然后从归档层中还原它。有关更多信息，请参阅回收站和归档 Amazon EBS 快照的定价和计费。
- 您不能在块设备映射中使用已归档快照或创建 Amazon EBS 卷。
- 您可以存档 Amazon Backup 使用 Amazon Backup 控制台 APIs、或命令行工具创建的快照。有关更多信息，请参阅《Amazon Backup 开发人员指南》中的制定备份计划。

限制

- 您只能归档状态为 `completed` 状态的快照。
- 您只能归档您在账户中拥有的快照。要归档与您共享的快照，首先将快照复制到您的账户，然后将快照副本归档。
- 在使用归档快照之前，必须先将其还原到标准层。要通过 `CreateVolume` 和 `RunInstances` API 操作从快照创建卷，以及共享或复制快照，都需要恢复到标准层。有关更多信息，请参阅 还原已归档的 Amazon EBS 快照。
- AMIs 只有禁用了所有关联的快照，您才能存档与一个或多个关联 AMIs 的快照。有关更多信息，请参阅禁用 AMI。
- 如果关联的快照已暂时恢复，则无法启用已禁用的 AMI。在启用 AMI 之前，必须永久恢复所有关联的快照。
- 在快照归档或快照还原过程启动后，您无法取消它。
- 您不能共享已归档的快照。如果归档了与其它账户共享的快照，则在归档快照后，与之共享快照的账户将失去访问权限。
- 您不能复制已归档的快照。如果需要复制归档的快照，则必须首先将其还原。
- 您不能为归档快照启用快速快照还原。快照归档后，快速快照还原会自动禁用。如果您需要使用快速快照还原，则必须在还原快照后手动启用该选项。

归档 Amazon EBS 快照的定价和计费

归档的快照按每 GB 每月 0.0125 美元的费率计费。例如，如果您归档 100GiB 快照，则每月需支付 1.25 美元（100GiB x 0.0125 美元）的费用。

快照还原的费率为每 GB 还原数据收费 0.03 美元。例如，如果您从归档层还原 100GiB 快照，则需要一次向您收取费用 3 美元（100GiB x 0.03 美元）。

快照还原到标准层后，快照按每 GB 每月 0.05 美元的标准费率计费。

有关更多信息，请参阅 Amazon EBS 定价。

按最短归档期收费

最短归档期为 90 天。如果您在最短 90 天的归档期限之前删除或永久还原归档的快照，则按比例收取的费用等于剩余天数的归档层存储费用（四舍五入到最接近的小时数）。例如，如果在 40 天之后删除或永久恢复归档快照，则将收取剩余 50 归天的最小存档期的费用。

> **Note**
>
> 在最短 90 天的归档期限之前暂时还原已归档的快照，不会产生此费用。

临时还原

当您临时还原快照时，快照将从归档层还原到标准层，并且快照的副本将保留在归档层中。在临时还原期间，您需要为标准层中的快照和归档层中的快照副本付费。从标准层中删除临时还原的快照时，您不再需要为其付费，而只需为归档层中的快照付费。

永久还原

当您永久还原快照时，快照将从归档层还原到标准层，并且快照将从归档层删除。您仅需为标准层中的快照付费。

删除快照

如果在归档快照时删除快照，则需要为已移动到归档层的快照数据付费。数据最短归档期限为 90 天，并要在删除时支付相应的费用。例如，如果您归档了 100GiB 快照，并且在仅归档 40GiB 之后删除快照，则对于已归档的 40GiB 而言，您需要支付最少 90 天的归档期费用 1.50 美元（每 GB 每月费率 0.0125 美元 * 40GB *（90 天 * 24 小时）/（24 小时/天 * 每月 30 天））。

如果在从归档层还原快照时删除快照，您需要为快照的完整大小（快照大小 x 0.03 美元）支付快照还原费用。例如，如果您从归档层还原 100GiB 快照，并且在快照还原完成之前的任何时候删除快照，则需支付 3 美元（100GiB 快照大小 x 0.03 美元）的费用。

回收站

归档的快照在回收站中时，按归档快照的费率计费。回收站中的归档快照的最短归档期限为 90 天，如果在最短归档期限到来之前被回收站删除，则会产生相应费用。换句话说，如果按照某保留规则，在最短期限 90 天之前从回收站中删除了归档的快照，则需要为剩余天数付费。

如果删除与回收站保留规则匹配的归档快照，则归档的快照将在保留规则定义的保留期内保留在回收站中。它会按归档快照的费率计费。

如果在还原快照时删除与保留规则匹配的快照，则还原的快照将在保留期剩余时间内保留在回收站中，并按标准快照费率计费。要使用快照，您必须首先从回收站中恢复快照。

有关更多信息，请参阅回收站。

成本跟踪

存档的快照 Amazon 成本和使用情况报告 以相同的资源 ID 和 Amazon 资源名称 (ARN) 出现在中。有关更多信息，请参阅 Amazon 成本和使用情况报告 《用户指南》。

您可以使用以下使用类型来确定相关成本：

- SnapshotArchiveStorage – 月度数据存储费
- SnapshotArchiveRetrieval – 快照还原的一次性费用
- SnapshotArchiveEarlyDelete – 在最短归档期限（90 天）之前删除或永久还原快照的费用

归档 Amazon EBS 快照的准则和最佳实践

本部分提供了归档快照的准则和最佳做法。

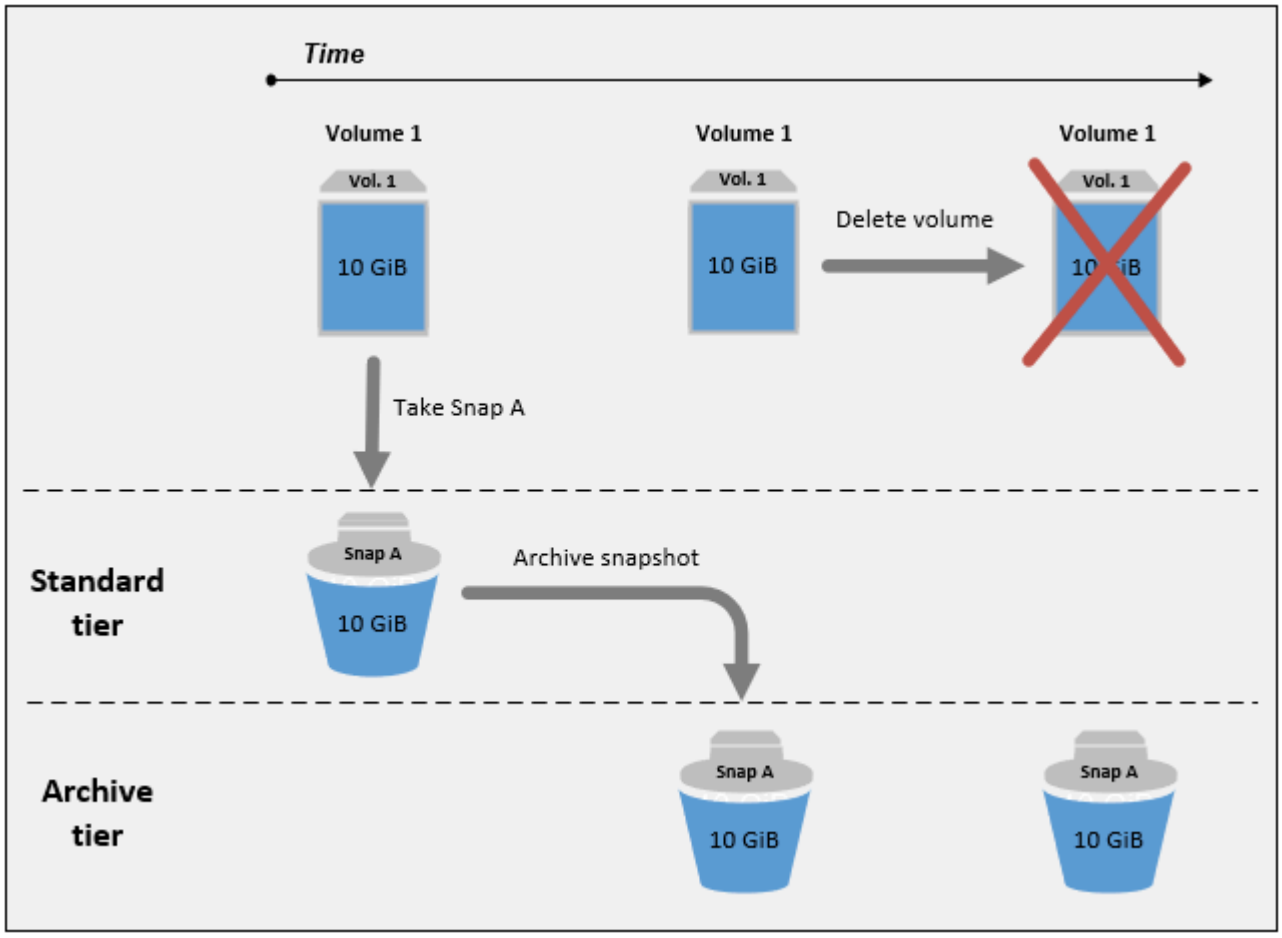
主题

- 归档卷的唯一快照
- 归档单个卷的增量快照
- 出于合规性原因归档完整快照
- 确定标准层存储成本的减少程度

归档卷的唯一快照

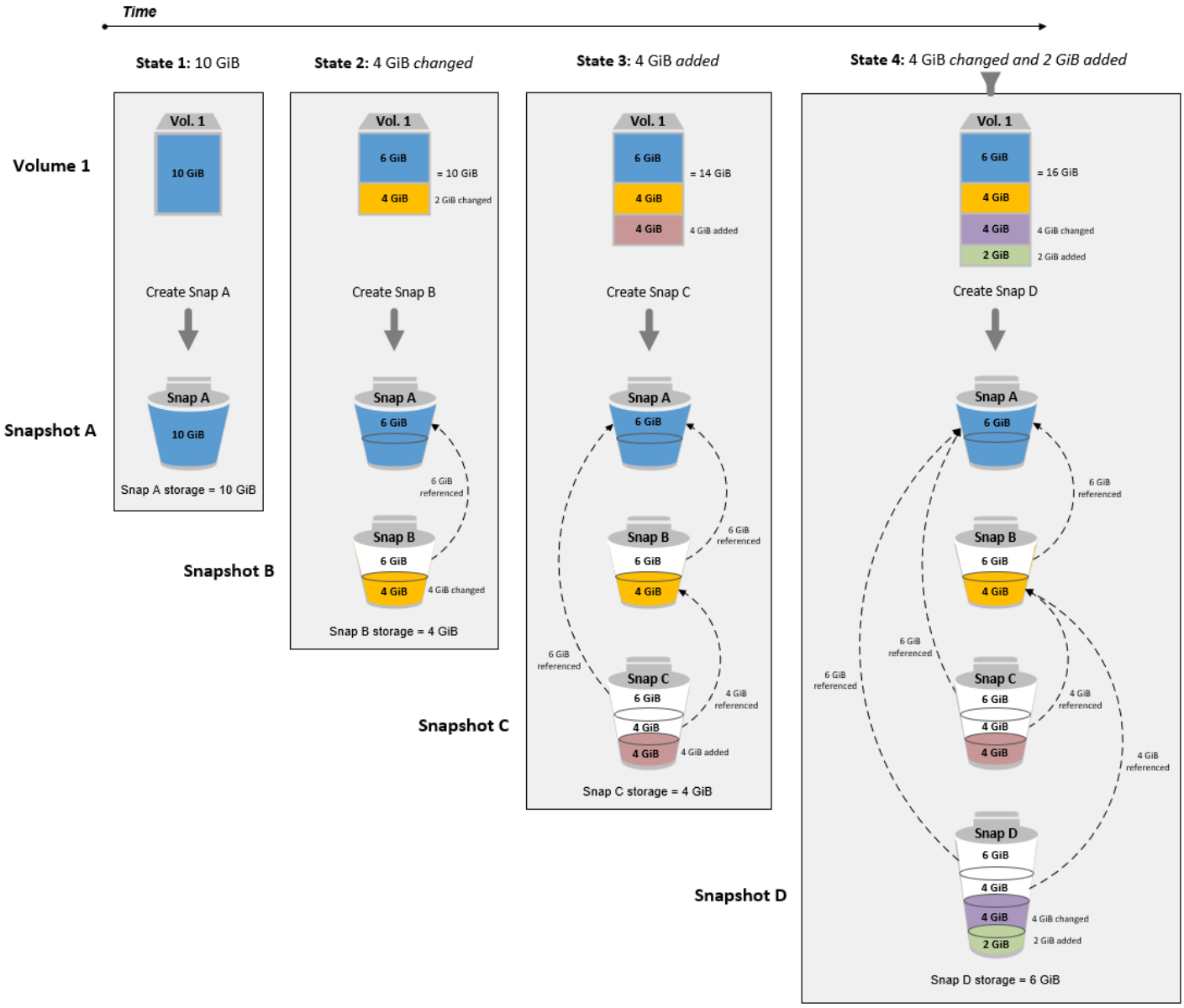
如果只存在卷的一个快照，则快照的大小始终与创建快照时写入卷的块的大小相同。归档此类快照时，标准层中的快照将转换为同等大小的完整快照，然后从标准层移动到归档层。

归档这些快照可以帮助您以更低的存储成本节省开支。如果不再需要源卷，则可以删除该卷以进一步节省存储成本。



归档单个卷的增量快照

归档增量快照时，增量快照将转换为完整快照，然后从标准层移动到归档层。例如，在下图中，如果您归档快照 B，快照将转换为大小为 10GiB 的完整快照并移动到归档层。同样，如果您归档快照 C，归档层中的完整快照大小为 14GiB。



如果要归档快照以降低标准层中的存储成本，您不应归档一组增量快照中的第一个快照。快照谱系中的后续快照引用了这些快照。在大多数情况下，归档这些快照不会降低存储成本。

> **Note**
>
> 您不应归档一组增量快照中的最后一个快照。最后一个快照是卷的最新快照。如果要在卷损坏或丢失的情况下从快照中创建卷，则需要在标准层中使用此快照。

如果归档了一个快照，而该快照包含了谱系中后续快照所引用的数据，那么与所引用数据关联的数据存储和存储成本将分配给后续快照。在这种情况下，归档这些快照不会降低数据存储成本。例如，在上一张图片中，如果归档快照 B，它的 4GiB 的数据相当于由快照 C 产生。在这种情况下，总体存储成本将增加，因为您需要为归档层的快照 B 完整版付费，而标准层的存储成本保持不变。

如果归档快照 C，标准层存储将减少 4GiB，因为该数据未被谱系中任何其它后续快照引用。而且，由于快照已转换为完整快照，您的归档层存储将增加 14GiB。

出于合规性原因归档完整快照

出于合规性考虑，您可能需要每月、每季度或每年创建卷的完整备份。对于这些备份，您可能需要独立快照而不向后或向前引用快照谱系中的其它快照。使用 EBS 快照归档功能归档的快照是完整快照，它们没有引用谱系中的其它快照。此外，为了遵循合规性要求，您可能需要保留这些快照数年。EBS 快照归档使归档这些完整快照以长期保留具备良好的成本效益。

确定标准层存储成本的减少程度

如果要归档增量快照以降低存储成本，您应考虑归档层中完整快照的大小和标准层存储空间减少的程度。本部分介绍如何进行设置。

> **Important**
>
> API 响应在被调用 point-in-time时的数据准确 APIs 无误。由于与快照相关的数据随着快照谱系的变化而发生变化，API 响应可能会有所不同。

要确定标准层存储空间和存储成本的降低，请使用以下步骤。

1. 对于要存档的快照，请检查快照的完整大小和创建快照的源卷。使用 d escribe- snapshots 命令--snapshot-id，为此，指定要存档的快照的 ID。

   ```
   $ aws ec2 describe-snapshots --snapshot-id snapshot_id
   ```

   FullSnapshotSizeInBytes响应值表示快照的完整大小（以字节为单位），VolumeId响应值表示源卷的 ID。

   例如，以下命令返回有关快照 snap-09c9114207084f0d9 的信息。

   ```
   $ aws ec2 describe-snapshots --snapshot-id snap-09c9114207084f0d9
   ```

以下示例输出显示完整快照大小为5678912341字节 (5.28 GiB)，源卷为。vol-0f3e2c292c52b85c3

```
{
    "Snapshots": [
        {
            "Description": "",
            "Tags": [],
            "Encrypted": false,
            "VolumeId": "vol-0f3e2c292c52b85c3",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2021-11-16T08:29:49.840Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "FullSnapshotSizeInBytes" : "5678912341",
            "SnapshotId": "snap-09c9114207084f0d9"
        }
    ]
}
```

2. 查找通过该源卷创建的所有快照。可以使用 describe-hosts 命令。请指定 volume-id 筛选条件，并指定在上一步中得到的卷 ID 作为筛选条件值。

```
$ aws ec2 describe-snapshots --filters "Name=volume-id, Values=volume_id"
```

例如，以下命令返回创建自卷的所有快照 vol-0f3e2c292c52b85c3。

```
$ aws ec2 describe-snapshots --filters "Name=volume-id,
 Values=vol-0f3e2c292c52b85c3"
```

以下是命令输出，表示三个快照通过卷创建 vol-0f3e2c292c52b85c3。

```
{
    "Snapshots": [
        {
            "Description": "",
            "Tags": [],
            "Encrypted": false,
            "VolumeId": "vol-0f3e2c292c52b85c3",
```

```
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2021-11-14T08:57:39.300Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-08ca60083f86816b0"
        },
        {
            "Description": "",
            "Tags": [],
            "Encrypted": false,
            "VolumeId": "vol-0f3e2c292c52b85c3",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2021-11-15T08:29:49.840Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-09c9114207084f0d9"
        },
        {
            "Description": "01",
            "Tags": [],
            "Encrypted": false,
            "VolumeId": "vol-0f3e2c292c52b85c3",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2021-11-16T07:50:08.042Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-024f49fe8dd853fa8"
        }
    ]
}
```

3. 使用上一个命令的输出，按快照的创建时间（从最旧到最新）对快照进行排序。每个快照的响应参数 StartTime 表示其创建时间（UTC 时间格式）。

   例如，上一步中返回的快照按创建时间（从最旧到最新）排列如下：

   1. snap-08ca60083f86816b0（最旧 — 在要存档的快照之前创建）
   2. snap-09c9114207084f0d9（要归档的快照）
   3. snap-024f49fe8dd853fa8（最新 – 紧接着需归档的快照之后创建）

4. 确定在需归档快照产生之前和之后紧邻着创建的快照。在这种情况下，您要归档快照 snap-09c9114207084f0d9，这是在三个快照集中创建的第二个增量快照。快照 snap-08ca60083f86816b0 正好在其之前创建，而快照 snap-024f49fe8dd853fa8 紧接其后创建。

5. 在需归档的快照中找到未引用的数据。首先，找出需归档快照以及正好在其之前创建的快照之间不同的数据块。使用 list-changed-blocks 命令。对于 --first-snapshot-id，请指定正好在需归档快照之前创建的快照 ID。对于 --second-snapshot-id，请指定需归档快照 ID。

```
$ aws ebs list-changed-blocks --first-snapshot-id snapshot_created_before --second-
snapshot-id snapshot_to_archive
```

例如，以下命令显示了以下两个快照之间不同数据块的块索引：快照 snap-08ca60083f86816b0（正好在需归档快照之前创建的快照），以及快照 snap-09c9114207084f0d9（需归档快照）。

```
$ aws ebs list-changed-blocks --first-snapshot-id snap-08ca60083f86816b0 --second-
snapshot-id snap-09c9114207084f0d9
```

下面显示了命令输出，其中省略了一些数据块。

```
{
    "BlockSize": 524288,
    "ChangedBlocks": [
        {
            "FirstBlockToken": "ABgBAX6y
+WH6Rm9y5zq1VyeTCmEzGmTT0jNZG1cDirFq1rOVeFbWXsH3W4z/",
            "SecondBlockToken": "ABgBASyx0bHHBnTERu
+9USLxYK/81UT0dbHIUFqUjQUkwTwK5qkjP8NSGyNB",
            "BlockIndex": 4
        },
        {
            "FirstBlockToken": "ABgBAcfL
+EfmQmlNgstqrFnYgsAxR4SDSO4LkNLYOOChGBWcfJnpn90E9XX1",
            "SecondBlockToken": "ABgBAdX0mtX6aBAt3EBy
+8jFCESMpig7csKjbO2Ocd08m2iNJV2Ue+cRwUqF",
            "BlockIndex": 5
        },
        {
            "FirstBlockToken": "ABgBAVBaFJmbP/eRHGh7vnJlAwyiyNUi3MKZmEMxs2wC3AmM/
fc6yCOAMb65",
```

```
            "SecondBlockToken":
 "ABgBAdewWkHKTcrhZmsfM7GbaHyXD1Ctcn2nppz4wYItZRmAo1M72fpXU0Yv",
            "BlockIndex": 13
        },
        {
            "FirstBlockToken": "ABgBAQGxwuf6z095L6DpRoVRVnOqPxmx9r7Wf6O+i
+ltZ0dwPpGN39ijztLn",
            "SecondBlockToken": "ABgBAUdlitCVI7c6hGsT4ckkKCw6bMRclnV
+bKjViu/9UESTcW7CD9w4J2td",
            "BlockIndex": 14
        },
        {
            "FirstBlockToken":
 "ABgBAZBfEv4EHS1aSXTXxSE3mBZG6CNeIkwxpljzmgSHICGlFmZCyJXzE4r3",
            "SecondBlockToken":
 "ABgBAVWR7QuQQB0AP2TtmNkgS4Aec5KAQVCldnpc91zBiNmSfW9ouIlbeXWy",
            "BlockIndex": 15
        },
        .....
        {
            "SecondBlockToken": "ABgBAeHwXPL+z3DBLjDhwjdAM9+CPGV5VO5Q3rEEA
+ku50P498hjnTAgMhLG",
            "BlockIndex": 13171
        },
        {
            "SecondBlockToken":
 "ABgBAbZcPiVtLx6U3Fb4lAjRdrkJMwW5M2tiCgIp6ZZpcZ8AwXxkjVUUHADq",
            "BlockIndex": 13172
        },
        {
            "SecondBlockToken": "ABgBAVmEd/pQ9VW9hWiOujOAKcauOnUFCO
+eZ5ASVdWLXWWC04ijfoDTpTVZ",
            "BlockIndex": 13173
        },
        {
            "SecondBlockToken": "ABgBAT/jeN7w
+8ALuNdaiwXmsSfM6tOvMoLBLJ14LKvavw4IiB1d0iykWe6b",
            "BlockIndex": 13174
        },
        {
            "SecondBlockToken": "ABgBAXtGvUhTjjUqkwKXfXzyR2GpQei/
+pJSG/19ESwvt7Hd8GHaUqVs6Zf3",
            "BlockIndex": 13175
        }
```

```
    ],
    "ExpiryTime": 1637648751.813,
    "VolumeSize": 8
}
```

接下来，使用相同的命令查找需归档快照与紧接其后创建的快照之间不同的数据块。对于 `--first-snapshot-id`，请指定需归档快照 ID。对于 `--second-snapshot-id`，请指定紧接着需归档快照之后创建的快照 ID。

```
$ aws ebs list-changed-blocks --first-snapshot-id snapshot_to_archive --second-snapshot-id snapshot_created_after
```

例如，以下命令显示了以下两个快照之间不同块的数据块索引：快照 `snap-09c9114207084f0d9`（在需归档快照之后立即创建的快照），以及快照 `snap-024f49fe8dd853fa8`（需归档快照）。

```
$ aws ebs list-changed-blocks --first-snapshot-id snap-09c9114207084f0d9 --second-snapshot-id snap-024f49fe8dd853fa8
```

下面显示了命令输出，其中省略了一些数据块。

```
{
    "BlockSize": 524288,
    "ChangedBlocks": [
        {
            "FirstBlockToken": "ABgBAVax0bHHBnTERu
+9USLxYK/81UT0dbSnkDk0gqwRFSFGWA7HYbkkAy5Y",
            "SecondBlockToken":
 "ABgBASEvi9x8Om7Htp37cKG2NT9XUzEbLHpGcayelomSoHpGy8LGyvG0yYfK",
            "BlockIndex": 4
        },
        {
            "FirstBlockToken": "ABgBAeL0mtX6aBAt3EBy+8jFCESMpig7csfMrI4ufnQJT3XBm/
pwJZ1n2Uec",
            "SecondBlockToken": "ABgBAXmUTg6rAI
+v0LvekshbxCVpJjWILvxgC0AG0GQBEUNRVHkNABBwXLkO",
            "BlockIndex": 5
        },
        {
```

```
            "FirstBlockToken":
 "ABgBATKwWkHKTcrhZmsfM7GbaHyXD1CtcnjIZv9YzisYsQTMHfTfh4AhS0s2",
            "SecondBlockToken": "ABgBAcmiPFovWgXQio
+VBrxOqGy4PKZ9SAAHaZ2HQBM9fQQU0+EXxQjVGv37",
            "BlockIndex": 13
        },
        {
            "FirstBlockToken":
 "ABgBAbRlitCVI7c6hGsT4ckkKCw6bMRclnARrMt1hUbIhFnfz8kmUaZOP2ZE",
            "SecondBlockToken": "ABgBAXe935n544+rxhJ0INB8q7pAeoPZkkD27vkspE/
qKyvOwpozYII6UNCT",
            "BlockIndex": 14
        },
        {
            "FirstBlockToken": "ABgBAd+yxCO26I
+1Nm2KmuKfrhjCkuaP6LXuol3opCNk6+XRGcct4suBHje1",
            "SecondBlockToken": "ABgBAcPpnXz821NtTvWBPTz8uUFXnS8jXubvghEjZulIjHgc
+7saWys77shb",
            "BlockIndex": 18
        },
        .....
        {
            "SecondBlockToken": "ABgBATni4sDE5rS8/a9pqV03lU/lKCW
+CTxFl3cQ5p2f2h1njpuUiGbqKGUa",
            "BlockIndex": 13190
        },
        {
            "SecondBlockToken": "ABgBARbXo7zFhu7IEQ/9VMYFCTCtCuQ
+iSlWVpBIshmeyeS5FD/M0i64U+a9",
            "BlockIndex": 13191
        },
        {
            "SecondBlockToken": "ABgBAZ8DhMk+rROXa4dZlNK45rMYnVIGGSyTeiMli/sp/
JXUVZKJ9sMKIsGF",
            "BlockIndex": 13192
        },
        {
            "SecondBlockToken":
 "ABgBATh6MBVE904l6sqOC27s1nVntFUpDwiMcRWGyJHy8sIgGL5yuYXHAVty",
            "BlockIndex": 13193
        },
        {
            "SecondBlockToken":
 "ABgBARuZykaFBWpCWrJPXaPCneQMbyVgnITJqj4c1kJWPIj5Gn61OQyy+giN",
```

```
            "BlockIndex": 13194
        }
    ],
    "ExpiryTime": 1637692677.286,
    "VolumeSize": 8
}
```

6. 比较上一步中两个命令返回的输出。如果两个命令输出中都显示相同的数据块索引，则表示该数据块包含未引用的数据。

   例如，上一步中的命令输出表明数据块 4、5、13 和 14 对于快照 `snap-09c9114207084f0d9` 来说是唯一的，而且快照谱系中的任何其他快照都不会引用这些数据块。

   要确定标准层存储空间的减少多少，请将两个命令输出中出现的数据块数乘以 512KiB，即得出快照数据块大小。

   例如，如果在两个命令输出中都出现 9950 个数据块索引，则表明您将减少标准层存储大约 4.85GiB（9950 个数据块 x 512KiB = 4.85GiB）。

7. 确定在标准层中存储未引用的数据块达 90 天的存储成本。将此值与在存档层中存储完整快照的成本（如步骤 1 中所述）进行比较。假设在最短 90 天的期限内没有从归档层还原完整快照，您可以通过比较这些值来确定节省的成本。有关更多信息，请参阅 归档 Amazon EBS 快照的定价和计费。

归档 Amazon EBS 快照所需的 IAM 权限

默认情况下，用户无权使用快照归档。要允许用户使用快照归档，您必须创建 IAM policy，以授予使用特定资源和 API 操作的权限。有关更多信息，请参阅《IAM 用户指南》中的创建 IAM policy。

要使用快照归档，用户需要以下权限。

- `ec2:DescribeSnapshotTierStatus`
- `ec2:ModifySnapshotTier`
- `ec2:RestoreSnapshotTier`

控制台用户可能还需要其他权限，例如 `ec2:DescribeSnapshots`。

要存档和恢复加密快照，需要以下额外 Amazon KMS 权限。

- `kms:CreateGrant`

- kms:Decrypt
- kms:DescribeKey

以下是 IAM policy 示例，授予了 IAM 用户归档、恢复和查看加密及未加密快照的权限。其包括控制台用户的 ec2:DescribeSnapshots 权限。如果不需要某些上述权限，您可以从策略中将其删除。

> **Tip**
>
> 为遵循最小特权原则，请不要允许对 kms:CreateGrant 拥有完全访问权限。相反，使用kms:GrantIsForAWSResource条件密钥允许用户仅在 Amazon 服务代表用户创建授权时才允许用户在 KMS 密钥上创建授权，如以下示例所示。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeSnapshotTierStatus",
            "ec2:ModifySnapshotTier",
            "ec2:RestoreSnapshotTier",
            "ec2:DescribeSnapshots",
            "kms:CreateGrant",
            "kms:Decrypt",
            "kms:DescribeKey"
        ],
        "Resource": "*",
        "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
    }]
}
```

要提供访问权限，请为您的用户、组或角色添加权限：

- 通过身份提供商在 IAM 中托管的用户：

创建适用于身份联合验证的角色。按照《IAM 用户指南》中针对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 用户：
  - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
  - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

归档 Amazon EBS 快照

您可以归档任何状态为 `completed` 的快照，以及自己账户中的快照。您无法归档状态为 `pending` 或 `error` 的快照，以及与您共享的快照。有关更多信息，请参阅 归档 Amazon EBS 快照的注意事项和限制。

如果快照与一个或多个关联 AMIs，则必须先禁用关联的快照，然后 AMIs 才能存档快照。有关更多信息，请参阅禁用 AMI。

存档的快照会保留其快照 ID、加密状态、 Amazon Identity and Access Management (IAM) 权限、所有者信息和资源标签。但是，快照还原和快照共享会在快照归档后自动禁用。

在归档处理过程中，您可以继续使用快照。一旦快照分层状态达到 `archival-complete` 状态，您无法再使用快照。

Console

归档快照

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择快照。
3. 在快照列表中，选择需归档快照，然后选择 Actions（操作）、Archive snapshot（归档快照）。
4. 如要确认，请选择 Archive snapshot（归档快照）。

Amazon CLI

归档快照

使用 命令。 modify-snapshot-tier Amazon CLI 对于 `--snapshot-id`，请指定需归档快照的 ID。对于 `--storage-tier`，请指定 `archive`。

```
aws ec2 modify-snapshot-tier \
    --snapshot-id snap-0abcdef1234567890 \
    --storage-tier archive
```

下面是示例输出。响应参数 TieringStartTime 以 UTC 时间格式（YYYY-MM-DDTHH:MM:SSZ）表示归档过程的启动日期和时间。

```
{
    "SnapshotId": "snap-0abcdef1234567890",
    "TieringStartTime": "2021-09-15T16:44:37.574Z"
}
```

PowerShell

归档快照

使用 Edit-EC2SnapshotTier cmdlet。以下 示例归档指定的快照。

```
Edit-EC2SnapshotTier `
    -SnapshotId snap-0abcdef1234567890 `
    -StorageTier "archive"
```

还原已归档的 Amazon EBS 快照

在使用归档快照之前，必须先将其还原到标准层。还原的快照具有与归档之前相同的快照 ID、加密状态、IAM 权限、所有者信息和资源标签。还原后，您可以像使用账户中的任何其它快照一样使用它。还原的快照始终是完整快照。

还原快照时，可以选择使用以下两种方式还原快照：permanently（永久）或 temporarily（暂时）。

如果永久还原快照，则快照将从归档层永久移动到标准层。在手动重新归档或手动删除快照之前，快照将保持还原状态并可供使用。永久还原快照时，快照将从归档层中删除。

如果临时还原快照，则在您指定的还原期内，快照将从归档层复制到标准层。快照将保持还原状态，并且只能在还原期间使用。在还原期间，快照的副本将保留在归档层中。超过期限后，快照将自动从标准层中删除。在还原期间，您可以随时延长或缩短还原期，或将还原类型更改为永久。有关更多信息，请参阅 修改临时还原的 Amazon EBS 快照的还原期。

如果您要还原与已禁用的 AMI 关联的快照，并且打算使用该 AMI，则必须先永久还原所有关联的快照，再重新启用已禁用的 AMI，然后才能使用该 AMI。如果关联的快照已暂时恢复，则无法启用 AMI。您可以使用以下命令来查找与 AMI 关联的所有快照。

```
aws ec2 describe-images --image-id ami_id \
  --query Images[*].BlockDeviceMappings[*].Ebs[].SnapshotId[]
```

Console

从归档中还原快照

打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。

1. 在导航窗格中，选择快照。
2. 在快照列表中，选择要还原的归档快照，然后选择 Actions（操作）、Restore snapshot from archive（从归档还原快照）。
3. 指定要执行的还原类型。在 Restore type（还原类型）中，执行下列操作之一：
   - 要永久还原快照，请选择 Permanent（永久）。
   - 要临时还原快照，请选择 Temporary（临时），然后在 Temporary restore period（临时还原期）中，输入要还原快照的天数。
4. 要确认，请选择 Restore snapshot（还原快照）。

Amazon CLI

永久还原已归档的快照

使用带--permanent-restore选项的 restore-snapshot-tier Amazon CLI 命令。对于 --snapshot-id，请指定需还原快照的 ID。

```
aws ec2 restore-snapshot-tier \
    --snapshot-id snap-0abcdef1234567890 \
    --permanent-restore
```

下面是示例输出。

```
{
    "SnapshotId": "snap-0abcdef1234567890",
```

```
    "IsPermanentRestore": true
}
```

临时还原已归档的快照

使用 命令。 restore-snapshot-tier Amazon CLI 忽略 `--permanent-restore` 选项。对于`--temporary-restore-days`，请指定恢复快照的天数。允许的范围是 1 到 180 天。如果未指定值，则默认值为 1 天。

以下示例暂时恢复指定的快照，还原期为 5 天。

```
aws ec2 restore-snapshot-tier \
    --snapshot-id snap-0abcdef1234567890 \
    --temporary-restore-days 5
```

下面是示例输出。

```
{
    "SnapshotId": "snap-0abcdef1234567890",
    "RestoreDuration": 5,
    "IsPermanentRestore": false
}
```

PowerShell

永久还原已归档的快照

使用 Restore-EC2SnapshotTier cmdlet。

```
Restore-EC2SnapshotTier `
    -SnapshotId snap-0abcdef1234567890 `
    -PermanentRestore $true
```

临时还原已归档的快照

使用 Restore-EC2SnapshotTier cmdlet。

```
Restore-EC2SnapshotTier `
    -SnapshotId snap-0abcdef1234567890 `
    -TemporaryRestoreDays 5
```

修改临时还原的 Amazon EBS 快照的还原期

临时还原快照时，必须指定快照在账户中保持还原状态的天数。还原期到期后，快照将自动从标准层中删除。

您可以随时更改临时还原快照的还原期。

您可以选择增加或缩短还原期，也可以将还原类型从临时更改为永久。

如果更改还原期，则新的还原期将从当前日期开始生效。例如，如果指定新的还原期 5 天，快照将从当前日期开始到 5 天内保持还原状态。

> **Note**
>
> 您可以通过将还原期设置为 1 天，提前结束临时还原。

如果将还原类型从临时更改为永久，则快照副本将从归档层中删除，并且在您手动重新归档或删除快照之前，该快照将保持在账户中并且可用。

Console

修改还原期或还原类型

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择快照。
3. 在快照列表中，选择此前暂时还原的快照，然后选择 Actions（操作）、Restore snapshot from archive（从归档还原快照）。
4. 在 Restore type（还原类型）中，执行下列操作之一：
   - 要将还原类型从临时更改为永久，请选择 Permanent（永久）。
   - 要延长或缩短还原期，请保留 Temporary（临时），然后在 Temporary restore period（临时还原期）中输入新的还原期（以天为单位）。
5. 要确认，请选择 Restore snapshot（还原快照）。

Amazon CLI

修改还原期或还原类型

使用 restore-snapshot-tier 命令。对于 --snapshot-id，请指定之前临时还原的快照的 ID。要将还原类型从临时更改为永久性，请指定 --permanent-restore 并忽略 --temporary-restore-days。要延长或缩短还原期，请省略 --permanent-restore，而且对于 --temporary-restore-days，请指定新的还原期（以天为单位）。

例如：延长或缩短还原期

以下命令将指定快照的还原周期更改为10天。

```
aws ec2 restore-snapshot-tier \
    --snapshot-id snap-0abcdef1234567890 \
    --temporary-restore-days 10
```

下面是示例输出。

```
{
    "SnapshotId": "snap-0abcdef1234567890",
    "RestoreDuration": 10,
    "IsPermanentRestore": false
}
```

示例：将还原类型更改为永久

以下命令将指定快照的还原类型从临时更改为永久。

```
aws ec2 restore-snapshot-tier \
    --snapshot-id snap-0abcdef1234567890 \
    --permanent-restore
```

下面是示例输出。

```
{
    "SnapshotId": "snap-0abcdef1234567890",
    "IsPermanentRestore": true
}
```

PowerShell

修改还原期或还原类型

使用 Restore-EC2SnapshotTier cmdlet。对于 -SnapshotId，请指定之前临时还原的快照的 ID。要将还原类型从临时更改为永久性，请指定 -PermanentRestore 并忽略 -TemporaryRestoreDays。要延长或缩短还原期，请省略 -PermanentRestore，而且对于 -TemporaryRestoreDays，请指定新的还原期（以天为单位）。

例如：延长或缩短还原期

以下命令将指定快照的还原周期更改为10天。

```
Restore-EC2SnapshotTier `
    -SnapshotId snap-0abcdef1234567890 `
    -TemporaryRestoreDays 10
```

示例：将还原类型更改为永久

以下命令将指定快照的还原类型从临时更改为永久。

```
Restore-EC2SnapshotTier `
    -SnapshotId snap-0abcdef1234567890 `
    -PermanentRestore $true
```

查看已归档的 Amazon EBS 快照

Console

查看快照的存储层信息

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择快照。
3. 在快照列表中，选择快照，然后选择 Storage tier（存储层）选项卡。

   该表提供以下信息：

   - Last tier change started on（上次层别更改始于）– 上次归档或还原的开始日期和时间。
   - Tier change progress（层更改进展）– 以百分比表示的上次归档或还原操作的进度。
   - Storage tier（存储层）– 快照的存储层。归档快照的状态始终为 archive，以及存储在标准层上的快照的状态始终为 standard，包括临时还原的快照。
   - Tiering status（分层状态）– 上次归档或还原操作的状态。
   - Archive completed on（归档完成时间）– 归档完成的日期和时间。

- Temporary restore expires on（临时还原到期时间）– 设置临时还原的快照过期的日期和时间。

Amazon CLI

查看有关归档快照的归档信息

使用 describe-snapshot-tier-status 命令。请指定 snapshot-id 筛选条件，请指定快照 ID 为筛选条件值。或者，要查看所有归档的快照，请省略筛选条件。

```
--filters "Name=snapshot-id, Values=snapshot_id"
```

输出包括以下响应参数：

- Status – 快照的状态。归档快照的状态始终为 completed。只有状态为 completed 的快照可以归档。
- LastTieringStartTime – 归档过程开始的日期和时间，采用 UTC 时间格式（YYYY-MM-DDTHH:MM:SSZ）。
- LastTieringOperationState – 归档过程的当前状态。可能的状态包括：archival-in-progress | archival-completed | archival-failed | permanent-restore-in-progress | permanent-restore-completed | permanent-restore-failed | temporary-restore-in-progress | temporary-restore-completed | temporary-restore-failed
- LastTieringProgress – 快照归档过程的进度，以百分比表示。
- StorageTier – 快照的存储层。归档快照的状态始终为 archive，以及存储在标准层上的快照的状态始终为 standard，包括临时还原的快照。
- ArchivalCompleteTime – 归档过程完成的日期和时间，采用 UTC 时间格式（YYYY-MM-DDTHH:MM:SSZ）。

示例：描述快照

以下示例显示有关指定快照的信息。

```
aws ec2 describe-snapshot-tier-status \
    --filters "Name=snapshot-id, Values=snap-0abcdef1234567890"
```

下面是示例输出。

```
{
    "SnapshotTierStatuses": [
        {
            "Status": "completed",
            "ArchivalCompleteTime": "2021-09-15T17:33:16.147Z",
            "LastTieringProgress": 100,
            "Tags": [],
            "VolumeId": "vol-01234567890abcdef",
            "LastTieringOperationState": "archival-completed",
            "StorageTier": "archive",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-0abcdef1234567890",
            "LastTieringStartTime": "2021-09-15T16:44:37.574Z"
        }
    ]
}
```

查看归档和标准层快照

可以使用 describe-hosts 命令。对于--snapshot-ids，请指定快照的 ID。

```
aws ec2 describe-snapshots --snapshot-ids snap-0abcdef1234567890
```

下面是示例输出。响应参数 StorageTier 说明快照当前是否已归档。archive 表示快照当前已归档并存储在归档层中，而 standard 表示快照当前尚未归档，并且存储在标准层中。

在以下示例输出中，只有 Snap A 已归档。Snap B 和 Snap C 尚未归档。

此外，响应参数 RestoreExpiryTime 仅为从归档中暂时还原的快照返回。它表示将何时从标准层中自动删除临时还原的快照。对于永久还原的快照，不会返回该值。

在以下示例输出中，Snap C 已暂时还原，它将在 2021-09-19T21:00:00.000Z（2021 年 9 月 19 日 UTC 21:00）自动从标准级别中移除。

```
{
    "Snapshots": [
        {
            "Description": "Snap A",
            "Encrypted": false,
            "VolumeId": "vol-01234567890aaaaaa",
            "State": "completed",
            "VolumeSize": 8,
```

```
            "StartTime": "2021-09-07T21:00:00.000Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-01234567890aaaaaa",
            "StorageTier": "archive",
            "Tags": []
        },
        {
            "Description": "Snap B",
            "Encrypted": false,
            "VolumeId": "vol-09876543210bbbbbb",
            "State": "completed",
            "VolumeSize": 10,
            "StartTime": "2021-09-14T21:00:00.000Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-09876543210bbbbbb",
            "StorageTier": "standard",
            "RestoreExpiryTime": "2019-09-19T21:00:00.000Z",
            "Tags": []
        },
        {
            "Description": "Snap C",
            "Encrypted": false,
            "VolumeId": "vol-054321543210cccccc",
            "State": "completed",
            "VolumeSize": 12,
            "StartTime": "2021-08-01T21:00:00.000Z",
            "Progress": "100%",
            "OwnerId": "123456789012",
            "SnapshotId": "snap-054321543210cccccc",
            "StorageTier": "standard",
            "Tags": []
        }
    ]
}
```

仅查看存储在归档层或标准层中的快照

可以使用 describe-hosts 命令。包括带有筛选器名称的`--filter`选项`storage-tier`。对于筛选器值，请指定`archive`或`standard`。以下示例仅显示存档的快照。

```
aws ec2 describe-snapshots --filters "Name=storage-tier,Values=archive"
```

PowerShell

查看有关已存档快照的存档信息

使用 Get-EC2SnapshotTierStatus cmdlet。

```
Get-EC2SnapshotTierStatus `
    -Filter @{Name="snapshot-id"; Values="snap-0abcdef1234567890"}
```

查看归档和标准层快照

使用 Get-EC2Snapshot cmdlet。

```
Get-EC2Snapshot `
    -SnapshotId snap-0abcdef1234567890
```

仅查看存储在归档层或标准层中的快照

使用 Get-EC2Snapshot cmdlet。以下示例仅显示存档的快照。

```
Get-EC2Snapshot `
    -Filter @{Name="storage-tier"; Values="archive"}
```

使用 CloudWatch 事件监控 Amazon EBS 快照存档

Amazon EBS 发出与快照归档操作相关的事件。您可以使用 Amazon Lambda 和 Amazon CloudWatch Events 以编程方式处理事件通知。尽最大努力发出事件。有关更多信息，请参阅 Amazon EventBridge 用户指南。

提供的事件如下：

- `archiveSnapshot` – 当快照归档操作成功或失败时发出。

  以下是在快照归档操作成功时发送事件的示例。

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Snapshot Notification",
   "source": "aws.ec2",
```

```
   "account": "123456789012",
   "time": "2021-05-25T13:12:22Z",
   "region": "us-east-1",
   "resources": [
     "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
   ],
   "detail": {
     "event": "archiveSnapshot",
     "result": "succeeded",
     "cause": "",
     "request-id": "123456789",
     "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
     "startTime": "2021-05-25T13:12:22Z",
     "endTime": "2021-05-45T15:30:00Z",
     "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
```

以下是在快照归档操作失败时发送事件的示例。

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "archiveSnapshot",
    "result": "failed",
    "cause": "Source snapshot ID is not valid",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}
```

- permanentRestoreSnapshot – 当永久还原操作成功或失败时发出。

以下是在快照还原操作成功时发送事件的示例。

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "permanentRestoreSnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-10-45T15:30:00Z"
  }
}
```

以下是在永久还原操作失败时发送事件的示例。

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "permanentRestoreSnapshot",
    "result": "failed",
    "cause": "Source snapshot ID is not valid",
    "request-id": "1234567890",
```

```
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}
```

- temporaryRestoreSnapshot – 当临时还原操作成功或失败时发出。

  以下是在快照暂时还原操作成功时发送事件的示例。

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "temporaryRestoreSnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "restoreExpiryTime": "2021-06-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}
```

  下面是在临时还原操作失败时发送事件的示例。

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
```

```
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "temporaryRestoreSnapshot",
    "result": "failed",
    "cause": "Source snapshot ID is not valid",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}
```

- `restoreExpiry` – 在临时还原快照的还原期到期时触发。

  示例如下：

```
{
   "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2021-05-25T13:12:22Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "restoryExpiry",
    "result": "succeeded",
    "cause": "",
    "request-id": "1234567890",
    "snapshot_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
    "startTime": "2021-05-25T13:12:22Z",
    "endTime": "2021-05-45T15:30:00Z",
    "recycleBinExitTime": "2021-10-45T15:30:00Z"
  }
}
```

删除 Amazon EBS 快照

当您不再需要卷的 Amazon EBS 快照后，可以将其删除。删除快照对卷没有影响。删除卷对从它生成的快照无任何影响。

主题

- 删除快照的注意事项
- 删除增量快照的工作原理
- 删除快照
- 删除多卷快照

删除快照的注意事项

删除快照时需考虑以下事项：

- 您不能删除注册 AMI 使用的 EBS 卷的根设备快照。即使已注册的 AMI 已弃用或禁用，此注意事项依然适用。您必须先注销 AMI，然后才能删除快照。有关更多信息，请参阅取消注册 AMI。
- 您无法删除由该 Amazon Backup 服务通过 Amazon 管理的快照 EC2。而是 Amazon Backup 使用删除备份保管库中相应的恢复点。有关更多信息，请参阅 Amazon Backup 开发人员指南中的删除备份。
- 您可以手动创建、保留和删除快照，也可以使用 Amazon Data Lifecycle Manager 来管理快照。有关更多信息，请参阅Amazon Data Lifecycle Manager。
- 尽管您可以删除仍在制作的快照，但该快照必须先完成，删除才能生效。这可能需要较长时间。如果您还具有并发快照限制，而您尝试再制作一个快照，可能会遇到 `ConcurrentSnapshotLimitExceeded` 错误。有关更多信息，请参阅 Amazon Web Services 一般参考 中 Amazon EBS 的服务配额。
- 如果您删除符合回收站保留规则的快照，快照将保留在回收站中，而不是立即删除。有关更多信息，请参阅回收站。
- 您无法删除与禁用 EBS AMIs 支持的快照。有关更多信息，请参阅禁用 AMI。
- 您无法删除与您共享的快照。
- 如果删除您拥有的共享快照，则所有与该快照共享的账户都将无法访问它。

删除增量快照的工作原理

如果定期拍摄卷快照，则这些快照为增量快照。这意味着该设备上在您的最新快照之后更改的数据块将保存在新快照中。尽管快照是以增量方式保存的，但是快照删除流程旨在让您能够仅保留最新的快照以创建卷。

如果数据存在于早期的单个快照或一系列快照中保存的卷上，并且该数据随后从卷中删除，则该数据仍被视为早期快照的唯一数据。只有引用唯一数据的所有快照都被删除，该唯一数据才会从快照序列中删除。

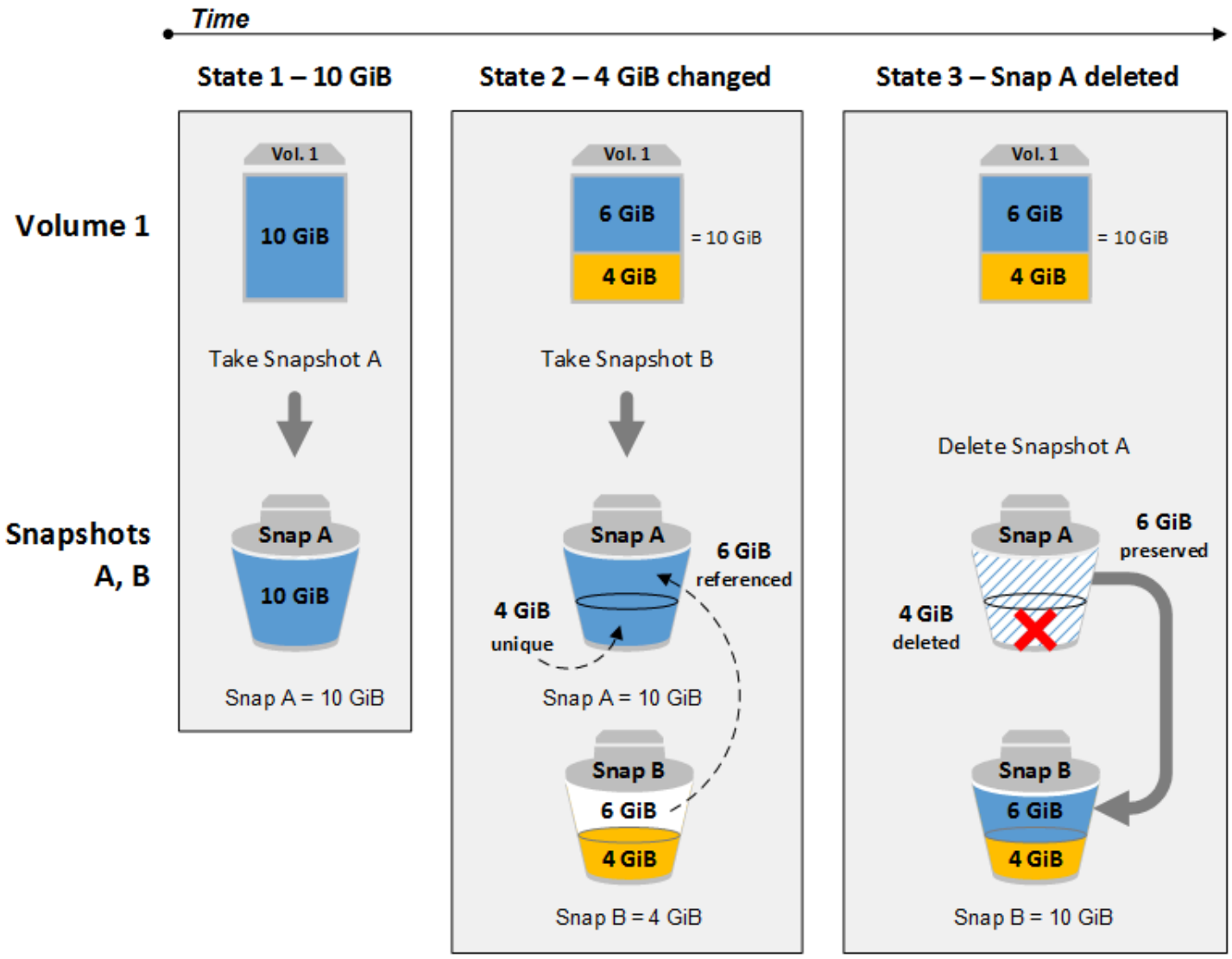
删除快照时，仅删除该快照专门引用的数据。只有在删除引用唯一数据的所有快照时，才会删除该唯一数据。删除卷的之前快照不会影响您使用该卷的之后快照创建卷的能力。

删除快照可能不会降低组织的数据存储成本。其他快照可引用已删除快照的数据，已引用的数据总是会被保留。如果您删除了一个快照，而该快照包含以后的快照使用的数据，那么与所引用数据关联的成本将分配到后来的快照。有关快照如何存储数据的更多信息，请参阅Amazon EBS 快照的工作原理和下面的示例。

在下图中，卷 1 在三个时间点上显示。某个快照已捕获前两种状态，在第三种状态中，某个快照已被删除。

- 在状态 1 中，该卷有 10 GiB 的数据。因为快照 A 是为该卷制作的首个快照，因此必须复制所有 10 GiB 数据。在此状态下，您需要为存储 10 GiB 的快照数据付费。
- 在状态 2 中，该卷仍包含 10 GiB 的数据，但是 4 GiB 已更改。快照 B 仅存储拍摄快照 A 后更改的 4 GiB，它引用已存储在快照 A 中的 6 GiB 未更改数据。在此状态下，您需要为存储 14 GiB 的快照数据（来自快照 A 的 10 GiB + 来自快照 B 的 4 GiB）付费。
- 在状态 3 中，音量保持不变，但快照 A 已删除。由于快照 A 中 6 GiB 的未更改数据仍由快照 B 引用，因此该数据会被保留并与快照 B 相关联。快照 A 中 4 GiB 的唯一数据已被删除，因为其他快照不再引用该数据。在此状态下，您需要为存储 10 GiB 的快照数据（从快照 A 中保留的 6 GiB 数据+在快照 B 中保留 4 GiB 的数据）付费。

删除快照及其由其他快照引用的部分数据



删除快照

Console

删除快照

1. 打开亚马逊 EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择快照。
3. 选择快照。
4. 选择 Actions（操作）、Delete snapshot（删除快照）。
5. 提示进行确认时，输入 **`delete`**，然后选择 Delete（删除）。

Amazon CLI

删除快照

使用 delete-snapshot 命令。

```
aws ec2 delete-snapshot --snapshot-id snap-0abcdef1234567890
```

PowerShell

删除快照

使用 Remove-EC2Snapshot cmdlet。

```
Remove-EC2Snapshot -SnapshotId snap-0abcdef1234567890
```

> **故障排除技巧**
>
> 如果您收到`Failed to delete snapshot`错误提示 AMI 当前正在使用快照，则必须先取消注册关联的 AMI，然后才能删除快照。您无法删除与 AMI 关联的快照。
> 如果您使用的是控制台且关联的 AMI 已禁用，则必须在AMIs屏幕上选择 “已禁用图像” 筛选器才能禁用查看 AMIs。

删除多卷快照

要删除多卷快照，请使用您在创建快照时应用于多卷快照集的标签检索集的所有快照。然后，分别删除这些快照。

系统不会阻止您删除多卷快照集中的各个快照。如果在 `pending state` 中删除快照，则只删除该快照。多卷快照集中的其他快照仍成功保留。

Amazon EBS 快速快照还原

Amazon EBS 快速快照还原（FSR）使您能够从创建时已完全初始化的快照创建卷。这会消除首次访问块时对其执行 I/O 操作的延迟。使用快速快照还原创建的卷可以立即交付其所有预置性能。

要开始使用，请在特定可用区中为特定快照启用快速快照还原。每一对快照和可用区指代一个快速快照还原。当您从其中一个已启用该功能的可用区中的快照创建卷时，该卷将使用快速快照还原进行还原。

您必须为每个快照明确启用快速快照还原。例如，如果从已启用快速快照还原的快照还原卷创建新的快照，则新快照不会自动启用快速快照还原功能。如果复制已启用快速快照还原的快照，则快照副本不会自动启用快速快照还原。

您可以使用快速快照还原的全部性能优势还原的卷数是由快照的卷创建积分决定的。有关更多信息，请参阅 Amazon EBS 快速快照还原卷创建积分。

您可以为您拥有的快照以及与您共享的公有快照和私有快照启用快速快照还原。

内容

- 注意事项
- 定价和计费
- Amazon EBS 快速快照还原卷创建积分
- 为 Amazon EBS 快照配置快速快照还原
- 检查 Amazon EBS 快照的快速快照还原状态
- 查看使用快速快照还原还原的 Amazon EBS 卷

注意事项

- Local Zones 和 Wavelen Amazon Outposts gth Zones 不支持快速快照恢复。
- 可以为大小为 16 TiB 或以下的快照启用快速快照还原。
- 配置的卷性能高达 64,000 IOPS 和 1,000 MiB/s throughput receive the full performance benefit of fast snapshot restore. For volumes provisioned with performance greater than 64,000 IOPS or 1,000 MiB/s 吞吐量，我们建议您初始化该卷以获得其全部性能。
- 每个区域最多可启用 5 个快照以用于快速快照还原。配额适用于您拥有的快照以及与您共享的快照。如果为与您共享的快照启用快速快照还原，则它将计入快速快照还原配额。它不计入快照所有者的快速快照还原配额。
- 当快照的快速快照还原状态发生变化时，Amazon EBS 会发出 Amazon CloudWatch 事件。有关更多信息，请参阅 EBS 快速快照还原事件。

定价和计费

对于为特定可用区中快照启用的快速快照还原，您需要按每分钟支付费用。收费按比例计算，最少 1 小时。

例如，假设您在 cn-northwest-1a 中为一个快照启用了一个月（30 天）的快速快照还原，则需要支付 ¥3905.28（1 个快照 x 1 个可用区 x 720 小时 x 每小时 ¥5.424）的费用。如果您在cn-northwest-1a、中为两个快照启用快速快照恢复cn-northwest-1b，则cn-northwest-1c需要支付 ¥23431.68（2快照 x 小时 x 每720小时 3 AZs x 每小时）的费用。¥5.424

如果为与您共享的公有快照或私有快照启用快速快照还原，则会对您的账户进行计费；不会对快照所有者进行计费。当快照所有者删除与您共享的快照或取消其共享时，系统会为您账户中的快照禁用快速快照还原，并停止计费。

有关更多信息，请参阅 Amazon EBS 定价。

Amazon EBS 快速快照还原卷创建积分

获得快速快照还原的全部性能优势的卷数是由快照的卷创建积分决定的。每个可用区的每个快照具有一积分存储桶。从快照中创建并启用了快速快照还原的每个卷使用积分存储桶中的一积分。存储桶中必须至少有一积分，您才能从快照创建初始化卷。如果您创建卷但存储桶中的积分少于一个，则创建卷时不能获得快速快照还原的优势。

当您为与您共享的快照启用快速快照还原时，您的账户中的共享快照会获得单独的信用存储桶。如果您从共享快照创建卷，则配额将从您的信用存储桶中消耗；这些配额不会从快照所有者的信用存储桶中消耗。

积分桶大小和充值率基于快照的大小（也是源卷的大小），而不是快照数据的大小。例如，如果您从一个拥有 150 GiB 数据的 200 GiB 卷创建快照，并启用它以进行快速快照恢复，则积分桶大小和充值率将基于 200 GiB。

当您为快照启用快速快照还原时，积分存储桶从零积分开始，并以设定的速率填满，直到达到最大积分容量。此外，在使用积分时，将随着时间的推移重填积分存储桶，直到其达到最大积分容量。

每积分存储桶的填充率计算如下：

```
MIN (10, (1024 ÷ snapshot_size_gib))
```

积分存储桶的大小计算如下：

```
MAX (1, MIN (10, (1024 ÷ snapshot_size_gib)))
```

例如，如果为大小为 128 GiB 的快照启用快速快照还原，则填充率为每分钟 0.1333 积分。

```
MIN (10, (1024 ÷ 128))
```

```
 = MIN (10, 8)
 = 8 credits per hour
 = 0.1333 credits per minute
```

积分存储桶的最大大小为 8 积分。

```
MAX (1, MIN (10, (1024 ÷ 128)))
 = MAX (1, MIN (10, 8))
 = MAX (1, 8)
 = 8 credits
```

在此示例中，启用快速快照还原时，积分存储桶以零积分开始。8 分钟后，积分存储桶有足够的积分来创建一个初始化卷（`0.1333 credits × 8 minutes = 1.066 credits`）。如果积分存储桶已满，您可以同时创建 8 个初始化卷（8 积分）。当存储桶低于其最大容量时，它将每分钟重填 `0.1333` 积分。

您可以使用 CloudWatch 指标来监控积分桶的大小以及每个存储桶中可用的积分数量。有关更多信息，请参阅 快速快照还原的指标。

从启用了快速快照还原的存储桶创建卷之后，您可以使用 describe-volumes 来描述卷，并检查输出中的 `fastRestored` 字段以确定是否使用快速快照还原将该卷创建为已初始化卷。

为 Amazon EBS 快照配置快速快照还原

默认情况下，对于快照禁用快速快照还原。您可以为您拥有的快照以及与您共享的快照启用或禁用快速快照还原。为快照启用或禁用快速快照还原时，所做的更改仅适用于您的账户。

> **Note**
>
> 当您为快照启用快速快照还原时，您的账户将按特定可用区中启用快速快照还原的每分钟计费。收费按比例计算，最少 1 小时。

当您删除您拥有的快照时，系统会在账户中自动禁用该快照的快速快照还原。如果您为与您共享的快照启用了快速快照还原，并且快照所有者删除或取消共享，则会自动为您账户中的共享快照禁用快速快照还原。

如果为共享的快照启用了快速快照还原，并且使用自定义 CMK 对其进行了加密，则在快照所有者撤消对自定义 CMK 的访问权限时，快速快照还原不会自动为快照禁用。您必须手动为该快照禁用快速快照还原。

为快照启用快速快照还原后，快照将进入 optimizing 状态。处于 optimizing 状态的快照在使用快照恢复卷时可以提供一些性能优势。只有在进入 enabled 状态后，它们才开始发挥快速快照还原的全部性能优势。

Console

配置快速快照恢复

1. 打开亚马逊 EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择快照。
3. 选择快照，然后选择 Actions（操作）、Manage fast snapshot restore（管理快速快照还原）。
4. 快速快照还原设置部分会列出所有可用区，您可以在其中为所选快照启用快速快照还原功能。Current status（当前状态）卷说明每个区域当前是启用还是禁用快速快照还原。

   要在当前禁用快照的区域中启用快速快照还原，选择该区域，然后选择 Enable（启用），并选择 Enable（启用）以确认。

   要在当前启用快照还原的区域中禁用快速快照还原，请选择该区域，然后选择 Disable（禁用）。
5. 进行必要的更改后，选择 Close（关闭）。

Amazon CLI

启用快速快照还原

使用 enable-fast-snapshot-restores 命令。

```
aws ec2 enable-fast-snapshot-restores \
    --availability-zones us-east-1a us-east-1b \
    --source-snapshot-ids snap-0abcdef1234567890
```

禁用快速快照还原

使用 disable-fast-snapshot-restores 命令。

```
aws ec2 disable-fast-snapshot-restores \
    --availability-zones us-east-1a \
    --source-snapshot-ids snap-0abcdef1234567890
```

以下示例使用describe-fast-snapshot-restores命令来描述您禁用的快速快照恢复。

```
aws ec2 describe-fast-snapshot-restores \
    --filters Name=state,Values=disabled
```

PowerShell

启用快速快照还原

使用 Enable-EC2FastSnapshotRestore cmdlet。

```
Enable-EC2FastSnapshotRestore `
    -AvailabilityZone us-east-1a us-east-1b `
    -SourceSnapshotId snap-0abcdef1234567890
```

禁用快速快照还原

使用 Disable-EC2FastSnapshotRestore cmdlet。

```
Disable-EC2FastSnapshotRestore `
    -AvailabilityZone us-east-1a `
    -SourceSnapshotId snap-0abcdef1234567890
```

以下示例使用 Get-EC2FastSnapshotRestorecmdlet 来描述您禁用的快速快照恢复。

```
Get-EC2FastSnapshotRestore `
    -Filter @{Name="state"; Values="disabled"}
```

检查 Amazon EBS 快照的快速快照还原状态

快照的快速快照还原可能处于以下状态之一。

- `enabling` – 发出了启用快速快照还原的请求。
- `optimizing` – 正在启用快速快照还原。对于快照优化，每个 TiB 需要 60 分钟的时间。处于此状态的快照在还原卷时提供了一些性能优势。
- `enabled` – 启用了快速快照还原。处于此状态且具有足够卷创建积分的快照在还原卷时可发挥全部性能优势。
- `disabling` – 发出了禁用快速快照还原的请求，或者启用快速快照还原的请求失败。
- `disabled` – 禁用了快速快照还原。您可以根据需要再次启用快速快照还原。

您可以查看您拥有的快照或与您共享的快照的快速快照恢复状态。

Console

查看快速快照恢复的状态

1. 打开亚马逊 EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择快照。
3. 选择快照。
4. 在 Details（详细信息）选项卡上，查看 Fast Snapshot Restore（快速快照还原），该选项卡表示快速快照还原的状态。

Amazon CLI

查看启用了快速快照恢复的快照

使用 describe-fast-snapshot-restores 命令。

```
aws ec2 describe-fast-snapshot-restores --filters Name=state,Values=enabled
```

下面是示例输出。

```
{
    "FastSnapshotRestores": [
        {
            "SnapshotId": "snap-0e946653493cb0447",
            "AvailabilityZone": "us-east-2a",
            "State": "enabled",
            "StateTransitionReason": "Client.UserInitiated - Lifecycle state
 transition",
            "OwnerId": "123456789012",
            "EnablingTime": "2020-01-25T23:57:49.596Z",
            "OptimizingTime": "2020-01-25T23:58:25.573Z",
            "EnabledTime": "2020-01-25T23:59:29.852Z"
        },
        {
            "SnapshotId": "snap-0e946653493cb0447",
            "AvailabilityZone": "us-east-2b",
            "State": "enabled",
            "StateTransitionReason": "Client.UserInitiated - Lifecycle state
 transition",
```

```
            "OwnerId": "123456789012",
            "EnablingTime": "2020-01-25T23:57:49.596Z",
            "OptimizingTime": "2020-01-25T23:58:25.573Z",
            "EnabledTime": "2020-01-25T23:59:29.852Z"
        }
    ]
}
```

PowerShell

查看启用了快速快照恢复的快照

使用 Get-EC2FastSnapshotRestore cmdlet。

```
Get-EC2FastSnapshotRestore `
    -Filter @{Name="state"; Values="enabled"}
```

查看使用快速快照还原还原的 Amazon EBS 卷

当您在可用区中，从已启用快速快照还原的快照创建卷时，将使用快速快照还原进行还原。

Amazon CLI

查看根据启用了快速快照还原功能的快照创建的卷

使用 describe-volumes 命令。

```
aws ec2 describe-volumes --filters Name=fast-restored,Values=true
```

下面是示例输出。

```
{
    "Volumes": [
        {
            "Attachments": [],
            "AvailabilityZone": "us-east-2a",
            "CreateTime": "2020-01-26T00:34:11.093Z",
            "Encrypted": true,
            "KmsKeyId": "arn:aws:kms:us-west-2:123456789012:key/8c5b2c63-b9bc-45a3-
a87a-5513e232e843",
            "Size": 20,
```

```
            "SnapshotId": "snap-0abcdef1234567890",
            "State": "available",
            "VolumeId": "vol-01234567890abcdef",
            "Iops": 100,
            "VolumeType": "gp2",
            "FastRestored": true
        }
    ]
}
```

PowerShell

查看根据启用了快速快照还原功能的快照创建的卷

使用 Get-EC2Volume cmdlet。

```
Get-EC2Volume -Filter @{Name="fast-restored"; Values="true"}
```

Amazon EBS 快照锁

您可以锁定 Amazon EBS 快照以防止意外或恶意删除，或者以 WORM (write-once-read-many) 格式将其存储在特定时间内。当一个快照处于锁定状态时，任何用户都无法将其删除，无论他们的 IAM 权限如何。您可以像使用任何其他快照一样继续使用锁定的快照。

> **Note**
>
> 快照锁定已由 Cohasset Associates 评估，可在受 SEC 17a-4、CFTC 和 FINRA 法规约束的环境中使用。有关快照锁定如何与这些法规相关的更多信息，请参阅 Cohasset Associates Compliance Assessment。

可以使用以下两种模式之一锁定快照：合规模式或监管模式，而且可以将快照锁定特定的一段时间或者锁定到某个特定日期。有关更多信息，请参阅锁定模式和锁定持续时间。

定价

您可以锁定和解锁快照，无需支付额外的费用。您需要为锁定的快照支付标准 Amazon EBS 快照存储费用。

主题

- Amazon EBS 快照锁定的概念
- Amazon EBS 快照锁定的注意事项
- 控制对 Amazon EBS 快照锁定的访问
- 锁定 Amazon EBS 快照
- 解锁 Amazon EBS 快照
- 更新 Amazon EBS 快照锁定设置
- 监控 Amazon EBS 快照锁定

Amazon EBS 快照锁定的概念

以下是开始使用快照锁定时需要理解的重要概念。

目录

- 锁定模式
- 锁定持续时间
- 冷静期
- 锁定状态

锁定模式

可以在以下两种模式之一中锁定快照：

监管模式

锁定快照之后，拥有适当 IAM 权限的用户可以随时解锁快照，还可以修改锁定模式以及锁定持续时间或到期日期。当在监管模式下锁定快照时，快照会立即被锁定；没有冷静期。要在监管模式下锁定快照之后将其删除，必须首先解锁快照，或者必须等待锁定过期。

通过确保只有某些用户有权解锁快照和修改快照锁定配置，您可以使用监管模式满足组织的数据监管要求。在合规模式下锁定快照之前，还可以利用监管模式测试锁定配置。

合规性模式

在合规模式下锁定快照时，可以选择指定在锁定快照之后立即开始的冷静期。在冷静期内，拥有适当权限的用户可以解锁快照、更改锁定模式、延长或缩短冷静期以及延长或缩短锁定持续时间或到期日期。在冷静期过期之后，您将无法解锁快照、更改锁定模式或者缩短锁定持续时间或过期日期；您只能延长锁定持续时间或过期日期。要在合规模式下锁定快照且冷静期过期之后将其删除，必须等待锁定过期。

> **Note**
>
> 通过在请求中省略冷静期，可以在合规模式下锁定快照而不设冷静期。如果这样做，锁定将立即生效，而且无法解锁快照、更改锁定模式或者缩短锁定持续时间或过期日期；您只能延长锁定持续时间或过期日期。

可以利用合规模式保护出于合规性原因不应在特定的时期内删除的快照。合规模式具有以下优点：

- 它支持对快照使用 WORM（一次写入多次读取）配置。
- 它提供了一层额外的防御，可保护快照免遭意外删除或恶意删除。
- 它实施了保留期，可防止特权用户提前删除，以满足贵组织的数据保护策略和程序。

> **Note**
>
> 要删除在锁定到期前锁定在合规模式下的快照，唯一的方法是关闭关联的 Amazon 账户。

锁定持续时间

锁定持续时间是指快照要保持锁定状态的时期。可以将锁定持续时间指定为以下选项之一，但不能同时指定这两者：

天数

将锁定持续时间指定为快照要保持锁定状态的天数。当指定的天数过后，会自动解锁快照。持续时间介于 1 天到 36500 天（100 年）不等。

锁定到期日期

锁定持续时间由未来的过期日期决定。快照将保持锁定状态，直到达到锁定过期日期为止。当达到锁定过期日期时，会自动解锁快照。

冷静期

冷静期是一个可选的时期，可以在合规模式下锁定快照时指定此时期。在冷静期内，拥有适当权限的用户可以解锁快照、更改锁定模式、延长或缩短冷静期以及延长或缩短锁定持续时间。当冷静期过期之后，无论用户拥有何种权限，都无法解锁快照、更改锁定模式、恢复冷静期或缩短锁定持续时间。

在冷静期内，无法删除快照。

如果指定了冷静期，则冷静期将在您锁定快照之后立即开始。如果省略了冷静期，则会立即在合规模式下锁定快照而不设冷静期。

冷静期介于 1 到 72 小时不等。要在合规模式下立即锁定快照而不设冷静期，请勿在请求中指定冷静期。

锁定状态

快照锁定可处于以下几种状态之一：

- `compliance-cooloff` – 已在合规模式下锁定快照，但它仍处于冷静期内。无法删除快照，但可以将它解锁，而且拥有适当权限的用户可以修改锁定设置。
- `governance` – 已在监管模式下锁定快照。无法删除快照，但可以将它解锁，而且拥有适当权限的用户可以修改锁定设置。
- `compliance` – 已在合规模式下锁定快照，且未设冷静期或者冷静期已过期。无法解锁或删除快照。只有拥有适当权限的用户才能延长锁定时间。
- `expired` – 已在合规或监管模式下锁定快照，但锁定已过期。未锁定快照，可以将其删除。

Amazon EBS 快照锁定的注意事项

锁定 Amazon EBS 快照时请记住以下事项。

- 只有当快照处于 `pending` 或 `completed` 状态时，才能将其锁定。
  - 如果在快照处于 `pending` 状态时将其锁定，并且将其锁定特定的持续时间，将只在快照达到 `completed` 状态时开始计算锁定持续时间。当快照处于 `pending` 状态时无法将其删除。
  - 如果在快照处于 `pending` 状态时将其锁定，但由于任何原因导致创建快照失败，锁定将被取消。
- 如果在冷静期过期之后延长了在合规模式下锁定的快照的锁定持续时间，将无法指定另一个冷静期。如果指定了冷静期，请求将失败。
- 您可以锁定已归档的快照。您可以存档已锁定的快照。
- 您可以锁定与 AMI 相关联的快照。
- 您可以取消注册具有已锁定的关联快照的 AMI。
- 您可以删除用来加密已锁定的快照的 KMS 密钥。
- 我们建议您不要锁定由创建的快照 Amazon Backup。 Amazon Backup 已经确保其快照在保留期到期之前不会被删除。要为由管理的快照添加额外的安全层 Amazon Backup，我们建议您使用 Amazon Backup 文件库锁定。有关更多信息，请参阅 Amazon Backup Vault Lock。
- 在创建快照期间或 AMI 注册期间，无法锁定快照。

- 您无法在 Amazon Outposts上锁定本地 Amazon EBS 快照。
- 要删除在锁定到期前锁定在合规模式下的快照，唯一的方法是关闭关联的 Amazon 账户。

  如果您在锁定快照时关闭 Amazon 帐户，则会在快照完好无损的情况下 Amazon 暂停您的帐户 90 天。如果您未在 90 天内重新打开账户，即使快照已被锁定，也会 Amazon 将其删除。

控制对 Amazon EBS 快照锁定的访问

默认情况下，用户无权使用快照锁定。要允许用户使用快照锁定，您必须创建 IAM policy，以授予使用特定资源和 API 操作的权限。有关更多信息，请参阅《IAM 用户指南》中的创建 IAM policy。

主题

- 所需的权限
- 使用条件键限制访问

所需的权限

要使用快照锁定，用户需要以下权限。

- `ec2:LockSnapshot` – 锁定快照。
- `ec2:UnlockSnapshot` – 解锁快照。
- `ec2:DescribeLockedSnapshots` – 查看快照锁定设置。

以下是一个示例 IAM policy，它授权用户锁定和解锁快照以及查看快照锁定设置。其包括控制台用户的 `ec2:DescribeSnapshots` 权限。如果不需要某些上述权限，您可以从策略中将其删除。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "ec2:LockSnapshot",
            "ec2:UnlockSnapshot",
            "ec2:DescribeLockedSnapshots",
            "ec2:DescribeSnapshots"
        ]
    }]
}
```

要提供访问权限，请为您的用户、组或角色添加权限：

- 通过身份提供商在 IAM 中托管的用户：

  创建适用于身份联合验证的角色。按照《IAM 用户指南》中针对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 用户：
  - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
  - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

使用条件键限制访问

可以使用条件键限制如何允许用户锁定快照。

主题

- ec2: SnapshotLockDuration
- ec2: CoolOffPeriod

ec2: SnapshotLockDuration

当锁定快照时，可以使用 `ec2:SnapshotLockDuration` 条件键将用户限制在特定的锁定持续时间内。

如下示例策略将禁止用户指定一个介于 10 到 50 天之间的锁定持续时间。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:LockSnapshot",
      "Resource": "arn:aws:ec2:region::snapshot/*"
      "Condition": {
        "NumericGreaterThan" : {
          "ec2:SnapshotLockDuration" : 10
        }
        "NumericLessThan":{
          "ec2:SnapshotLockDuration": 50
```

```
        }
      }
    }
  ]
}
```

ec2: CoolOffPeriod

可以使用 `ec2:CoolOffPeriod` 条件键防止用户在未设冷静期的情况下在合规模式下锁定快照。

如下示例策略将禁止用户在合规模式下锁定快照时指定超过 48 小时的冷静期。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:LockSnapshot",
      "Resource": "arn:aws:ec2:region::snapshot/*"
      "Condition": {
        "NumericGreaterThan": {
          "ec2:CoolOffPeriod": 48
        }
      }
    }
  ]
}
```

锁定 Amazon EBS 快照

您可以锁定处于 `pending` 或 `completed` 状态的快照。有关更多信息，请参阅 Amazon EBS 快照锁定的注意事项。

Console

要锁定一个快照

1. 打开亚马逊 EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择快照。
3. 选择要锁定的快照，然后选择操作、快照设置、管理快照锁定。
4. 选择锁定快照。

5. 对于锁定模式，选择监管模式或合规模式。有关更多信息，请参阅 锁定模式。
6. 对于锁定持续时间，执行以下操作之一：

   - 要将快照锁定一个特定的时期，请选择锁定快照，然后以天或年为单位输入此时期。
   - 要将快照锁定到特定的日期和时间，请选择锁定快照直到，然后选择过期日期和时间。

   有关更多信息，请参阅 锁定持续时间。
7. （仅限合规模式）对于冷静期，请指定一个冷静期，在此期间内可以解锁快照和修改锁定配置。有关更多信息，请参阅 冷静期。
8. （仅限合规模式）要确认您希望在合规模式下锁定快照，而且在冷静期过期后将无法解锁快照，请选择确认。
9. 选择保存锁定设置。

Amazon CLI

要在监管模式下锁定快照

使用锁定快照命令。对于 `--lock-mode`，请指定 `governance`。要在特定时间段内锁定快照`--lock-duration`，请指定以天为单位的时段。

```
aws ec2 lock-snapshot \
    --snapshot-id snap-0abcdef1234567890 \
    --lock-mode governance \
    --lock-duration 30
```

要将快照锁定到特定日期`--expiration-date`，请在 UTC 时区中指定锁定必须到期的日期和时间。

```
aws ec2 lock-snapshot \
    --snapshot-id snap-0abcdef1234567890 \
    --lock-mode governance \
    --expiration-date YYYY-MM-DDThh:mm:ss.sssZ
```

要在合规模式下锁定快照

使用锁定快照命令。对于 `--lock-mode`，请指定 `compliance`。对于`--cool-off-period`，可以选择指定冷静期（以小时为单位）。要在特定时间段内锁定快照`--lock-duration`，请为其指定锁定快照的天数。

```
aws ec2 lock-snapshot \
    --snapshot-id snap-0abcdef1234567890 \
    --lock-mode compliance \
    --cool-off-period 24 \
    --lock-duration 30
```

要将快照锁定到特定日期--expiration-date，请在 UTC 时区中指定锁定必须到期的日期和时间。

```
aws ec2 lock-snapshot \
    --snapshot-id snap-0abcdef1234567890 \
    --lock-mode compliance \
    --expiration-date YYYY-MM-DDThh:mm:ss.sssZ
```

PowerShell

要在监管模式下锁定快照

使用 Lock-EC2Snapshot cmdlet。您可以选择指定快照锁的持续时间（以天为单位）。

```
Lock-EC2Snapshot `
    -SnapshotId snap-0abcdef1234567890 `
    -LockMode "governance" `
    -LockDuration 30
```

或者，您可以将快照锁定到特定日期（UTC 时区）。

```
Lock-EC2Snapshot `
    -SnapshotId snap-0abcdef1234567890 `
    -LockMode "governance" `
    -ExpirationDate YYYY-MM-DDThh:mm:ss.sssZ
```

要在合规模式下锁定快照

使用 Lock-EC2Snapshot cmdlet。您可以选择指定冷静期，以小时为单位。您也可以选择指定快照锁的持续时间（以天为单位）。

```
Lock-EC2Snapshot `
    -SnapshotId snap-0abcdef1234567890 `
```

```
    -LockMode "compliance" `
    -CoolOffPeriod 24 `
    -LockDuration 30
```

或者，您可以将快照锁定到特定日期（UTC 时区）。

```
Lock-EC2Snapshot `
    -SnapshotId snap-0abcdef1234567890 `
    -LockMode "compliance" `
    -ExpirationDate YYYY-MM-DDThh:mm:ss.sssZ
```

解锁 Amazon EBS 快照

只有当在监管模式下锁定了快照，或者在合规模式下锁定了快照且快照仍处于冷静期内时，才能解锁快照。

Console

解锁快照

1. 打开亚马逊 EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择快照。
3. 选择要解锁的快照，然后选择操作、快照设置、管理快照锁定。
4. 选择解锁快照，然后再次选择解锁快照进行确认。

Amazon CLI

要解锁快照

使用解锁快照命令。

```
aws ec2 unlock-snapshot --snapshot-id snap-0abcdef1234567890
```

PowerShell

解锁快照

使用 Unlock-EC2Snapshot cmdlet。

```
Unlock-EC2Snapshot -SnapshotId snap-0abcdef1234567890
```

更新 Amazon EBS 快照锁定设置

允许的更新取决于锁定状态：

- governance – 您可以更改锁定模式以及延长或缩短锁定持续时间或过期日期。
- compliance-cooloff – 您可以更改锁定模式、延长或缩短冷静期以及延长或缩短锁定持续时间或过期日期。
- compliance – 您只能延长锁定持续时间或过期日期。

Console

要更新快照锁定设置

1. 打开亚马逊 EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择快照。
3. 选择要为其修改锁定设置的快照，然后选择操作、快照设置、管理快照锁定。
4. 根据需要更新设置，然后选择保存锁定设置。

Amazon CLI

要更新快照锁定设置

使用锁定快照命令。指定快照的 ID 和要修改的选项。以下示例更改了到期日期。

```
aws ec2 lock-snapshot \
    --snapshot-id snap-0abcdef1234567890 \
    --lock-mode governance \
    --expiration-date YYYY-MM-DDThh:mm:ss.sssZ
```

PowerShell

要更新快照锁定设置

使用 Lock-EC2Snapshot cmdlet。指定快照的 ID 和要修改的选项。以下示例更改了到期日期。

```
Lock-EC2Snapshot `
```

```
    -SnapshoId snap-0abcdef1234567890 `
    -LockMode "governance" `
    -ExpirationDate YYYY-MM-DDThh:mm:ss.sssZ
```

监控 Amazon EBS 快照锁定

您可以使用以下工具监控与 Amazon EBS 快照锁定相关的操作：

主题

- 使用监控亚马逊 EBS 快照锁定 Amazon CloudTrail
- 使用亚马逊监控亚马逊 EBS 快照锁定 EventBridge

使用监控亚马逊 EBS 快照锁定 Amazon CloudTrail

您可以将快照锁定的 API 调用作为事件进行监控，包括来自控制台的调用和对的代码调用 APIs。使用收集到的信息 CloudTrail，您可以确定发出的请求、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。

有关更多信息，请参阅使用记录 API 调用 Amazon CloudTrail。

使用亚马逊监控亚马逊 EBS 快照锁定 EventBridge

Amazon EBS 发出与快照锁定操作相关的事件。您可以使用 Amazon Lambda 和 Amazon EventBridge 以编程方式处理事件通知。尽最大努力发出事件。有关更多信息，请参阅 Amazon EventBridge 用户指南。

系统将发出以下事件：

- 成功在监管或合规模式下锁定快照。

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef"
```

```
  ],
  "detail": {
    "event": "lockSnapshot",
    "result": "succeeded",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef",
    "source": 012345678901,
    "lockState": "compliance-cooloff",
    "lockCreatedOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockExpiresOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockDuration": 123,
    "lockStartDurationTime": "yyyy-mm-ddThh:mm:ssZ",
    "cooOffPeriod": 24,
    "coolOffPeriodExpiresOn": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

- 当快照处于 pending 状态且被锁定时，锁定事件失败，而且快照无法达到 completed 状态。

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "lockSnapshot",
    "result": "failed",
    "cause": "snapshot failed",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef",
    "lockState": "pending-compliance",
    "lockCreatedOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockDuration": 123,
    "lockStartDurationTime": "yyyy-mm-ddThh:mm:ssZ",
    "cooOffPeriod": 24,
    "coolOffPeriodExpiresOn": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

- 锁定已过期

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "lockDurationExpiry",
    "result": "succeeded",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef",
    "lockState": "expired",
    "lockCreatedOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockExpiresOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockDuration": 123
  }
}
```

- 在合规模式下锁定之后，冷静期已过期。

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef"
  ],
  "detail": {
    "event": "cooloffperiodExpiry",
    "result": "succeeded",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567890abcdef",
    "lockState": "compliance",
    "lockCreatedOn": "yyyy-mm-ddThh:mm:ssZ",
    "lockExpiresOn": "yyyy-mm-ddThh:mm:ssZ",
```

```
    "lockDuration": 123,
    "lockStartDurationTime": "yyyy-mm-ddThh:mm:ssZ",
    "cooOffPeriod": 24,
    "coolOffPeriodExpiresOn": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

阻止 Amazon EBS 快照的公开访问

要防止公开共享您的快照，您可以启用阻止公开访问快照。在为一个区域阻止公开访问快照之后，将自动阻止任何尝试在此区域公开共享快照的行为。这样可以帮助您提高快照的安全性，并保护您的快照数据免遭未经授权的访问或意外访问。

可以在两种模式之一中阻止公开访问快照：

- 阻止所有共享 – 阻止所有公开共享快照的行为。此账户中的用户无法请求新的公开共享。此外，已公开共享的快照将被视为私有快照，且不可公开访问。
- 阻止新共享 – 仅阻止对快照进行公开共享的新行为。此账户中的用户无法请求新的公开共享。不过，已经公开共享的快照仍可公开访问。

注意事项

在使用阻止快照公开访问功能时，请记住以下事项。

- 阻止公开访问快照并不会阻止共享私有快照。
- 如果在阻止所有共享模式下启用阻止快照公开访问，则不会更改对已公开共享的快照的权限。实际上，它会阻止这些快照公开可见和可公开访问。因此，这些快照的属性仍然表明它们是公开共享的，尽管它们不可公开访问。

  如果您稍后禁用阻止公开访问或更改模式以阻止新共享，则这些快照将再次公开可用。
- 阻止公开访问快照是一个区域性设置。它适用于启用了此功能的区域中的所有快照。您需要在希望阻止公开共享快照的每个区域中启用阻止公开访问快照。
- 阻止公开访问是一个账户级别的设置。它适用于账户中的所有用户，包括管理员用户。您无法在组织级别启用阻止公开访问快照。
- 封锁公共访问设置可以直接在账户中配置，也可以使用声明性策略进行配置。使用声明式策略可同时将设置应用于多个区域，也可以同时应用于多个账户。当使用声明式策略时，您无法直接在账户中

修改设置。本主题介绍如何直接在账户中配置设置。有关使用声明式策略的信息，请参阅《Amazon Organizations User Guide》中的 Declarative policies。

- 阻止对快照的公开访问不会阻止公开共享 EBS AMIs 支持的内容。如果您启用了对快照的封锁公共访问，用户仍然可以公开共享 EBS 支持的内容 AMIs。如果公开共享由 EBS 支持的 AMI，有权访问此 AMI 的用户可以从与它关联的快照创建卷。要防止公开共享您的 AMIs，请启用 “阻止公共访问” AMIs。
- 开启本地快照后，不支持对快照进行公开访问 Amazon Outposts。

定价

可以阻止公开访问快照，无需支付额外的费用。

目录

- 用于阻止 Amazon EBS 快照公开访问的 IAM 权限
- 配置阻止 Amazon EBS 快照的公开访问
- 查看阻止 Amazon EBS 快照公开访问设置
- 禁用阻止 Amazon EBS 快照公开访问
- 使用监控对 Amazon EBS 快照的封锁公开访问 EventBridge

用于阻止 Amazon EBS 快照公开访问的 IAM 权限

默认情况下，用户无权阻止公开访问快照。要允许用户使用“阻止公开访问快照”，您必须创建 IAM policy，以授权使用特定 API 操作。创建策略后，必须向您的用户、组或角色添加权限。

要阻止公开访问快照，用户需要拥有以下权限。

- `ec2:EnableSnapshotBlockPublicAccess` – 启用阻止公开访问快照以及修改此模式。
- `ec2:DisableSnapshotBlockPublicAccess` – 禁用阻止公开访问快照。
- `ec2:GetSnapshotBlockPublicAccessState` – 查看一个区域的阻止公开访问快照设置。

以下是 IAM policy 示例。如果不需要某些上述权限，您可以从策略中将其删除。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
```

```
        "Action": [
            "ec2:EnableSnapshotBlockPublicAccess",
            "ec2:DisableSnapshotBlockPublicAccess",
            "ec2:GetSnapshotBlockPublicAccessState"
        ],
        "Resource": "*"
    }]
}
```

要提供访问权限，请为您的用户、组或角色添加权限：

- 通过身份提供商在 IAM 中托管的用户：

  创建适用于身份联合验证的角色。按照《IAM 用户指南》中针对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 用户：
  - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
  - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

配置阻止 Amazon EBS 快照的公开访问

启用阻止公开访问快照，以防止在此区域中公开共享快照。启用此功能之后，将阻止在此区域中公开共享快照的请求。

Important

如果在阻止所有共享模式下启用阻止快照公开访问，则不会更改对已公开共享的快照的权限。实际上，它会阻止这些快照公开可见和可公开访问。因此，这些快照的属性仍然表明它们是公开共享的，尽管它们不可公开访问。
如果您稍后禁用阻止公开访问或更改模式以阻止新共享，则这些快照将再次公开可用。

Note

此设置是在账户级别配置，可以直接在账户中配置，也可以使用声明式策略进行配置。必须在要防止公开共享快照的每个 Amazon Web Services 区域 位置进行配置。使用声明式策略可同时将设置应用于多个区域，也可以同时应用于多个账户。当使用声明式策略时，您无法直接在

账户中修改设置。本主题介绍如何直接在账户中配置设置。有关使用声明式策略的信息，请参阅《Amazon Organizations User Guide》中的 Declarative policies。

Console

要配置阻止公开访问快照

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择EC2 控制面板，然后在账户属性（右侧）中，选择数据保护和安全。
3. 在阻止公开访问 EBS 快照部分中，选择管理。
4. 选择阻止公开访问，然后选择以下选项之一：
   - 阻止所有公开访问 – 阻止所有公开共享快照的行为。此账户中的用户无法请求新的公开共享。此外，已公开共享的快照将被视为私有快照，且不可公开访问。
   - 阻止新的公开共享 – 仅阻止公开共享快照的新行为。此账户中的用户无法请求新的公开共享。不过，已经公开共享的快照仍可公开访问。
5. 选择更新。

Amazon CLI

要启用或修改阻止公开访问快照

使用 enable-snapshot-block-public-access 命令。对于 `--state`，请指定下列值之一：

- `block-all-sharing` – 阻止所有公开共享快照的行为。此账户中的用户无法请求新的公开共享。此外，已公开共享的快照将被视为私有快照，且不可公开访问。
- `block-new-sharing` – 仅阻止公开共享快照的新行为。此账户中的用户无法请求新的公开共享。不过，已经公开共享的快照仍可公开访问。

为特定区域启用或修改阻止快照公开访问

```
aws ec2 enable-snapshot-block-public-access \
    --state block-new-sharing \
    --region us-east-1
```

下面是示例输出。

```
{
    "State": "block-new-sharing"
}
```

为所有区域启用或修改阻止快照公开访问

```
echo -e "Region   \t Public Access State" ; \
echo -e "-------------- \t ----------------------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 enable-snapshot-block-public-access \
            --region $region \
            --state block-new-sharing \
            --output text)
        echo -e "$region \t $output"
    );
done
```

下面是示例输出。

```
Region           Public Access State
--------------   ----------------------
ap-south-1       block-new-sharing
eu-north-1       block-new-sharing
eu-west-3        block-new-sharing
...
```

PowerShell

要启用或修改阻止公开访问快照

使用 Enable-EC2SnapshotBlockPublicAccess 命令。对于 `-State`，请指定下列值之一：

- `block-all-sharing` – 阻止所有公开共享快照的行为。此账户中的用户无法请求新的公开共享。此外，已公开共享的快照将被视为私有快照，且不可公开访问。
- `block-new-sharing` – 仅阻止公开共享快照的新行为。此账户中的用户无法请求新的公开共享。不过，已经公开共享的快照仍可公开访问。

为特定区域启用或修改阻止快照公开访问

```
Enable-EC2SnapshotBlockPublicAccess `
    -Region us-east-1 `
    -State block-new-sharing
```

下面是示例输出。

```
Value
-----
block-new-sharing
```

为所有区域启用或修改阻止快照公开访问

```
(Get-EC2Region -Region us-east-1).RegionName | `
    ForEach-Object {
    [PSCustomObject]@{
        Region            = $_
        PublicAccessState = (
            Enable-EC2SnapshotBlockPublicAccess `
                -Region $_ `
                -State block-new-sharing)
    }
} | Format-Table -AutoSize
```

下面是示例输出。

```
Region         PublicAccessState
------         -----------------
ap-south-1     block-new-sharing
eu-north-1     block-new-sharing
eu-west-3      block-new-sharing
...
```

查看阻止 Amazon EBS 快照公开访问设置

对于您账户中的每个区域，阻止公开访问可能处于以下状态之一。

- 阻止所有共享 – 阻止所有公开共享快照的行为。此账户中的用户无法请求新的公开共享。此外，已经公开共享的快照将被视为私有快照，且不可公开访问。

- 阻止新共享 – 仅阻止公开共享快照的新行为。此账户中的用户无法请求新的公开共享。不过，已经公开共享的快照仍可公开访问。
- 未阻止 – 未阻止公开共享。用户可以公开共享快照。

Console

要查看用来阻止公开访问快照的设置

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择EC2 控制面板，然后在账户属性（右侧）中，选择数据保护和安全。
3. 阻止公开访问 EBS 快照部分会显示当前设置。

Amazon CLI

要查看用来阻止公开访问快照的设置

使用 get-snapshot-block-public-access-stat e 命令。

- 对于特定区域

```
aws ec2 get-snapshot-block-public-access-state
```

在此示例输出中，该ManagedBy字段表示配置该设置的实体，并account表示该设置是直接在账户中配置的。值为 declarative-policy 表示该设置是由声明式策略所配置。有关更多信息，请参阅《Amazon Organizations User Guide》中的 Declarative policies。

```
{
    "State": "unblocked",
    "ManagedBy": "account"
}
```

- 对于所有区域

```
echo -e "Region   \t Public Access State" ; \
echo -e "-------------- \t ----------------------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
```

```
        --output text
    );
    do (output=$(
        aws ec2 get-snapshot-block-public-access-state \
            --region $region \
            --output text)
        echo -e "$region \t $output"
    );
done
```

下面是示例输出。

```
Region           Public Access State
--------------   ----------------------
ap-south-1       unblocked
eu-north-1       unblocked
eu-west-3        unblocked
```

PowerShell

要查看用来阻止公开访问快照的设置

使用 Get-EC2SnapshotBlockPublicAccessStatecmdlet。

- 对于特定区域

```
Get-EC2SnapshotBlockPublicAccessState -Region us-east-1
```

下面是示例输出。

```
Value
-----
block-new-sharing
```

- 对于所有区域

```
(Get-EC2Region -Region us-east-1).RegionName | `
    ForEach-Object {
    [PSCustomObject]@{
        Region            = $_
        PublicAccessState = (Get-EC2SnapshotBlockPublicAccessState -Region $_)
```

```
    }
} | Format-Table -AutoSize
```

下面是示例输出。

```
Region           Public Access State
--------------   ----------------------
ap-south-1       unblocked
eu-north-1       unblocked
eu-west-3        unblocked
...
```

禁用阻止 Amazon EBS 快照公开访问

禁用阻止公开访问快照，以允许在此区域中公开共享快照。禁用此功能之后，用户可以在此区域公开共享快照。

Important

如果在阻止所有共享模式下启用阻止快照公开访问，则不会更改对已公开共享的快照的权限。实际上，它会阻止这些快照公开可见和可公开访问。因此，这些快照的属性仍然表明它们是公开共享的，尽管它们不可公开访问。
如果禁用阻止公开访问，则这些快照将再次公开可用。

Note

此设置是在账户级别配置，可以直接在账户中配置，也可以使用声明式策略进行配置。必须在每个要允许公开共享快照 Amazon Web Services 区域 的地方进行配置。使用声明式策略可同时将设置应用于多个区域，也可以同时应用于多个账户。当使用声明式策略时，您无法直接在账户中修改设置。本主题介绍如何直接在账户中配置设置。有关使用声明式策略的信息，请参阅《Amazon Organizations User Guide》中的 Declarative policies。

Console

禁用快照的屏蔽公共访问权限

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择EC2 控制面板，然后在账户属性（右侧）中，选择数据保护和安全。
3. 在阻止公开访问 EBS 快照部分中，选择管理。
4. 清除阻止公开访问，然后选择更新。

Amazon CLI

要禁用阻止公开访问快照

使用 disable-snapshot-block-public-access 命令。

- 对于特定区域

```
aws ec2 disable-snapshot-block-public-access --region us-east-1
```

下面是示例输出。

```
{
    "State": "unblocked"
}
```

- 对于所有区域

```
echo -e "Region   \t Public Access State" ; \
echo -e "-------------- \t ----------------------" ; \
for region in $(
    aws ec2 describe-regions \
        --region us-east-1 \
        --query "Regions[*].[RegionName]" \
        --output text
    );
    do (output=$(
        aws ec2 disable-snapshot-block-public-access \
            --region $region \
            --output text)
        echo -e "$region \t $output"
    );
```

```
done
```

下面是示例输出。

```
Region           Public Access State
--------------   ----------------------
ap-south-1       unblocked
eu-north-1       unblocked
eu-west-3        unblocked
```

PowerShell

禁用快照的屏蔽公共访问权限

使用 Disable-EC2SnapshotBlockPublicAccesscmdlet。

- 对于特定区域

```
Disable-EC2SnapshotBlockPublicAccess -Region us-east-1
```

下面是示例输出。

```
Value
-----
unblocked
```

- 对于所有区域

```
(Get-EC2Region -Region us-east-1).RegionName | `
    ForEach-Object {
    [PSCustomObject]@{
        Region            = $_
        PublicAccessState = (Disable-EC2SnapshotBlockPublicAccess -Region $_)
    }
} | `
Format-Table -AutoSize
```

下面是示例输出。

```
Region         PublicAccessState
```

```
------          -----------------
ap-south-1      unblocked
eu-north-1      unblocked
eu-west-3       unblocked
...
```

使用监控对 Amazon EBS 快照的封锁公开访问 EventBridge

Amazon EBS 将发出与阻止公开访问快照相关的事件。您可以使用 Amazon Lambda 和 Amazon EventBridge 以编程方式处理事件通知。尽最大努力发出事件。有关更多信息，请参阅 Amazon EventBridge 用户指南。

系统将发出以下事件：

- 在“阻止所有共享”模式下，启用阻止公开访问快照

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Block Public Access Enabled",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2019-05-31T21:49:54Z",
  "region": "us-east-1",
  "detail": {
    "SnapshotBlockPublicAccessState": "block-all-sharing",
    "message": "Block Public Access was successfully enabled in 'block-all-sharing'
 mode"
  }
}
```

- 在“阻止新共享”模式下，启用阻止公开访问快照

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Block Public Access Enabled",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2019-05-31T21:49:54Z",
  "region": "us-east-1",
  "detail": {
```

```
    "SnapshotBlockPublicAccessState": "block-new-sharing",
    "message": "Block Public Access was successfully enabled in 'block-new-sharing'
 mode"
  }
}
```

- 禁用阻止公开访问快照

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Block Public Access Disabled",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2019-05-31T21:49:54Z",
  "region": "us-east-1",
  "detail": {
    "SnapshotBlockPublicAccessState": "unblocked",
    "message": "Block Public Access was successfully disabled"
  }
}
```

Amazon EBS local snapshots on Outposts

Amazon EBS 快照是您的 EBS 卷的 point-in-time副本。

默认情况下，EBS 卷的快照位于 Amazon Outpost 存储在 Amazon S3 中，所在区域为 Outpost。 你也可以在 Outposts 上使用 Amazon EBS 本地快照将卷的快照存储在 Outpost 本地在 Amazon S3 上的 Outpost 本身。这样可以确保快照数据驻留在 Outpost，并在您的办公场所内。此外，您可以使用 Amazon Identity and Access Management (IAM) 策略和权限来设置数据驻留强制政策，以确保快照数据不会离开 Outpost。 如果您居住的国家或地区尚未由某个地区提供服务，并且有数据驻留要求，则 Amazon 此功能特别有用。

此主题提供有关使用 Outposts 上的 Amazon EBS 本地快照 的信息。有关 Amazon EBS 快照和在某个 Amazon 地区使用快照的更多信息，请参阅Amazon EBS 快照。

有关更多信息，请参阅Amazon Outposts 家庭和Amazon Outposts 家庭文档。

主题

- 常见问题

- 先决条件
- 注意事项
- 使用 IAM 控制访问
- 使用本地快照

常见问题

1. 什么是 本地快照？

   默认情况下，Amazon EBS 上各卷的快照 Outpost 存储在 Amazon S3 中，所在区域为 Outpost。如果 Outpost 已在 Outposts 上配置了 S3，你可以选择将快照存储在本地 Outpost 本身。本地快照采用增量更新，这意味着只保存在最新快照之后更改的卷数据块。您可以使用这些快照在同一个卷上还原一个卷 Outpost 随时作为快照。有关 Amazon EBS 快照的更多信息，请参阅 Amazon EBS 快照。

2. 为什么应该使用 本地快照？

   快照是备份数据的便捷方法。使用本地快照时，您的所有快照数据都存储在本地的 Outpost。 这意味着它不会离开您的场所。如果您居住的国家或地区尚未由某个地区提供服务，并且有居留要求，则 Amazon 此功能特别有用。

   此外，使用本地快照可以帮助减少用于区域与区域之间通信的带宽 Outpost 在带宽受限的环境中。

3. 如何在上强制执行快照数据驻留 Outpost?

   您可以使用 Amazon Identity and Access Management (IAM) 策略来控制委托人（Amazon 账户、IAM 用户和 IAM 角色）在处理本地快照时拥有的权限，并强制执行数据驻留。您可以创建阻止委托人从以下位置创建快照的策略 Outpost 卷和实例，并将快照存储在一个 Amazon 区域中。目前，正在从中复制快照和图像 Outpost 不支持到某个区域。有关更多信息，请参阅 使用 IAM 控制访问。

4. 是否支持多卷、崩溃一致性本地快照？

   是的，您可以从上的实例创建多卷、崩溃一致的本地快照 Outpost.

5. 我该如何创建本地快照？

   您可以使用 Amazon Command Line Interface (Amazon CLI) 或 Amazon EC2 控制台手动创建快照。有关更多信息，请参阅使用本地快照。您还可以使用 Amazon Data Lifecycle Manager 自动执行本地快照的生命周期。有关更多信息，请参阅 在上自动执行快照 Outpost。

6. 如果我的，我能否创建、使用或删除本地快照 Outpost 失去与其区域的连接？

   不是。 的 Outpost 必须与其区域建立连接，因为该区域提供对快照运行状况至关重要的访问、授权、日志记录和监控服务。如果没有连接，则您无法创建新的本地快照、创建卷或从现有本地快照实例启动实例，也无法删除本地快照。

7. 删除本地快照多久后 Amazon S3 存储容量可供使用？

   Amazon S3 存储容量在删除引用它们的本地快照和卷后 72 小时内可供使用。

8. 我怎样才能确保我的 Amazon S3 容量不会用完 Outpost?

   我们建议您使用 Amazon CloudWatch 警报来监控您的 Amazon S3 存储容量，并删除不再需要的快照和卷，以免存储容量耗尽。如果您在使用 Amazon Data Lifecycle Manager 自动执行本地快照的生命周期，请确保快照保留策略保留快照的时间不超过所需时长。

9. 如果我的本地 Amazon S3 容量用完了会发生什么 Outpost?

   如果您在 Amazon S3 上用完了本地 Amazon S3 容量 Outpost，Amazon Data Lifecycle Manager 将无法在上成功创建本地快照 Outpost。 Amazon Data Lifecycle Manager 将尝试在上创建本地快照 Outpost，但是快照会立即过渡到`error`状态，它们最终会被 Amazon Data Lifecycle Manager 删除。我们建议您使用 `SnapshotsCreateFailed` Amazon CloudWatch 指标来监控快照生命周期策略，以防快照创建失败。有关更多信息，请参阅 使用监控数据生命周期管理器策略 CloudWatch。

10. 我能否在 Spot 实例和 Spot 队列中使用本地快照并由本地快照提供 AMIs 支持？

    不可以，您不能使用本地快照或由本地快照 AMIs 支持来启动 Spot 实例或 Spot 队列。

11. 我能否在 Amazon A EC2 uto Scaling 中使用本地快照并由本地快照提供 AMIs 支持？

    可以，您可以使用本地快照并由本地快照 AMIs 支持的子网在同一子网中启动 Auto Scaling 组 Outpost 作为快照。Amazon A EC2 uto Scaling 组服务相关角色必须有权使用用于加密快照的 KMS 密钥。

    您不能使用本地快照或由本地快照 AMIs 支持的在 Amazon 区域中启动 Auto Scaling 群组。

先决条件

将快照存储在 Outpost，你必须有一个 Outpost 那是在 Outposts 上用 S3 配置的。有关 Outposts 上的 S3 的更多信息，请参阅 Amaz on S3 on Outposts 用户指南中的 Out post s 上的 S3。

注意事项

使用本地快照时请记住以下事项。

- 这些区域有：Outpost 必须连接到其 Amazon 区域才能使用本地快照。
- 快照元数据存储在与之关联的 Amazon 区域中 Outpost。 这不包括任何快照数据。
- 快照存储在 Outpost 默认情况下已加密。不支持非加密快照。在上创建的快照 Outpost 以及复制到的快照 Outpost 使用该地区的默认 KMS 密钥或您在请求时指定的其他 KMS 密钥进行加密。
- 当您在上创建卷时 Outpost 在本地快照中，您无法使用其他 KMS 密钥重新加密卷。从 本地快照 创建的卷必须使用与源快照相同的 KMS 密钥 进行加密。
- 从中删除本地快照后 Outpost，则删除的快照所使用的 Amazon S3 存储容量将在 72 小时内变为可用。有关更多信息，请参阅 删除本地快照。
- 您无法从中导出本地快照 Outpost.
- 您不能为本地快照启用快速快照还原。
- 本地快照 APIs 不支持 EBS 直接。
- 您无法复制本地快照或 AMIs 从 Outpost 到一个 Amazon 区域，从一个区域 Outpost 到另一个人，或者在一个 Outpost。 但是，您可以将快照从一个 Amazon 区域复制到 Outpost。 有关更多信息，请参阅将快照从一个 Amazon 区域复制到 Outpost。
- 将快照从一个区域复制到某个 Amazon 区域时 Outpost，则数据通过服务链路传输。同时复制多个快照可能会影响上运行的其他服务 Outpost.
- 您不能共享本地快照。
- 您必须使用 IAM policy 来确保满足数据驻留要求。有关更多信息，请参阅使用 IAM 控制访问。
- 本地快照执行增量备份。只保存卷中在最近快照之后发生更改的数据块。每个本地快照都包含将数据（拍摄快照时存在的数据）还原到新 EBS 卷所需的全部信息。有关更多信息，请参阅 Amazon EBS 快照的工作原理。
- 您不能使用 IAM 策略强制执行数据驻留CopySnapshot和CopyImage操作。

使用 IAM 控制访问

您可以使用 Amazon Identity and Access Management (IAM) 策略来控制委托人（Amazon 账户、IAM 用户和 IAM 角色）在处理本地快照时拥有的权限。以下示例策略可用于授予或拒绝对本地快照执行特定操作的权限。

> **Important**
>
> 从中复制快照和图像 Outpost 目前不支持到某个区域。因此，您目前无法使用 IAM 策略强制执行数据驻留CopySnapshot和CopyImage操作。

主题

- 为快照执行数据驻留
- 禁止委托人删除本地快照

为快照执行数据驻留

以下示例策略禁止所有委托人从上的卷和实例创建快照 Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef`并将快照数据存储在 Amazon 区域中。委托人仍然可以创建本地快照。此策略可确保所有快照都保留在 Outpost.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots"
            ],
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
            "Condition": {
                "StringEquals": {
                    "ec2:SourceOutpostArn": "arn:aws:outposts:us-
east-1:123456789012:outpost/op-1234567890abcdef0"
                },
                "Null": {
                    "ec2:OutpostArn": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshot",
```

```
                "ec2:CreateSnapshots"
            ],
            "Resource": "*"
        }
    ]
}
```

禁止委托人删除本地快照

以下示例策略禁止所有委托人删除存储在上的本地快照 Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ec2:DeleteSnapshot"
            ],
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
            "Condition": {
                "StringEquals": {
                    "ec2:OutpostArn": "arn:aws:outposts:us-east-1:123456789012:outpost/
op-1234567890abcdef0"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteSnapshot"
            ],
            "Resource": "*"
        }
    ]
}
```

使用本地快照

下面几节介绍如何使用本地快照。

主题

- 存储快照的规则
- 使用上的卷创建本地快照 Outpost
- AMIs 从本地快照创建
- 将快照从一个 Amazon 区域复制到 Outpost
- AMIs 从一个 Amazon 区域复制到一个 Outpost
- 从本地快照创建卷
- 从由本地快照 AMIs 支持的实例启动
- 删除本地快照
- 在上自动执行快照 Outpost

存储快照的规则

以下规则适用于快照存储：

- 如果卷的最新快照存储在 Outpost，则所有连续的快照都必须存储在同一个快照上 Outpost.
- 如果卷的最新快照存储在某个 Amazon 区域中，则所有连续的快照都必须存储在同一个区域中。要开始从该卷创建本地快照，请执行以下操作：

  1. Amazon 在该区域创建卷的快照。
  2. 将快照复制到 Outpost 来自该 Amazon 地区。
  3. 从本地快照创建新卷：
  4. 将卷连接到上的实例 Outpost.

  对于新卷 Outpost，下一个快照可以存储在 Outpost 或在该 Amazon 地区。然后必须将所有后续快照存储在同一位置。
- 本地快照，包括在上创建的快照 Outpost 并将快照复制到 Outpost 来自某个 Amazon 区域，只能用于在同一区域上创建卷 Outpost.
- 如果您在上创建卷 Outpost 从某个区域的快照中，该新卷的所有连续快照都必须位于同一区域。
- 如果您在上创建卷 Outpost 从本地快照中，该新卷的所有连续快照都必须位于同一快照上 Outpost.

使用上的卷创建本地快照 Outpost

您可以根据自己的卷创建本地快照 Outpost。 你可以选择将快照存储在同一个地方 Outpost 作为源卷，或者在 “区域” 中为 Outpost.

本地快照可用于在同一个上创建卷 Outpost 只有。

有关更多信息，请参阅 创建 Amazon EBS 快照

AMIs 从本地快照创建

您可以使用本地快照和存储在该地区的快照的组合来创建 Amazon 系统映像 (AMIs) Outpost。 例如，如果你有一个 Outpost 在中`us-east-1`，您可以创建一个 AMI，其数据卷由其上的本地快照支持 Outpost，以及由该`us-east-1`区域快照支持的根卷。

> **Note**
>
> - 你不能创建 AMIs 包含存储在多个快照中的备份快照 Outposts.
> - 你目前无法 AMIs 直接从上的实例创建 Outpost 使用 CreateImageAPI 或亚马逊 EC2控制台进行 Outpost.
> - AMIs 由本地快照支持的，可用于在同一快照上启动实例 Outpost 只有。

要在上创建 AMI Outpost 来自某个区域的快照

1. 将快照从该地区复制到 Outpost。 有关更多信息，请参阅将快照从一个 Amazon 区域复制到 Outpost。
2. 使用 Amazon EC2 控制台或 register-image 命令使用上的快照副本创建 AMI Outpost。 有关更多信息，请参阅通过快照创建 AMI。

要在上创建 AMI Outpost 从一个实例上的 Outpost

1. 在上创建实例的快照 Outpost 并将快照存储在 Outpost。 有关更多信息，请参阅创建 Amazon EBS 快照。
2. 使用 Amazon EC2 控制台或 register-image 命令使用本地快照创建 AMI。有关更多信息，请参阅从快照创建 AMI。

在区域中通过实例创建 AMI Outpost

1. 在上创建实例的快照 Outpost 并将快照存储在该区域。有关更多信息，请参阅 使用上的卷创建本地快照 Outpost或 创建 Amazon EBS 快照。
2. 使用亚马逊 EC2 控制台或 regi ster-image 命令使用该地区的快照副本创建 AMI。有关更多信息，请参阅从快照创建 AMI。

将快照从一个 Amazon 区域复制到 Outpost

您可以将快照从一个 Amazon 区域复制到 Outpost。 只有当快照位于的区域时，您才能执行此操作 Outpost。 如果快照位于其他区域，则必须先将快照复制到该区域 Outpost，然后将其从该区域复制到 Outpost.

> **Note**
>
> 您无法从中复制本地快照 Outpost 到一个区域，从一个区域 Outpost 到另一个，或者在同一个之内 Outpost.

有关更多信息，请参阅 复制 Amazon EBS 快照。

AMIs 从一个 Amazon 区域复制到一个 Outpost

您可以 AMIs 从一个 Amazon 地区复制到 Outpost。 当您将 AMI 从一个区域复制到某个区域时 Outpost，所有与 AMI 关联的快照都将从该区域复制到 Outpost.

您可以将 AMI 从一个区域复制到 Outpost 仅当与 AMI 关联的快照位于的区域中时 Outpost。 如果快照位于不同的区域，则必须先将 AMI 复制到该区域 Outpost，然后将其从该区域复制到 Outpost.

> **Note**
>
> 您无法从中复制 AMI Outpost 到一个区域，从一个区域 Outpost 到另一个人，或者在一个 Outpost.

您可以 AMIs 从一个地区复制到 Outpost 仅使用 copy-image Amazon CLI 命令。

从本地快照创建卷

您可以在上创建卷 Outpost 来自本地快照。必须在同一个上创建卷 Outpost 作为源快照。您不能使用本地快照在该地区为以下内容创建卷 Outpost.

从 本地快照 创建卷时，不能使用不同的 KMS 密钥 对卷重新加密。从 本地快照 创建的卷必须使用与源快照相同的 KMS 密钥 进行加密。

有关更多信息，请参阅 创建 Amazon EBS 卷。

从由本地快照 AMIs 支持的实例启动

您可以启动由本地快照支持的实例。 AMIs 您必须在同一个上启动实例 Outpost 作为源 AMI。有关更多信息，请参阅在您的上启动实例 Outpost（在 Amazon Outposts 用户指南中）。

删除本地快照

您可以从中删除本地快照 Outpost。 从中删除快照后 Outpost，则删除的快照所使用的 Amazon S3 存储容量将在删除快照和引用该快照的卷后的 72 小时内变为可用。

由于 Amazon S3 存储容量不会立即可用，因此我们建议您使用亚马逊 CloudWatch 警报来监控您的 Amazon S3 存储容量。应删除不再需要的快照和卷，以避免存储容量耗尽。

有关删除快照的更多信息，请参阅删除快照。

在上自动执行快照 Outpost

您可以创建 Amazon Data Lifecycle Manager 快照生命周期策略，自动创建、复制、保留和删除您的卷和实例的快照 Outpost。 您可以选择是将快照存储在某个区域中，还是将其存储在本地区域 Outpost。此外，您可以自动将在一个 Amazon 区域中创建和存储的快照复制到 Outpost.

下表提供了支持功能的概述。

资源位置	快照目标	跨区域复制		快速快照还原	跨账户共享
		复制到区域	目的 Outpost		
区域	区域	✓	✓	✓	✓
Outpost	区域	✓	✓	✓	✓

Outpost	Outpost	✗	✗	✗	✗

注意事项

- 目前仅支持 Amazon EBS 快照生命周期策略。不支持由 EBS 支持的 AMI 策略和跨账户共享事件策略。
- 如果有策略管理某个区域中卷或实例的快照，则快照将在源资源所在同一区域中创建。
- 如果策略管理卷或实例的快照 Outpost，然后可以在源上创建快照 Outpost，或者为此，在地区里 Outpost.
- 单个策略无法同时管理一个区域的快照和一个区域的快照 Outpost。 如果您需要在某个地区和某个区域上自动创建快照 Outpost，则必须创建单独的策略。
- 在上创建的快照不支持快速快照恢复 Outpost，或者用于复制到的快照 Outpost.
- 在上创建的快照不支持跨账户共享 Outpost.

有关创建可管理本地快照的快照生命周期的更多信息，请参阅自动化快照生命周期。

Local Zones 中的本地快照

Amazon EBS 快照是您的 EBS 卷的 point-in-time副本。

本地区域中 EBS 卷的快照可以存储在同一 Amazon 本地区域的 Amazon S3 中，也可以存储在该本地区域的父区域中。将快照存储在本地区域可以确保快照数据在特定的国家、州或直辖市进行处理和存储，从而帮助您满足数据驻留需求。您还可以使用 IAM 设置数据驻留强制政策，以确保快照数据不会离开本地区域。

Local Zones 非常适合需要个位数毫秒延迟或本地数据处理的应用程序，它使 Amazon 基础设施更靠近最终用户和业务中心。此外，您还可以满足监管和合规性敏感型工作负载的数据驻留要求。有关更多信息，请参阅什么是 L Amazon ocal Zones。

支持 Amazon S3 的本地区域目前支持本地快照。有关更多信息，请参阅 L Amazon ocal Zones 功能。
。

主题

- 常见问题
- 注意事项

- 使用 IAM 控制访问

常见问题

1. Local Zones 中的本地快照是什么？

   本地区域中的本地快照是存储在本地区域的 Amazon S3 中的快照。默认情况下，本地区域中 Amazon EBS 卷的快照存储在父区域的 Amazon S3 中。如果本地区域支持 Amazon S3，则可以选择将快照存储在本地区域中。与 Regi Amazon ons 中的快照一样，Local Zones 中的本地快照是增量的，这意味着仅保存最近一次快照后发生更改的卷块。您可以随时使用这些快照在同一本地区域中恢复 Amazon EBS 卷。

2. 我为什么要使用本地快照？

   使用 Local Zones 中的本地快照通过确保快照数据位于特定地理位置（例如国家、州或直辖市）来满足数据驻留或数据隔离要求。

3. 如何在 Local Zones 中强制执行快照数据驻留？

   您可以使用 Amazon Identity and Access Management (IAM) 策略来控制委托人（Amazon 账户、IAM 用户和 IAM 角色）在 Local Zones 中使用本地快照时所拥有的权限，并强制执行数据驻留。例如，您可以创建一个策略，禁止用户从 Local Zones 中的卷创建快照并将这些快照存储在某个 Amazon 区域中。有关更多信息，请参阅 使用 IAM 控制访问。

4. 是否支持多卷、崩溃一致的本地快照？

   是的，您可以从本地区域中的实例在 Local Zones 中创建多卷、崩溃一致的本地快照。

5. 如何在 Local Zones 中创建本地快照？

   您可以使用 Amazon CLI 或 Amazon EC2 控制台在 Local Zones 中手动创建本地快照。有关更多信息，请参阅创建 EBS 卷的快照。您还可以使用 Amazon Data Lifecycle Manager 自动调整本地区域中本地快照的生命周期。有关更多信息，请参阅为 EBS 快照创建 Amazon Data Lifecycle Manager 自定义策略。

6. 我能否在 Local Zones 中复制本地快照？

   不，您目前无法将快照从一个区域复制到本地区域、从一个本地区域复制到一个区域，或者从一个本地区域复制到另一个本地区域。

7. 如何从 Local Zones 中的本地快照中恢复数据？

   您只能使用本地区域中的本地快照在同一个本地区域中创建 Amazon EBS 卷。

8. Local Zones 中的本地快照是如何加密的？

   默认情况下，本地快照可以解密或加密。默认加密时，本地快照使用与源 Amazon EBS 卷相同的 Amazon KMS 密钥进行加密。从本地快照创建卷时，无法使用其他 KMS 密钥重新加密该卷。从本地快照创建的卷必须使用与源快照相同的 Amazon KMS 密钥进行加密。

9. 我能否在 Local Zones 中 AMIs 使用本地快照创建 EBS 支持？

   不，您目前无法在 Local Zones 中 AMIs 使用本地快照创建 EBS 支持。

10. 我能否在 Local Zones 中共享本地快照？

    可以，您可以与其他已在其账户中启用本地区域的 Amazon 账户共享 Local Zones 中的本地快照。

11. 我能否创建卷的本地快照，然后切换到在父区域创建快照？

    不可以，在创建卷的本地快照后，您无法在父区域中连续创建该卷的快照。由于所有快照都是增量快照，因此如果卷的最新快照是本地快照，则该卷的所有连续快照都必须是本地快照。

注意事项

在 Local Zones 中使用本地快照时，请记住以下几点。

- 支持 Amazon S3 的本地区域目前支持本地快照。
- 以下功能不能与 Local Zones 中的本地快照一起使用：
  - 虚拟机导入/导出操作
  - 快速快照还原
  - EBS 直播 APIs
  - 回收站
  - 快照存档
- 您必须使用 IAM 策略来强制执行您的数据驻留要求。有关更多信息，请参阅 使用 IAM 控制访问。
- 如果卷的最新快照是本地快照，则所有连续的快照都必须是本地快照。同样，如果卷的最新快照存储在某个 Amazon 区域中，则所有连续的快照都必须存储在同一个区域中。

使用 IAM 控制访问

您可以使用 Amazon Identity and Access Management (IAM) 策略来控制委托人（Amazon 账户、IAM 用户和 IAM 角色）在 Local Zones 中使用本地快照时所拥有的权限。以下是示例策略，您可以使用这些策略来授予或拒绝对 Local Zones 中的本地快照执行特定操作的权限。

主题

- 在 Local Zones 中强制本地快照的数据驻留
- 防止在 Local Zones 中共享本地快照
- 防止委托人删除 Local Zones 中的本地快照

在 Local Zones 中强制本地快照的数据驻留

以下示例策略限制用户只能在 Local Zones 中使用本地区域中的卷和实例创建本地快照。它可以防止用户在区域中使用本地区域中的卷和实例创建快照。

```
{
    "Version": "2012-10-17",
    "Statement":
    [
        {
            "Effect": "Deny",
            "Action":
            [
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots"
            ],
            "Resource": "*",
            "Condition":
            {
                "StringEquals":
                {
                    "ec2:Location": "regional",
                    "ec2:SourceAvailabilityZone": "local_zone"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action":
            [
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots"
            ],
            "Resource": "*",
            "Condition":
            {
```

```
                "StringEquals":
                {
                    "ec2:SourceAvailabilityZone": "local_zone"
                },
                "Null":
                {
                    "ec2:Location": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action":
            [
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots"
            ],
            "Resource": "*"
        }
    ]
}
```

防止在 Local Zones 中共享本地快照

以下示例策略禁止所有用户共享 Local Zones 中的本地快照。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ec2:ModifySnapshotAttribute"
            ],
            "Resource": "arn:aws:ec2:region::snapshot/*",
            "Condition": {
                "StringEquals": {
                    "ec2:AvailabilityZone": "local_zone"
                }
            }
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "ec2:ModifySnapshotAttribute"
            ],
            "Resource": "*"
        }
    ]
}
```

防止委托人删除 Local Zones 中的本地快照

以下示例策略禁止所有用户删除 Local Zones 中的本地快照。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ec2:DeleteSnapshot"
            ],
            "Resource": "arn:aws:ec2:region::snapshot/*",
            "Condition": {
                "StringEquals": {
                    "ec2:AvailabilityZone": "local_zone"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteSnapshot"
            ],
            "Resource": "*"
        }
    ]
}
```

Amazon EBS 加密

使用 Amazon EBS 加密作为与亚马逊实例关联的 Amazon EBS 资源的直接加密解决方案。 EC2 借助 Amazon EBS 加密，您无需构建、维护和保护自己的密钥管理基础设施。创建加密卷和快照时，Amazon EBS 加密使用 Amazon KMS keys 。

加密操作发生在托管 EC2 实例的服务器上，从而确保两者的安全， data-at-rest以及实例 data-in-transit与其连接的 EBS 存储之间的安全。

您可以同时将加密卷和未加密卷附加到实例。所有亚马逊 EC2 实例类型都支持 Amazon EBS 加密。

内容

- Amazon EBS 加密的工作原理
- Amazon EBS 加密要求
- 默认启用 Amazon EBS 加密
- 加密 EBS 资源
- 轮换用于 Amazon EBS 加密的 Amazon KMS 密钥
- Amazon EBS 加密示例

Amazon EBS 加密的工作原理

您可以加密 EC2 实例的启动卷和数据卷。

在创建加密的 EBS 卷并将其附加到支持的实例类型后，将对以下类型的数据进行加密：

- 卷中的静态数据
- 在卷和实例之间移动的所有数据
- 从卷创建的所有快照
- 从这些快照创建的所有卷

Amazon EBS 通过数据密钥使用行业标准的 AES-256 数据加密来加密卷。数据密钥由生成， Amazon KMS 然后 Amazon KMS 用 Amazon KMS 密钥加密，然后与您的卷信息一起存储。Amazon EBS 会在您创建亚马逊 EBS 资源的每个区域自动创建唯一 Amazon 托管式密钥 的。KMS 密钥的别名是 `aws/ebs`。默认情况下，Amazon EBS 使用此 KMS 密钥 进行加密。或者，您可以使用自己创建的对称客

户管理加密密钥。使用您自己的 KMS 密钥 可以提高灵活性，包括提供创建、轮换和禁用 KMS 密钥 的能力。

Amazon EC2 Amazon KMS 与您合作加密和解密您的 EBS 卷的方式略有不同，具体取决于您创建加密卷时使用的快照是加密还是未加密。

快照加密时 EBS 加密的工作原理

当您使用自己拥有的加密快照创建加密卷时，Amazon 会按 EC2如下方式 Amazon KMS 对您的 EBS 卷进行加密和解密：

1. Amazon EC2 向发送GenerateDataKeyWithoutPlaintext请求 Amazon KMS，指定您为批量加密选择的 KMS 密钥。
2. 如果使用与快照相同的 KMS 密钥加密卷，则 Amazon KMS 使用与快照相同的数据密钥并使用相同的 KMS 密钥对其进行加密。如果使用不同的 KMS 密钥对卷进行加密，则 Amazon KMS 会生成新的数据密钥并使用您指定的 KMS 密钥对其进行加密。加密的数据密钥会发送到 Amazon EBS，并与卷元数据存储在一起。
3. 当您将加密卷附加到实例时，Amazon EC2 会向发送CreateGrant请求， Amazon KMS 以便它可以解密数据密钥。
4. Amazon KMS 解密加密的数据密钥并将解密后的数据密钥发送给 Amazon。 EC2
5. Amazon EC2 使用 Nitro 硬件中的明文数据密钥来加密该卷的磁盘 I/O。只要卷附加到实例，纯文本数据密钥就会保留在内存中。

快照未加密时 EBS 加密的工作原理

当您使用未加密的快照创建加密卷时，Amazon 会按 EC2 如下方式 Amazon KMS 对您的 EBS 卷进行加密和解密：

1. Amazon EC2 向发送CreateGrant请求 Amazon KMS，以便它可以加密根据快照创建的卷。
2. Amazon EC2 向发送GenerateDataKeyWithoutPlaintext请求 Amazon KMS，指定您为批量加密选择的 KMS 密钥。
3. Amazon KMS 生成新的数据密钥，使用您为卷加密选择的 KMS 密钥对其进行加密，然后将加密的数据密钥发送到 Amazon EBS，以便与卷元数据一起存储。
4. Amazon EC2 向发送解密请求 Amazon KMS 以解密加密的数据密钥，然后使用该密钥对卷数据进行加密。

5. 当您将加密卷附加到实例时，Amazon EC2 会向发送CreateGrant请求 Amazon KMS，以便它可以解密数据密钥。
6. 当您将加密卷附加到实例时，Amazon EC2 会向发送解密请求 Amazon KMS，指定加密的数据密钥。
7. Amazon KMS 解密加密的数据密钥并将解密后的数据密钥发送给 Amazon。 EC2
8. Amazon EC2 使用 Nitro 硬件中的明文数据密钥来加密该卷的磁盘 I/O。只要卷附加到实例，纯文本数据密钥就会保留在内存中。

有关更多信息，请参阅开发者指南中的亚马逊 Elastic Block Store (Amazon EBS) 的使用方式 Amazon KMS和 EC2亚马逊示例二。Amazon Key Management Service

不可用的 KMS 密钥如何影响数据密钥

当 KMS 密钥不可用时，您可以立即发现（取决于最终一致性）。KMS 密钥的密钥状态会出现变更，以反映其新情况，并且加密操作中使用 KMS 密钥的所有请求都将失败。

当您执行使 KMS 密钥不可用的操作时，不会立即对 EC2 实例或连接的 EBS 卷产生影响。当卷连接到实例时，Amazon EC2 使用数据密钥而不是 KMS 密钥来加密所有磁盘 I/O。

但是，当加密的 EBS 卷与 EC2 实例分离时，Amazon EBS 会从 Nitro 硬件中删除数据密钥。下次将加密的 EBS 卷连接到 EC2 实例时，连接会失败，因为 Amazon EBS 无法使用 KMS 密钥来解密该卷的加密数据密钥。要再次使用 EBS 卷，您必须使该 KMS 密钥可重新使用。

> **Tip**
>
> 如果您不再希望访问存储在 EBS 卷中的数据，该数据使用由 KMS 密钥生成的数据密钥进行加密，但您打算使其无法使用，我们建议您在使 KMS 密钥不可用之前将 EBS 卷与 EC2 实例分离。

有关更多信息，请参见《Amazon Key Management Service 开发人员指南》中的不可用的 KMS 密钥如何影响数据密钥。

Amazon EBS 加密要求

在您开始之前，确认您满足以下要求。

要求

- 支持的卷类型
- 支持的实例类型
- 用户的权限
- 实例的权限

支持的卷类型

所有 EBS 卷类型都支持加密。您可能希望加密卷具有与未加密卷相同的 IOPS 性能，同时对延迟的影响最低。您可以采用与访问未加密卷相同的方式来访问加密卷。加密和解密是以透明方式处理的，并且不需要您或您的应用程序执行额外操作。

支持的实例类型

Amazon EBS 加密适用于所有当前一代和上一代实例类型。

用户的权限

当您使用 KMS 密钥进行 EBS 加密时，KMS 密钥策略允许任何有权访问所需 Amazon KMS 操作的用户使用此 KMS 密钥来加密或解密 EBS 资源。您必须授予用户调用以下操作的权限才能使用 EBS 加密：

- `kms:CreateGrant`
- `kms:Decrypt`
- `kms:DescribeKey`
- `kms:GenerateDataKeyWithoutPlainText`
- `kms:ReEncrypt`

> **Tip**
>
> 为遵循最小特权原则，请不要允许对 `kms:CreateGrant` 拥有完全访问权限。相反，使用`kms:GrantIsForAWSResource`条件密钥允许用户仅在 Amazon 服务代表用户创建授权时才允许用户在 KMS 密钥上创建授权，如以下示例所示。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "kms:CreateGrant",
            "Resource": [
                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-a123-456d-a12b-
a123b4cd56ef"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

有关更多信息，请参阅《Amazon Key Management Service 开发人员指南》中 “默认密钥策略” 部分中的允许访问 Amazon 账户和启用 IAM 策略。

实例的权限

当实例尝试与加密的 AMI、卷或快照进行交互时，系统会向该实例的仅限身份角色发放 KMS 密钥授权。仅限身份的角色是一个 IAM 角色，实例使用该角色代表您与加密的 AMIs、卷或快照进行交互。

仅限身份角色无需手动创建或删除，也没有与之关联的策略。此外，您无法访问仅限身份的角色凭证。

> **Note**
>
> 您的实例上的应用程序不使用仅限身份的角色来访问其他 Amazon KMS 加密资源，例如 Amazon S3 对象或 Dynamo DB 表。这些操作是使用 Amazon EC2 实例角色的 Amazon 凭证或您在实例上配置的其他凭证完成的。

仅限身份的角色受服务控制策略 (SCPs) 和 KMS 密钥策略的约束。如果 SCP 或 KMS 密钥拒绝仅限身份的角色访问 KMS 密钥，则您可能无法启动带有加密卷或使用加密 AMIs 卷或快照的 EC2 实例。

如果您要使用`aws:SourceIp`、`aws:VpcSourceIp`、或`aws:SourceVpce` Amazon 全局条件密钥创建基于网络位置拒绝访问的 SCP 或密钥策略，则必须确保这些策略声明不适用于仅限实例的角色。`aws:SourceVpc`有关示例策略，请参阅数据外围策略示例。

仅限身份的角色 ARNs 使用以下格式：

```
arn:aws-partition:iam::account_id:role/aws:ec2-infrastructure/instance_id
```

向实例颁发密钥授予时，密钥授予将颁发给特定于该实例的代入角色会话。被授权者主体 ARN 使用以下格式：

```
arn:aws-partition:sts::account_id:assumed-role/aws:ec2-infrastructure/instance_id
```

默认启用 Amazon EBS 加密

您可以将您的 Amazon 账户配置为强制对您创建的新 EBS 卷和快照副本进行加密。例如，Amazon EBS 加密当您启动实例时创建的 EBS 卷以及您从未加密的快照复制的快照。有关从未加密转换为加密 EBS 资源的示例，请参阅加密未加密的资源。

默认情况下，加密对现有 EBS 卷或快照没有影响。

注意事项

- 默认加密是区域特定的设置。如果您为某个区域启用了它，则无法为该区域中单独的卷或快照禁用。
- Amazon EBS 加密默认支持所有当前一代和上一代实例类型。
- 如果将快照复制到新 KMS 密钥并将其加密，则会创建完整（非增量）副本。这会产生额外的存储成本。
- 使用 Amazon Server Migration Service (SMS) 迁移服务器时，请勿默认开启加密。如果默认情况下已启用加密，并且您遇到增量复制失败，请默认关闭加密。改为在创建复制作业时启用 AMI 加密。

Console

默认为某个区域启用加密

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 从导航栏中选择区域。
3. 从导航窗格中选择EC2 控制面板。
4. 在页面的右上角，选择账户属性，然后选择数据保护和安全。
5. 在 EBS 加密部分，选择管理。
6. 选择 启用。您可以保留 Amazon 托管式密钥 使用代表您aws/ebs创建的别名作为默认加密密钥，或者选择对称的客户托管加密密钥。

7. 选择更新 EBS 加密。

Amazon CLI

查看默认设置的加密

使用 get-ebs-encryption-by-defaul t命令。

- 对于特定区域

```
aws ec2 get-ebs-encryption-by-default --region region
```

- 对于您账户中的所有区域

```
echo -e "Region      \t Encrypt \t Key"; \
echo -e "----------- \t ------- \t -------" ; \
for region in $(aws ec2 describe-regions --region us-east-1 --query "Regions[*].
[RegionName]" --output text);
do
    default=$(aws ec2 get-ebs-encryption-by-default --region $region --query
 "{Encryption_By_Default:EbsEncryptionByDefault}" --output text);
    kms_key=$(aws ec2 get-ebs-default-kms-key-id --region $region | jq
 '.KmsKeyId');
    echo -e "$region \t $default \t\t $kms_key";
done
```

默认启用加密

使用 enable-ebs-encryption-by-defaul t命令。

- 对于特定区域

```
aws ec2 enable-ebs-encryption-by-default --region region
```

- 对于您账户中的所有区域

```
echo -e "Region      \t Encrypt \t Key"; \
echo -e "----------- \t ------- \t -------" ; \
for region in $(aws ec2 describe-regions --region us-east-1 --query "Regions[*].
[RegionName]" --output text);
do
```

```
    default=$(aws ec2 enable-ebs-encryption-by-default --region $region --query
 "{Encryption_By_Default:EbsEncryptionByDefault}" --output text);
    kms_key=$(aws ec2 get-ebs-default-kms-key-id --region $region | jq
 '.KmsKeyId');
    echo -e "$region \t $default \t\t $kms_key";
done
```

默认禁用加密

使用 disable-ebs-encryption-by-defaul t命令。

- 对于特定区域

```
aws ec2 disable-ebs-encryption-by-default --region region
```

- 对于您账户中的所有区域

```
echo -e "Region      \t Encrypt \t Key"; \
echo -e "----------- \t ------- \t -------" ; \
for region in $(aws ec2 describe-regions --region us-east-1 --query "Regions[*].
[RegionName]" --output text);
do
    default=$(aws ec2 disable-ebs-encryption-by-default --region $region --query
 "{Encryption_By_Default:EbsEncryptionByDefault}" --output text);
    kms_key=$(aws ec2 get-ebs-default-kms-key-id --region $region | jq
 '.KmsKeyId');
    echo -e "$region \t $default \t\t $kms_key";
done
```

PowerShell

查看默认设置的加密

使用 Get-EC2EbsEncryptionByDefault cmdlet。

- 对于特定区域

```
Get-EC2EbsEncryptionByDefault -Region region
```

- 对于您账户中的所有区域

```
(Get-EC2Region).RegionName |`
    ForEach-Object {
    [PSCustomObject]@{
        Region                    = $_;
        EC2EbsEncryptionByDefault = Get-EC2EbsEncryptionByDefault -Region $_;
        EC2EbsDefaultKmsKeyId     = Get-EC2EbsDefaultKmsKeyId -Region $_
    } } |`
    Format-Table -AutoSize
```

默认启用加密

使用 Enable-EC2EbsEncryptionByDefault cmdlet。

- 对于特定区域

```
Enable-EC2EbsEncryptionByDefault -Region region
```

- 对于您账户中的所有区域

```
(Get-EC2Region).RegionName |`
    ForEach-Object {
    [PSCustomObject]@{
        Region                    = $_;
        EC2EbsEncryptionByDefault = Enable-EC2EbsEncryptionByDefault -Region $_;
        EC2EbsDefaultKmsKeyId     = Get-EC2EbsDefaultKmsKeyId -Region $_
    } } | `
    Format-Table -AutoSize
```

默认禁用加密

使用 Disable-EC2EbsEncryptionByDefault cmdlet。

- 对于特定区域

```
Disable-EC2EbsEncryptionByDefault -Region region
```

- 对于您账户中的所有区域

```
(Get-EC2Region).RegionName |`
```

```
    ForEach-Object {
    [PSCustomObject]@{
        Region                     = $_;
        EC2EbsEncryptionByDefault = Disable-EC2EbsEncryptionByDefault -Region $_;
        EC2EbsDefaultKmsKeyId      = Get-EC2EbsDefaultKmsKeyId -Region $_
    } } | `
    Format-Table -AutoSize
```

您无法更改与现有快照或加密卷关联的 KMS 密钥。但是，您可在快照复制操作期间关联另一个 KMS 密钥，从而使生成的已复制快照由新 KMS 密钥 进行加密。

加密 EBS 资源

您可以通过启用加密来加密 EBS 卷：使用默认加密，或者在创建要加密的卷时启用加密。

加密卷时，可以指定用于加密该卷的对称加密 KMS 密钥。如果未指定 KMS 密钥，则用于加密的 KMS 密钥 取决于源快照的加密状态及其所有权。有关更多信息，请参阅加密结果表。

> **Note**
>
> 如果您正在使用 API 或 Amazon CLI 指定 KMS 密钥，请注意这会异步对 KMS 密钥 Amazon 进行身份验证。如果您指定了无效的 KMS 密钥 ID、别名或 ARN，则操作可能会显示完成，但最终失败。

您无法更改与现有快照或卷关联的 KMS 密钥。但是，您可在快照复制操作期间关联另一个 KMS 密钥，从而使生成的已复制快照由新 KMS 密钥 进行加密。

在创建时加密空卷

创建新的空 EBS 卷时，可以通过为特定卷创建操作启用加密来对其进行加密。如果默认情况下启用了 EBS 加密，则会使用 EBS 加密的默认 KMS 密钥 自动加密卷。您也可以为特定的卷创建操作指定不同的对称加密 KMS 密钥。卷从其首次可用时开始加密，因此您的数据始终安全。有关详细步骤，请参阅创建 Amazon EBS 卷。

默认情况下，您在创建卷时选择的 KMS 密钥 会对从该卷拍摄的快照加密，并对从这些加密的快照还原的卷加密。您无法从加密卷或快照删除加密，这意味着从加密快照还原的卷或者加密快照的副本始终加密。

加密卷的快照无法公开，但您可以与特定账户共享加密快照。有关详细指导，请参阅与其他账户共享 Amazon EBS 快照 Amazon。

加密未加密的资源

您不能直接加密现有的未加密卷或快照。

要加密未加密的卷，请创建该卷的快照，然后使用该快照创建新的加密卷。有关更多信息，请参阅创建快照和创建卷。

要加密未加密的快照，请创建该快照的加密副本。有关更多信息，请参阅 复制快照。

如果您在默认情况下启用账户加密功能，则从未加密的快照创建的卷和快照副本将始终处于加密状态。否则，您必须在请求中指定加密参数。有关更多信息，请参阅 默认启用加密。

轮换用于 Amazon EBS 加密的 Amazon KMS 密钥

加密最佳实践建议不要广泛重复使用加密密钥。

要创建用于 Amazon EBS 加密的新加密材料，您可以创建一个新的客户自主管理型密钥，然后更改您的应用程序以使用该新的 KMS 密钥。或者，您可以为现有客户管理的密钥启用自动密钥轮换。

当您为客户托管密钥启用自动密钥轮换时，每年会为 KMS 密钥 Amazon KMS 生成新的加密材料。Amazon KMS 保存加密材料的所有先前版本，以便您可以继续解密和使用以前使用该 KMS 密钥材料加密的卷和快照。 Amazon KMS 在您删除 KMS 密钥之前，不会删除任何轮换的密钥材料。

当您使用轮换的客户托管密钥加密新卷或快照时，将 Amazon KMS 使用当前（新）密钥材料。当您使用轮换的客户自主管理型密钥解密卷或快照时， Amazon KMS 将使用用于加密它的加密材料版本。如果使用先前版本的加密材料对卷或快照进行加密，则 Amazon KMS 将继续使用先前版本对其进行解密。 Amazon KMS 不会在密钥轮换后重新加密先前加密的卷或快照以使用新的加密材料。它们仍然使用最初加密时使用的加密材料进行加密。无需更改代码，您就可以在应用程序和 Amazon 服务中安全地使用轮换的客户托管密钥。

> **Note**
>
> - 只有具有 Amazon KMS 创建密钥材料的对称客户托管密钥才支持自动密钥轮换。
> - Amazon KMS Amazon 托管式密钥 每年自动轮换。您无法启用或禁用 Amazon 托管式密钥的密钥轮换。

有关更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的 轮换 KMS 密钥。

Amazon EBS 加密示例

创建加密 EBS 资源时，除非您在卷创建参数或 AMI 或实例的块设备映射中指定了不同的 客户托管密钥，否则它将使用您账户的用于 EBS 加密的默认 KMS 密钥 进行加密。

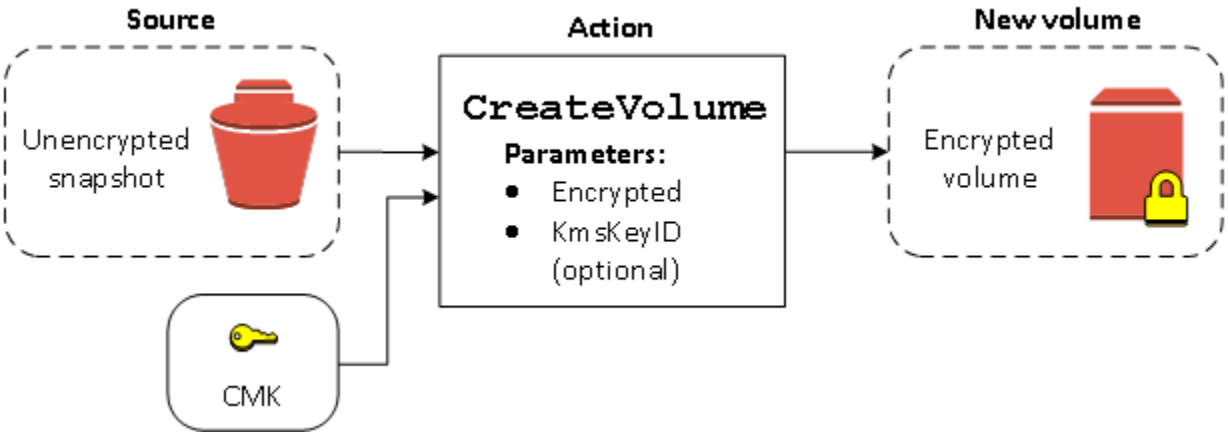
以下示例说明如何管理卷和快照的加密状态。有关加密案例的完整列表，请参阅加密结果表。

示例

- 还原未加密的卷（未启用默认加密）
- 还原未加密的卷（启用了默认加密）
- 复制未加密的快照（未启用默认加密）
- 复制未加密的快照（启用了默认加密）
- 重新加密已加密卷
- 重新加密已加密快照
- 在加密卷与未加密卷之间迁移数据
- 加密结果

还原未加密的卷（未启用默认加密）

未启用默认加密时，从未加密快照还原的卷在默认情况下不加密。但是，您可以设置 `Encrypted` 参数和可选的 `KmsKeyId` 参数来加密生成的卷。下图说明了该过程。

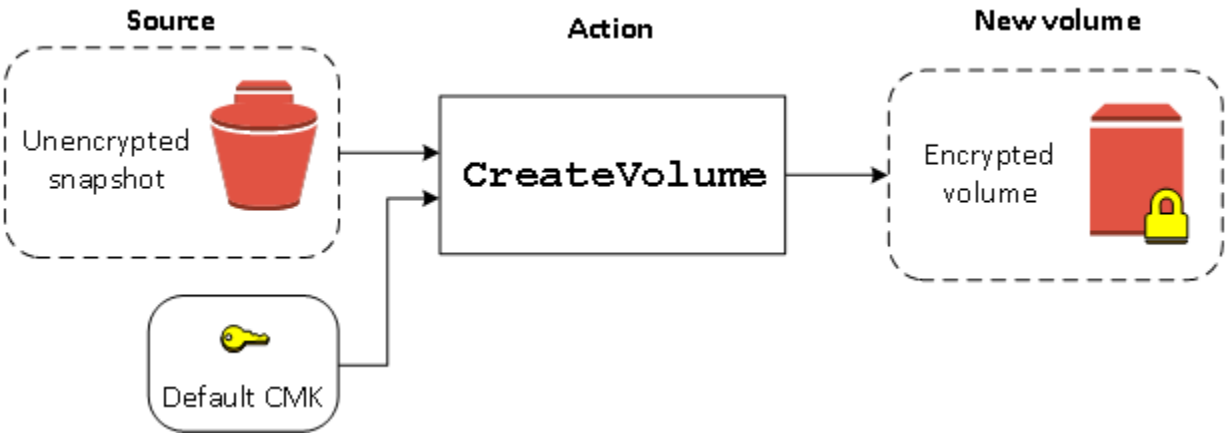


如果您省略 `KmsKeyId` 参数，则将使用您用于 EBS 加密的默认 KMS 密钥 加密生成的卷。您必须指定 KMS 密钥 ID 以使用不同的 KMS 密钥 加密卷。

有关更多信息，请参阅 创建 Amazon EBS 卷。

还原未加密的卷（启用了默认加密）

在您启用了默认加密时，从未加密快照还原的卷必须加密，无需使用默认 KMS 密钥 的加密参数。下图说明了这种简单默认案例：

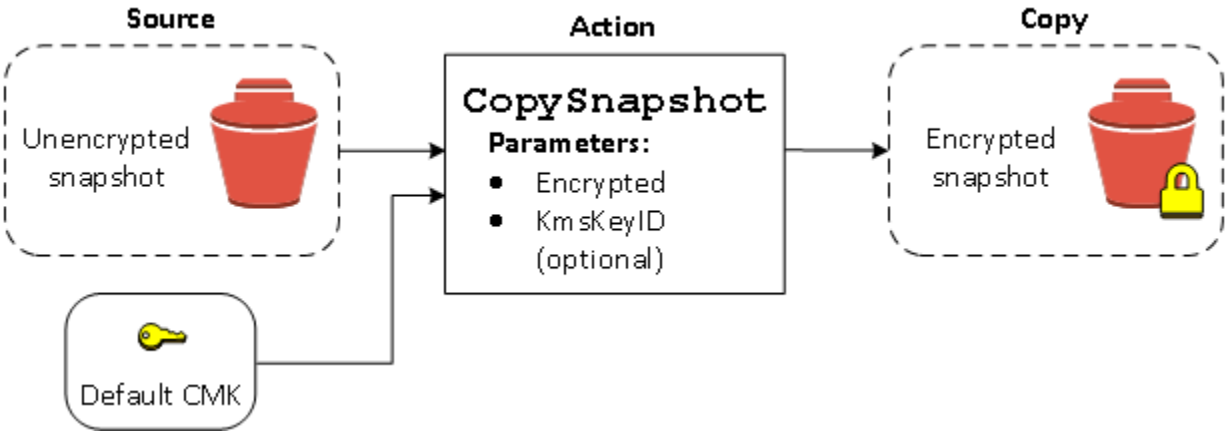


如果您要使用对称客户管理加密密钥来加密还原的卷，则必须提供 Encrypted 和 KmsKeyId 参数，如 还原未加密的卷（未启用默认加密） 中所示。

复制未加密的快照（未启用默认加密）

未启用默认加密时，未加密快照的副本在默认情况下不加密。但是，您可以设置 Encrypted 参数和可选的 KmsKeyId 参数来加密生成的快照。如果省略 KmsKeyId，则使用默认 KMS 密钥 加密生成的快照。您必须指定 KMS 密钥 ID 以使用不同的对称加密 KMS 密钥对卷进行加密。

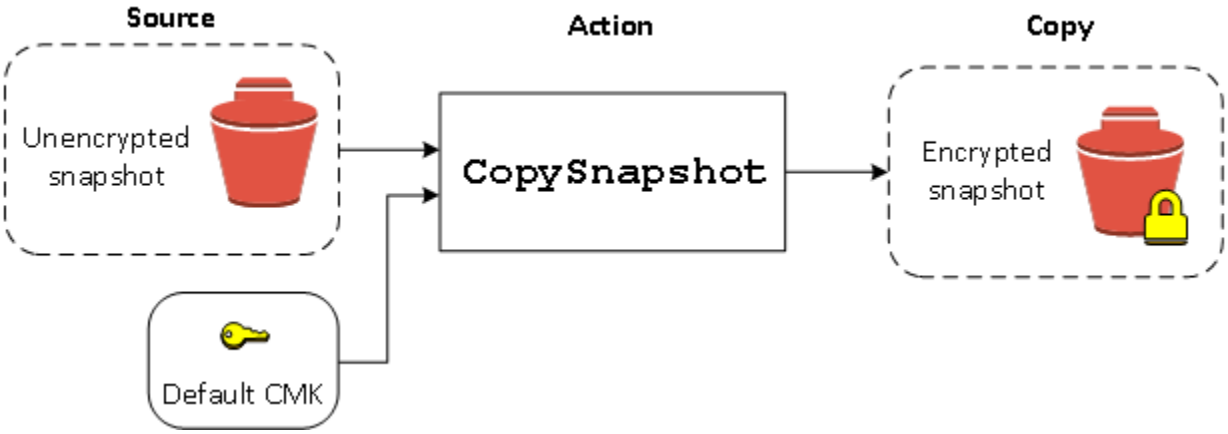
下图说明了该过程。



您可以将未加密的快照复制到加密的快照，然后从加密的快照中创建卷来加密 EBS 卷。有关更多信息，请参阅复制 Amazon EBS 快照。

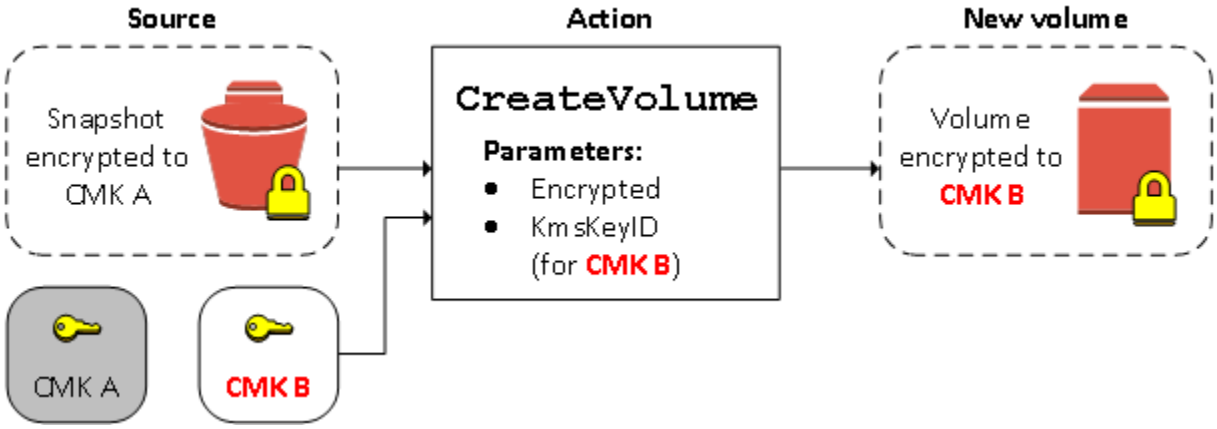
复制未加密的快照（启用了默认加密）

在您启用了默认加密时，未加密快照的副本必须加密，无需使用默认 KMS 密钥 的加密参数。下图说明了这种默认情况：



重新加密已加密卷

对加密快照执行 `CreateVolume` 操作时，您可以选择使用不同的 KMS 密钥 重新加密它。下图说明了该过程。在本例中，您拥有两个 KMS 密钥，即 KMS 密钥 A 和 KMS 密钥 B。源快照由 KMS 密钥 A 加密。在卷创建期间，由于 KMS 密钥 B 的 KMS 密钥 ID 被指定为一个参数，因此源数据被自动解密，然后由 KMS 密钥 B 重新加密。

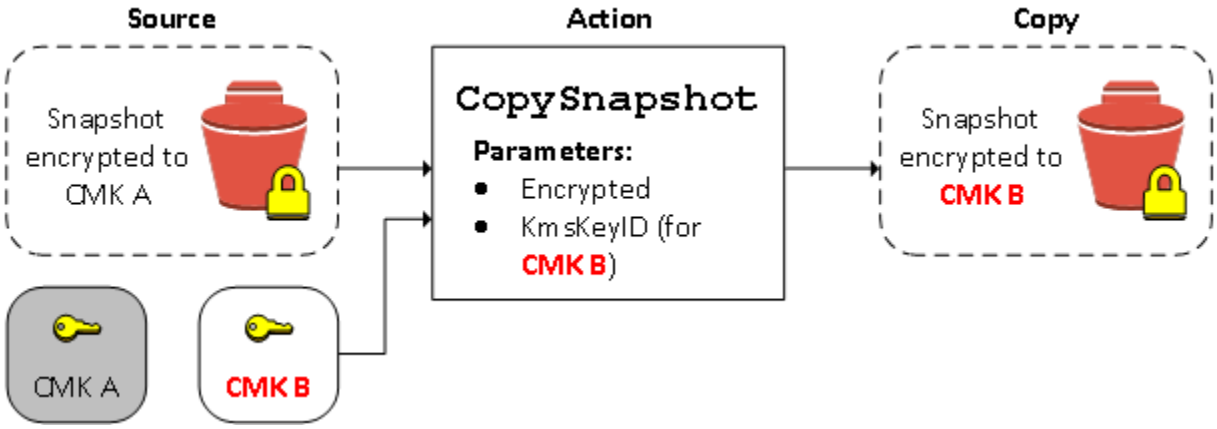


有关更多信息，请参阅 创建 Amazon EBS 卷。

重新加密已加密快照

由于能够在复制过程中加密快照，您可以将新的对称加密 KMS 密钥应用于您拥有的已加密过的快照。从生成的副本还原的卷只能使用新的 KMS 密钥 进行访问。下图说明了该过程。在本例中，您拥有两个

KMS 密钥，即 KMS 密钥 A 和 KMS 密钥 B。源快照由 KMS 密钥 A 加密。在复制期间，由于 KMS 密钥 B 的 KMS 密钥 ID 被指定为一个参数，因此源数据由 KMS 密钥 B 自动重新加密。



在相关的场景中，您可以选择将新加密参数应用于已与您共享的快照的副本。默认情况下，系统会使用快照拥有者共享的 KMS 密钥 对该副本进行加密。但是，我们建议您使用您控制的其他 KMS 密钥 创建共享快照的副本。这样，即使原始 KMS 密钥 遭到泄露或拥有者出于任何原因撤销了 KMS 密钥，您也不会失去对卷的访问权限。有关更多信息，请参阅加密和快照复制。

在加密卷与未加密卷之间迁移数据

当您可以访问加密卷和未加密卷时，可以在它们之间自由传输数据。 EC2 透明地执行加密和解密操作。

Linux 实例

例如，使用 rsync 命令复制数据。在以下命令中，源数据位于 `/mnt/source` 中，目标卷挂载在 `/mnt/destination` 中。

```
[ec2-user ~]$ sudo rsync -avh --progress /mnt/source/ /mnt/destination/
```

Windows 实例

例如，使用 robocopy 命令复制数据。在以下命令中，源数据位于 `D:\` 中，目标卷挂载在 `E:\` 中。

```
PS C:\> robocopy D:\sourcefolder E:\destinationfolder /e /copyall /eta
```

我们建议使用文件夹而不是复制整个卷，因为这可避免隐藏文件夹的潜在问题。

加密结果

下表描述了每种可能的设置组合的加密结果。

是否已启用加密？	默认启用加密？	卷来源	默认值（未指定客户托管密钥）	自定义（指定客户托管密钥）
否	否	新（空）卷	未加密	不适用
否	否	您拥有的未加密快照	未加密	
否	否	您拥有的加密快照	按相同密钥加密	
否	否	与您共享的未加密快照	未加密	
否	否	与您共享的加密快照	由默认客户托管密钥加密*	
是	否	新卷	由默认客户托管密钥加密	由指定的客户托管密钥加密**
是	否	您拥有的未加密快照	由默认客户托管密钥加密	
是	否	您拥有的加密快照	按相同密钥加密	
是	否	与您共享的未加密快照	由默认客户托管密钥加密	
是	否	与您共享的加密快照	由默认客户托管密钥加密	
否	是	新（空）卷	由默认客户托管密钥加密	不适用
否	是	您拥有的未加密快照	由默认客户托管密钥加密	
否	是	您拥有的加密快照	按相同密钥加密	
否	是	与您共享的未加密快照	由默认客户托管密钥加密	

是否已启用加密？	默认启用加密？	卷来源	默认值（未指定客户托管密钥）	自定义（指定客户托管密钥）
否	是	与您共享的加密快照	由默认客户托管密钥加密	
是	是	新卷	由默认客户托管密钥加密	由指定的客户托管密钥加密
是	是	您拥有的未加密快照	由默认客户托管密钥加密	
是	是	您拥有的加密快照	按相同密钥加密	
是	是	与您共享的未加密快照	由默认客户托管密钥加密	
是	是	与您共享的加密快照	由默认客户托管密钥加密	

* 这是用于 Amazon 账户和地区的 EBS 加密的默认客户托管密钥。默认情况下，这是 EBS Amazon 托管式密钥 的唯一密钥，或者您可以指定客户托管密钥。

**这是在启动时为卷指定的客户托管密钥。使用此客户托管密钥代替 Amazon 账户和地区的默认客户托管密钥。

Amazon EBS 卷性能

几个因素（包括 I/O 特性以及实例和卷的配置）会对 Amazon EBS 的性能造成影响。如果您遵循我们的 Amazon EBS 和亚马逊 EC2 商品详情页面上的指南，通常会取得良好的业绩。但是，在某些情况下，您可能需要进行一些调整才能获得峰值性能。除了基准测试之外，我们建议您根据实际工作负载信息来调整性能，以确定最佳配置。当您学习了使用 EBS 卷的基础知识后，最好了解一下所需的 I/O 性能，以及可用于提升 Amazon EBS 性能以满足这些要求的选项。

Amazon 对 EBS 卷类型性能的更新可能不会立即对现有卷生效。要查看较早卷上的全部性能，您需要先在其上执行 `ModifyVolume` 操作。有关更多信息，请参阅 使用弹性卷操作修改 Amazon EBS 卷。

内容

- Amazon EBS 性能提示
- Amazon EBS 优化
- 初始化 Amazon EBS 卷
- 可配置的实例带宽权重
- Amazon EBS I/O 特性和监控
- Amazon EBS 和 RAID 配置
- 对 Amazon EBS 卷进行基准测试

Amazon EBS 性能提示

这些提示代表了在各种用户场景下能够获得最佳 EBS 卷性能的最佳实践。

使用 EBS 优化的实例

对于不支持 EBS 优化吞吐量的实例，网络流量可能会与实例和 EBS 卷之间的流量产生冲突；而在 EBS 优化实例中，这两种流量相互独立。部分 EBS 优化实例配置（例如 C3、R3 和 M3）会产生额外成本，另一些实例（例如 M4、C4、C5 和 D2）始终可进行 EBS 优化而不会产生额外成本。有关更多信息，请参阅 Amazon EBS 优化。

配置实例带宽

对于支持的实例类型，您可以将实例带宽权重配置为使用带宽权重将 Amazon EBS 带宽提高 25%。`ebs-1`此功能允许您优化实例在 EBS 和 VPC 网络之间的网络资源分配，从而有可能提高 I/O 密集型工作负载的 EBS 性能。有关更多信息，请参阅 可配置的实例带宽权重。

了解如何计算性能

度量 EBS 卷的性能时，应了解所需采用的度量单位以及如何计算性能，这十分重要。有关更多信息，请参阅Amazon EBS I/O 特性和监控。

了解工作负载

EBS 卷的最高性能、I/O 操作的大小和数量，以及完成每个操作所需时间之间存在着某种关系。这些因素（性能、I/O 和延迟）相互影响，不同应用程序对各个因素的敏感程度也不同。有关更多信息，请参阅对 Amazon EBS 卷进行基准测试。

请注意，从快照中初始化卷时，性能将会下降

当您首次访问从快照创建的新 EBS 卷上的每个数据块时，延迟会大大增加。您可以使用以下其中一个选项来避免这一性能下降：

- 在将卷部署到生产环境之前访问每个块。此过程称为初始化（以前称为预热）。有关更多信息，请参阅创建后手动初始化卷。
- 在快照上启用快速快照还原，以确保从中创建的 EBS 卷在创建时已完全初始化，并立即提供所有预置的性能。有关更多信息，请参阅Amazon EBS 快速快照还原。

可能导致 HDD 性能下降的因素

如果创建吞吐量优化型 HDD（`st1`）或 Cold HDD（`sc1`）卷的快照，则在快照处理过程中，性能可能会降低，最坏情况下会降低到卷的基准值。这种情况是这些卷类型特有的。其他可能会限制性能的因素包括迫使吞吐量超过实例的支持能力，在初始化从快照创建的卷时损失性能，以及卷上的小型随机 I/O 过多。有关计算 HDD 卷吞吐量的更多信息，请参阅 Amazon EBS 卷类型。

如果您的应用程序没有发送足够多的 I/O 请求，性能可能也会受影响。这可通过查看卷的队列长度和 I/O 大小来监控。队列长度是您的应用程序向卷发起的待处理 I/O 请求的数量。为实现最大程度的一致性，在执行 1MiB 的顺序 I/O 时，HDD 卷必须保持 4 或更大的队列长度（四舍五入为最近的整数）。有关确保稳定的卷性能的更多信息，请参阅 Amazon EBS I/O 特性和监控

为 st1 和 sc1 上的高吞吐量读取密集型工作负载增加预读值（仅限 Linux 实例）

一些工作负载读取操作量大，并会访问操作系统页缓存中的块设备（例如从文件系统访问）。在这种情况下，为了实现最大的吞吐量，我们建议您将预读取设置配置为 1 MiB。此 per-block-device设置只能应用于您的 HDD 卷。

要检查您的块储存设备的当前预读数值，请使用以下命令：

```
$ sudo blockdev --report /dev/<device>
```

块储存设备信息采用以下格式返回：

```
RO    RA   SSZ   BSZ   StartSec            Size   Device
rw   256   512  4096       4096      8587820544   /dev/<device>
```

以上显示的设备报告预读取值为 256（默认值）。将此数字乘以扇区大小（512 字节）就可获得预读取缓冲区的大小，在此例中为 128 KiB。要将缓冲区值设置为 1 MiB，请使用以下命令：

```
$ sudo blockdev --setra 2048 /dev/<device>
```

再次运行第一个命令，验证预读取设置现在显示 2048。

仅当您的工作负载包括大型顺序 I/O 时，才使用此设置。如果它主要包含的是小型随机 I/O，则此设置会降低性能。一般来说，如果工作负载主要包括小型随机 I/O，则应考虑使用通用型 SSD（gp2 和 gp3）卷，而不是 st1 或 sc1 卷。

使用现代 Linux 内核（仅限 Linux 实例）

借助对间接描述符的支持，使用现代 Linux 内核。任何 Linux 内核 3.8 及以上版本以及任何当前一代的实例都支持此功能 EC2 。如果您的平均 I/O 大小达到或接近 44 KiB，则说明您可能是在不支持间接描述符的情况下使用实例或内核。有关从 Amazon CloudWatch 指标得出平均 I/O 大小的信息，请参阅Amazon EBS I/O 特性和监控。

要在 st1 或 sc1卷上实现最大吞吐量，建议您将值 256 应用于 xen_blkfront.max 参数（对于低于 4.6 的 Linux 内核版本）或 xen_blkfront.max_indirect_segments 参数（对于 Linux 内核版本 4.6 及更高版本）。可在操作系统 boot 命令行中设置相应的参数。

例如，在具有较早内核的 Amazon Linux AMI 中，您可以将它添加到在 `/boot/grub/menu.lst` 中找到的 GRUB 配置的 kernel 行末尾：

```
kernel /boot/vmlinuz-4.4.5-15.26.amzn1.x86_64 root=LABEL=/ console=ttyS0
 xen_blkfront.max=256
```

对于更高版本的内核，该命令将类似于以下内容：

```
kernel /boot/vmlinuz-4.9.20-11.31.amzn1.x86_64 root=LABEL=/ console=tty1 console=ttyS0
 xen_blkfront.max_indirect_segments=256
```

重启实例，让此设置生效。

有关更多信息，请参阅为半 AMIs虚拟化配置 GRUB。对于其他 Linux 发行版（尤其是不使用 GRUB 引导加载程序的版本）可能需要采用不同方法来调整内核参数。

使用 RAID 0 以最大限度利用实例资源

某些实例类型可以实现的 I/O 吞吐量大于可以为单个 EBS 卷配置的量。可以将多个卷一起加入到 RAID 0 配置中，以将可用带宽用于这些实例。有关更多信息，请参阅 Amazon EBS 和 RAID 配置。

监控 Amazon EBS 卷性能

您可以使用亚马逊、状态检查和 EBS 详细性能统计数据来监控和分析 Amazon CloudWatch EBS 卷的性能。有关更多信息，请参阅亚马逊 EBS 的亚马逊 CloudWatch 指标和Amazon EBS 的详细绩效统计数据。

Amazon EBS 优化

Amazon EBS 优化型实例使用经过优化的配置堆栈，并为 Amazon EBS I/O 提供额外的专用容量。这种优化通过最小化 Amazon EBS I/O 与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。

EBS 优化的实例将专用带宽提供给 Amazon EBS。当附加到 EBS 优化实例时，通用型 SSD（`gp2` 和 `gp3`）卷可在给定年度 99% 的时间内提供至少 90% 的预置 IOPS 性能，而预置 IOPS SSD（`io1` 和 `io2`）卷可在给定年度 99.9% 的时间内提供至少 90% 的预置 IOPS 性能。吞吐量优化型 HDD（`st1`）和 Cold HDD（`sc1`）在给定年度 99% 的时间内提供至少 90% 的预期吞吐量性能。不合规时间近似均匀分配，目标是达到 99% 的每小时预计总吞吐量。有关更多信息，请参阅 Amazon EBS 卷类型。

有关更多信息，请参阅《亚马逊 EC2 用户指南》中的 Ama zon EBS 优化实例。

初始化 Amazon EBS 卷

当您从快照创建卷时，必须从 Amazon S3 下载快照中的存储块并将其写入卷，然后您才能访问它们。此过程称为卷初始化。在此期间，卷的 I/O 延迟可能会增加，性能可能会降低。只有将所有存储块下载并写入卷后，才能实现全卷性能。

> **Note**
>
> 空卷在创建后便能实现其最大性能，不需要初始化。

默认的卷初始化率在整个初始化过程中会波动，这可能会使完成时间变得不可预测。

为了最大限度地减少与卷初始化相关的性能影响，您可以使用以下选项：

主题

- 使用 Amazon EBS 预配置速率进行卷初始化
- 使用已启用的快照进行快速快照恢复
- 创建后手动初始化卷

使用 Amazon EBS 预配置速率进行卷初始化

当您根据快照创建 Amazon EBS 卷时，您可以选择为卷初始化指定 Amazon EBS 预配置速率（卷初始化速率），范围在 100 到 300 MiB/s 之间。如果您指定卷初始化速率，则快照块将在创建后从 Amazon S3 下载并以指定的速率写入该卷。这使您能够创建在可预测的时间内完全初始化并完全达到性能的卷。

当您同时创建多个卷并且需要在可预测的时间内初始化所有卷时，使用卷初始化率特别有用。

> **Note**
>
> 所有亚马逊 EBS 卷类型和所有亚马逊 EC2 实例类型（包括亚马逊 Mac 实例）都支持 Amazon EBS 卷初始化的预配置速率。 EC2

您可以指定卷初始化速率：

- 对于个人卷创建请求
- 对于实例启动请求中的 EBS 卷块设备映射
- 对于启动模板中的 EBS 卷块设备映射
- 对于由根卷替换任务创建的 EBS 卷
- 适用于亚马逊 EKS 集群（由 EBS CSI 驱动程序创建）和 Amazon ECS 集群上的 EBS 卷

主题

- 工作方式
- 注意事项
- 限额
- 监控
- 计费

工作方式

当您创建具有卷初始化速率的卷时，快照块将按您指定的速率从 Amazon S3 下载到该卷。

初始化卷所花费的时间取决于以下因素：

- 快照数据的大小，而不是正在创建的卷的大小。

> **Tip**
>
> 要查找快照的数据大小，请查看 desc ribe- snapshots 命令输出中的`FullSnapshotSizeInBytes`字段或控制台中的完整快照大小字段。

- 您指定的卷初始化速率

例如，如果您使用包含 10 GiB 数据的快照创建一个 20 GiB 的卷，并且您指定的卷初始化速率为 300 MiB/s, the volume will be fully initialized in approximately 34.1 seconds (10 GiB / 300 MiB/s = 34.1 秒）。同样，如果您同时创建 10 个具有相同快照和卷初始化速率的卷，则所有 10 个卷将在 34.1 秒内完全初始化。

注意事项

- 您可以将卷初始化速率指定为 100 到 300 MiB/s 之间。

- 指定卷初始化速率时，费用和完成时间基于快照数据的大小（而不是卷的大小）和您指定的速率。有关更多信息，请参阅 计费。
- 在 99% 的时间内，Amazon EBS 提供的平均速率在您指定的卷初始化率的 10% 以内。
- 如果您指定卷初始化速率并使用支持快速快照还原的快照，Amazon EBS 将使用指定的速率而不是快速快照还原。要改用快速快照还原，请不要指定卷初始化速率。
- 如果 Amazon EBS 由于容量限制或已超出配额而无法以指定的卷初始化速率初始化卷，则请求将失败。
- 您无法为在 Local Zones 或 Wavelength Z Amazon Outposts ones 上创建的卷指定卷初始化速率。

限额

MiB/s on the cumulative volume initialization rate that you can request across concurrent volume creation requests. For example, you can make 50 concurrent volume creation requests with a rate of 100 MiB/s (50 simultaneous requests * 100 MiB/s rate), or 25 concurrent requests with a rate of 200 MiB/s (25 simultaneous requests * 200 MiB/s速率上限为 5,000）。此限制以每个地区为单位适用。如果请求超过此限制，则会失败。要么等待一些正在处理的请求完成，要么申请增加配额。有关更多信息，请参阅 Amazon EBS 的限额。

监控

当您创建具有卷初始化速率的卷时，Amazon EventBridge 事件将在初始化完成后的五分钟内发送到您的账户。有关更多信息，请参阅 EBS 卷初始化事件。

如果您在初始化完成之前或初始化完成后的 5 分钟内删除该卷，则可能不会收到该事件。

计费

当您创建具有卷初始化速率的卷时，您需要按指定初始化速率的每 GiB 快照数据按每 MiB 的费率收费。费率因地区而异。有关更多信息，请参阅 Amazon EBS 定价。

您需要根据快照数据的大小而不是卷的大小付费。例如，如果您为一个大小为 100 GiB 但只有 50 GiB 数据的卷创建快照，则该快照的卷大小为 100 GiB，但快照数据大小为 50 GiB。如果您使用该快照创建卷并指定卷初始化速率，则费用将基于 50 GiB 的快照数据。

> **Tip**
>
> 要查找快照的数据大小，请查看 desc ribe- snapshots 命令输出中的`FullSnapshotSizeInBytes`字段或控制台中的完整快照大小字段。

公式如下：

```
rate for Region x snapshot data size
          x volume initialization rate
```

音量进入active状态后，您将立即收到全额账单。失败的请求不计费。

如果您在卷初始化完成之前删除了卷，则仍需要按请求的卷初始化速率付费。

使用已启用的快照进行快速快照恢复

如果您使用启用了快速快照恢复功能的快照创建卷，则该卷将在创建时完全初始化，并立即提供其全部性能。有关使用快速快照还原的更多信息，请参阅Amazon EBS 快速快照还原。

创建后手动初始化卷

您可以在创建 Amazon EBS 卷后手动初始化，以帮助最大限度地减少卷初始化对性能的影响。

在创建 Amazon EBS 卷后，您可以使用以下过程手动初始化。

> **Important**
>
> 在初始化已从快照创建的 Provisioned IOPS SSD 卷时，该卷的性能可能会下降到预期水平的 50% 以下，这会导致该卷在 I/O 性能状态检查中显示 warning 状态。这是预期行为，并且您可在初始化 Provisioned IOPS SSD 卷时忽略该卷上的 warning 状态。有关更多信息，请参阅 Amazon EBS 卷状态检查。

Linux 实例

在 Linux 上初始化从快照创建的卷

1. 将新还原的卷附加到您的 Linux 实例。
2. 使用 lsblk 命令列出实例上的块储存设备。

```
$ lsblk
NAME  MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
xvdf  202:80   0  30G  0 disk
xvda1 202:1    0   8G  0 disk /
```

在此处可以看到新卷 /dev/xvdf 已附加，但是未挂载（因为 MOUNTPOINT 列下没有列出任何路径）。

3. 使用 dd 或 fio 实用程序对设备上的所有数据块进行读取。默认情况下，dd 命令将安装在 Linux 系统上，但 fio 要快得多，因为它允很多线程读取。

> **Note**
>
> 此步骤可能需要几分钟到几小时的时间，具体取决于您的 EC2实例带宽、为卷预配置的 IOPS 以及卷的大小。

[dd] 应将 if（输入文件）参数设置为要初始化的驱动器。应将 of（输出文件）参数设置为 Linux 空虚拟设备 /dev/null。bs 参数设置读取操作的数据块大小；要获得最佳性能，这应设置为 1 MB。

> **Important**
>
> 不当使用 dd 可能容易损坏卷的数据。请务必严格遵循下面的示例命令。只有 if=/dev/*xvdf* 参数将因您要读取的设备的名称而异。

```
$ sudo dd if=/dev/xvdf of=/dev/null bs=1M
```

[fio] 如果您在系统上安装了 fio，请使用以下命令初始化您的卷。应将 --filename（输入文件）参数设置为要初始化的驱动器。

```
$ sudo fio --filename=/dev/xvdf --rw=read --bs=1M --iodepth=32 --ioengine=libaio --direct=1 --name=volume-initialize
```

要在 Amazon Linux 上安装 fio，请使用以下命令：

```
sudo yum install -y fio
```

要在 Ubuntu 上安装 fio，请使用以下命令：

```
sudo apt-get install -y fio
```

操作完成时，您会看到读取操作的报告。卷现在已准备就绪，可供使用。有关更多信息，请参阅使 Amazon EBS 卷可供使用。

Windows 实例

在使用上述任何一种工具前，请在您的系统上收集有关磁盘的信息，如下所述：

收集有关系统磁盘的信息

1. 使用 wmic 命令列出系统上的可用磁盘：

```
wmic diskdrive get size,deviceid
```

下面是示例输出：

```
DeviceID            Size
\\.\PHYSICALDRIVE2  80517265920
\\.\PHYSICALDRIVE1  80517265920
\\.\PHYSICALDRIVE0  128849011200
\\.\PHYSICALDRIVE3  107372805120
```

2. 使用 dd 或 fio 识别要初始化的磁盘。C: 驱动器位于 \\.\PHYSICALDRIVE0。如果您不确定要使用的盘符，则可以使用 diskmgmt.msc 实用工具将驱动器盘符与磁盘盘符进行比较。

Use the dd utility

完成以下过程，以安装并使用 dd 来初始化卷。

重要注意事项

- 初始化卷需要几分钟到几小时不等，具体取决于您的 EC2 实例带宽、为该卷预配置的 IOPS 以及卷的大小。
- 不当使用 dd 可能容易损坏卷的数据。一定要准确地遵循此程序。

安装适用于 Windows 的 dd

适用于 Windows 程序的 dd 的使用体验类似于 Linux 和 Unix 系统中常用的 dd 程序，通过它您可以初始化已从快照创建的 Amazon EBS 卷。最新的测试版支持 /dev/null 虚拟设备。如果安装早期版本，则可以使用 nul 虚拟设备。完整的文档可在 http://www.chrysocome.net/dd 上获得。

1. 可从 http://www.chrysocome.net/dd 下载适用于 Windows 的最新二进制版本的 dd。
2. （可选）为命令行实用工具创建易于查找和记住的文件夹，例如 `C:\bin`。如果您已拥有用于命令行实用工具的指定文件夹，则可以在以下步骤中改用该文件夹。
3. 解压缩二进制程序包并将 `dd.exe` 文件复制到命令行实用工具文件夹（例如 `C:\bin`）。
4. 将命令行实用工具文件夹添加到 Path 环境变量，以便您可以从任何位置运行该文件夹中的程序。

   a. 选择开始，打开计算机的上下文（右键单击）菜单，然后选择属性。
   b. 依次选择高级系统设置和环境变量。
   c. 对于系统变量，选择变量 Path，然后选择编辑。
   d. 在变量值中，将一个分号和命令行实用工具文件夹的位置（**`;C:\bin\`**）附加到现有值末尾）。
   e. 选择确定关闭编辑系统变量窗口。
5. 打开新的命令提示符窗口。上一步不会在您当前的“命令提示符”窗口中更新环境变量。完成上一步后打开的命令提示符窗口将更新。

使用适用于 Windows 的 dd 来初始化卷

运行以下命令可读取指定设备上的所有数据块（并将输出发送到 `/dev/null` 虚拟设备）。该命令可安全初始化现有数据。

```
dd if=\\.\PHYSICALDRIVEn of=/dev/null bs=1M --progress --size
```

如果 dd 尝试读取卷末尾以外的空间，您可能会收到一个错误。您可以放心地忽略此错误。

如果您使用的是早期版本的 dd 命令，则不支持 `/dev/null` 设备。相反，您可以按如下方式使用 `nul` 设备。

```
dd if=\\.\PHYSICALDRIVEn of=nul bs=1M --progress --size
```

Use the fio utility

完成以下过程，以安装并使用 fio 来初始化卷。

安装适用于 Windows 的 fio

适用于 Windows 的 fio 程序的使用体验类似于 Linux 和 Unix 系统中常用的 fio 程序，允许您初始化已从快照创建的 Amazon EBS 卷。有关更多信息，请参阅 https://github.com/axboe/fio。

1. 可通过展开最新版本的资产并选择 MSI 安装程序来下载 fio MSI 安装程序。
2. 安装 fio。

使用适用于 Windows 的 fio 初始化卷

1. 运行类似如下的命令来初始化卷：

```
fio --filename=\\.\PHYSICALDRIVEn  --rw=read --bs=128k --iodepth=32 --direct=1
 --name=volume-initialize
```

2. 操作完成时，您即准备就绪，可使用新卷。有关更多信息，请参阅 使 Amazon EBS 卷可供使用。

可配置的实例带宽权重

实例带宽配置 (IBC) 是一项功能，可让您调整亚马逊实例的 Amazon EBS 和 VPC 联网之间的网络带宽分配。 EC2 此功能可以帮助您优化具有特定带宽要求的工作负载的性能。仅部分实例支持实例带宽配置。有关更多信息，请参阅实例带宽权重配置。

对于 EBS 性能，使用ebs-1带宽权重可将基准 EBS 带宽增加 25%，同时将 VPC 网络带宽减少相同的绝对值。这对于需要更高 EBS 吞吐量的 I/O 密集型工作负载可能有好处。

在规划工作负载时，请仔细考虑您的 I/O 大小和模式。较小的 I/O 大小通常受带宽限制的影响较小，而较大的 I/O 大小或连续工作负载可能会受到带宽变化的更显著影响。至关重要的是要彻底测试您的特定工作负载，以确保在所选带宽权重下获得最佳性能。

注意事项

- 部分实例类型支持可配置的实例带宽。有关更多信息，请参阅支持的实例类型。
- 使用ebs-1带宽权重可将 EBS 带宽提高多达 25%，从而提高 I/O 密集型应用程序的性能。但是，请记住，VPC 网络带宽将减少相同的绝对值（EBS 和网络之间的总带宽规格不会改变）。
- 带宽权重的变化会显著影响 I/O 性能。随着vpc-1带宽权重的增加，网络带宽会增加，但是 EBS 卷的 IOPS 可能会低于预期。这是因为您可能会在 IOPS 限制之前达到 EBS 带宽限制，尤其是在 I/O 大小较大的情况下。例如，由于 EBS 带宽降低，通常支持 240,000 IOPS、I/O 大小为 16 KiB 的实例类型在使用vpc-1带宽权重时可能会降低 IOPS。
- 务必测试您的特定工作负载，以确保您选择的带宽权重满足您的性能需求。

- 您可以在实例启动期间配置带宽权重，也可以针对已停止的实例修改带宽权重。有关更多信息，请参阅为您的实例配置带宽权重。
- 您可以配置实例带宽权重，无需支付额外费用。

Amazon EBS I/O 特性和监控

在给定卷配置中，某些 I/O 特性会对 EBS 卷的性能表现造成影响。

- 支持 SSD 的卷、通用型 SSD（gp2和gp3）和预配置 IOPS 固态硬盘（io1和io2），无论 I/O 操作是随机还是顺序操作，都能提供一致的性能。
- 支持 HDD 的卷，即吞吐量优化 HDD (st1) 和 Cold HDD (sc1)，仅在 I/O 操作量大且连续运行时才能提供最佳性能。

要了解 SSD 和 HDD 卷在您的应用程序中性能如何，务必要知道卷上的需求之间的联系、卷能支持的 IOPS 数量、完成 I/O 操作所需的时间，以及卷的吞吐量限制。

主题

- IOPS
- 卷队列长度和延迟
- I/O 大小和卷吞吐量限制
- 使用监控 I/O 特性 CloudWatch
- 监控实时 I/O 性能统计信息
- 相关资源

IOPS

IOPS 是一种计量单位，表示的效率input/output operations per second. The operations are measured in KiB, and the underlying drive technology determines the maximum amount of data that a volume type counts as a single I/O. I/O size is capped at 256 KiB for SSD volumes and 1,024 KiB for HDD volumes because SSD volumes handle small or random I/O远高于 HDD 卷。

当小型 I/O 操作在物理上连续进行时，Amazon EBS 会尝试将这些操作合并为单个 I/O 操作，直至最大 I/O 大小。同样，当 I/O 操作大于最大 I/O 大小时，Amazon EBS 会尝试将这些操作分为较小的 I/O 操作。下表显示了一些示例。

卷类型	最大 I/O 大小	来自应用程序的 I/O 操作	IOPS 数量	备注
SSD	256 KiB	1 个 1024 KiB I/O 操作	4（1024÷256=4）	亚马逊 EBS 将 1,024 KiB 的 I/O 操作拆分为四个较小的 256 KiB 操作。
		8 个连续 32KiB I/O 操作	1（8x32=256）	Amazon EBS 将 8 个连续 32 KiB I/O 操作合并为一个 256 KiB 操作。
		8 个随机 32 KiB I/O 操作	8	Amazon EBS 分别计算随机 I/O 操作。
HDD	1,024 KiB	1 个 1024 KiB I/O 操作	1	I/O 操作已经等于最大 I/O 大小。它不会被合并或拆分。
		8 个连续 128KiB I/O 操作	1（8x128=1024）	Amazon EBS 将 8 个连续 128 KiB I/O 操作合并为一个 1,024 KiB I/O 操作。
		8 个随机 32 KiB I/O 操作	8	Amazon EBS 分别计算随机 I/O 操作。

因此，当您创建一个支持 3,000 IOPS 的 SSD 卷（通过预置具有 3,000 IOPS 的 `io1` 或 `io2` 卷、将 `gp2` 卷大小调整为 1,000 GiB，或者使用 `gp3` 卷）并将其附加到可以提供足够带宽的 EBS 优化实例时，您可以每秒传输最高 3000 次数据 I/O，其吞吐量由 I/O 大小决定。

卷队列长度和延迟

卷队列长度是指等待设备处理的 I/O 请求的数量。延迟是 I/O 操作的真实 end-to-end客户机时间，换句话说，就是从向 EBS 发送 I/O 到收到来自 EBS 的 I/O 读取或写入已完成的确认之间经过的时间。队列长度必须进行适当调整，以便与 I/O 大小和延迟匹配，避免在访客操作系统上或在到 EBS 的网络链路上产生瓶颈。

每个工作负载的最佳队列长度不同，具体取决于您的特定应用程序对于 IOPS 和延迟的敏感程度。如果您的工作负载未提供足够的 I/O 请求来充分利用 EBS 卷的可用性能，则卷可能无法提供您预置 IOPS 或吞吐量。

事务密集型应用程序对 I/O 延迟增加很敏感，很适合支持 SSD 的卷。您可以通过使卷保持较小的队列长度和较高的 IOPS 数量，来维持高 IOPS 和低延迟。持续迫使一个卷的 IOPS 高于它能够支持的 IOPS 可能增加 I/O 延迟。

吞吐量密集型应用程序对 I/O 延迟增加较不敏感，很适合使用 HDD 支持的卷。您可以在执行大型顺序 I/O 时维持大队列长度，从而对 HDD 卷保持高吞吐量。

I/O 大小和卷吞吐量限制

对于 SSD 卷，如果 I/O 大小非常大，由于达到卷的吞吐量限制，您的 IOPS 数可能会少于预配置数量。例如，如果gp2容量低于 1,000 GiB 且可用的突发积分，其 IOPS 限制为 3,000，而卷吞吐量限制MiB/s. If you are using a 256 KiB I/O size, your volume reaches its throughput limit at 1000 IOPS (1000 x 256 KiB = 250 MiB). For smaller I/O sizes (such as 16 KiB), this same volume can sustain 3,000 IOPS because the throughput is well below 250 MiB/s. (These examples assume that your volume's I/O为 250 则未达到实例的吞吐量限制。 ）有关每种 EBS 卷类型吞吐量限制的更多信息，请参阅 Amazon EBS 卷类型。

对于较小的 I/O 操作，您可能会看到从实例内部测量的 higher-than-provisioned IOPS 值。当实例操作系统在将小型 I/O 操作传递到 Amazon EBS 之前将其合并为一个较大的操作时，会发生这种情况。

如果您的工作负载在 HDD 支持的 `st1` 和 `sc1` 卷上使用顺序 I/O，则从实例内部进行度量时，您的 IOPS 值可能会高于预期数量。当实例操作系统将顺序 I/O 进行合并，并以 1024 KiB 大小为单位来对其进行计数时，会发生这种情况。如果您的工作负载使用小型随机 I/O，则吞吐量可能会低于您的预期。这是因为我们会将每个随机的非顺序 I/O 计入总的 IOPS 计数，这可能导致您比预期更快达到卷的 IOPS 限制。

无论您的 EBS 卷类型如何，如果您在配置中没有达到预期的 IOPS 或吞吐量，请确保您的 EC2 实例带宽不是限制因素。您应始终使用最新一代的 EBS 优化实例（或包含 10 Gb/s network connectivity) for

optimal performance. Another possible cause for not experiencing the expected IOPS is that you are not driving enough I/O 个 EBS 卷的实例）。

使用监控 I/O 特性 CloudWatch

您可以使用每个卷的CloudWatch 卷指标来监控这些 I/O 特征。

监视停滞的 I/O

VolumeStalledIOCheck 监控 EBS 卷的状态以确定您的卷何时受损。该指标是一个二进制值，将根据 EBS 卷能否完成 I/O 操作返回 0（通过）或1（失败）状态。

如果该VolumeStalledIOCheck指标失败，您可以等待 Amazon 问题得到解决，也可以采取措施，例如更换受影响的卷或停止并重新启动该卷所连接的实例。在大多数情况下，当该指标失败时，EBS 将在几分钟内自动诊断并恢复您的卷。您可以使用中的 Pause I/O 操作 Amazon Fault Injection Service 来运行受控实验，以测试您的架构并基于此指标进行监控，从而提高存储故障恢复能力。

监控卷的 I/O 延迟

您可以分别使用和VolumeAvgWriteLatency指标监控 Amazon EBS 卷的读取VolumeAvgReadLatency和写入操作的平均延迟。

如果您的 I/O 延迟高于您的需求，请确保您的应用程序尝试驱动的 IOPS 或吞吐量不会超过您为卷预配置的。使用以下公式计算在特定时间段内为您的卷带来的平均 IOPS 和吞吐量，然后将其与卷的预配置 IOPS 和吞吐量进行比较。

$$\text{Estimated average IOPS in ops/s} = \frac{\text{Sum(VolumeReadOps)} + \text{Sum(VolumeWriteOps)}}{\text{Period} - \text{Sum(VolumeIdleTime)}}$$

$$\text{Estimated average throughput in KiB/s} = \frac{(\text{Sum(VolumeReadBytes)} + \text{Sum(VolumeWriteBytes)}) / 1024}{\text{Period} - \text{Sum(VolumeIdleTime)}}$$

您还可以监控VolumeIOPSExceededCheck和VolumeThroughputExceededCheck指标，以确定您的工作负载是否在给定分钟内持续尝试提高 IOPS 或吞吐量大于卷的预配置性能。如果驱动的 IOPS 持续超过卷的预配置 IOPS 性能，则该VolumeIOPSExceededCheck指标将返回。1如果驱动吞吐量持续超过卷的预配置吞吐量性能，则该VolumeThroughputExceededCheck指标将返回1。如果驱动的 IOPS 和吞吐量在卷的预配置性能范围内，则返回指标。0

如果您的应用程序需要的 IOPS 数量超出您的卷所能提供的数量，则应考虑使用以下选项之一：

- gp3、io2 或 io1 卷，预置了足够 IOPS 以实现所需延迟
- 更大的 gp2 卷，提供足够的基准 IOPS 性能

HDD 支持的 st1 和 sc1 卷经过特别设计，旨在对使用 1024 KiB 最大 I/O 大小的工作负载提供最佳性能。要确定卷的平均 I/O 大小，请VolumeWriteBytes除以VolumeWriteOps。同样的计算也适用于读取操作。如果平均 I/O 大小低于 64 KiB，则提高发送到 st1 或 sc1 卷的 I/O 操作的大小应该能够提高性能。

监控**gp2**、**st1**和**sc1**音量的突发存储桶平衡

BurstBalance 以剩余余额百分比的形式显示 gp2、st1 和 sc1 卷的突增存储桶余额。当您的突增存储桶耗尽时，卷 I/O（对于 gp2 卷）或卷吞吐量（对于 st1 和 sc1 卷）会限定在基准水平。检查 BurstBalance 值以确定卷是否因为此原因而受限制。有关可用 Amazon EBS 指标的完整列表，请参阅亚马逊 EBS 的亚马逊 CloudWatch 指标和基于 Nitro 的实例的 Amazon EBS 指标。

监控实时 I/O 性能统计信息

您可以访问附加到基于 Nitro的亚马逊实例的 Amazon EBS 卷的实时详细性能统计数据。 EC2

您可以组合这些统计数据来得出平均延迟和 IOPS，或者检查 I/O 操作是否已完成。您还可以查看应用程序超过 EBS 卷或所连接实例的预配置 IOPS 或吞吐量限制的总时间。通过跟踪这些统计数据随时间推移的增长情况，您可以确定是否需要提高预配置 IOPS 或吞吐量限制以优化应用程序的性能。详细的性能统计数据还包括读取和写入 I/O 操作的直方图，这些直方图通过跟踪延迟区间内完成的 I/O 操作总数来提供 I/O 延迟的分布情况。

有关更多信息，请参阅 Amazon EBS 的详细绩效统计数据。

相关资源

有关 Amazon EBS I/O 特征的更多信息，请参阅以下 re:Invent 演示文稿：Amazon EBS：为性能而设计。

Amazon EBS 和 RAID 配置

通过 Amazon EBS，您可以使用可与传统裸机服务器结合使用的任何标准 RAID 配置，只要实例的操作系统支持该特定 RAID 配置。这是因为，所有 RAID 都是在软件级别上实现的。

Amazon EBS 卷的数据可在可用区内多个服务器间进行复制，以防由于任何单个组件发生故障导致数据丢失。此复制使得 Amazon EBS 卷的可靠程度比普通磁盘高 10 倍。有关更多信息，请参阅 Amazon EBS 功能。

内容

- RAID 配置选项
- 创建 RAID 0 阵列
- 创建 RAID 阵列中卷的快照

RAID 配置选项

相比在单个 Amazon EBS 卷上配置，通过创建 RAID 0 阵列，文件系统可以获得更高性能。如果 I/O 性能至关重要，请使用 RAID 0。I/O 通过 RAID 0 在卷内以条带状分布。如果您添加卷，则会直接增加吞吐量和 IOPS。但是，请记住，条带的性能仅限于集中性能最差的卷，并且集中的单个卷丢失会导致阵列数据完全丢失。

RAID 0 阵列的最终大小是阵列中各个卷的大小之和，带宽是阵列中各个卷的可用带宽之和。例如，预置 IOPS 为 4000 的两个 500 GiB `io1` 卷将创建可用带宽为 8000 IOPS、吞吐量为 1000 MiB/s 的 1000 GiB RAID 0 阵列。

> **Important**
>
> 不建议对 Amazon EBS 使用 RAID 5 和 RAID 6，因为这些 RAID 模式的奇偶校验写入操作会使用您的卷的一些可用 IOPS。根据您的 RAID 阵列配置，这些 RAID 模式提供的可用 IOPS 比 RAID 0 配置少 20-30%。成本增加也是与这些 RAID 模式有关的一个因素；在使用相同的卷大小和速度时，一个 2 卷 RAID 0 阵列明显胜过两倍成本的 4 卷 RAID 6 阵列。
>
> RAID 1 也不建议用于 Amazon EBS。与非 RAID 配置相比，RAID 1 需要更多的 Amazon EC2 到 Amazon EBS 带宽，因为数据是同时写入多个卷的。此外，RAID 1 不提供任何写入性能改进。

创建 RAID 0 阵列

使用以下过程创建 RAID 0 阵列。

注意事项

- 在执行此过程之前，您必须确定 RAID 0 阵列的大小以及预调配多少 IOPS。

- 为阵列创建具有相等大小和 IOPS 性能值的卷。确保您创建的阵列不会超过 EC2 实例的可用带宽。
- 您应避免从 RAID 卷启动。如果有一台设备出现故障，您可能无法启动操作系统。

Linux 实例

在 Linux 上创建 RAID 0 阵列

1. 为阵列创建 Amazon EBS 卷。有关更多信息，请参阅 创建 Amazon EBS 卷。
2. 将 Amazon EBS 卷附加到要承载该阵列的实例。有关更多信息，请参阅将 Amazon EBS 卷附加到亚马逊 EC2 实例。
3. 使用 mdadm 命令从新附加的 Amazon EBS 卷创建逻辑 RAID 设备。将阵列中的卷数替换为*number_of_volumes*阵列中每个卷的设备名称（例如/dev/xvdf）*device_name*。也可以*MY_RAID*用自己的唯一名称代替数组。

   > **Note**
   > 您可以使用 lsblk 命令列出实例上的设备以找到设备名称。

   要创建 RAID 0 阵列，请运行以下命令（注意，--level=0 选项用于将阵列条带化）：

   ```
   [ec2-user ~]$ sudo mdadm --create --verbose /dev/md0 --level=0 --name=MY_RAID --raid-devices=number_of_volumes device_name1 device_name2
   ```

   > **Tip**
   > 如您遇到 mdadm: command not found 错误，请使用以下命令安装 mdadm：sudo yum install mdadm。

4. 给 RAID 阵列一些时间进行初始化和同步。您可以借助下面的命令跟踪这些操作的进度：

   ```
   [ec2-user ~]$ sudo cat /proc/mdstat
   ```

   下面是示例输出：

   ```
   Personalities : [raid0]
   md0 : active raid0 xvdc[1] xvdb[0]
   ```

```
      41910272 blocks super 1.2 512k chunks

unused devices: <none>
```

通常，您可以通过下面的命令显示有关 RAID 阵列的详细信息：

```
[ec2-user ~]$ sudo mdadm --detail /dev/md0
```

下面是示例输出：

```
/dev/md0:
           Version : 1.2
     Creation Time : Wed May 19 11:12:56 2021
        Raid Level : raid0
        Array Size : 41910272 (39.97 GiB 42.92 GB)
      Raid Devices : 2
     Total Devices : 2
       Persistence : Superblock is persistent

       Update Time : Wed May 19 11:12:56 2021
             State : clean
    Active Devices : 2
   Working Devices : 2
    Failed Devices : 0
     Spare Devices : 0

        Chunk Size : 512K

Consistency Policy : none

              Name : MY_RAID
              UUID : 646aa723:db31bbc7:13c43daf:d5c51e0c
            Events : 0

    Number   Major   Minor   RaidDevice State
       0     202       16        0      active sync   /dev/sdb
       1     202       32        1      active sync   /dev/sdc
```

5. 在您的 RAID 阵列上创建一个文件系统，并为该文件系统分配一个稍后在装载该文件系统时使用的标签。例如，要创建带有标签的 ext4 文件系统*MY_RAID*，请运行以下命令：

```
[ec2-user ~]$ sudo mkfs.ext4 -L MY_RAID /dev/md0
```

根据应用程序的要求或操作系统的限制，您可以使用其他文件系统类型，如 ext3 或 XFS（请参阅您的文件系统文档以了解相应的文件系统创建命令）。

6. 要确保 RAID 阵列在启动时自动重组，请创建一个包含 RAID 信息的配置文件：

```
[ec2-user ~]$ sudo mdadm --detail --scan | sudo tee -a /etc/mdadm.conf
```

> **Note**
>
> 如果您使用的是 Linux 发行版而非 Amazon Linux，您可能需要修改此命令。例如，您可能需要将文件放在不同的位置，或者添加 `--examine` 参数。有关更多信息，请在 Linux 实例上运行 man mdadm.conf。

7. 创建新的 Ramdisk Image 以为新的 RAID 配置正确地预加载块储存设备模块：

```
[ec2-user ~]$ sudo dracut -H -f /boot/initramfs-$(uname -r).img $(uname -r)
```

8. 为 RAID 阵列创建装载点。

```
[ec2-user ~]$ sudo mkdir -p /mnt/raid
```

9. 最后，在已创建的装载点上安装 RAID 设备：

```
[ec2-user ~]$ sudo mount LABEL=MY_RAID /mnt/raid
```

RAID 设备现已准备就绪，可供使用。

10. （可选）要在每次系统重启时装载此 Amazon EBS 卷，可在 `/etc/fstab` 文件中为该设备添加一个条目。

    a. 创建 `/etc/fstab` 文件的备份，当您进行编辑时意外损坏或删除了此文件的情况下，可以使用该备份。

    ```
    [ec2-user ~]$ sudo cp /etc/fstab /etc/fstab.orig
    ```

    b. 使用您常用的文本编辑器（如 `/etc/fstab` 或 nano）打开 vim 文件。

c. 注释掉任何以“UUID=”开头的行，然后，在文件末尾，使用以下格式为您的 RAID 卷添加新行：

```
device_label mount_point file_system_type fs_mntops fs_freq fs_passno
```

此行的最后三个字段分别是文件系统装载选项、文件系统转储频率和启动时的文件系统检查顺序。如果您不知道这些值应该是什么，请使用以下示例中的值（defaults,nofail 0 2））。有关 /etc/fstab 条目的更多信息，请参阅 fstab 手册页面（方法：在命令行输入 man fstab）。例如，要在设备上的装载点 /mnt/raid 装载带 MY_RAID 标签的 ext4 文件系统，请将以下条目添加到 /etc/fstab。

> **Note**
>
> 如果您要在未附加该卷的情况下启动实例（例如，以便该卷可以在不同实例之间向后和向前移动），则应添加 nofail 装载选项，该选项允许实例即使在卷安装过程中出现错误时也可启动。Debian 衍生物（例如 Ubuntu）还必须添加 nobootwait 装载选项。

```
LABEL=MY_RAID       /mnt/raid   ext4    defaults,nofail        0       2
```

d. 在您将新条目添加到 /etc/fstab 后，需要检查您的条目是否有效。运行 sudo mount -a 命令以在 /etc/fstab 中装载所有文件系统。

```
[ec2-user ~]$ sudo mount -a
```

如果上述命令未产生错误，说明您的 /etc/fstab 文件正常，您的文件系统会在下次启动时自动装载。如果该命令产生了任何错误，请检查这些错误并尝试更正 /etc/fstab。

> **Warning**
>
> /etc/fstab 文件中的错误可能显示系统无法启动。请勿关闭 /etc/fstab 文件中有错误的系统。

e. （可选）如果您无法确定如何更正 /etc/fstab 错误，则始终可以使用以下命令还原您的备份 /etc/fstab 文件。

```
[ec2-user ~]$ sudo mv /etc/fstab.orig /etc/fstab
```

Windows 实例

在 Windows 上创建 RAID 0 阵列

1. 为阵列创建 Amazon EBS 卷。有关更多信息，请参阅 创建 Amazon EBS 卷。
2. 将 Amazon EBS 卷附加到要承载该阵列的实例。有关更多信息，请参阅将 Amazon EBS 卷附加到亚马逊 EC2 实例。
3. 连接到您的 Windows 实例。有关更多信息，请参阅连接到 Windows 实例。
4. 打开命令提示符并键入 diskpart 命令。

```
diskpart

Microsoft DiskPart version 6.1.7601
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: WIN-BM6QPPL51CO
```

5. 在 DISKPART 提示符处，使用以下命令列出可用磁盘。

```
DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online           30 GB      0 B
  Disk 1    Online            8 GB      0 B
  Disk 2    Online            8 GB      0 B
```

   标识您要在阵列中使用的磁盘并记下其磁盘编号。

6. 您要在阵列中使用的每个磁盘都必须是不包含任何现有卷的联机动态磁盘。使用以下步骤可将基本磁盘转换为动态磁盘并删除任何现有卷。

   a. 使用以下命令选择要在阵列中使用的磁盘，*n*替换为磁盘号。

```
DISKPART> select disk n

Disk n is now the selected disk.
```

b. 如果所选磁盘列为 Offline 状态，则通过运行 online disk 命令使它联机。

c. 如果所选磁盘在前面的 Dyn 命令输出的 list disk 列中没有星号，则需要将它转换为动态磁盘。

```
DISKPART> convert dynamic
```

> **Note**
>
> 如果显示磁盘写保护错误，可以使用 ATTRIBUTE DISK CLEAR READONLY 命令清除只读标记，然后重试动态磁盘转换。

d. 使用 detail disk 命令检查所选磁盘是否存在现有卷。

```
DISKPART> detail disk

XENSRC PVDISK SCSI Disk Device
Disk ID: 2D8BF659
Type   : SCSI
Status : Online
Path   : 0
Target : 1
LUN ID : 0
Location Path : PCIROOT(0)#PCI(0300)#SCSI(P00T01L00)
Current Read-only State : No
Read-only  : No
Boot Disk  : No
Pagefile Disk  : No
Hibernation File Disk  : No
Crashdump Disk  : No
Clustered Disk  : No

  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 2     D   NEW VOLUME   FAT32  Simple      8189 MB  Healthy
```

记下磁盘上的任何卷编号。在该示例中，卷编号是 2。如果没有卷，则您可以跳过下一步。

e. （仅当上一步中标识了卷时才需要）选择并删除磁盘上在上一步中标识的所有现有卷。

> **Warning**
>
> 这会销毁卷上的所有现有数据。

i. 选择音量，*n*用您的卷号代替。

```
DISKPART> select volume n
Volume n is the selected volume.
```

ii. 删除卷。

```
DISKPART> delete volume

DiskPart successfully deleted the volume.
```

iii. 对所选磁盘上需要删除的每个卷重复这些子步骤。

f. 对您要在阵列中使用的每个磁盘重复Step 6。

7. 验证您要使用的磁盘现在是否为动态。在这种情况下，我们将磁盘 1 和磁盘 2 用于 RAID 卷。

```
DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online           30 GB      0 B
  Disk 1    Online            8 GB      0 B   *
  Disk 2    Online            8 GB      0 B   *
```

8. 创建 RAID 阵列。在 Windows 上，RAID 0 卷指条带卷。

   要在磁盘 1 和 2 上创建条带卷阵列，请使用以下命令（注意，`stripe` 选项用于将阵列条带化）：

```
DISKPART> create volume stripe disk=1,2
DiskPart successfully created the volume.
```

9. 验证您的新卷。

```
DISKPART> list volume
```

```
DISKPART> list volume

Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
----------  ---  -----------  -----  ----------  -------  ---------  --------
Volume 0     C                NTFS   Partition     29 GB  Healthy    System
Volume 1                      RAW    Stripe        15 GB  Healthy
```

请注意，Type 列现在表示卷 1 是 stripe 卷。

10. 选择并格式化您的卷，以便可以开始使用它。

    a. 选择要格式化的音量，*n*用卷号代替。

    ```
    DISKPART> select volume n

    Volume n is the selected volume.
    ```

    b. 格式化卷。

    > **Note**
    >
    > 要执行完整格式化，请省略 quick 选项。

    ```
    DISKPART> format quick recommended label="My new volume"

      100 percent completed

    DiskPart successfully formatted the volume.
    ```

    c. 向卷分配可用驱动器号。

    ```
    DISKPART> assign letter f

    DiskPart successfully assigned the drive letter or mount point.
    ```

新卷现在已准备就绪，可供使用。

创建 RAID 阵列中卷的快照

如果要使用快照备份 RAID 阵列中 EBS 卷上的数据，则必须确保快照的一致性。原因在于这些卷的快照是独立创建的。从不同步的快照恢复 RAID 阵列中的 EBS 卷会降低阵列的完整性。

要为 RAID 阵列创建一组一致的快照，请使用 EBS 多卷快照。多卷快照允许您在连接到实例的多个 EBS 卷上拍摄 point-in-time、数据协调和崩溃一致的快照。 EC2 您不需要停止实例以在多个卷之间协调来确保一致性，因为快照将跨多个 EBS 卷自动拍摄。有关更多信息，请参阅创建 Amazon EBS 快照下的创建多卷快照的步骤。

对 Amazon EBS 卷进行基准测试

您可以通过模拟 I/O 工作负载来测试 Amazon EBS 卷的性能。过程如下所述：

1. 启动 EBS 优化实例。
2. 创建新的 EBS 卷。
3. 将这些卷附加到您的 EBS 优化实例。
4. 配置并挂载块储存设备。
5. 安装工具以便测试 I/O 性能。
6. 测试卷的 I/O 性能。
7. 删除卷并终止实例，确保不会继续引发更改。

> **Important**
>
> 某些过程可能会对您进行基准测试的 EBS 卷上的现有数据造成破坏。基准测试程序适用于出于测试目的而特别创建的卷，并不适用于生产卷。

设置实例

为了获得最佳的 EBS 卷性能，我们建议您使用 EBS 优化实例。EBS 优化的实例通过实例在 Amazon 和 A EC2 mazon EBS 之间提供专用的吞吐量。EBS 优化的实例在 Amazon 和 A EC2 mazon EBS 之间提供专用带宽，其规格取决于实例类型。

要创建 EBS 优化实例，请在使用 Amazon EC2 控制台启动实例时选择 “作为 EBS 优化实例启动”，或者在使用命令行--ebs-optimized时指定。请确保选择的实例类型支持该选项。

设置 Provisioned IOPS SSD 或 通用型 SSD 卷

要使用亚马逊 EC2 控制台创建预配置 IOPS 固态硬盘（**io1**和**io2**）或通用固态硬盘（**gp2**和**gp3**）卷，请为卷类型选择预配置 IOPS 固态硬盘 (io1)、预配置 IOPS 固态硬盘 (io2) 、通用固态硬盘 (gp2) 或通用固态硬盘 (gp3)。在命令行中，为 `io1` 参数指定 `io2`、`gp2`、`gp3` 或 --volume-type。对于 `io1`、`io2` 和 `gp3` 卷，请指定 --iops 参数的每秒 I/O 操作数（IOPS）。有关更多信息，请参阅Amazon EBS 卷类型和创建 Amazon EBS 卷。

（仅限 Linux 实例）要了解这些示例测试，我们建议您创建一个包含 6 个卷的高性能 RAID 0 阵列。因为您是按照预配置的 GB 数量（以及为 io1、io2 和 gp3 卷预配置的 IOPS 数量，而不是卷的数量）付费，因此创建多个较小卷并使用它们来创建条带集不会产生额外费用。如果您是使用 Oracle Orion 来测试卷的性能，则它可以模拟 Oracle ASM 的条带化操作，因此我们建议您让 Orion 执行条带化分区。如果您使用的是其他基准测试工具，则需要自己对卷执行条带化分区。

有关如何创建 RAID 0 阵列的更多信息，请参阅创建 RAID 0 阵列。

设置吞吐量优化型 HDD（**st1**）卷或 Cold HDD（**sc1**）卷

要创建`st1`卷，请在使用 Amazon EC2 控制台创建卷时选择 “吞吐量优化 HDD”，或者--type **st1**在使用命令行时指定。要创建`sc1`卷，请在使用 Amazon EC2 控制台创建卷时选择 Cold HDD，或者--type **sc1**在使用命令行时指定。有关创建 EBS 卷的信息，请参阅创建 Amazon EBS 卷。有关将这些卷附加到您的实例的信息，请参阅 将 Amazon EBS 卷附加到亚马逊 EC2 实例。

（仅限 Linux 实例） Amazon 提供了一个用于的 JSON 模板 Amazon CloudFormation ，可简化此设置过程。访问模板并将其另存为 JSON 文件。 Amazon CloudFormation 允许您配置自己的 SSH 密钥，并提供了一种更简单的方法来设置性能测试环境来评估容`st1`量。此模板会创建一个最新一代的实例以及一个 2 TiB 的 `st1` 卷，然后将该卷附加到 `/dev/xvdf` 处的实例。

（仅限 Linux 实例）使用模板创建 HDD 卷

1. 在 https://console.aws.amazon.com/cloudformat ion 上打开 Amazon CloudFormation 控制台。
2. 选择 Create Stack。
3. 选择 Upload a Template to Amazon S3，然后选择之前获得的 JSON 模板。
4. 为堆栈命名，例如 “ebs-perf-testing”，然后选择实例类型（默认为 r3.8xlarge）和 SSH 密钥。
5. 选择 Next 两次，然后选择 Create Stack。
6. 新堆栈的状态从 CREATE_IN_PROGRESS 变为 COMPLETE 后，选择 Outputs（输出）以获取新实例的公有 DNS 条目，新实例将附加一个 2TiB 的 `st1` 卷。

7. 以用户 **ec2-user** 的身份使用 SSH 连接到您的新堆栈（使用从上一步的 DNS 条目中获得的主机名）。
8. 继续执行安装基准测试工具。

安装基准测试工具

下表列出了您可用于对 EBS 卷的性能进行基准测试的部分可用工具。

Linux 实例

工具	描述

fio	用于测试 I/O 性能。（请注意，fio 依赖于 `libaio-devel` 。）
	
	要在 Amazon Linux 上安装 fio，请运行以下命令：
	
	`$ sudo yum install -y fio`
	
	要在 Ubuntu 上安装 fio，请执行以下命令：
	
	`sudo apt-get install -y fio`

Oracle Orion 校准工具	用于校准要与 Oracle 数据库搭配使用的存储系统的 I/O 性能。

Windows 实例

工具	描述
DiskSpd	DiskSpd 是微软 Windows、Windows Server 和云服务器基础架构工程团队推出的存储性能工具。它可在 d https://github.com/Microsoft/iskspd/ 发行版上下载。 下载 `diskspd.exe` 可执行文件后，以管理权限打开命令提示符（通过选择“以管理员身份运行”），然后导航到复制 `diskspd.exe` 文件的目录。

工具	描述
	将所需的 diskspd.exe 可执行文件从相应的可执行文件的文件夹（amd64fre、armfre 或 x86fre）复制到简短的路径，如 C:\DiskSpd 。在大多数情况下，您需要 DiskSpd 从该amd64fre文件夹中获得 64 位版本的。 的源代码托管在：https://github.com/Microsoft/diskspd GitHub 上。 DiskSpd
CrystalDiskMark	CrystalDiskMark 是一款简单的磁盘基准测试软件。它可在以下网址下载：https://crystalmark。 info/en/software/crystaldiskmark/。

这些基准测试工具可支持各种测试参数。您应该使用命令来测试您的卷支持的工作负载。下面提供的命令示例可帮助您入门。

选择卷队列长度

基于工作负载和卷类型选择最佳卷队列长度。

SSD 支持的卷的队列长度

要确定支持 SSD 的卷上工作负载的最佳队列长度，建议您将每 1000 IOPS（通用型 SSD 卷的基准量，Provisioned IOPS SSD 卷的预置量）对应 1 个队列长度作为目标。然后，您可以监控应用程序性能，并根据应用程序需求调整该值。

在达到预配置 IOPS、吞吐量或最佳系统队列长度值之前，增加队列长度有好处，当前队列长度设置为 32。举例来说，预配置 3,000 IOPS 的卷应该将队列长度设置为 3。您应该尝试将这些值调高或调低，看看对于您的应用程序，什么样的设置能够实现最佳性能。

HDD 支持的卷的队列长度

要确定 HDD 卷上工作负载的最佳队列长度，建议您在执行 1MiB 顺序 I/O 时以至少为 4 的队列长度作为目标。然后，您可以监控应用程序性能，并根据应用程序需求调整该值。例如，突发吞吐量分别为 500 MiB/s and IOPS of 500 should target a queue length of 4, 8, or 16 while performing 1,024 KiB, 512 KiB, or 256 KiB sequential I/Os 的 2 TiB st1 卷。您应该尝试将这些值调高或调低，看看对于您的应用程序，什么样的设置能够实现最佳性能。

禁用 C 状态

在运行基准测试之前，您应禁用处理器 C 状态。支持此功能的 CPU 中的核心在暂时空闲时，会进入 C 状态以节省功耗。在调用核心以恢复处理时，将经过一段特定的时间，核心才能再次全速运行。此延迟可能会干扰处理器基准测试例程。有关 C 状态以及哪些 EC2 实例类型支持这些状态的更多信息，请参阅您的 EC2实例的处理器状态控制。

Linux 实例

您可在 Amazon Linux、RHEL 和 CentOS 上按以下所示禁用 C 状态：

1. 获取 C 状态数。

```
$ cpupower idle-info | grep "Number of idle states:"
```

2. 从 c1 到 cN 禁用 C 状态。理想情况下，核心应处于状态 c0。

```
$ for i in `seq 1 $((N-1))`; do cpupower idle-set -d $i; done
```

Windows 实例

在 Windows 上，您可以按以下所示禁用 C 状态：

1. 在 PowerShell，获取当前的有功功率方案。

```
$current_scheme = powercfg /getactivescheme
```

2. 获取电源方案 GUID。

```
(Get-WmiObject -class Win32_PowerPlan -Namespace "root\cimv2\power" -Filter
 "ElementName='High performance'").InstanceID
```

3. 获取电源设置 GUID。

```
(Get-WmiObject -class Win32_PowerSetting -Namespace "root\cimv2\power" -Filter
 "ElementName='Processor idle disable'").InstanceID
```

4. 获取电源设置子组 GUID。

```
(Get-WmiObject -class Win32_PowerSettingSubgroup -Namespace "root\cimv2\power" -
Filter "ElementName='Processor power management'").InstanceID
```

5. 通过将索引的值设置为 1 来禁用 C 状态。值为 0 表示已禁用 C 状态。

```
powercfg /
setacvalueindex <power_scheme_guid> <power_setting_subgroup_guid> <power_setting_guid>
 1
```

6. 设置活动方案以确保设置已保存。

```
powercfg /setactive <power_scheme_guid>
```

执行基准测试

以下步骤介绍各种 EBS 卷类型的基准测试命令。

对附加了 EBS 卷的 EBS 优化实例运行以下命令。如果已从快照创建 EBS 卷，在执行基准测试之前，请确保初始化这些卷。有关更多信息，请参阅 创建后手动初始化卷。

> **Tip**
>
> 您可以使用 EBS 详细性能统计数据提供的 I/O 延迟直方图来比较基准测试中的 I/O 性能分布。有关更多信息，请参阅 Amazon EBS 的详细绩效统计数据。

完成对卷的测试后，可参阅以下主题来帮助清除卷：删除 Amazon EBS 卷和终止实例。

基准 Provisioned IOPS SSD 和 通用型 SSD 卷

Linux 实例

在您创建的 RAID 0 阵列上运行 fio。

以下命令可执行 16 KB 随机写入操作。

```
$ sudo fio --directory=/mnt/p_iops_vol0 --ioengine=psync --name fio_test_file --
direct=1 --rw=randwrite --bs=16k --size=1G --numjobs=16 --time_based --runtime=180 --
group_reporting --norandommap
```

以下命令可执行 16 KB 随机读取操作。

```
$ sudo fio --directory=/mnt/p_iops_vol0 --name fio_test_file --direct=1 --rw=randread
 --bs=16k --size=1G --numjobs=16 --time_based --runtime=180 --group_reporting --
norandommap
```

有关解析结果的更多信息，请参阅以下教程：使用 fio 检查磁盘 IO 性能。

Windows 实例

在您创建的卷上运行 DiskSpd。

以下命令将使用位于 C: 驱动器上的 20GB 测试文件运行 30 秒随机 I/O 测试（25% 的写入比率和 75% 的读取比率以及 8K 块大小）。它将使用八个工作线程，每个线程具有四个未完成的 I/O 和一个 1GB 的写入熵值种子。测试结果将保存到名为 DiskSpeedResults.txt 的文本文件中。这些参数模拟 SQL Server OLTP 工作负载。

```
diskspd -b8K -d30 -o4 -t8 -h -r -w25 -L -Z1G -c20G C:\iotest.dat > DiskSpeedResults.txt
```

有关解释结果的更多信息，请参阅本教程：使用磁盘检查磁盘 IO 性能。SPd

st1 和 sc1 卷（Linux 实例）基准测试

在 fio 或 st1 卷上运行 sc1。

> **Note**
>
> 在执行这些测试之前，请按为 st1 和 sc1 上的高吞吐量读取密集型工作负载增加预读值（仅限 Linux 实例）所述在实例上设置缓冲 I/O。

以下命令针对附加的 st1 块设备（例如 /dev/xvdf）执行 1MiB 的顺序读取操作：

```
$ sudo fio --filename=/dev/<device> --direct=1 --rw=read --randrepeat=0
 --ioengine=libaio --bs=1024k --iodepth=8 --time_based=1 --runtime=180 --
name=fio_direct_read_test
```

以下命令针对附加的 st1 块储存设备执行 1 MiB 的顺序写入操作：

```
$ sudo fio --filename=/dev/<device> --direct=1 --rw=write --randrepeat=0
 --ioengine=libaio --bs=1024k --iodepth=8 --time_based=1 --runtime=180 --
name=fio_direct_write_test
```

有些工作负载可对块储存设备的不同部分混合执行顺序读取和顺序写入操作。要对此类工作负载进行基准测试，我们建议您为读取和写入操作单独、同时使用 fio 作业，并为每个作业使用 fio `offset_increment` 选项将块储存设备的不同位置作为目标。

运行此类工作负载比顺序写入或顺序读取工作负载要复杂一些。使用文本编辑器创建一个 fio 作业文件，在此示例中名为 `fio_rw_mix.cfg`，包含以下内容：

```
[global]
clocksource=clock_gettime
randrepeat=0
runtime=180

[sequential-write]
bs=1M
ioengine=libaio
direct=1
iodepth=8
filename=/dev/<device>
do_verify=0
rw=write
rwmixread=0
rwmixwrite=100

[sequential-read]
bs=1M
ioengine=libaio
direct=1
iodepth=8
filename=/dev/<device>
do_verify=0
rw=read
rwmixread=100
rwmixwrite=0
offset=100g
```

然后运行以下命令：

```
$ sudo fio fio_rw_mix.cfg
```

有关解析结果的更多信息，请参阅以下教程：使用 fio 检查磁盘 IO 性能。

对于 fio 和 st1 卷而言，通过多个 sc1 作业来执行直接 I/O（即使使用顺序读入或写入操作）可能会导致吞吐量小于预期数值。建议您使用一个直接 I/O 作业并使用 iodepth 参数来控制并发 I/O 操作的数量。

使用 Amazon Data Lifecycle Manager 自动备份

您可以使用 Amazon Data Lifecycle Manager 自动创建、保留和删除 EBS 快照和 E AMIs BS 支持的快照。当您执行自动快照和 AMI 管理时，它可以帮助您：

- 通过实施定期备份计划来保护重要数据。
- 创建 AMIs 可以定期刷新的标准化。
- 按照审核员的要求或内部合规性保留备份。
- 通过删除过时的备份来降低存储成本。
- 创建将数据备份到隔离区域或账户的灾难恢复备份策略。

与亚马逊 EventBridge 和的监控功能相结合 Amazon CloudTrail，Amazon Data Lifecycle Manager 可为亚马逊 EC2 实例和单个 EBS 卷提供完整的备份解决方案，无需支付额外费用。

> **Important**
>
> - Amazon Data Lifecycle Manager 无法管理快照或通过任何其他方式 AMIs 创建的快照。
> - Amazon Data Lifecycle Manager 无法自动创建、保留和删除由实例存储支持的实例。 AMIs

内容

- 限额
- Amazon Data Lifecycle Manager 的工作原理
- Amazon Data Lifecycle Manager 默认策略与自定义策略
- 创建 Amazon Data Lifecycle Manager 默认策略
- 为 EBS 快照创建 Amazon Data Lifecycle Manager 自定义策略
- 为 EBS 支持的 Amazon Data Lifecycle Manager 自定义策略 AMIs
- 使用 Data Lifecycle Manager 自动化跨账户快照副本
- 修改 Amazon Data Lifecycle Manager 策略
- 删除 Amazon Data Lifecycle Manager 策略
- 使用 IAM 控制对 Amazon Data Lifecycle Manager 的访问

- 监控 Amazon Data Lifecycle Manager 策略
- 亚马逊 Data Lifecycle Manager 的服务终端节点
- 在 VPC 和 Amazon EBS 之间创建私有连接
- 排查 Amazon Data Lifecycle Manager 问题

限额

您的 Amazon 账户具有以下与 Amazon Data Lifecycle Manager 相关的配额：

描述	配额
每个区域的自定义生命周期策略	100
每个区域的 EBS 快照的默认策略	1
每个区域的 EBS 支持的 AMIs 默认策略	1
每个资源的标签	45

Amazon Data Lifecycle Manager 的工作原理

以下是 Amazon Data Lifecycle Manager 的关键要素。

元素

- 策略
- 策略计划（仅限自定义策略）
- 目标资源标签（仅限自定义策略）
- 快照
- EBS 支持 AMIs
- Amazon Data Lifecycle Manager 标签

策略

借助 Amazon Data Lifecycle Manager，您可以创建策略来定义备份创建和保留要求。这些策略通常会指定以下内容：

- 策略类型-定义策略管理的备份资源的类型（快照或 EBS 支持 AMIs）。
- 目标资源 – 定义策略的目标资源类型（实例或 EBS 卷）。
- 创建频率 — 定义策略运行和创建快照的频率或 AMIs。
- 保留阈值-定义策略在快照创建 AMIs 后保留多长时间。
- 其他操作 – 定义策略应执行的其他操作，例如跨区域复制、存档或资源标记。

Amazon Data Lifecycle Manager 提供默认策略和自定义策略。

默认策略

默认策略会备份某个区域中最近没有备份的所有卷和实例。您可以选择通过指定排除参数来排除卷和实例。

Amazon Data Lifecycle Manager 支持以下默认策略：

- EBS 快照的默认策略 – 以卷为目标，自动创建、保留和删除快照。
- EBS 支持的默认策略 AMIs — 以实例为目标，自动创建、保留和注销 EBS 支持的实例。 AMIs

每个账户和 Amazon 区域中的每个资源类型只能有一个默认策略。

自定义策略

自定义策略根据分配的标签将特定资源作为目标，并支持高级功能，例如快速快照还原、快照存档、跨账户复制以及前置和后置脚本。自定义策略最多可以包含 4 个计划，其中每个计划可以有自己的创建频率、保留阈值和高级功能配置。

Amazon Data Lifecycle Manager 支持以下自定义策略：

- EBS 快照策略 – 以卷或实例为目标，自动创建、保留和删除 EBS 快照。
- EBS 支持的 AMI 策略 — 以实例为目标，自动创建、保留和注销 EBS 支持的实例。 AMIs
- 跨账户复制事件策略 – 为与您共享的快照自动执行跨区域复制操作。

有关更多信息，请参阅 Amazon Data Lifecycle Manager 默认策略与自定义策略。

策略计划（仅限自定义策略）

策略计划定义了策略何时创建快照或 AMIs 创建快照。策略最多可以有四个计划 – 一个强制要求的计划和最多三个可选计划。

将多个计划添加到单个策略允许您使用相同的策略创建快照或 AMIs 以不同的频率创建快照。例如，您可以创建一个策略来按每日、每周、每月和每年的频率创建快照。这样就无需管理多个策略。

对于每个计划，您可以定义频率、快速快照还原设置（仅限快照生命周期策略）、跨区域复制规则和标签。分配给计划的标签会自动分配给快照 AMIs ，或者在计划启动时创建的标签。此外，Amazon Data Lifecycle Manager 还会根据计划的频率自动为每个快照或 AMI 分配系统生成的标签。

每个计划都会根据其频率单独启动。如果同时启动多个计划，Amazon Data Lifecycle Manager 只会创建一个快照或 AMI，并采用保留期限最长的计划保留设置。启动的所有计划的标签都会应用于该快照或 AMI。

- （仅限快照生命周期策略）如果为启动的多个计划启用了快速快照还原，则会在所有启动的计划中指定的所有可用区内为该快照启用快速快照还原。为每个可用区使用所启动计划的最长保留期限设置。
- 如果为启动的多个计划启用了跨区域复制，则该快照或 AMI 会被复制到启动的所有计划中指定的所有区域。应用所启动计划的最长保留期限。

目标资源标签（仅限自定义策略）

Amazon Data Lifecycle Manager 自定义策略使用资源标签来标识要备份的资源。在创建快照或 EBS 支持的 AMI 策略时，可以指定多个目标资源标签。至少具有指定目标资源标签之一的指定类型（实例或卷）的所有资源都将根据策略被设为目标。例如，如果您创建以卷为目标的快照策略并指定 `purpose=prod`、`costcenter=prod` 和 `environment=live` 作为目标资源标签，则该策略将以具有上述任意标签键值对的所有卷为目标。

如果要在资源上运行多个策略，可以为目标资源分配多个标签，然后创建单独的策略，每个策略都以特定的资源标签为目标。

您不能在标签键中使用 \ 或 = 字符。目标资源标签区分大小写。有关更多信息，请参阅标记资源。

快照

快照是备份 EBS 卷中的数据的主要方式。为节省存储成本，连续快照为增量快照，只包含自上一个快照以来更改的卷数据。在您删除卷的一系列快照中的一个快照时，只删除该快照独有的数据。将保留卷的其余捕获历史记录。有关更多信息，请参阅 Amazon EBS 快照。

EBS 支持 AMIs

亚马逊机器映像（AMI）提供启动实例所需的信息。在需要具有相同配置的多个实例时，您可以从单个 AMI 启动多个实例。Amazon Data Lifecycle Manager 仅支持 EBS 支持 AMIs 。EBS 支持AMIs 包括连接到源实例的每个 EBS 卷的快照。有关更多信息，请参阅亚马逊机器映像（AMI）。

Amazon Data Lifecycle Manager 标签

Amazon Data Lifecycle Manager 将以下系统标签应用于所有按策略 AMIs 创建的快照，以将其与通过任何其他方式 AMIs 创建的快照区分开来：

- `aws:dlm:lifecycle-policy-id`
- `aws:dlm:lifecycle-schedule-name`
- `aws:dlm:expirationTime` – 适用于根据基于期限的计划创建的快照。指示何时从标准层中删除快照。
- `dlm:managed`
- `aws:dlm:archived` – 适用于按计划存档的快照。
- `aws:dlm:pre-script` – 用于使用前置脚本创建的快照。
- `aws:dlm:post-script` – 用于使用后置脚本创建的快照。

您还可以指定要应用于快照和 AMIs 在创建快照时应用的自定义标签。您不能在标签键中使用 \ 或 = 字符。

Amazon Data Lifecycle Manager 用于将卷与快照策略关联的目标标签可以选择性地应用于策略创建的快照。同样，可以选择将用于将实例与 AMI 策略关联的目标标签应用于策略 AMIs 创建的标签。

Amazon Data Lifecycle Manager 默认策略与自定义策略

本节比较了默认策略和自定义策略，并重点介绍了其相似之处和不同之处。

主题

- EBS 快照策略比较
- EBS 支持的 AMI 策略比较

EBS 快照策略比较

下表重点介绍了 EBS 快照的默认策略和自定义 EBS 快照策略之间的区别。

功能	EBS 快照的默认策略	自定义 EBS 快照策略
托管备份资源	EBS 快照	EBS 快照
目标资源类型	卷	卷或实例
资源目标定位	将该区域中所有没有近期快照的卷作为目标。您可以指定排除参数来排除特定卷。	仅将具有特定标签的卷或实例作为目标。
排除参数	是，可以排除启动卷、特定卷类型和带有特定标签的卷。	是，在以实例作为目标时可以排除启动卷和带有特定标签的卷。
支持 Amazon Outposts	否	是
支持多个计划	否	是，每份策略最多 4 个计划
支持的保留类型	仅限基于期限的保留	基于期限和基于计数的保留
快照创建频率	每 1 到 7 天一次。	使用 cron 表达式的每日、每周、每月、每年或自定义频率。
快照保留	2 到 14 天。	最多 1000 张快照（基于计数）或最多 100 年（基于期限）。
支持应用程序一致性快照	否	是，使用前置和后置脚本
支持快照存档	否	是
支持快速快照还原	否	是
支持跨区域复制	是，使用默认设置 [1]	是，使用自定义设置

功能	EBS 快照的默认策略	自定义 EBS 快照策略
支持跨账户共享	否	是
支持扩展删除 [2]	是	否

[1] 对于默认策略：

- 您无法将标签复制到跨区域副本。
- 副本使用的保留期与源快照相同。
- 副本的加密状态与源快照相同。如果目标区域在默认情况下启用了加密功能，则即使源快照未加密，副本也始终处于加密状态。副本始终使用目标区域的默认 KMS 密钥进行加密。

[2] 对于默认策略和自定义策略：

- 如果删除了目标实例或卷，Amazon Data Lifecycle Manager 会根据保留期继续删除快照，直至（但不包括）最后一个快照。对于默认策略，您可以扩展删除以包括最后一个快照。
- 如果策略被删除或进入错误或禁用状态，Amazon Data Lifecycle Manager 将停止删除快照。对于默认策略，您可以扩展删除以继续删除快照，包括最后一个快照。

EBS 支持的 AMI 策略比较

下表重点介绍了 EBS 支持的默认策略和 EBS 支持的 AMIs 自定义 AMI 策略之间的区别。

功能	EBS 支持的默认策略 AMIs	EBS 支持的自定义 AMI 策略
托管备份资源	EBS 支持 AMIs	EBS 支持 AMIs
目标资源类型	实例	实例
资源目标定位	瞄准该地区中所有没有最新实例的实例 AMIs。您可以指定排除参数来排除特定实例。	仅将具有特定标签的实例作为目标。
创建 AMI 之前重启实例	否	是

功能	EBS 支持的默认策略 AMIs	EBS 支持的自定义 AMI 策略
排除参数	是，可以排除带有特定标签的实例。	否
支持多个计划	否	是，每份策略最多 4 个计划。
AMI 创建频率	每 1 到 7 天一次。	使用 cron 表达式的每日、每周、每月、每年或自定义频率。
支持的保留类型	仅限基于期限的保留。	基于期限和基于计数的保留。
AMIs 保留	2 到 14 天。	最多 1000 年 AMIs（基于计数）或最多 100 年（基于年龄）。
支持 AMI 弃用	否	是
支持跨区域复制	是，使用默认设置 [1]	是，使用自定义设置
支持扩展删除 [2]	是	否

[1] 对于默认策略：

- 您无法将标签复制到跨区域副本。
- 副本使用的保留期与源 AMI 相同。
- 副本的加密状态与源 AMI 相同。如果目标区域默认启用了加密功能，则即使源未加密，副本也始终会 AMIs 被加密。副本始终使用目标区域的默认 KMS 密钥进行加密。

[2] 对于默认策略和自定义策略：

- 如果目标实例终止，Amazon Data Lifecycle Manager 会根据保留期继续取消 AMIs 注册，直到最后一个实例取消注册，但不包括最后一个实例。对于默认策略，您可以扩展取消注册以包括最后一个 AMI。
- 如果策略被删除或进入错误或禁用状态，Amazon Data Lifecycle Manager 将停止注销注册 AMIs。对于默认策略，您可以延长删除时间以继续取消注册 AMIs，包括最后一个取消注册。

创建 Amazon Data Lifecycle Manager 默认策略

要 AMIs 从实例创建定期由 EBS 支持的实例，请使用 EBS 支持的默认策略。 AMIs要创建所有卷的快照（无论其附加状态如何）或者如果您想要排除特定卷，请使用 EBS 快照的默认策略。

本节介绍如何创建默认策略。

主题

- 默认策略注意事项
- 创建 Amazon EBS 快照的默认策略
- 为 EBS 支持的创建默认策略 AMIs
- 跨账户和区域启用 Data Lifecycle Manager 默认策略

默认策略注意事项

使用默认策略时请记住以下事项：

- 默认策略不备份最近有备份（快照或）的目标资源（实例或卷 AMIs）。创建频率决定备份哪些资源。只有当卷或实例的最后一个快照或 AMI 的时间超过策略的创建频率时，才会对其进行备份。例如，如果您将创建频率指定为 3 天，则 EBS 快照的默认策略仅在上次卷的快照超过 3 天时才会创建该卷的快照。
- 默认情况下，除非指定了排除参数，否则默认策略会将该区域的所有实例或卷作为目标。
- 默认策略将创建最少的唯一快照集。例如，如果您启用 EBS 支持的 AMI 策略和 EBS 快照策略，则该快照策略将不会复制已由 EBS 支持的 AMI 策略备份的卷的快照。
- 默认策略将仅开始以至少已有 24 小时历史的资源作为目标。
- 如果您删除卷或终止默认策略所针对的实例，Amazon Data Lifecycle Manager 将继续根据截至但不包括上次备份的保留期删除之前创建的备份（快照或 AMIs）。如果不需要此备份，您必须手动将其删除。

  如果您希望 Amazon Data Lifecycle Manager 删除最后一个备份，则可以启用扩展删除。
- 如果默认策略被删除或进入错误或禁用状态，Amazon Data Lifecycle Manager 将停止删除之前创建的备份（快照或 AMIs）。如果您希望 Amazon Data Lifecycle Manager 继续删除备份（包括最后一个备份），则必须在删除策略之前或策略的状态更改为已禁用或已删除之前启用扩展删除。
- 当您创建并启用默认策略时，Amazon Data Lifecycle Manager 会将目标资源随机分配到四小时的时间窗口期。目标资源在其分配的窗口期间以指定的创建频率进行备份。例如，如果策略的创建频率为

3 天，并且目标资源分配给 12:00 - 16:00 的窗口期间，则该资源将每 3 天在 12:00 - 16:00 期间备份一次。

创建 Amazon EBS 快照的默认策略

以下过程演示了如何创建 EBS 快照的默认策略。

Console

创建 EBS 快照的默认策略

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择生命周期管理器，然后选择创建生命周期策略。
3. 对于策略类型，请选择默认策略，然后选择 EBS 快照策略。
4. 对于描述，输入策略的简短描述。
5. 对于 IAM 角色，请选择有权管理快照的 IAM 角色。

   我们建议您选择默认值以使用 Amazon Data Lifecycle Manager 提供的默认 IAM 角色。但是，您还可以使用之前创建的自定义 IAM 角色。
6. 对于创建频率，请指定您希望策略运行的频率并创建卷的快照。

   您指定的频率还决定了备份哪些卷。该策略将仅备份在指定频率内未通过任何其他方式备份的卷。例如，如果您将创建频率指定为 3 天，则该策略将仅为过去 3 天内未备份的卷创建快照。
7. 对于保留期，请指定您希望策略将其创建的快照保留的时长。当快照达到保留阈值时，将被自动删除。保留期必须大于或等于创建频率。
8. （可选）配置排除参数，以从计划备份中排除特定卷。策略运行时，将不会备份已排除的卷。

   a. 要排除启动卷，请选择排除启动卷。如果您排除启动卷，则该策略将仅备份数据（非启动）卷。换句话说，其不会创建作为启动卷附加到实例的卷的快照。

   b. 要排除特定的卷类型，请选择排除特定卷类型，然后选择要排除的卷类型。该策略将仅备份其余类型的卷。

   c. 要排除具有特定标签的卷，请选择添加标签，然后指定标签键和值。该策略不会创建具有任何指定标签的卷的快照。
9. （可选）在高级设置中，请指定策略应执行的其他操作。

   a. 要将分配的标签从源卷复制到其快照，请选择从卷复制标签。

b. 禁用扩展删除后：

- 如果删除了源卷，Amazon Data Lifecycle Manager 会根据保留期继续删除之前创建的快照，直至（但不包括）最后一个快照。如果您希望 Amazon Data Lifecycle Manager 删除所有快照，包括最后一个快照，请选择扩展删除。
- 如果策略被删除或进入 `error` 或 `disabled` 状态，Amazon Data Lifecycle Manager 将停止删除快照。如果您希望 Amazon Data Lifecycle Manager 继续删除快照，包括最后一个快照，请选择扩展删除。

> **Note**
>
> 如果启用“扩展删除”，则可以同时覆盖上述两种行为。

c. 要将该策略创建的快照复制到其他区域，请选择创建跨区域副本，然后选择最多 3 个目标区域。

- 如果源快照已加密或默认情况下启用了目标区域的加密功能，则会在目标区域中使用 EBS 加密的默认 KMS 密钥对复制的快照进行加密。
- 如果源快照未加密且默认情况下禁用目标区域的加密功能，则复制的快照为未加密快照。

10. （可选）要向策略添加标签，请选择添加标签，然后指定标签键和值。
11. 选择创建默认策略。

> **Note**
>
> 如果发生 `Role with name AWSDataLifecycleManagerDefaultRole already exists` 错误，请参阅 排查 Amazon Data Lifecycle Manager 问题 来了解更多信息。

Amazon CLI

创建 EBS 快照的默认策略

使用 create-lifecycle-policy 命令。您可以通过以下两种方法之一来指定请求参数，具体取决于您的用例或偏好：

- 方法 1：

```
$ aws dlm create-lifecycle-policy \
--state ENABLED | DISABLED \
--description "policy_description" \
--execution-role-arn role_arn \
--default-policy VOLUME \
--create-interval creation_frequency_in_days (1-7) \
--retain-interval retention_period_in_days (2-14) \
--copy-tags | --no-copy-tags \
--extend-deletion | --no-extend-deletion \
--cross-region-copy-targets TargetRegion=destination_region_code \
--exclusions ExcludeBootVolumes=true | false,
 ExcludeTags=[{Key=tag_key,Value=tag_value}], ExcludeVolumeTypes="standard | gp2 |
 gp3 | io1 | io2 | st1 | sc1"
```

例如，要创建 EBS 快照的默认策略，该策略以该地区所有卷为目标、使用默认 IAM 角色、每天运行（默认）并将快照保留 7 天（默认），您需要指定以下参数：

```
$ aws dlm create-lifecycle-policy \
--state ENABLED \
--description "Daily default snapshot policy" \
--execution-role-arn arn:aws:iam::account_id:role/
AWSDataLifecycleManagerDefaultRole \
--default-policy VOLUME
```

- 方法 2：

```
$ aws dlm create-lifecycle-policy \
--state ENABLED | DISABLED \
--description "policy_description" \
--execution-role-arn role_arn \
--default-policy VOLUME \
--policy-details file://policyDetails.json
```

其中 policyDetails.json 包含以下内容：

```
{
    "PolicyLanguage": "SIMPLIFIED",
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceType": "VOLUME",
    "CopyTags": true | false,
    "CreateInterval": creation_frequency_in_days (1-7),
```

```
    "RetainInterval": retention_period_in_days (2-14),
    "ExtendDeletion": true | false,
    "CrossRegionCopyTargets": [{"TargetRegion":"destination_region_code"}],
    "Exclusions": {
        "ExcludeBootVolume": true | false,
  "ExcludeVolumeTypes": ["standard | gp2 | gp3 | io1 | io2 | st1 | sc1"],
        "ExcludeTags": [{
            "Key": "exclusion_tag_key",
            "Value": "exclusion_tag_value"
        }]
    }
}
```

为 EBS 支持的创建默认策略 AMIs

以下过程向您展示如何为 EBS AMIs 支持的创建默认策略。

Console

为 EBS 支持的创建默认策略 AMIs

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Lifecycle Manager，然后选择创建生命周期策略。
3. 对于策略类型，请选择默认策略，然后选择由 EBS 支持的 AMI 策略。
4. 对于描述，输入策略的简短描述。
5. 对于 IAM 角色，请选择有权管理的 IAM 角色 AMIs。

   我们建议您选择默认值以使用 Amazon Data Lifecycle Manager 提供的默认 IAM 角色。但是，您还可以使用之前创建的自定义 IAM 角色。
6. 对于创建频率，请指定您希望策略的运行频率和 AMIs 从您的实例创建的频率。

   您指定的频率还决定了备份哪些实例。该策略将仅备份在指定频率内未通过任何其他方式备份的实例。例如，如果您将创建频率指定为 3 天，则该策略将 AMIs 仅使用过去 3 天内未备份的实例进行创建。
7. 对于保留期，请指定您希望策略保留其创建 AMIs 的保留期限。当 AMI 达到保留阈值时，将会被自动取消注册并删除其关联的快照。保留期必须大于或等于创建频率。
8. （可选）配置排除参数，以从计划备份中排除特定实例。策略运行时，将不会备份已排除的实例。

- 要排除具有特定标签的实例，请选择添加标签，然后指定标签键和值。该策略不会 AMIs 从具有任何指定标签的实例中创建。

9. （可选）在高级设置中，请指定策略应执行的其他操作。

   a. 要将分配的标签从源实例复制到其实例 AMIs，请选择从实例复制标签。

   b. 禁用扩展删除后：

      - 如果源实例终止，Amazon Data Lifecycle Manager 将继续注销之前创建的 AMIs 直到最后一个实例，但不包括基于保留期的最后一个实例。如果您想让 Amazon Data Lifecycle Manager 取消全部注册 AMIs，包括最后一个，请选择延长删除时间。
      - 如果策略被删除或进入`error`或`disabled`状态，Amazon Data Lifecycle Manager 将停止注销注册 AMIs。如果您想让 Amazon Data Lifecycle Manager 继续注 AMIs销（包括最后一个注销），请选择延长删除时间。

      > **Note**
      >
      > 如果启用“扩展删除”，则可以同时覆盖上述两种行为。

   c. 要将该策略 AMIs 创建的复制到其他区域，请选择创建跨区域副本，然后最多选择 3 个目标区域。

      - 如果源 AMI 已加密，或者目标区域默认启用了加密，则在目标区域使用默认 KMS 密钥对复制 AMIs 的 EBS 进行加密。
      - 如果源 AMI 未加密，且目标区域默认禁用加密，则副 AMIs 本未加密。

10. （可选）要向策略添加标签，请选择添加标签，然后指定标签键和值。

11. 选择创建默认策略。

> **Note**
>
> 如果发生 `Role with name AWSDataLifecycleManagerDefaultRoleForAMIManagement already exists` 错误，请参阅 排查 Amazon Data Lifecycle Manager 问题 来了解更多信息。

Amazon CLI

为 EBS 支持的创建默认策略 AMIs

使用 create-lifecycle-policy 命令。您可以通过以下两种方法之一来指定请求参数，具体取决于您的用例或偏好：

- 方法 1：

```
$ aws dlm create-lifecycle-policy \
--state ENABLED | DISABLED \
--description "policy_description" \
--execution-role-arn role_arn \
--default-policy INSTANCE \
--create-interval creation_frequency_in_days (1-7) \
--retain-interval retention_period_in_days (2-14) \
--copy-tags | --no-copy-tags \
--extend-deletion | --no-extend-deletion \
--cross-region-copy-targets TargetRegion=destination_region_code \
--exclusions ExcludeTags=[{Key=tag_key,Value=tag_value}]
```

例如，要为由 EBS 支持的 AMIs 默认策略创建针对该地区所有实例、使用默认 IAM 角色、每天运行（默认）并保留 AMIs 7 天（默认）的默认策略，您需要指定以下参数：

```
$ aws dlm create-lifecycle-policy \
--state ENABLED \
--description "Daily default AMI policy" \
--execution-role-arn arn:aws:iam::account_id:role/
AWSDataLifecycleManagerDefaultRoleForAMIManagement \
--default-policy INSTANCE
```

- 方法 2：

```
$ aws dlm create-lifecycle-policy \
--state ENABLED | DISABLED \
--description "policy_description" \
--execution-role-arn role_arn \
--default-policy INSTANCE \
--policy-details file://policyDetails.json
```

其中 policyDetails.json 包含以下内容：

```
{
    "PolicyLanguage": "SIMPLIFIED",
    "PolicyType": "IMAGE_MANAGEMENT",
    "ResourceType": "INSTANCE",
    "CopyTags": true | false,
    "CreateInterval": creation_frequency_in_days (1-7),
    "RetainInterval": retention_period_in_days (2-14),
    "ExtendDeletion": true | false,
 "CrossRegionCopyTargets": [{"TargetRegion":"destination_region_code"}],
    "Exclusions": {
        "ExcludeTags": [{
            "Key": "exclusion_tag_key",
            "Value": "exclusion_tag_value"
        }]
    }
}
```

跨账户和区域启用 Data Lifecycle Manager 默认策略

使用 Amazon CloudFormation StackSets，您只需一次操作即可在多个账户和 Amazon 地区启用亚马逊数据生命周期管理器默认策略。

您可以使用堆栈集通过以下方式之一启用默认策略：

- 在整个 Amazon 组织中-确保在整个 Amazon 组织或组织中的特定组织单位中统一启用和配置默认策略。这是使用服务管理权限完成的。 Amazon CloudFormation StackSets 代表您创建所需的 IAM 角色。
- 跨特定 Amazon 账户-确保在特定目标账户中一致启用和配置默认策略。这需要自行管理权限。您可以创建在堆栈集管理员账户和目标账户之间建立信任关系所需的 IAM 角色。

有关更多信息，请参阅《Amazon CloudFormation 用户指南》中的堆栈集的权限模型。

使用以下过程在整个 Amazon 组织、特定或特定目标账户中启用 Amazon Data Lifecy OUs cle Manager 的默认策略。

先决条件

根据启用默认策略的方式，执行以下操作之一：

- （跨 Amazon 组织）您必须启用组织中的所有功能并使用激活可信访问权限 Amazon Organizations。您还必须使用组织的管理账户或委派管理员账户。
- （跨特定目标账户）您必须通过创建在堆栈集管理员账户和目标账户之间建立信任关系所需的角色来授予自行管理权限。

Console

跨 Amazon 组织或跨特定目标账户启用默认策略

1. 在 https://console.aws.amazon.com/cloudformation 上打开 Amazon CloudFormation 控制台。
2. 在导航窗格中，选择 StackSets，然后选择创建 StackSet。
3. 对于权限，根据启用默认策略的方式，执行以下操作之一：
   - （在整个 Amazon 组织中）选择服务管理权限。
   - （跨特定目标账户）选择自助服务权限。然后，对于 IAM 管理员角色 ARN，选择您为管理员账户创建的 IAM 服务角色，对于 IAM 执行角色名称，输入您在目标账户中创建的 IAM 服务角色的名称。
4. 对于准备模板，选择使用示例模板。
5. 对于示例模板，执行以下操作之一：
   - （EBS 快照的默认策略）选择为 EBS 快照创建 Amazon Data Lifecycle Manager 默认策略。
   - （EBS 支持的默认策略 AMIs）选择 EBS 支持的创建 Amazon Data Lifecycle Manager 的默认策略。 AMIs
6. 选择下一步。
7. 在StackSet 名称和StackSet 描述中，输入描述性名称和简短描述。
8. 在参数部分，根据需要配置默认策略设置。

   > **Note**
   >
   > 对于关键工作负载，我们建议 CreateInterval = 1 天和 RetainInterval = 7 天。

9. 选择下一步。
10. （可选）在 “标签” 中，指定标签以帮助您识别 StackSet 和堆栈资源。
11. 对于托管执行，选择活动。

12. 选择下一步。
13. 对于 Add stacks to stack set（将堆栈添加到堆栈集），选择 Deploy new stacks（部署新堆栈）。
14. 根据启用默认策略的方式，执行以下操作之一：

    - （跨 Amazon 组织）对于部署目标，请选择以下选项之一：
      - 要在整个 Amazon 组织中部署，请选择部署到组织。
      - 要部署到特定组织单位（OU），请选择部署到组织单位，然后在 OU ID 中输入 OU ID。要添加其他 OUOUs，请选择添加另一个 OU。
    - （跨特定目标账户）对于账户，执行以下操作之一：
      - 要部署到特定的目标账户，请选择在账户中部署堆栈，然后在账户号中 IDs 输入目标账户的。
      - 要部署到特定 OU 中的所有账户，选择将堆栈部署到组织单位中的所有账户，然后对于组织编号，输入目标 OU 的 ID。
15. 对于自动部署，选择已激活。
16. 对于账户删除行为，选择保留堆栈。
17. 对于指定区域，选择要在其中启用默认策略的特定区域，或者选择添加所有区域以在所有区域中启用默认策略。
18. 选择下一步。
19. 查看堆栈集设置，选择我确认 Amazon CloudFormation 可能会创建 IAM 资源，然后选择提交。

Amazon CLI

在整个 Amazon 组织中启用默认策略

1. 创建堆栈集。使用 create-stack-set 命令。

   对于 `--permission-model`，请指定 `SERVICE_MANAGED`。

   对于`--template-url`，请指定以下模板之一 URLs：

   - （EBS AMIs 支持的默认策略）`https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/DataLifecycleManagerAMIDefaultPolicy.yaml`

- （EBS 快照的默认策略）https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/DataLifecycleManagerEBSSnapshotDefaultPolicy.yaml

对于 --parameters，指定默认策略的设置。有关支持的参数、参数描述和有效值，请使用 URL 下载模板，然后使用文本编辑器查看模板。

对于 --auto-deployment，请指定 Enabled=true,RetainStacksOnAccountRemoval=true。

```
$ aws cloudformation create-stack-set \
--stack-set-name stackset_name \
--permission-model SERVICE_MANAGED \
--template-url template_url \
--parameters "ParameterKey=param_name_1,ParameterValue=param_value_1"
 "ParameterKey=param_name_2,ParameterValue=param_value_2" \
--auto-deployment "Enabled=true, RetainStacksOnAccountRemoval=true"
```

2. 部署堆栈集。使用 create-stack-instances 命令。

对于 --stack-set-name，指定您在上一步中创建的堆栈集的名称。

对于--deployment-targets OrganizationalUnitIds，请指定要部署到整个组织的根 OU 或要部署 IDs 到组织 OUs 中的特定组织的 OU 的 ID。

对于--regions，请指定要在其中启用默认策略的 Amazon 区域。

```
$ aws cloudformation create-stack-instances \
--stack-set-name stackset_name \
--deployment-targets OrganizationalUnitIds='["root_ou_id"]' | '["ou_id_1",
 "ou_id_2]' \
--regions '["region_1", "region_2"]'
```

在特定目标账户中启用默认策略

1. 创建堆栈集。使用 create-stack-set 命令。

对于--template-url，请指定以下模板之一 URLs：

- （EBS AMIs 支持的默认策略）https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/DataLifecycleManagerAMIDefaultPolicy.yaml
- （EBS 快照的默认策略）https://s3.amazonaws.com/cloudformation-stackset-sample-templates-us-east-1/DataLifecycleManagerEBSSnapshotDefaultPolicy.yaml

对于 --administration-role-arn，指定您之前为堆栈集管理员创建的 IAM 服务角色的 ARN。

对于 --execution-role-name，指定您在目标账户中创建的 IAM 服务角色的名称。

对于 --parameters，指定默认策略的设置。有关支持的参数、参数描述和有效值，请使用 URL 下载模板，然后使用文本编辑器查看模板。

对于 --auto-deployment，请指定 Enabled=true,RetainStacksOnAccountRemoval=true。

```
$ aws cloudformation create-stack-set \
--stack-set-name stackset_name \
--template-url template_url \
--parameters "ParameterKey=param_name_1,ParameterValue=param_value_1"
 "ParameterKey=param_name_2,ParameterValue=param_value_2" \
--administration-role-arn administrator_role_arn \
--execution-role-name target_account_role \
--auto-deployment "Enabled=true, RetainStacksOnAccountRemoval=true"
```

2. 部署堆栈集。使用 create-stack-instances 命令。

对于 --stack-set-name，指定您在上一步中创建的堆栈集的名称。

对于--accounts，请 IDs 指定目标 Amazon 帐户的。

对于--regions，请指定要在其中启用默认策略的 Amazon 区域。

```
$ aws cloudformation create-stack-instances \
--stack-set-name stackset_name \
--accounts '["account_ID_1","account_ID_2"]' \
--regions '["region_1", "region_2"]'
```

为 EBS 快照创建 Amazon Data Lifecycle Manager 自定义策略

以下程序说明了如何使用 Amazon Data Lifecycle Manager 来自动执行 Amazon EBS 快照生命周期。

主题

- 创建快照生命周期策略
- 快照生命周期策略的注意事项
- 其他资源
- 使用 Data Lifecycle Manager 自动生成应用程序一致性快照
- Data Lifecycle Manager 前置和后置脚本的其他使用场景
- Amazon Data Lifecycle Manager 前置和后置脚本的工作原理
- 识别使用 Data Lifecycle Manager 前置和后置脚本创建的快照
- 监控 Amazon Data Lifecycle Manager 前置和后置脚本

创建快照生命周期策略

使用以下过程之一创建快照生命周期策略。

Console

要创建快照策略

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，依次选择 Elastic Block Store 和 Lifecycle Manager (生命周期管理器)，然后选择 Create lifecycle policy (创建生命周期策略)。
3. 在选择策略类型页面上，选择 EBS 快照策略，然后选择下一步。
4. 在目标资源部分中，执行以下操作：

   a. 对于目标资源类型，选择要备份的资源的类型。选择 `Volume` 创建各个卷的快照，或选择 `Instance` 从挂载到实例的卷创建多卷快照。

   b. (Outpost 且仅限本地区域客户）指定目标资源的位置。

      对于目标资源位置，请指定目标资源的位置。

- 要将资源定位到某个区域，请选择Amazon 区域。Amazon Data Lifecycle Manager 将仅备份当前区域中具有匹配目标标签的所有指定类型的资源。快照是在同一区域创建的。
- 要瞄准本地区域中的资源，请选择 L Amazon ocal Zones。Amazon Data Lifecycle Manager 将仅备份当前区域中所有本地区域中具有匹配目标标签的指定类型的所有资源。快照可以在与源资源相同的本地区域中创建，也可以在其父区域中创建。
- 要瞄准资源和 Outpost，选择 Amazon Outpost。 Amazon Data Lifecycle Manager 将备份所有具有匹配目标标签的指定类型的资源 Outposts 在你的账户中。可以在同一个上创建快照 Outpost 作为源资源，或者位于其父区域。

c. 对于目标资源标签，选择标识要备份的卷或实例的资源标签。策略只备份具有指定标签键和值对的资源。

5. 对于 Description (描述)，输入策略的简短描述。
6. 对于 IAM 角色，选择一个有权管理快照以及描述卷和实例的 IAM 角色。要使用 Amazon Data Lifecycle Manager 提供的默认角色。请选择默认角色。或者，要使用您之前创建的自定义 IAM 角色，请选择选择其他角色，然后选择要使用的角色。
7. 对于策略标签，选择要应用于生命周期策略的标签。您可以使用这些标签对策略进行标识和分类。
8. 对于 Policy status（策略状态），选择 Enable（启用），以在下次计划时间开启策略运行，或者选择 Disable policy（禁用策略）以禁止策略运行。如果您现在不启用该策略，则该策略仅在创建后手动启用之后开始创建快照。
9. （仅限以实例为目标的策略）从多卷快照集中排除卷。

   默认情况下，Amazon Data Lifecycle Manager 将创建附加到目标实例的所有卷的快照。不过，您可以选择创建附加卷子集的快照。在 Parameters （参数）部分，执行以下操作：

   - 如果您不想创建附加到目标实例的根卷的快照，请选择 Exclude root volume（排除根卷）。如果选择此选项，则只有附加到目标实例的数据（非根）卷才会包含在多卷快照集中。
   - 如果要创建附加到目标实例的数据（非根）卷子集的快照，请选择排除特定的数据卷，然后指定用于标识不应创建快照的数据卷的标签。Amazon Data Lifecycle Manager 不会为具有任何指定标签的数据卷创建快照。Amazon Data Lifecycle Manager 仅为不具有任何指定标签的数据卷创建快照。
10. 选择下一步。
11. 在配置计划屏幕上，配置策略计划。一个策略最多可以有 4 个计划。计划 1 是强制要求的计划。计划 2、3、4 是可选计划。对于您添加的每个策略计划，请执行以下操作：

a. 在计划详细信息部分中，执行以下操作：

i. 对于计划名称，请指定计划的描述性名称。

ii. 在频率和相关字段中配置策略运行之间的间隔。

您可以按每日、每周、每月或每年计划配置策略运行。或者，选择自定义 cron 表达式以指定不超过一年的间隔时间。有关更多信息，请参阅 Amazon EventBridge 用户指南中的 Cron 和费率表达式。

> **Note**
>
> 如果您需要为此计划启用 snapshot archiving（快照存档），则必须选择 monthly（每月）或 yearly（每年）频率，或者指定一个创建频率至少为 28 天的 cron 表达式。
> 如果指定一个将在特定周次的特定日期（例如，当月第二周星期四）创建快照的每月频率，则对于基于计数的计划，存档层的保留计数必须为 4 或以上。

iii. 对于开始时间，请指定计划开始运行策略的时间。第一次策略运行在计划时间之后的一小时内开始。时间必须输入 hh:mm UTC 格式。

iv. 对于保留类型，请指定计划创建的快照的保留策略。

您可以根据其总计数或存在时间保留快照。

- 基于计数的保留
  - 禁用快照归档后，范围为 1 到 1000。当达到保留阈值时，最早的快照将永久删除。
  - 启用快照归档后，范围为 0（创建后立即归档）到 1000。达到保留阈值时，最早的快照将转换为完整快照，然后移动到存档层。
- 基于时长的保留
  - 禁用快照归档后，范围为 1 天到 100 年。当达到保留阈值时，最早的快照将永久删除。
  - 启用快照归档后，范围为 0 天（创建后立即归档）到 100 年。达到保留阈值时，最早的快照将转换为完整快照，然后移动到存档层。

> **Note**
>
> - 所有计划必须具有相同的保留类型（基于期限或基于计数）。您只能为“计划 1”指定保留类型。计划 2、3、4 会继承计划 1 的保留类型。每个计划都可以有自己的保留计数或期限。
> - 如果您启用了快速快照还原、跨区域复制或快照共享，则必须指定 1 或更大的保留计数，或者 1 天或更长的保留期。

v. （Amazon Outposts 仅限本地区域客户）指定快照目标。

对于快照目标 – 请指定策略创建的快照目标。

- 如果该政策针对的是某个区域中的资源，则必须在同一区域创建快照。 Amazon 已选定您的区域。
- 如果该策略以本地区域中的资源为目标，则可以在与源资源相同的本地区域中创建快照，也可以在其父区域中创建快照。
- 如果该策略将资源定位在 Outpost，你可以在同一个上面创建快照 Outpost 作为源资源，或者位于其父区域。

b. 配置快照标签。

在标记部分中，请执行以下操作：

i. 要将所有用户定义的标签从源卷复制到计划创建的快照，请选择从源中复制标签。

ii. 要指定分配给由该计划创建的快照的其他标签，请选择添加标签。

c. 配置应用程序一致性快照的前置和后置脚本。

有关更多信息，请参阅 使用 Data Lifecycle Manager 自动生成应用程序一致性快照。

d. （仅限以卷为目标的策略）配置快照存档。

在快照存档部分，请执行以下操作：

> **Note**
>
> 您在一个策略中只能为一个计划启用快照存档。

i. 要为此计划启用快照存档，请选择 Archive snapshots created by this schedule（将此计划创建的快照存档）。

> **Note**
>
> 只有在快照创建频率为每月或每年，或者指定一个创建频率至少为 28 天的 cron 表达式时，才能启用快照存档。

ii. 为存档层中的快照指定保留规则。

- 对于基于计数的计划，指定要在存档层中保留的快照数量。当达到保留阈值时，最老的快照将从存档层中永久删除。例如，假设您指定 3，则计划将在存档层中最多保留 3 个快照。存档第四个快照时，系统将会删除存档层中三个现有快照中最老的一个。
- 对于基于期限的计划，指定要在存档层中保留快照的期限。当达到保留阈值时，最老的快照将从存档层中永久删除。例如，假设您指定 120 天，则计划将在该期限届满时自动从存档层中删除快照。

> **Important**
>
> 存档快照的最短保留期为 90 天。必须指定一个会将快照保留至少 90 天的保留规则。

e. 启用快速快照还原。

要为计划创建的快照启用快速快照还原，请在快速快照还原部分中选择启用快速快照还原。如果您启用快速快照还原，则必须选择要在其中启用该功能的可用区。如果计划使用基于时间的保留计划，则必须指定为每个快照启用快速快照还原的时间段。如果计划使用基于计数的保留，您必须指定要启用快速快照还原的最大快照数。

如果计划在上创建快照 Outpost，则无法启用快速快照恢复。存储在上的本地快照不支持快速快照恢复 Outpost.

> **Note**
>
> 对于为特定可用区中快照启用的快速快照还原，您需要按每分钟支付费用。收费按比例计算，最少 1 小时。

f. 配置跨区域复制。

将按计划创建的快照复制到 Outpost 或者到其他区域，在 “跨区域复制” 部分中，选择 “启用跨区域复制”。

如果计划在某个区域中创建快照，则可以将快照复制到最多三个其他区域或 Outposts 在你的账户中。您必须为每个目标区域指定单独的跨区域复制规则，或者 Outpost.

对于每个地区或 Outpost，您可以选择不同的保留策略，也可以选择是复制所有标签还是不复制标签。如果源快照已加密或默认启用加密，则会加密已复制的快照。如果源快照未加密，您可以启用加密。如果未指定 KMS 密钥，则会在每个目标区域中使用 EBS 加密的默认 KMS 密钥 对快照进行加密。如果您为目标区域指定 KMS 密钥，则选定的 IAM 角色必须具有对 KMS 密钥 的访问权限。

> **Note**
>
> 您必须确保没有超过每个区域的并发快照副本数。

如果该策略在上创建快照 Outpost，那么你就无法将快照复制到某个区域或其他区域 Outpost 而且跨区域复制设置不可用。

g. 配置跨账户共享。

在跨账户共享中，将策略配置为自动与其他 Amazon 账户共享按计划创建的快照。执行以下操作：

i. 要启用与其他 Amazon 账户共享，请选择启用跨账户共享。

ii. 要添加要与之共享快照的账户，请选择添加账户，输入 12 位 Amazon 账户 ID，然后选择添加。

iii. 要在特定时间段后自动取消共享所共享的快照，请选择 Unshare automatically（自动取消共享）。如果您选择自动将共享快照取消共享，则自动取消快照共享前的持续时间不能超过策略保留其快照的期限。例如，如果策略的保留配置可将快照保留 5 天，

则您可以将策略配置为在最多 4 天的时间后自动取消快照共享。这适用于采用基于存在时间和基于计数的快照保留配置的策略。

如果不启用自动取消共享，快照将一直共享直至删除。

> **Note**
>
> 您只能共享未加密的快照或使用 客户托管密钥 加密的快照。您无法共享使用默认 EBS 加密 KMS 密钥 加密的快照。如果您共享加密快照，则还必须与目标账户共享用于加密源卷的 KMS 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其他账户中的用户使用 KMS 密钥。

h. 要添加其他计划，请选择位于页面顶部的添加其他计划。每个其他计划请按照本主题之前所述填写字段。

i. 添加所需计划之后，请选择查看策略。

12. 查看策略摘要，然后选择创建策略。

> **Note**
>
> 如果发生 `Role with name AWSDataLifecycleManagerDefaultRole already exists` 错误，请参阅 排查 Amazon Data Lifecycle Manager 问题 来了解更多信息。

Command line

使用create-lifecycle-policy命令创建快照生命周期策略。对于 `PolicyType`，请指定 `EBS_SNAPSHOT_MANAGEMENT`。

> **Note**
>
> 为简化语法，以下示例使用包含策略详细信息的 JSON 文件 `policyDetails.json`。

示例 1 – 具有两个计划的快照生命周期策略

此示例创建的快照生命周期策略可创建标签键 costcenter 的值为 115 的所有卷的快照。该策略包含两个计划。第一个计划在每天 3:00 UTC 创建快照。第二个计划在每周五 17:00 UTC 创建一个周快照。

```
aws dlm create-lifecycle-policy \
    --description "My volume policy" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

以下是 policyDetails.json 文件的示例。

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": [
        "VOLUME"
    ],
    "TargetTags": [{
        "Key": "costcenter",
        "Value": "115"
    }],
    "Schedules": [{
        "Name": "DailySnapshots",
        "TagsToAdd": [{
            "Key": "type",
            "Value": "myDailySnapshot"
        }],
        "CreateRule": {
            "Interval": 24,
            "IntervalUnit": "HOURS",
            "Times": [
                "03:00"
            ]
        },
        "RetainRule": {
            "Count": 5
        },
        "CopyTags": false
    },
    {
        "Name": "WeeklySnapshots",
        "TagsToAdd": [{
```

```
            "Key": "type",
            "Value": "myWeeklySnapshot"
        }],
        "CreateRule": {
            "CronExpression": "cron(0 17 ? * FRI *)"
        },
        "RetainRule": {
            "Count": 5
        },
        "CopyTags": false
    }
]}
```

如果请求成功，此命令将返回新创建的策略 ID。下面是示例输出。

```
{
   "PolicyId": "policy-0123456789abcdef0"
}
```

示例 2 - 以实例为目标并创建数据（非根）卷子集快照的快照生命周期策略

此示例创建的快照生命周期策略可从标记为 code=production 的实例创建多卷快照集。该策略仅包含一个计划。该计划不会创建标记为 code=temp 的数据卷的快照。

```
aws dlm create-lifecycle-policy \
    --description "My volume policy" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

以下是 policyDetails.json 文件的示例。

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key": "code",
        "Value": "production"
```

```
    }],
    "Parameters": {
        "ExcludeDataVolumeTags": [{
            "Key": "code",
            "Value": "temp"
        }]
    },
    "Schedules": [{
        "Name": "DailySnapshots",
        "TagsToAdd": [{
            "Key": "type",
            "Value": "myDailySnapshot"
        }],
        "CreateRule": {
            "Interval": 24,
            "IntervalUnit": "HOURS",
            "Times": [
                "03:00"
            ]
        },
        "RetainRule": {
            "Count": 5
        },
        "CopyTags": false
    }
]}
```

如果请求成功，此命令将返回新创建的策略 ID。下面是示例输出。

```
{
   "PolicyId": "policy-0123456789abcdef0"
}
```

示例 3-自动生成本地快照的快照生命周期策略 Outpost resources

此示例创建了一个快照生命周期策略，该策略可创建所有卷team=dev上标有标签的卷的快照 Outposts。 该策略在同一个上创建快照 Outposts 作为源卷。该策略从 12 UTC 开始每 00:00 小时创建一次快照。

```
aws dlm create-lifecycle-policy \
    --description "My local snapshot policy" \
    --state ENABLED \
```

```
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

以下是 policyDetails.json 文件的示例。

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": "VOLUME",
 "ResourceLocations": "OUTPOST",
    "TargetTags": [{
        "Key": "team",
        "Value": "dev"
    }],
    "Schedules": [{
        "Name": "on-site backup",
        "CreateRule": {
            "Interval": 12,
            "IntervalUnit": "HOURS",
            "Times": [
                "00:00"
            ],
 "Location": [
  "OUTPOST_LOCAL"
 ]
        },
        "RetainRule": {
            "Count": 1
        },
        "CopyTags": false
    }
]}
```

示例 4-在区域中创建快照并将其复制到的快照生命周期策略 Outpost

以下示例策略创建带 team=dev 标记的卷的快照。快照在源卷所在的同一区域中创建。从 12 UTC 开始，每 00:00 小时创建一次快照，并保留最多 1 个快照。该策略还将快照复制到 Outpost arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0，使用默认加密 KMS 密钥对复制的快照进行加密，并将副本保留1一个月。

```
aws dlm create-lifecycle-policy \
    --description "Copy snapshots to Outpost" \
```

```
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

以下是 policyDetails.json 文件的示例。

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": "VOLUME",
    "ResourceLocations": "CLOUD",
    "TargetTags": [{
        "Key": "team",
        "Value": "dev"
    }],
    "Schedules": [{
        "Name": "on-site backup",
        "CopyTags": false,
        "CreateRule": {
            "Interval": 12,
            "IntervalUnit": "HOURS",
            "Times": [
                "00:00"
            ],
            "Location": "CLOUD"
        },
        "RetainRule": {
            "Count": 1
        },
        "CrossRegionCopyRules" : [
        {
            "Target": "arn:aws:outposts:us-east-1:123456789012:outpost/
op-1234567890abcdef0",
            "Encrypted": true,
            "CopyTags": true,
            "RetainRule": {
                "Interval": 1,
                "IntervalUnit": "MONTHS"
            }
        }]
    }
]}
```

示例 5 – 快照生命周期策略，具有已启用归档并基于期限的计划

此示例将创建一个以带有 Name=Prod 标签的卷为目标的快照生命周期策略。此策略采用基于期限的计划，该计划会在每月第一天 09:00 创建快照。此计划会在标准层中将每个快照保留一天，之后将其转移到至存档层。快照在存档层中存储 90 天后将被删除。

```
aws dlm create-lifecycle-policy \
    --description "Copy snapshots to Outpost" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

以下是 policyDetails.json 文件的示例。

```
{
    "ResourceTypes": [ "VOLUME"],
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "Schedules" : [
      {
        "Name": "sched1",
        "TagsToAdd": [
          {"Key":"createdby","Value":"dlm"}
        ],
        "CreateRule": {
          "CronExpression": "cron(0 9 1 * ? *)"
        },
        "CopyTags": true,
        "RetainRule":{
          "Interval": 1,
          "IntervalUnit": "DAYS"
        },
        "ArchiveRule": {
            "RetainRule":{
              "RetentionArchiveTier": {
                 "Interval": 90,
                 "IntervalUnit": "DAYS"
              }
            }
        }
      }
    ],
    "TargetTags": [
```

```
      {
        "Key": "Name",
        "Value": "Prod"
      }
    ]
}
```

示例 6 – 快照生命周期策略，具有已启用归档并基于计数的计划

此示例将创建一个以带有 Purpose=Test 标签的卷为目标的快照生命周期策略。此策略采用基于计数的计划，该计划会在每月第一天 09:00 创建快照。此计划将在快照创建后立即将其存档，并在存档层中最多保留三个快照。

```
aws dlm create-lifecycle-policy \
    --description "Copy snapshots to Outpost" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

以下是 policyDetails.json 文件的示例。

```
{
    "ResourceTypes": [ "VOLUME"],
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "Schedules" : [
      {
        "Name": "sched1",
        "TagsToAdd": [
          {"Key":"createdby","Value":"dlm"}
        ],
        "CreateRule": {
          "CronExpression": "cron(0 9 1 * ? *)"
        },
        "CopyTags": true,
        "RetainRule":{
          "Count": 0
        },
        "ArchiveRule": {
            "RetainRule":{
              "RetentionArchiveTier": {
                 "Count": 3
              }
```

```
            }
        }
      }
    ],
    "TargetTags": [
      {
        "Key": "Purpose",
        "Value": "Test"
      }
    ]
}
```

快照生命周期策略的注意事项

以下一般注意事项适用于快照生命周期策略：

- 快照生命周期策略仅针对与策略位于同一区域的实例或卷。
- 第一个快照创建操作将在指定的开始时间后一小时内开始。后续快照创建操作将在计划时间的一小时内开始。
- 您可以创建多个策略来备份卷或实例。例如，假设一个卷有两个标签，其中标签 A 是每 12 小时创建一次快照的策略 A 的目标，标签 B 是每 24 小时创建一次快照的策略 B 的目标，则 Amazon Data Lifecycle Manager 将根据这两个策略的计划创建快照。或者，您可以通过创建包含多个计划的单个策略来实现相同的结果。例如，您可以创建仅针对标签 A 的单个策略，并指定两个计划，以分别用于每 12 小时和每 24 小时一次的策略。
- 目标资源标签区分大小写。
- 如果从策略所针对的资源中删除目标标签，则 Amazon Data Lifecycle Manager 不再管理标准层和存档层中的现有快照；如不再需要，您必须手动将其删除。
- 如果您创建了以实例为目标的策略，并且在创建策略后将新卷挂载到目标实例，则在下次运行策略时，新添加的卷将包含在备份中。策略运行时挂载到实例的所有卷都包括在内。
- 如果您创建了具有基于 cron 的自定义计划的策略，并且配置为仅创建一个快照，则该策略不会在达到保留阈值时自动删除该快照。如果不再需要快照，则必须手动删除该快照。
- 如果您创建基于存在时间的策略，其保留期短于创建频率，Amazon Data Lifecycle Manager 将始终保留最后一张快照，直到创建下一张快照。例如，如果基于存在时间的策略每月创建一个快照，保留期为七天，则 Amazon Data Lifecycle Manager 会将每个快照保留一个月，即使保留期为七天。

共享快照时需考虑以下事项：

- 您只能为将卷作为目标的快照策略启用快照存档。
- 对于每个策略，您只能为一个计划指定一个存档规则。
- 如果您使用控制台，则只有在创建频率为每月或每年，或者指定一个创建频率至少为 28 天的 cron 表达式时，才能启用快照存档。

  如果您使用的是 Amazon CLI、 Amazon API 或 Amazon SDK，则只有在计划中包含创建频率至少为 28 天的 cron 表达式时，才能启用快照存档。
- 存档层中的最短保留期为 90 天。
- 快照存档时，快照将在移动到存档层时转换为完整快照。这可能会导致快照存储成本增加。有关更多信息，请参阅 归档 Amazon EBS 快照的定价和计费。
- 快照存档时将会禁用快速快照还原和快照共享。
- 如果在某个闰年中，您的保留规则导致存档保留期少于 90 天，则 Amazon Data Lifecycle Manager 会确保快照至少保留 90 天。
- 如果您手动将 Amazon Data Lifecycle Manager 创建的快照存档，并且该快照在达到计划的保留阈值时仍在存档，则 Amazon Data Lifecycle Manager 将不再管理该快照。但是，如果您在达到计划的保留阈值之前将快照还原到标准层，则该计划将继续按照保留规则管理快照。
- 如果您将 Amazon Data Lifecycle Manager 创建的快照永久或临时还原到标准层，并且该快照在达到计划的保留阈值时仍处于标准层中，则 Amazon Data Lifecycle Manager 将不再管理该快照。但是，如果您在达到计划的保留阈值之前重新将快照存档，则计划将在达到保留阈值时删除快照。
- Amazon Data Lifecycle Manager 存档的快照会使用您的 `Archived snapshots per volume` 和 `In-progress snapshot archives per account` 限额。
- 如果计划在重试 24 小时后仍无法将快照存档，则该快照将保留在标准层中，并按照本应从存档层中删除的时间来计划删除时间。例如，假设计划将快照存档 120 天，则在存档失败后，快照会保留在标准层中 120 天，然后才会被永久删除。对于基于计数的计划，快照不会计入计划的保留计数。
- 快照存档的区域必须与创建快照的区域相同。如果您启用了跨区域复制和快照存档，Amazon Data Lifecycle Manager 不会将快照副本存档。
- Amazon Data Lifecycle Manager 存档的快照将会使用 `aws:dlm:archived=true` 系统标签进行标记。此外，如果创建快照的计划已启用存档并且基于期限，则将会使用 `aws:dlm:expirationTime` 系统标签标记所创建的快照，以注明计划将快照存档的日期和时间。

以下注意事项适用于排除根卷和数据（非根）卷：

- 如果您选择排除启动卷，并且指定的标签因此排除所有附加到实例的额外数据卷，那么 Amazon Data Lifecycle Manager 将不会为受影响的实例创建任何快照，而是会发布一

个SnapshotsCreateFailedCloudWatch 指标。有关更多信息，请参阅 使用监控策略 CloudWatch。

删除或终止快照生命周期策略用作目标的卷或实例时应注意以下事项：

- 对于具有基于计数的保留计划的策略用作目标的卷或实例，如果您将该卷删除或将该实例终止，则 Amazon Data Lifecycle Manager 将不再管理标准层和存档层中之前从已删除的卷或已终止的实例创建的快照。如果不再需要较早版本的快照，您必须手动将其删除。
- 对于具有基于期限的保留计划的策略用作目标的卷或实例，如果您将该卷删除或将该实例终止，则该策略将继续按照既定计划从标准层和存档层中删除从已删除的卷或实例创建的快照，直到但不包括最后一个快照。如果不再需要最后一个快照，则必须手动删除该快照。

快照生命周期策略和快速快照还原应注意以下事项：

- Amazon Data Lifecycle Manager 只能为大小为 16 TiB 或以下的快照启用快速快照还原。有关更多信息，请参阅 Amazon EBS 快速快照还原。
- 即使您删除或禁用了策略，为该策略禁用了快速快照还原，或者为该可用区禁用了快速快照还原，已启用快速快照还原的快照仍会保持启用状态。您必须手动为这些快照禁用快速快照还原。
- 如果您为策略启用了快速快照还原，并且超出了可启用快速快照还原的最大快照数，Amazon Data Lifecycle Manager 将按计划创建快照，但不会为其启用快速快照还原。在删除启用了快速快照还原的快照后，将为 Amazon Data Lifecycle Manager 创建的下一个快照启用快速快照还原。
- 快照启用快速快照还原后，每 TiB 需要 60 分钟来优化快照。我们建议您配置相应的计划，以确保在 Amazon Data Lifecycle Manager 创建下一个快照之前对每个快照进行完全优化。
- 如果您为以实例为目标的策略启用快速快照还原，Amazon Data Lifecycle Manager 会为多卷快照集中的各个快照单独启用快速快照还原。如果 Amazon Data Lifecycle Manager 无法为多卷快照集中的其中一个快照启用快速快照还原，它仍会尝试为快照集中的其余快照启用快速快照还原。
- 对于为特定可用区中快照启用的快速快照还原，您需要按每分钟支付费用。收费按比例计算，最少 1 小时。有关更多信息，请参阅 定价和计费。

> **Note**
>
> 根据生命周期策略的配置，您可以在多个可用区同时为多个快照启用快速快照还原。

跨账户共享快照时需注意以下事项：

- 您只能共享未加密的快照或使用 客户托管密钥 加密的快照。
- 您无法共享使用默认 EBS 加密 KMS 密钥 加密的快照。
- 如果您共享加密快照，则还必须与目标账户共享用于加密源卷的 KMS 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其他账户中的用户使用 KMS 密钥。

以下注意事项适用于快照策略和回收站：

- 如果 Amazon Data Lifecycle Manager 删除快照并在达到策略的保留阈值时将其发送到回收站，并且您从回收站手动还原快照，则必须在不再需要该快照时手动删除它。Amazon Data Lifecycle Manager 将不再管理该快照。
- 如果您手动删除由策略创建的快照，并且该快照在达到策略的保留阈值时位于回收站中，则 Amazon Data Lifecycle Manager 将不会删除该快照。当快照存储在回收站中时，Amazon Data Lifecycle Manager 不管理快照。

  如果在达到策略的保留阈值之前从回收站还原了快照，那么当达到策略的保留阈值时，Amazon Data Lifecycle Manager 将删除快照。

  如果在达到策略的保留阈值之前从回收站还原了快照，则 Amazon Data Lifecycle Manager 将不再删除快照。如果不再需要快照，则必须手动删除该快照。

以下注意事项适用于处于 error（错误）状态的快照生命周期策略：

- 对于具有基于存在时间的保留计划的策略，则设置为在策略处于 `error` 状态时过期的快照将无限期保留。您必须手动删除快照。重新启用该策略时，Amazon Data Lifecycle Manager 会在其保留期限到期时恢复删除快照。
- 对于具有基于计数的保留计划的策略，策略会在其处于 `error` 状态时停止创建和删除快照。当您重新启用该策略时，Amazon Data Lifecycle Manager 将恢复创建快照，并在达到保留阈值时恢复删除快照。

快照策略和快照锁定应注意以下事项：

- 如果您手动锁定由 Amazon Data Lifecycle Manager 创建的快照，并且在达到计划的保留阈值时该快照仍处于锁定状态，则 Amazon Data Lifecycle Manager 将不再管理该快照。如果不再需要快照，则必须手动删除该快照。

- 如果您手动锁定由 Amazon Data Lifecycle Manager 创建并启用了“快速快照还原”功能的快照，并且在达到保留阈值时该快照仍处于锁定状态，则 Amazon Data Lifecycle Manager 将不会禁用“快速快照还原”功能或删除该快照。如果不再需要快照，则必须手动禁用“快速快照还原”功能并删除该快照。
- 如果您手动将 Amazon Data Lifecycle Manager 创建的快照注册到 AMI，然后锁定该快照，并且在达到保留阈值时该快照仍处于锁定状态并与 AMI 关联，则 Amazon Data Lifecycle Manager 将继续尝试删除该快照。当 AMI 取消注册并解锁快照时，Amazon Data Lifecycle Manager 将自动删除该快照。

其他资源

有关更多信息，请参阅使用 Amazon Data Lifecycle Manager Amazon 存储自动化 Amazon EBS 快照和 AMI 管理博客。

使用 Data Lifecycle Manager 自动生成应用程序一致性快照

您可以通过在以实例为目标的快照生命周期策略中启用前置和后置脚本，使用 Amazon Data Lifecycle Manager 自动生成应用程序一致性快照。

Amazon Data Lifecycle Manager 与 Amazon Systems Manager （ Systems Manager ）集成，以支持应用程序一致性快照。Amazon Data Lifecycle Manager 使用 Systems Manager（ SSM ）命令文档（包括前置和后置脚本）来自动执行完成应用程序一致性快照所需的操作。在 Amazon Data Lifecycle Manager 启动快照创建之前，其会运行前置脚本中的命令来冻结和刷新 I/O。在 Amazon Data Lifecycle Manager 启动快照创建后，其会运行后置脚本中的命令来解冻 I/O。

使用 Amazon Data Lifecycle Manager，您可以自动生成以下内容的应用程序一致性快照：

- 使用卷影复制服务（ VSS ）的 Windows 应用程序
- SAP HANA 使用 Amazon 托管 SSDM 文档。有关更多信息，请参阅 Amazon EBS snapshots for SAP HANA。
- 使用 SSM 文档模板自行管理的数据库，例如 MySQL、PostgreSQL InterSystems 或 IRIS

主题

- 使用前置和后置脚本的要求
- 应用程序一致性快照入门
- 使用 Amazon Data Lifecycle Manager 进行 VSS 备份的注意事项

- 应用程序一致性快照的共同责任

使用前置和后置脚本的要求

下表概述了将前置和后置脚本与 Amazon Data Lifecycle Manager 一起使用的要求。

	应用程序一致性快照		
要求	VSS 备份	自定义 SSM 文档	其他用例
SSM 代理已安装并在目标实例上运行	✓	✓	✓
目标实例已满足 VSS 系统要求	✓		
与目标实例关联的启用 VSS 的实例配置文件	✓		
安装在目标实例上的 VSS 组件	✓		
使用脚本前和后置脚本命令准备 SSM 文档		✓	✓
准备 Amazon Data Lifecycle Manager IAM 角色运行前脚本和后脚本	✓	✓	✓
创建以实例为目标的快照策略，并针对前脚本和后脚本进行配置	✓	✓	✓

应用程序一致性快照入门

本节介绍使用 Amazon Data Lifecycle Manager 自动生成应用程序一致性快照所需遵循的步骤。

步骤 1：准备目标实例

您需要使用 Amazon Data Lifecycle Manager 为应用程序一致性快照准备目标实例。根据您的用例执行以下操作之一。

Prepare for VSS Backups

为 VSS 备份准备目标实例

1. 在目标实例上安装 SSM Agent（如果尚未安装）。如果目标实例上已安装 SSM Agent，请跳过此步骤。

   有关更多信息，请参阅在 Windows 服务器的 EC2 实例上使用 SSM 代理。
2. 确保 SSM Agent 正在运行。有关更多信息，请参阅正在检查 SSM Agent 状态并启动代理。
3. 为亚马逊 EC2 实例设置 Systems Manager。有关更多信息，请参阅Amazon Systems Manager 用户指南中的为亚马逊 EC2 实例设置 Systems Manager。
4. 确保满足 VSS 备份的系统要求。
5. 将启用 VSS 的实例配置文件附加到目标实例。
6. 安装 VSS 组件。

Prepare for SAP HANA backups

为 SAP HANA 备份准备目标实例

1. 在目标实例上准备 SAP HANA 环境。

   a. 使用 SAP HANA 设置实例。如果您还没有现成的 SAP HANA 环境，则可以参考 SAP HANA Environment Setup on Amazon。

   b. 以合适的管理员用户身份登录 SystemDB。

   c. 创建要与 Amazon Data Lifecycle Manager 一起使用的数据库备份用户。

   ```
   CREATE USER username PASSWORD password NO FORCE_FIRST_PASSWORD_CHANGE;
   ```

   例如，以下命令创建了一个名为 `dlm_user` 并且密码为 `password` 的用户。

   ```
   CREATE USER dlm_user PASSWORD password NO FORCE_FIRST_PASSWORD_CHANGE;
   ```

   d. 将 `BACKUP OPERATOR` 角色分配给您在上一步中创建的数据库备份用户。

```
GRANT BACKUP OPERATOR TO username
```

例如，以下命令将角色分配给名为 dlm_user 的用户。

```
GRANT BACKUP OPERATOR TO dlm_user
```

e. 以管理员身份登录操作系统，例如 *sid*adm。

f. 创建一个 hdbuserstore 条目来存储连接信息，这样 SAP HANA SSM 文档就可以连接到 SAP HANA，而无需用户输入信息。

```
hdbuserstore set DLM_HANADB_SNAPSHOT_USER
 localhost:3hana_instance_number13 username password
```

例如：

```
hdbuserstore set DLM_HANADB_SNAPSHOT_USER localhost:30013 dlm_user password
```

g. 测试连接。

```
hdbsql -U DLM_HANADB_SNAPSHOT_USER "select * from dummy"
```

2. 在目标实例上安装 SSM Agent（如果尚未安装）。如果目标实例上已安装 SSM Agent，请跳过此步骤。

   有关更多信息，请参阅在 Linux EC2 实例上手动安装 SSM 代理。

3. 确保 SSM Agent 正在运行。有关更多信息，请参阅正在检查 SSM Agent 状态并启动代理。

4. 为亚马逊 EC2 实例设置 Systems Manager。有关更多信息，请参阅Amazon Systems Manager 用户指南中的为亚马逊 EC2 实例设置 Systems Manager。

Prepare for custom SSM documents

为 SSM 文档准备目标实例

1. 在目标实例上安装 SSM Agent（如果尚未安装）。如果目标实例上已安装 SSM Agent，请跳过此步骤。

   - （Linux 实例）在 Linux EC2 实例上手动安装 SSM 代理

- （Windows 实例）在 Windows 服务器的 EC2 实例上使用 SSM 代理

2. 确保 SSM Agent 正在运行。有关更多信息，请参阅正在检查 SSM Agent 状态并启动代理。
3. 为亚马逊 EC2 实例设置 Systems Manager。有关更多信息，请参阅Amazon Systems Manager 用户指南中的为亚马逊 EC2 实例设置 Systems Manager。

步骤 2：准备 SSM 文档

> **Note**
>
> 只有自定义 SSM 文档才需要执行此步骤。VSS 备份或 SAP HANA 不需要执行此步骤。对于 VSS 备份和 SAP HANA，Amazon Data Lifecycle Manager 使用 Amazon 托管 SSM 文档。

如果要为自管理的数据库（例如 MySQL、PostgreSQL 或 InterSystems IRIS）自动生成应用程序一致性快照，则必须创建一个 SSM 命令文档，其中包含用于在启动快照创建之前冻结和刷新 I/O 的预脚本，以及用于在启动快照创建后解冻 I/O 的后置脚本。

如果您的 MySQL、PostgreSQL InterSystems 或 IRIS 数据库使用标准配置，则可以使用下面的示例 SSM 文档内容创建 SSM 命令文档。如果您的 MySQL、PostgreSQL InterSystems 或 IRIS 数据库使用非标准配置，则可以使用以下示例内容作为 SSM 命令文档的起点，然后对其进行自定义以满足您的要求。或者，如果想要从头开始创建新的 SSM 文档，则可以使用下面的 SSM 文档空白模板，并在相应的文档部分中添加前置和后置命令。

> **请注意以下几点：**
>
> - 您负责确保 SSM 文档为数据库配置执行正确且必需的操作。
> - 只有当 SSM 文档中的前置和后置脚本能够成功冻结、刷新和解冻 I/O 时，才能保证快照具有应用程序一致性。
> - SSM 文档必须包含 `allowedValues` 的必填字段，包括 `pre-script`、`post-script` 和 `dry-run`。Amazon Data Lifecycle Manager 将根据这些部分的内容在您的实例上执行命令。如果您的 SSM 文档没有这些部分，则 Amazon Data Lifecycle Manager 会将其视为执行失败。

MySQL sample document content

```
###============================================================================###
```

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.

# Permission is hereby granted, free of charge, to any person obtaining a copy of
 this
# software and associated documentation files (the "Software"), to deal in the
 Software
# without restriction, including without limitation the rights to use, copy, modify,
# merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
# permit persons to whom the Software is furnished to do so.

# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
 IMPLIED,
# INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
# PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
# HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
# OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
# SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
###############################################################################
schemaVersion: '2.2'
description: Amazon Data Lifecycle Manager Pre/Post script for MySQL databases
parameters:
  executionId:
    type: String
    default: None
    description: (Required) Specifies the unique identifier associated with a pre
 and/or post execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]
{4}-[a-fA-F0-9]{12})$
  command:
  # Data Lifecycle Manager will trigger the pre-script and post-script actions
 during policy execution.
  # 'dry-run' option is intended for validating the document execution without
 triggering any commands
  # on the instance. The following allowedValues will allow Data Lifecycle Manager
 to successfully
  # trigger pre and post script actions.
    type: String
    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should
 be executed.
    allowedValues:
    - pre-script
    - post-script
    - dry-run
```

```
mainSteps:
- action: aws:runShellScript
  description: Run MySQL Database freeze/thaw commands
  name: run_pre_post_scripts
  precondition:
    StringEquals:
    - platformType
    - Linux
  inputs:
    runCommand:
    - |
      #!/bin/bash


 ###============================================================================###
      ### Error Codes

 ###============================================================================###
      # The following Error codes will inform Data Lifecycle Manager of the type of
 error
      # and help guide handling of the error.
      # The Error code will also be emitted via AWS Eventbridge events in the
 'cause' field.
      # 1 Pre-script failed during execution - 201
      # 2 Post-script failed during execution - 202
      # 3 Auto thaw occurred before post-script was initiated - 203
      # 4 Pre-script initiated while post-script was expected - 204
      # 5 Post-script initiated while pre-script was expected - 205
      # 6 Application not ready for pre or post-script initiation - 206

      ###====================================================================###
      ### Global variables
      ###====================================================================###
      START=$(date +%s)
      # For testing this script locally, replace the below with OPERATION=$1.
      OPERATION={{ command }}
      FS_ALREADY_FROZEN_ERROR='freeze failed: Device or resource busy'
      FS_ALREADY_THAWED_ERROR='unfreeze failed: Invalid argument'
      FS_BUSY_ERROR='mount point is busy'

      # Auto thaw is a fail safe mechanism to automatically unfreeze the application
 after the
```

```
    # duration specified in the global variable below. Choose the duration based
on your
    # database application's tolerance to freeze.
    export AUTO_THAW_DURATION_SECS="60"

    # Add all pre-script actions to be performed within the function below
    execute_pre_script() {
        echo "INFO: Start execution of pre-script"
        # Check if filesystem is already frozen. No error code indicates that
filesystem
        # is not currently frozen and that the pre-script can proceed with
freezing the filesystem.
        check_fs_freeze
        # Execute the DB commands to flush the DB in preparation for snapshot
        snap_db
        # Freeze the filesystem. No error code indicates that filesystem was
succefully frozen
        freeze_fs

        echo "INFO: Schedule Auto Thaw to execute in ${AUTO_THAW_DURATION_SECS}
seconds."
        $(nohup bash -c execute_schedule_auto_thaw  >/dev/null 2>&1 &)
    }

    # Add all post-script actions to be performed within the function below
    execute_post_script() {
        echo "INFO: Start execution of post-script"
        # Unfreeze the filesystem. No error code indicates that filesystem was
successfully unfrozen.
        unfreeze_fs
        thaw_db
    }

    # Execute Auto Thaw to automatically unfreeze the application after the
duration configured
    # in the AUTO_THAW_DURATION_SECS global variable.
    execute_schedule_auto_thaw() {
        sleep ${AUTO_THAW_DURATION_SECS}
        execute_post_script
    }

    # Disable Auto Thaw if it is still enabled
    execute_disable_auto_thaw() {
        echo "INFO: Attempting to disable auto thaw if enabled"
```

```
        auto_thaw_pgid=$(pgrep -f execute_schedule_auto_thaw | xargs -i ps -hp {}
-o pgid)
        if [ -n "${auto_thaw_pgid}" ]; then
            echo "INFO: execute_schedule_auto_thaw process found with pgid
${auto_thaw_pgid}"
            sudo pkill -g ${auto_thaw_pgid}
            rc=$?
            if [ ${rc} != 0 ]; then
                echo "ERROR: Unable to kill execute_schedule_auto_thaw process.
retval=${rc}"
            else
                echo "INFO: Auto Thaw  has been disabled"
            fi
        fi
    }

    # Iterate over all the mountpoints and check if filesystem is already in
freeze state.
    # Return error code 204 if any of the mount points are already frozen.
    check_fs_freeze() {
        for target in $(lsblk -nlo MOUNTPOINTS)
        do
            # Freeze of the root and boot filesystems is dangerous and pre-script
does not freeze these filesystems.
            # Hence, we will skip the root and boot mountpoints while checking if
filesystem is in freeze state.
            if [ $target == '/' ]; then continue; fi
            if [[ "$target" == *"/boot"* ]]; then continue; fi

            error_message=$(sudo mount -o remount,noatime $target 2>&1)
            # Remount will be a no-op without a error message if the filesystem is
unfrozen.
            # However, if filesystem is already frozen, remount will fail with
busy error message.
            if [ $? -ne 0 ];then
                # If the filesystem is already in frozen, return error code 204
                if [[ "$error_message" == *"$FS_BUSY_ERROR"* ]];then
                    echo "ERROR: Filesystem ${target} already frozen. Return Error
Code: 204"
                    exit 204
                fi
                # If the check filesystem freeze failed due to any reason other
than the filesystem already frozen, return 201
```

```
                echo "ERROR: Failed to check_fs_freeze on mountpoint $target due
to error - $errormessage"
                exit 201
            fi
        done
    }

    # Iterate over all the mountpoints and freeze the filesystem.
    freeze_fs() {
        for target in $(lsblk -nlo MOUNTPOINTS)
        do
            # Freeze of the root and boot filesystems is dangerous. Hence, skip
filesystem freeze
            # operations for root and boot mountpoints.
            if [ $target == '/' ]; then continue; fi
            if [[ "$target" == *"/boot"* ]]; then continue; fi
            echo "INFO: Freezing $target"
            error_message=$(sudo fsfreeze -f $target 2>&1)
            if [ $? -ne 0 ];then
                # If the filesystem is already in frozen, return error code 204
                if [[ "$error_message" == *"$FS_ALREADY_FROZEN_ERROR"* ]]; then
                    echo "ERROR: Filesystem ${target} already frozen. Return Error
Code: 204"
                    sudo mysql -e 'UNLOCK TABLES;'
                    exit 204
                fi
                # If the filesystem freeze failed due to any reason other than the
filesystem already frozen, return 201
                echo "ERROR: Failed to freeze mountpoint $targetdue due to error -
$errormessage"
                thaw_db
                exit 201
            fi
            echo "INFO: Freezing complete on $target"
        done
    }

    # Iterate over all the mountpoints and unfreeze the filesystem.
    unfreeze_fs() {
        for target in $(lsblk -nlo MOUNTPOINTS)
        do
            # Freeze of the root and boot filesystems is dangerous and pre-script
does not freeze these filesystems.
```

```
            # Hence, will skip the root and boot mountpoints during unfreeze as
well.
            if [ $target == '/' ]; then continue; fi
            if [[ "$target" == *"/boot"* ]]; then continue; fi
            echo "INFO: Thawing $target"
            error_message=$(sudo fsfreeze -u $target 2>&1)
            # Check if filesystem is already unfrozen (thawed). Return error code
204 if filesystem is already unfrozen.
            if [ $? -ne 0 ]; then
                if [[ "$error_message" == *"$FS_ALREADY_THAWED_ERROR"* ]]; then
                    echo "ERROR: Filesystem ${target} is already in thaw state.
Return Error Code: 205"
                    exit 205
                fi
                # If the filesystem unfreeze failed due to any reason other than
the filesystem already unfrozen, return 202
                echo "ERROR: Failed to unfreeze mountpoint $targetdue due to error
- $errormessage"
                exit 202
            fi
            echo "INFO: Thaw complete on $target"
        done
    }

    snap_db() {
        # Run the flush command only when MySQL DB service is up and running
        sudo systemctl is-active --quiet mysqld.service
        if [ $? -eq 0 ]; then
            echo "INFO: Execute MySQL Flush and Lock command."
            sudo mysql -e 'FLUSH TABLES WITH READ LOCK;'
            # If the MySQL Flush and Lock command did not succeed, return error
code 201 to indicate pre-script failure
            if [ $? -ne 0 ]; then
                echo "ERROR: MySQL FLUSH TABLES WITH READ LOCK command failed."
                exit 201
            fi
            sync
        else
            echo "INFO: MySQL service is inactive. Skipping execution of MySQL
Flush and Lock command."
        fi
    }

    thaw_db() {
```

```
        # Run the unlock command only when MySQL DB service is up and running
        sudo systemctl is-active --quiet mysqld.service
        if [ $? -eq 0 ]; then
            echo "INFO: Execute MySQL Unlock"
            sudo mysql -e 'UNLOCK TABLES;'
        else
            echo "INFO: MySQL service is inactive. Skipping execution of MySQL
 Unlock command."
        fi
    }

    export -f execute_schedule_auto_thaw
    export -f execute_post_script
    export -f unfreeze_fs
    export -f thaw_db

    # Debug logging for parameters passed to the SSM document
    echo "INFO: ${OPERATION} starting at $(date) with executionId:
 ${EXECUTION_ID}"

    # Based on the command parameter value execute the function that supports
    # pre-script/post-script operation
    case ${OPERATION} in
        pre-script)
            execute_pre_script
            ;;
        post-script)
            execute_post_script
            execute_disable_auto_thaw
            ;;
        dry-run)
            echo "INFO: dry-run option invoked - taking no action"
            ;;
        *)
            echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
            exit 1 # return failure
            ;;
    esac

    END=$(date +%s)
    # Debug Log for profiling the script time
```

```
      echo "INFO: ${OPERATION} completed at $(date). Total runtime: $((${END} -
 ${START})) seconds."
```

PostgreSQL sample document content

```
###############################################################################
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.

# Permission is hereby granted, free of charge, to any person obtaining a copy of
 this
# software and associated documentation files (the "Software"), to deal in the
 Software
# without restriction, including without limitation the rights to use, copy, modify,
# merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
# permit persons to whom the Software is furnished to do so.

# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
 IMPLIED,
# INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
# PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
# HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
# OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
# SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
###############################################################################
schemaVersion: '2.2'
description: Amazon Data Lifecycle Manager Pre/Post script for PostgreSQL databases
parameters:
  executionId:
    type: String
    default: None
    description: (Required) Specifies the unique identifier associated with a pre
 and/or post execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]
{4}-[a-fA-F0-9]{12})$
  command:
  # Data Lifecycle Manager will trigger the pre-script and post-script actions
 during policy execution.
  # 'dry-run' option is intended for validating the document execution without
 triggering any commands
  # on the instance. The following allowedValues will allow Data Lifecycle Manager
 to successfully
  # trigger pre and post script actions.
    type: String
```

```
    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should
 be executed.
    allowedValues:
    - pre-script
    - post-script
    - dry-run

mainSteps:
- action: aws:runShellScript
  description: Run PostgreSQL Database freeze/thaw commands
  name: run_pre_post_scripts
  precondition:
    StringEquals:
    - platformType
    - Linux
  inputs:
    runCommand:
    - |
      #!/bin/bash


 ###============================================================================###
      ### Error Codes

 ###============================================================================###
      # The following Error codes will inform Data Lifecycle Manager of the type of
 error
      # and help guide handling of the error.
      # The Error code will also be emitted via AWS Eventbridge events in the
 'cause' field.
      # 1 Pre-script failed during execution - 201
      # 2 Post-script failed during execution - 202
      # 3 Auto thaw occurred before post-script was initiated - 203
      # 4 Pre-script initiated while post-script was expected - 204
      # 5 Post-script initiated while pre-script was expected - 205
      # 6 Application not ready for pre or post-script initiation - 206


 ###============================================================================###
      ### Global variables

 ###============================================================================###
      START=$(date +%s)
```

```
    OPERATION={{ command }}
    FS_ALREADY_FROZEN_ERROR='freeze failed: Device or resource busy'
    FS_ALREADY_THAWED_ERROR='unfreeze failed: Invalid argument'
    FS_BUSY_ERROR='mount point is busy'

    # Auto thaw is a fail safe mechanism to automatically unfreeze the application
after the
    # duration specified in the global variable below. Choose the duration based
on your
    # database application's tolerance to freeze.
    export AUTO_THAW_DURATION_SECS="60"

    # Add all pre-script actions to be performed within the function below
    execute_pre_script() {
        echo "INFO: Start execution of pre-script"
        # Check if filesystem is already frozen. No error code indicates that
filesystem
        # is not currently frozen and that the pre-script can proceed with
freezing the filesystem.
        check_fs_freeze
        # Execute the DB commands to flush the DB in preparation for snapshot
        snap_db
        # Freeze the filesystem. No error code indicates that filesystem was
succefully frozen
        freeze_fs

        echo "INFO: Schedule Auto Thaw to execute in ${AUTO_THAW_DURATION_SECS}
seconds."
        $(nohup bash -c execute_schedule_auto_thaw  >/dev/null 2>&1 &)
    }

    # Add all post-script actions to be performed within the function below
    execute_post_script() {
        echo "INFO: Start execution of post-script"
        # Unfreeze the filesystem. No error code indicates that filesystem was
successfully unfrozen
        unfreeze_fs
    }

    # Execute Auto Thaw to automatically unfreeze the application after the
duration configured
    # in the AUTO_THAW_DURATION_SECS global variable.
    execute_schedule_auto_thaw() {
        sleep ${AUTO_THAW_DURATION_SECS}
```

```
        execute_post_script
    }

    # Disable Auto Thaw if it is still enabled
    execute_disable_auto_thaw() {
        echo "INFO: Attempting to disable auto thaw if enabled"
        auto_thaw_pgid=$(pgrep -f execute_schedule_auto_thaw | xargs -i ps -hp {}
-o pgid)
        if [ -n "${auto_thaw_pgid}" ]; then
            echo "INFO: execute_schedule_auto_thaw process found with pgid
${auto_thaw_pgid}"
            sudo pkill -g ${auto_thaw_pgid}
            rc=$?
            if [ ${rc} != 0 ]; then
                echo "ERROR: Unable to kill execute_schedule_auto_thaw process.
retval=${rc}"
            else
                echo "INFO: Auto Thaw  has been disabled"
            fi
        fi
    }

    # Iterate over all the mountpoints and check if filesystem is already in
freeze state.
    # Return error code 204 if any of the mount points are already frozen.
    check_fs_freeze() {
        for target in $(lsblk -nlo MOUNTPOINTS)
        do
            # Freeze of the root and boot filesystems is dangerous and pre-script
does not freeze these filesystems.
            # Hence, we will skip the root and boot mountpoints while checking if
filesystem is in freeze state.
            if [ $target == '/' ]; then continue; fi
            if [[ "$target" == *"/boot"* ]]; then continue; fi

            error_message=$(sudo mount -o remount,noatime $target 2>&1)
            # Remount will be a no-op without a error message if the filesystem is
unfrozen.
            # However, if filesystem is already frozen, remount will fail with
busy error message.
            if [ $? -ne 0 ];then
                # If the filesystem is already in frozen, return error code 204
                if [[ "$error_message" == *"$FS_BUSY_ERROR"* ]];then
```

```
                    echo "ERROR: Filesystem ${target} already frozen. Return Error
Code: 204"
                    exit 204
                fi
                # If the check filesystem freeze failed due to any reason other
than the filesystem already frozen, return 201
                echo "ERROR: Failed to check_fs_freeze on mountpoint $target due
to error - $errormessage"
                exit 201
            fi
        done
    }

    # Iterate over all the mountpoints and freeze the filesystem.
    freeze_fs() {
        for target in $(lsblk -nlo MOUNTPOINTS)
        do
            # Freeze of the root and boot filesystems is dangerous. Hence, skip
filesystem freeze
            # operations for root and boot mountpoints.
            if [ $target == '/' ]; then continue; fi
            if [[ "$target" == *"/boot"* ]]; then continue; fi
            echo "INFO: Freezing $target"
            error_message=$(sudo fsfreeze -f $target 2>&1)
            if [ $? -ne 0 ];then
                # If the filesystem is already in frozen, return error code 204
                if [[ "$error_message" == *"$FS_ALREADY_FROZEN_ERROR"* ]]; then
                    echo "ERROR: Filesystem ${target} already frozen. Return Error
Code: 204"
                    exit 204
                fi
                # If the filesystem freeze failed due to any reason other than the
filesystem already frozen, return 201
                echo "ERROR: Failed to freeze mountpoint $targetdue due to error -
$errormessage"
                exit 201
            fi
            echo "INFO: Freezing complete on $target"
        done
    }

    # Iterate over all the mountpoints and unfreeze the filesystem.
    unfreeze_fs() {
        for target in $(lsblk -nlo MOUNTPOINTS)
```

```
        do
            # Freeze of the root and boot filesystems is dangerous and pre-script
does not freeze these filesystems.
            # Hence, will skip the root and boot mountpoints during unfreeze as
well.
            if [ $target == '/' ]; then continue; fi
            if [[ "$target" == *"/boot"* ]]; then continue; fi
            echo "INFO: Thawing $target"
            error_message=$(sudo fsfreeze -u $target 2>&1)
            # Check if filesystem is already unfrozen (thawed). Return error code
204 if filesystem is already unfrozen.
            if [ $? -ne 0 ]; then
                if [[ "$error_message" == *"$FS_ALREADY_THAWED_ERROR"* ]]; then
                    echo "ERROR: Filesystem ${target} is already in thaw state.
Return Error Code: 205"
                    exit 205
                fi
                # If the filesystem unfreeze failed due to any reason other than
the filesystem already unfrozen, return 202
                echo "ERROR: Failed to unfreeze mountpoint $targetdue due to error
- $errormessage"
                exit 202
            fi
            echo "INFO: Thaw complete on $target"
        done
    }

    snap_db() {
        # Run the flush command only when PostgreSQL DB service is up and running
        sudo systemctl is-active --quiet postgresql
        if [ $? -eq 0 ]; then
            echo "INFO: Execute Postgres CHECKPOINT"
            # PostgreSQL command to flush the transactions in memory to disk
            sudo -u postgres psql -c 'CHECKPOINT;'
            # If the PostgreSQL Command did not succeed, return error code 201 to
indicate pre-script failure
            if [ $? -ne 0 ]; then
                echo "ERROR: Postgres CHECKPOINT command failed."
                exit 201
            fi
            sync
        else
            echo "INFO: PostgreSQL service is inactive. Skipping execution of
CHECKPOINT command."
```

```
        fi
    }

    export -f execute_schedule_auto_thaw
    export -f execute_post_script
    export -f unfreeze_fs

    # Debug logging for parameters passed to the SSM document
    echo "INFO: ${OPERATION} starting at $(date) with executionId:
 ${EXECUTION_ID}"

    # Based on the command parameter value execute the function that supports
    # pre-script/post-script operation
    case ${OPERATION} in
        pre-script)
            execute_pre_script
            ;;
        post-script)
            execute_post_script
            execute_disable_auto_thaw
            ;;
        dry-run)
            echo "INFO: dry-run option invoked - taking no action"
            ;;
        *)
            echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
            exit 1 # return failure
            ;;
    esac

    END=$(date +%s)
    # Debug Log for profiling the script time
    echo "INFO: ${OPERATION} completed at $(date). Total runtime: $((${END} -
 ${START})) seconds."
```

InterSystems IRIS sample document content

```
###============================================================================###
# MIT License
#
# Copyright (c) 2024 InterSystems
#
```

```
# Permission is hereby granted, free of charge, to any person obtaining a copy
# of this software and associated documentation files (the "Software"), to deal
# in the Software without restriction, including without limitation the rights
# to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
# copies of the Software, and to permit persons to whom the Software is
# furnished to do so, subject to the following conditions:
#
# The above copyright notice and this permission notice shall be included in all
# copies or substantial portions of the Software.
#
# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
# IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
# FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
# AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
# LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
# OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
# SOFTWARE.
###======================================================================================###
schemaVersion: '2.2'
description: SSM Document Template for Amazon Data Lifecycle Manager Pre/Post script
 feature for InterSystems IRIS.
parameters:
  executionId:
    type: String
    default: None
    description: Specifies the unique identifier associated with a pre and/or post
 execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]
{4}-[a-fA-F0-9]{12})$
  command:
    type: String
    # Data Lifecycle Manager will trigger the pre-script and post-script actions.
 You can also use this SSM document with 'dry-run' for manual testing purposes.
    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should
 be executed.
    #The following allowedValues will allow Data Lifecycle Manager to successfully
 trigger pre and post script actions.
    allowedValues:
    - pre-script
    - post-script
    - dry-run

mainSteps:
```

```
- action: aws:runShellScript
  description: Run InterSystems IRIS Database freeze/thaw commands
  name: run_pre_post_scripts
  precondition:
    StringEquals:
    - platformType
    - Linux
  inputs:
    runCommand:
    - |
      #!/bin/bash

 ###============================================================================###
      ### Global variables

 ###============================================================================###
      DOCKER_NAME=iris
      LOGDIR=./
      EXIT_CODE=0
      OPERATION={{ command }}
      START=$(date +%s)

      # Check if Docker is installed
      # By default if Docker is present, script assumes that InterSystems IRIS is
 running in Docker
      # Leave only the else block DOCKER_EXEC line, if you run InterSystems IRIS
 non-containerised (and Docker is present).
      # Script assumes irissys user has OS auth enabled, change the OS user or
 supply login/password depending on your configuration.
      if command -v docker &> /dev/null
      then
        DOCKER_EXEC="docker exec $DOCKER_NAME"
      else
        DOCKER_EXEC="sudo -i -u irissys"
      fi



      # Add all pre-script actions to be performed within the function below
      execute_pre_script() {
        echo "INFO: Start execution of pre-script"

        # find all iris running instances
        iris_instances=$($DOCKER_EXEC iris qall 2>/dev/null | tail -n +3 | grep
 '^up' | cut -c5-  | awk '{print $1}')
```

```
        echo "`date`: Running iris instances $iris_instances"

        # Only for running instances
        for INST in $iris_instances; do

          echo "`date`: Attempting to freeze $INST"

          # Detailed instances specific log
          LOGFILE=$LOGDIR/$INST-pre_post.log

          #check Freeze status before starting
          $DOCKER_EXEC irissession $INST -U '%SYS'
 "##Class(Backup.General).IsWDSuspendedExt()"
          freeze_status=$?
          if [ $freeze_status -eq 5 ]; then
            echo "`date`:   ERROR: $INST IS already FROZEN"
            EXIT_CODE=204
          else
            echo "`date`:   $INST is not frozen"
            # Freeze
            # Docs: https://docs.intersystems.com/irislatest/csp/documatic/
%25CSP.Documatic.cls?LIBRARY=%25SYS&CLASSNAME=Backup.General#ExternalFreeze
            $DOCKER_EXEC irissession $INST -U '%SYS'
 "##Class(Backup.General).ExternalFreeze(\"$LOGFILE\",,,,,,600,,,300)"
            status=$?

            case $status in
              5) echo "`date`:   $INST IS FROZEN"
                ;;
              3) echo "`date`:   $INST FREEZE FAILED"
                EXIT_CODE=201
                ;;
              *) echo "`date`:   ERROR: Unknown status code: $status"
                EXIT_CODE=201
                ;;
            esac
            echo "`date`:   Completed freeze of $INST"
          fi
        done
        echo "`date`: Pre freeze script finished"
      }

      # Add all post-script actions to be performed within the function below
      execute_post_script() {
```

```
        echo "INFO: Start execution of post-script"

        # find all iris running instances
        iris_instances=$($DOCKER_EXEC iris qall 2>/dev/null | tail -n +3 | grep
 '^up' | cut -c5-  | awk '{print $1}')
        echo "`date`: Running iris instances $iris_instances"

        # Only for running instances
        for INST in $iris_instances; do

          echo "`date`: Attempting to thaw $INST"

          # Detailed instances specific log
          LOGFILE=$LOGDIR/$INST-pre_post.log

          #check Freeze status befor starting
          $DOCKER_EXEC irissession $INST -U '%SYS'
 "##Class(Backup.General).IsWDSuspendedExt()"
          freeze_status=$?
          if [ $freeze_status -eq 5 ]; then
            echo "`date`:  $INST is in frozen state"
            # Thaw
            # Docs: https://docs.intersystems.com/irislatest/csp/documatic/
%25CSP.Documatic.cls?LIBRARY=%25SYS&CLASSNAME=Backup.General#ExternalFreeze
            $DOCKER_EXEC irissession $INST -U%SYS
 "##Class(Backup.General).ExternalThaw(\"$LOGFILE\")"
            status=$?

            case $status in
              5) echo "`date`:   $INST IS THAWED"
                  $DOCKER_EXEC irissession $INST -U%SYS
 "##Class(Backup.General).ExternalSetHistory(\"$LOGFILE\")"
                 ;;
              3) echo "`date`:   $INST THAW FAILED"
                  EXIT_CODE=202
                 ;;
              *) echo "`date`:   ERROR: Unknown status code: $status"
                  EXIT_CODE=202
                 ;;
            esac
            echo "`date`:   Completed thaw of $INST"
          else
            echo "`date`:   ERROR: $INST IS already THAWED"
            EXIT_CODE=205
```

```
          fi
        done
        echo "`date`: Post thaw script finished"
      }

      # Debug logging for parameters passed to the SSM document
        echo "INFO: ${OPERATION} starting at $(date) with executionId:
 ${EXECUTION_ID}"

      # Based on the command parameter value execute the function that supports
      # pre-script/post-script operation
      case ${OPERATION} in
        pre-script)
          execute_pre_script
          ;;
        post-script)
          execute_post_script
            ;;
        dry-run)
          echo "INFO: dry-run option invoked - taking no action"
          ;;
        *)
          echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
          # return failure
          EXIT_CODE=1
          ;;
      esac

      END=$(date +%s)
      # Debug Log for profiling the script time
      echo "INFO: ${OPERATION} completed at $(date). Total runtime: $((${END} -
 ${START})) seconds."
      exit $EXIT_CODE
```

有关更多信息，请参阅GitHub 存储库。

Empty document template

```
###======================================================================###
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.

# Permission is hereby granted, free of charge, to any person obtaining a copy of
 this
```

```
# software and associated documentation files (the "Software"), to deal in the
 Software
# without restriction, including without limitation the rights to use, copy, modify,
# merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
# permit persons to whom the Software is furnished to do so.

# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
 IMPLIED,
# INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
# PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
# HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
# OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
# SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
###############################################################################
schemaVersion: '2.2'
description: SSM Document Template for Amazon Data Lifecycle Manager Pre/Post script
 feature
parameters:
  executionId:
    type: String
    default: None
    description: (Required) Specifies the unique identifier associated with a pre
 and/or post execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]
{4}-[a-fA-F0-9]{12})$
  command:
  # Data Lifecycle Manager will trigger the pre-script and post-script actions
 during policy execution.
  # 'dry-run' option is intended for validating the document execution without
 triggering any commands
  # on the instance. The following allowedValues will allow Data Lifecycle Manager
 to successfully
  # trigger pre and post script actions.
    type: String
    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should
 be executed.
    allowedValues:
    - pre-script
    - post-script
    - dry-run

mainSteps:
- action: aws:runShellScript
```

```
 description: Run Database freeze/thaw commands
 name: run_pre_post_scripts
 precondition:
   StringEquals:
   - platformType
   - Linux
 inputs:
   runCommand:
   - |
     #!/bin/bash


###############################################################################
     ### Error Codes

###############################################################################
     # The following Error codes will inform Data Lifecycle Manager of the type of
error
     # and help guide handling of the error.
     # The Error code will also be emitted via AWS Eventbridge events in the
'cause' field.
     # 1 Pre-script failed during execution - 201
     # 2 Post-script failed during execution - 202
     # 3 Auto thaw occurred before post-script was initiated - 203
     # 4 Pre-script initiated while post-script was expected - 204
     # 5 Post-script initiated while pre-script was expected - 205
     # 6 Application not ready for pre or post-script initiation - 206


###############################################################################
     ### Global variables

###############################################################################
     START=$(date +%s)
     # For testing this script locally, replace the below with OPERATION=$1.
     OPERATION={{ command }}

     # Add all pre-script actions to be performed within the function below
     execute_pre_script() {
         echo "INFO: Start execution of pre-script"
     }

     # Add all post-script actions to be performed within the function below
     execute_post_script() {
```

```
            echo "INFO: Start execution of post-script"
        }

        # Debug logging for parameters passed to the SSM document
        echo "INFO: ${OPERATION} starting at $(date) with executionId:
 ${EXECUTION_ID}"

        # Based on the command parameter value execute the function that supports
        # pre-script/post-script operation
        case ${OPERATION} in
            pre-script)
                execute_pre_script
                ;;
            post-script)
                execute_post_script
                ;;
            dry-run)
                echo "INFO: dry-run option invoked - taking no action"
                ;;
            *)
                echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
                exit 1 # return failure
                ;;
        esac

        END=$(date +%s)
        # Debug Log for profiling the script time
        echo "INFO: ${OPERATION} completed at $(date). Total runtime: $((${END} -
 ${START})) seconds."
```

获得 SSM 文档内容后，请参照以下过程之一创建自定义 SSM 文档。

Console

创建 SSM 命令文档

1. 打开 Amazon Systems Manager 控制台，网址为https://console.aws.amazon.com//systems-manager/。
2. 在导航窗格中，选择文档，然后选择创建文档、命令或会话。
3. 对于名称，为文档输入一个描述性名称。

4. 对于“目标类型”，选择/AWS::EC2::Instance。
5. 对于文档类型，请选择命令。
6. 在内容字段中，选择 YAML，然后粘贴文档内容。
7. 在文档标签部分，添加标签键为 DLMScriptsAccess、标签值为 true 的标签。

> **Important**
>
> 该DLMScriptsAccess:true标签是步骤 3：准备 Amazon Data Lifecycle Manager IAM 角色中使用的AWSDataLifecycleManagerSSMFull访问 Amazon 托管策略所必需的。该策略使用 aws:ResourceTag 条件键来限制对带有此标签的 SSM 文档的访问权限。

8. 选择创建文档。

Amazon CLI

创建 SSM 命令文档

使用 create-document 命令。对于 --name，请为文档指定一个描述性名称。对于 --document-type，请指定 Command。对于 --content，请指定包含 SSM 文档内容的.yaml 文件的路径。对于 --tags，请指定 "Key=DLMScriptsAccess,Value=true"。

```
$ aws ssm create-document \
--content file://path/to/file/documentContent.yaml \
--name "document_name" \
--document-type "Command" \
--document-format YAML \
--tags "Key=DLMScriptsAccess,Value=true"
```

步骤 3：准备 Amazon Data Lifecycle Manager IAM 角色

> **Note**
>
> 如果出现以下情况，则需要执行此步骤：
>
> - 创建或更新使用自定义 IAM 角色的启用前置/后置脚本的快照策略。
> - 使用命令行创建或更新使用默认值的启用前置/后置脚本的快照策略。

如果您使用控制台创建或更新启用脚本前/后脚本的快照策略，该策略使用默认角色管理快照（AWSDataLifecycleManagerDefaultRole），请跳过此步骤。在这种情况下，我们会自动将AWSDataLifecycleManagerSSMFull访问策略附加到该角色。

您必须确保您用于策略的 IAM 角色授予 Amazon Data Lifecycle Manager 权限，以执行在策略作为目标的实例上运行前置和后置脚本所需的 SSM 操作。

Amazon Data Lifecycle Manager 提供了包含所需权限的托管策略（AWSDataLifecycleManagerSSMFull访问权限）。您可以将此策略附加到您的 IAM 角色以管理快照，从而确保其包含这些权限。

Important

使用预脚本和后置脚本时， AWSDataLifecycleManagerSSMFull访问管理策略使用`aws:ResourceTag`条件键来限制对特定 SSM 文档的访问。要允许 Amazon Data Lifecycle Manager 访问 SSM 文档，您必须确保您的 SSM 文档带有 `DLMScriptsAccess:true` 标签。

或者，您可以手动创建自定义策略或将所需权限直接分配给您使用的 IAM 角色。您可以使用与 A AWSData LifecycleManager SSMFull ccess 托管策略中定义的相同权限，但是，`aws:ResourceTag`条件键是可选的。如果您决定不包含该条件键，则无需用 `DLMScriptsAccess:true` 标记您的 SSM 文档。

使用以下方法之一将AWSDataLifecycleManagerSSMFull访问策略添加到您的 IAM 角色。

Console

将托管策略附加到您的自定义角色

1. 使用 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
2. 在导航面板中，选择 Roles（角色）。
3. 搜索并选择用于管理快照的自定义角色。
4. 在权限选项卡上，选择添加权限、附加策略。
5. 搜索并选择AWSDataLifecycleManagerSSMFull访问托管策略，然后选择添加权限。

Amazon CLI

将托管策略附加到您的自定义角色

使用 attach-role-policy 命令。对于 ---role-name，请指定您自定义角色的名称。对于 --policy-arn，请指定 arn:aws:iam::aws:policy/AWSDataLifecycleManagerSSMFullAccess。

```
$ aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AWSDataLifecycleManagerSSMFullAccess \
--role-name your_role_name
```

步骤 4：创建快照生命周期策略

要自动生成应用程序一致性快照，您必须创建以实例为目标的快照生命周期策略，并为该策略配置前置和后置脚本。

Console

创建快照生命周期策略

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，依次选择 Elastic Block Store 和 Lifecycle Manager (生命周期管理器)，然后选择 Create lifecycle policy (创建生命周期策略)。
3. 在选择策略类型页面上，选择 EBS 快照策略，然后选择下一步。
4. 在目标资源部分中，执行以下操作：
   a. 对于目标资源类型，请选择 Instance。
   b. 对于目标资源标签，请指定识别要备份的实例的资源标签。仅备份具有指定标签的资源。
5. 对于 IAM 角色，可以选择 AWSDataLifecycleManagerDefaultRole（用于管理快照的默认角色），也可以选择您创建并准备使用前脚本和发布脚本的自定义角色。
6. 根据需要配置计划和其他选项。我们建议您将快照创建时间计划在与您工作负载相匹配的时间段，例如在维护窗口期间。

   对于 SAP HANA，我们建议您启用“快速快照还原”。

> **Note**
>
> 如果您为 VSS 备份启用计划，则无法启用排除特定数据卷或从源中复制标签。

7. 在前置和后置脚本部分中，选择启用前置和后置脚本，然后根据您的工作负载执行以下操作：

   - 要创建 Windows 应用程序的应用程序一致性快照，请选择 VSS 备份。
   - 要创建您的 SAP HANA 工作负载的应用程序一致性快照，请选择 SAP HANA。
   - 要使用自定义 SSM 文档为所有其他数据库和工作负载（包括自行管理的 MySQL、PostgreSQL InterSystems 或 IRIS 数据库）创建应用程序一致的快照，请选择自定义 SSM 文档。

     1. 对于自动化选项，请选择前置和后置脚本。
     2. 对于 SSM 文档，请选择您准备的 SSM 文档。

8. 根据您所选的选项，配置以下其他选项：

   - 脚本超时 – （仅限自定义 SSM 文档）如果脚本运行尝试尚未完成，则在此超时期间后，Amazon Data Lifecycle Manager 的尝试失败。如果脚本未在其超时期间内完成，Amazon Data Lifecycle Manager 的尝试失败。超时期间分别适用于前置和后置脚本。最小的默认超时期间为 10 秒。最长超时期间为 120 秒。
   - 重试失败的脚本 – 选择此选项可重试未在其超时期间内完成的脚本。如果前置脚本失败，则 Amazon Data Lifecycle Manager 会重试整个快照创建过程，包括运行前置和后置脚本。如果后置脚本失败，则 Amazon Data Lifecycle Manager 将仅重试后置脚本；在这种情况下，前置脚本将完成并且可能已创建快照。
   - 默认创建崩溃一致性快照 – 如果前置脚本运行失败，则选择此选项以默认创建崩溃一致性快照。如果未启用前置和后置脚本，则这是 Amazon Data Lifecycle Manager 的默认快照创建行为。如果您启用了重试，则只有在所有重试尝试都用尽之后，Amazon Data Lifecycle Manager 才会默认创建崩溃一致性快照。如果前置脚本失败并且您没有默认创建崩溃一致性快照，则 Amazon Data Lifecycle Manager 将不会在该计划运行期间为实例创建快照。

   > **Note**
   >
   > 如果您要为 SAP HANA 创建快照，则可能需要禁用此选项。无法以相同的方式还原 SAP HANA 工作负载的崩溃一致性快照。

9. 选择创建默认策略。

> **Note**
>
> 如果发生 `Role with name AWSDataLifecycleManagerDefaultRole already exists` 错误，请参阅 排查 Amazon Data Lifecycle Manager 问题 来了解更多信息。

Amazon CLI

创建快照生命周期策略

使用create-lifecycle-policy命令，并将`Scripts`参数包含在中`CreateRule`。有关参数的更多信息，请参阅 Amazon Data Lifecycle Manager API Reference。

```
$ aws dlm create-lifecycle-policy \
--description "policy_description" \
--state ENABLED \
--execution-role-arn iam_role_arn \
--policy-details file://policyDetails.json
```

其中 `policyDetails.json` 包含以下内容之一，具体取决于您的用例：

- VSS 备份

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key": "tag_key",
        "Value": "tag_value"
    }],
    "Schedules": [{
        "Name": "schedule_name",
        "CreateRule": {
            "CronExpression": "cron_for_creation_frequency",
            "Scripts": [{
                "ExecutionHandler":"AWS_VSS_BACKUP",
                "ExecuteOperationOnScriptFailure":true|false,
                "MaximumRetryCount":retries (0-3)
```

```
            }]
        },
        "RetainRule": {
            "Count": retention_count
        }
    }]
}
```

- SAP HANA 备份

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key": "tag_key",
        "Value": "tag_value"
    }],
    "Schedules": [{
        "Name": "schedule_name",
        "CreateRule": {
            "CronExpression": "cron_for_creation_frequency",
            "Scripts": [{
                "Stages": ["PRE","POST"],
                "ExecutionHandlerService":"AWS_SYSTEMS_MANAGER",
                "ExecutionHandler":"AWSSystemsManagerSAP-
CreateDLMSnapshotForSAPHANA",
                "ExecuteOperationOnScriptFailure":true|false,
                "ExecutionTimeout":timeout_in_seconds (10-120),
                "MaximumRetryCount":retries (0-3)
            }]
        },
        "RetainRule": {
            "Count": retention_count
        }
    }]
}
```

- 自定义 SSM 文档

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
```

```
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key": "tag_key",
        "Value": "tag_value"
    }],
    "Schedules": [{
        "Name": "schedule_name",
        "CreateRule": {
            "CronExpression": "cron_for_creation_frequency",
            "Scripts": [{
                "Stages": ["PRE","POST"],
                "ExecutionHandlerService":"AWS_SYSTEMS_MANAGER",
                "ExecutionHandler":"ssm_document_name|arn",
                "ExecuteOperationOnScriptFailure":true|false,
                "ExecutionTimeout":timeout_in_seconds (10-120),
                "MaximumRetryCount":retries (0-3)
            }]
        },
        "RetainRule": {
            "Count": retention_count
        }
    }]
}
```

使用 Amazon Data Lifecycle Manager 进行 VSS 备份的注意事项

借助 Amazon Data Lifecycle Manager，您可以备份和恢复在亚马逊 EC2 实例上运行的支持 VSS（卷影复制服务）的 Windows 应用程序。如果应用程序已在 Windows VSS 中注册了 VSS 写入器，则 Amazon Data Lifecycle Manager 会为该应用程序创建具有应用程序一致性的快照。

> **Note**
>
> Amazon Data Lifecycle Manager 目前 EC2 仅支持在亚马逊上运行的资源的应用程序一致性快照，特别适用于备份场景，在这种情况下，可以通过将现有实例替换为根据备份创建的新实例来恢复应用程序数据。并非所有实例类型或应用程序都支持 VSS 备份。有关更多信息，请参阅《亚马逊 EC2 用户指南》中的应用程序一致性 Windows VSS 快照。

不支持的实例类型

VSS 备份不支持以下 Amazon EC2 实例类型。如果您的策略以这些实例类型之一为目标，则 Amazon Data Lifecycle Manager 可能仍会创建 VSS 备份，但快照可能不会使用所需的系统标签进行标记。没有这些标签，快照在创建后将无法由 Amazon Data Lifecycle Manager 进行管理。您可能需要手动删除这些快照。

- T3：`t3.nano` | `t3.micro`
- T3a：`t3a.nano` | `t3a.micro`
- T2：`t2.nano` | `t2.micro`

应用程序一致性快照的共同责任

您必须确保：

- SSM 代理已安装并在您的目标实例上运行 up-to-date
- Systems Manager 有权在目标实例上执行所需操作
- Amazon Data Lifecycle Manager 有权执行在目标实例上运行前置和后置脚本所需的 Systems Manager 操作。
- 对于自定义工作负载，例如自行管理的 MySQL、PostgreSQL InterSystems 或 IRIS 数据库，您使用的 SSM 文档包含用于冻结、刷新和解冻 I/O 的正确和必需的操作。
- 快照创建时间与您的工作负载计划保持一致。例如，请尝试在计划的维护窗口期内安排快照创建。

Amazon Data Lifecycle Manager 应确保：

- 快照创建将在计划快照创建时间的 60 分钟内启动。
- 在启动快照创建之前运行前置脚本。
- 在前置脚本成功且快照创建已启动后运行前置脚本。只有在前置脚本成功的情况下，Amazon Data Lifecycle Manager 才会运行后置脚本。如果前置脚本失败，Amazon Data Lifecycle Manager 将不会运行后置脚本。
- 快照在创建时会用相应的标签进行标记。
- CloudWatch 当脚本启动时，以及脚本失败或成功时，都会发出指标和事件。

Data Lifecycle Manager 前置和后置脚本的其他使用场景

除了使用前置和后置脚本自动生成应用程序一致性快照外，您还可以同时或单独使用前置和后置脚本，以在创建快照之前或之后自动执行其他管理任务。例如：

- 创建快照之前使用前置脚本来应用补丁。这可以帮助您在应用每周或每月定期软件更新后创建快照。

> **Note**
>
> 如果您选择仅运行前置脚本，则默认情况下会启用默认创建崩溃一致性快照。

- 创建快照后使用后置脚本应用补丁。这可以帮助您在应用每周或每月定期软件更新之前创建快照。

其他用例入门

本节介绍将前置和/或后置脚本用于应用程序一致性快照以外的用例中时需要执行的步骤。

步骤 1：准备目标实例

为前置和/或后置脚本准备目标实例

1. 在目标实例上安装 SSM Agent（如果尚未安装）。如果目标实例上已安装 SSM Agent，请跳过此步骤。
   - （Linux 实例）在 Linux EC2 实例上手动安装 SSM 代理
   - （Windows 实例）在 Windows 服务器的 EC2 实例上使用 SSM 代理
2. 确保 SSM Agent 正在运行。有关更多信息，请参阅正在检查 SSM Agent 状态并启动代理。
3. 为亚马逊 EC2 实例设置 Systems Manager。有关更多信息，请参阅Amazon Systems Manager 用户指南中的为亚马逊 EC2 实例设置 Systems Manager。

步骤 2：准备 SSM 文档

您必须创建一个 SSM 命令文档，其中包含要运行的命令的前置和/或后置脚本。

您可以使用下面的 SSM 文档空白模板创建 SSM 文档，并在相应的文档部分中添加前置和后置脚本命令。

> **⚠ 请注意以下几点：**
>
> - 您负责确保 SSM 文档为工作负载执行正确和必需的操作。
> - SSM 文档必须包含 `allowedValues` 的必填字段，包括 `pre-script`、`post-script` 和 `dry-run`。Amazon Data Lifecycle Manager 将根据这些部分的内容在您的实例上执行命

令。如果您的 SSM 文档没有这些部分，则 Amazon Data Lifecycle Manager 会将其视为执行失败。

```
###====================================================================================###
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.

# Permission is hereby granted, free of charge, to any person obtaining a copy of this
# software and associated documentation files (the "Software"), to deal in the Software
# without restriction, including without limitation the rights to use, copy, modify,
# merge, publish, distribute, sublicense, and/or sell copies of the Software, and to
# permit persons to whom the Software is furnished to do so.

# THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED,
# INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
# PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
# HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
# OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE
# SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
###====================================================================================###
schemaVersion: '2.2'
description: SSM Document Template for Amazon Data Lifecycle Manager Pre/Post script
 feature
parameters:
  executionId:
    type: String
    default: None
    description: (Required) Specifies the unique identifier associated with a pre and/
or post execution
    allowedPattern: ^(None|[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-
[a-fA-F0-9]{12})$
  command:
  # Data Lifecycle Manager will trigger the pre-script and post-script actions during
 policy execution.
  # 'dry-run' option is intended for validating the document execution without
 triggering any commands
  # on the instance. The following allowedValues will allow Data Lifecycle Manager to
 successfully
  # trigger pre and post script actions.
    type: String
    default: 'dry-run'
    description: (Required) Specifies whether pre-script and/or post-script should be
 executed.
```

```
    allowedValues:
    - pre-script
    - post-script
    - dry-run

mainSteps:
- action: aws:runShellScript
  description: Run Database freeze/thaw commands
  name: run_pre_post_scripts
  precondition:
    StringEquals:
    - platformType
    - Linux
  inputs:
    runCommand:
    - |
      #!/bin/bash


 ###########################################################################################
      ### Error Codes

 ###########################################################################################
      # The following Error codes will inform Data Lifecycle Manager of the type of
 error
      # and help guide handling of the error.
      # The Error code will also be emitted via AWS Eventbridge events in the 'cause'
 field.
      # 1 Pre-script failed during execution - 201
      # 2 Post-script failed during execution - 202
      # 3 Auto thaw occurred before post-script was initiated - 203
      # 4 Pre-script initiated while post-script was expected - 204
      # 5 Post-script initiated while pre-script was expected - 205
      # 6 Application not ready for pre or post-script initiation - 206


 ###########################################################################################
      ### Global variables

 ###########################################################################################
      START=$(date +%s)
      # For testing this script locally, replace the below with OPERATION=$1.
      OPERATION={{ command }}
```

```
      # Add all pre-script actions to be performed within the function below
      execute_pre_script() {
          echo "INFO: Start execution of pre-script"
      }

      # Add all post-script actions to be performed within the function below
      execute_post_script() {
          echo "INFO: Start execution of post-script"
      }

      # Debug logging for parameters passed to the SSM document
      echo "INFO: ${OPERATION} starting at $(date) with executionId: ${EXECUTION_ID}"

      # Based on the command parameter value execute the function that supports
      # pre-script/post-script operation
      case ${OPERATION} in
          pre-script)
              execute_pre_script
              ;;
          post-script)
              execute_post_script
              ;;
          dry-run)
              echo "INFO: dry-run option invoked - taking no action"
              ;;
          *)
              echo "ERROR: Invalid command parameter passed. Please use either pre-
script, post-script, dry-run."
              exit 1 # return failure
              ;;
      esac

      END=$(date +%s)
      # Debug Log for profiling the script time
      echo "INFO: ${OPERATION} completed at $(date). Total runtime: $((${END} -
 ${START})) seconds."
```

步骤 3：准备 Amazon Data Lifecycle Manager IAM 角色

> **Note**
>
> 如果出现以下情况，则需要执行此步骤：

- 创建或更新使用自定义 IAM 角色的启用前置/后置脚本的快照策略。
- 使用命令行创建或更新使用默认值的启用前置/后置脚本的快照策略。

如果您使用控制台创建或更新启用脚本前/后脚本的快照策略，该策略使用默认角色管理快照（AWSDataLifecycleManagerDefaultRole），请跳过此步骤。在这种情况下，我们会自动将AWSDataLifecycleManagerSSMFull访问策略附加到该角色。

您必须确保用于策略的 IAM 角色授予 Amazon Data Lifecycle Manager 权限，以执行在策略作为目标的实例上运行前置和后置脚本所需的 SSM 操作的权限。

Amazon Data Lifecycle Manager 提供了包含所需权限的托管策略（AWSDataLifecycleManagerSSMFull访问权限）。您可以将此策略附加到您的 IAM 角色以管理快照，从而确保其包含这些权限。

Important

使用预脚本和后置脚本时， AWSDataLifecycleManagerSSMFull访问管理策略使用`aws:ResourceTag`条件键来限制对特定 SSM 文档的访问。要允许 Amazon Data Lifecycle Manager 访问 SSM 文档，您必须确保您的 SSM 文档带有 `DLMScriptsAccess:true` 标签。

或者，您可以手动创建自定义策略或将所需权限直接分配给您使用的 IAM 角色。您可以使用与 A AWSData LifecycleManager SSMFull ccess 托管策略中定义的相同权限，但是，`aws:ResourceTag`条件键是可选的。如果您决定不使用该条件键，则无需使用 `DLMScriptsAccess:true` 标记您的 SSM 文档。

使用以下方法之一将AWSDataLifecycleManagerSSMFull访问策略添加到您的 IAM 角色。

Console

将托管策略附加到您的自定义角色

1. 使用 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
2. 在导航面板中，选择 Roles（角色）。
3. 搜索并选择用于管理快照的自定义角色。

4. 在权限选项卡上，选择添加权限、附加策略。
5. 搜索并选择AWSDataLifecycleManagerSSMFull访问托管策略，然后选择添加权限。

Amazon CLI

将托管策略附加到您的自定义角色

使用 attach-role-policy 命令。对于 `---role-name`，请指定您自定义角色的名称。对于 `--policy-arn`，请指定 `arn:aws:iam::aws:policy/AWSDataLifecycleManagerSSMFullAccess`。

```
$ aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AWSDataLifecycleManagerSSMFullAccess \
--role-name your_role_name
```

创建快照生命周期策略

Console

创建快照生命周期策略

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，依次选择 Elastic Block Store 和 Lifecycle Manager (生命周期管理器)，然后选择 Create lifecycle policy (创建生命周期策略)。
3. 在选择策略类型页面上，选择 EBS 快照策略，然后选择下一步。
4. 在目标资源部分中，执行以下操作：
   a. 对于目标资源类型，请选择 `Instance`。
   b. 对于目标资源标签，请指定识别要备份的实例的资源标签。仅备份具有指定标签的资源。
5. 对于 IAM 角色，可以选择 AWSDataLifecycleManagerDefaultRole（用于管理快照的默认角色），也可以选择您创建并准备使用前脚本和发布脚本的自定义角色。
6. 根据需要配置计划和其他选项。我们建议您将快照创建时间计划在与您工作负载相匹配的时间段，例如在维护窗口期间。
7. 在前置和后置脚本部分中，选择启用前置和后置脚本，然后执行以下操作：
   a. 选择自定义 SSM 文档。
   b. 对于自动化选项，请选择与要运行的脚本相匹配的选项。

c. 对于 SSM 文档，请选择您准备的 SSM 文档。

8. 如果需要，请配置以下其他选项：

- 脚本超时 – 如果脚本运行尝试尚未完成，则在此超时期间后，Amazon Data Lifecycle Manager 的尝试失败。如果脚本未在其超时期间内完成，Amazon Data Lifecycle Manager 的尝试失败。超时期间分别适用于前置和后置脚本。最小的默认超时期间为 10 秒。最长超时期间为 120 秒。
- 重试失败的脚本 – 选择此选项可重试未在其超时期间内完成的脚本。如果前置脚本失败，则 Amazon Data Lifecycle Manager 会重试整个快照创建过程，包括运行前置和后置脚本。如果后置脚本失败，则 Amazon Data Lifecycle Manager 将仅重试后置脚本；在这种情况下，前置脚本将完成并且可能已创建快照。
- 默认创建崩溃一致性快照 – 如果前置脚本运行失败，则选择此选项以默认创建崩溃一致性快照。如果未启用前置和后置脚本，则这是 Amazon Data Lifecycle Manager 的默认快照创建行为。如果您启用了重试，则只有在所有重试尝试都用尽之后，Amazon Data Lifecycle Manager 才会默认创建崩溃一致性快照。如果前置脚本失败并且您没有默认创建崩溃一致性快照，则 Amazon Data Lifecycle Manager 将不会在该计划运行期间为实例创建快照。

9. 选择创建默认策略。

> **Note**
>
> 如果发生 `Role with name AWSDataLifecycleManagerDefaultRole already exists` 错误，请参阅 排查 Amazon Data Lifecycle Manager 问题 来了解更多信息。

Amazon CLI

创建快照生命周期策略

使用create-lifecycle-policy命令，并将`Scripts`参数包含在中`CreateRule`。有关参数的更多信息，请参阅 Amazon Data Lifecycle Manager API Reference。

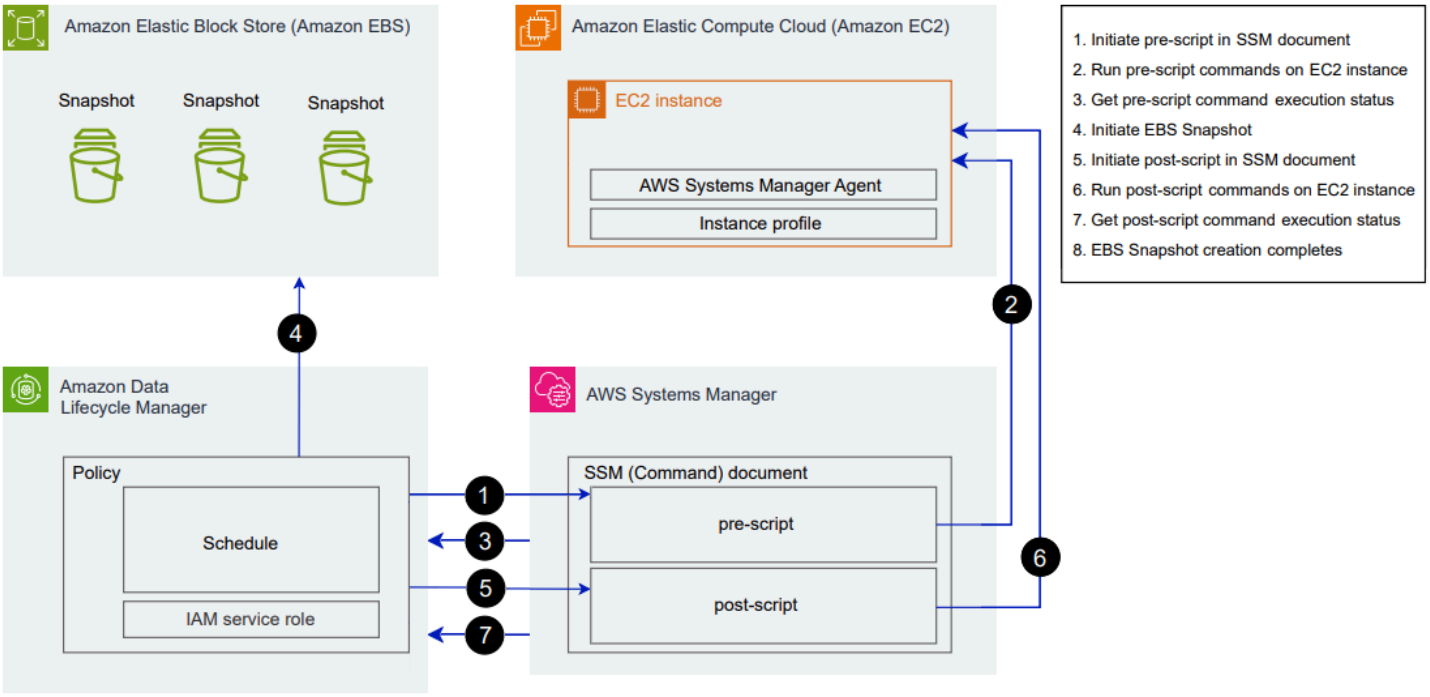
```
$ aws dlm create-lifecycle-policy \
--description "policy_description" \
--state ENABLED \
--execution-role-arn iam_role_arn \
--policy-details file://policyDetails.json
```

其中 policyDetails.json 包含以下内容。

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key": "tag_key",
        "Value": "tag_value"
    }],
    "Schedules": [{
        "Name": "schedule_name",
        "CreateRule": {
            "CronExpression": "cron_for_creation_frequency",
            "Scripts": [{
                "Stages": ["PRE" | "POST" | "PRE","POST"],
                "ExecutionHandlerService":"AWS_SYSTEMS_MANAGER",
                "ExecutionHandler":"ssm_document_name|arn",
                "ExecuteOperationOnScriptFailure":true|false,
                "ExecutionTimeout":timeout_in_seconds (10-120),
                "MaximumRetryCount":retries (0-3)
            }]
        },
        "RetainRule": {
            "Count": retention_count
        }
    }]
}
```

Amazon Data Lifecycle Manager 前置和后置脚本的工作原理

下图显示了使用自定义 SSM 文档时前置和后置脚本的流程。这不适用于 VSS 备份。



在计划创建快照时，会发生以下操作和跨服务交互。

1. Amazon Data Lifecycle Manager 通过调用 SSM 文档并传递 `pre-script` 参数来启动前置脚本操作。

   > **Note**
   >
   > 只有在运行前置脚本时才会执行步骤 1 到 3。如果您仅运行后置脚本，则会跳过步骤 1 到 3。

2. Systems Manager 向在目标实例上运行的 SSM Agent 发送前置脚本命令。SSM Agent 在实例上运行命令，并将状态信息发送回 Systems Manager。

   例如，如果使用 SSM 文档创建应用程序一致性快照，则前置脚本可能会冻结并刷新 I/O，以确保在拍摄快照之前将所有缓冲的数据写入卷。

3. Systems Manager 向 Amazon Data Lifecycle Manager 发送前置脚本命令状态更新。如果前置脚本失败，则 Amazon Data Lifecycle Manager 将执行以下操作之一，具体取决于您配置前置和后置脚本选项的方式：

重试	默认创建崩溃一致性快照	操作
已启用，剩余重试次数	已启用	重试脚本，直到脚本成功或重试次数用尽
次数用尽但未成功完成	已启用	创建崩溃一致性快照，且不运行后置脚本。
已启用，剩余重试次数	已禁用	重试脚本，直到脚本成功或重试次数用尽
次数用尽但未成功完成	已禁用	跳过为目标实例创建快照，且不运行后置脚本。
已禁用	已启用	创建崩溃一致性快照，且不运行后置脚本。
已禁用	已禁用	跳过为目标实例创建快照，且不运行后置脚本。

4. Amazon Data Lifecycle Manager 启动快照创建。
5. Amazon Data Lifecycle Manager 通过调用 SSM 文档并传递 `post-script` 参数来启动后置脚本操作。

> **Note**
>
> 只有在运行前置脚本时才会执行步骤 5 到 7。如果您仅运行后置脚本，则会跳过步骤 1 到 3。

6. Systems Manager 向在目标实例上运行的 SSM Agent 发送后置脚本命令。SSM Agent 在实例上运行命令，并将状态信息发送回 Systems Manager。

   例如，如果 SSM 文档启用了应用程序一致性快照，则此后置脚本可能会解冻 I/O，以确保您的数据库在拍摄快照后恢复正常 I/O 操作。
7. 如果您运行后置脚本且 Systems Manager 指示该脚本已成功完成，则该过程完成。

   如果后置脚本失败，则 Amazon Data Lifecycle Manager 将执行以下操作之一，具体取决于您配置前置和后置脚本选项的方式：

重试	操作
已启用，剩余重试次数	重试后置脚本，直到脚本成功或重试次数用尽
次数用尽，但未成功	跳过后置脚本
已禁用	跳过后置脚本

请记住，如果后置脚本失败，则前置脚本（如已启用）将成功完成，并且可能已创建快照。您可能需要对实例采取进一步操作以确保其按预期运行。例如，如果前置脚本暂停并刷新了 I/O，但后置脚本未能解冻 I/O，则可能需要将数据库配置为自动解冻 I/O，或者需要手动解冻 I/O。

8. 后置脚本完成后，快照创建过程可能会完成。完成快照所需的时间取决于快照的大小。

识别使用 Data Lifecycle Manager 前置和后置脚本创建的快照

Amazon Data Lifecycle Manager 会自动为使用前置和后置脚本创建的快照分配以下系统标签。

- 密钥：`aws:dlm:pre-script`；值：`SUCCESS|FAILED`

  标签值为 `SUCCESS` 表示前置脚本已成功执行。标签值为 `FAILED` 表示前置脚本未成功执行。

- 密钥：`aws:dlm:post-script`；值：`SUCCESS|FAILED`

  标签值为 `SUCCESS` 表示后置脚本已成功执行。标签值为 `FAILED` 表示后置脚本未成功执行。

对于自定义 SSM 文档和 SAP HANA 备份，如果快照同时用 `aws:dlm:pre-script:SUCCESS` 和 `aws:dlm:post-script:SUCCESS` 标记，则可以推断成功创建了应用程序一致性快照。

此外，使用 VSS 备份创建的应用程序一致性快照会自动标记：

- 密钥：`AppConsistent tag`；值：`true|false`

  标签值为 `true` 表示 VSS 备份成功且快照具有应用程序一致性。标签值为 `false` 表示 VSS 备份未成功，并且快照不符合应用程序一致性。

监控 Amazon Data Lifecycle Manager 前置和后置脚本

亚马逊 CloudWatch 指标

Amazon Data Lifecycle Manager 会在前脚本和后脚本失败和成功以及 VSS 备份失败和成功时发布以下 CloudWatch 指标。

- `PreScriptStarted`
- `PreScriptCompleted`
- `PreScriptFailed`
- `PostScriptStarted`
- `PostScriptCompleted`
- `PostScriptFailed`
- `VSSBackupStarted`
- `VSSBackupCompleted`
- `VSSBackupFailed`

有关更多信息，请参阅 使用监控数据生命周期管理器策略 CloudWatch。

Amazon EventBridge

当前脚本或后脚本启动、成功或失败时，Amazon Data Lifecycle Manager 会发出以下亚马逊 EventBridge 事件

- `DLM Pre Post Script Notification`

有关更多信息，请参阅 使用监控数据生命周期管理器策略 EventBridge。

为 EBS 支持的 Amazon Data Lifecycle Manager 自定义策略 AMIs

以下程序说明了如何使用 Amazon Data Lifecycle Manager 来自动执行 EBS 支持的 AMI 生命周期。

主题

- 创建 AMI 生命周期策略
- AMI 生命周期策略的注意事项
- 其他资源

创建 AMI 生命周期策略

使用以下程序之一创建 AMI 生命周期策略。

Console

创建 AMI 策略

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，依次选择 Elastic Block Store 和 Lifecycle Manager (生命周期管理器)，然后选择 Create lifecycle policy (创建生命周期策略)。
3. 在选择策略类型页面，选择 EBS 支持的 AMI 策略，然后选择下一步。
4. 在目标资源部分，对于目标资源标签，选择标识要备份的卷或实例的资源标签。策略只备份具有指定标签键和值对的资源。
5. 对于 Description (描述)，输入策略的简短描述。
6. 对于 IAM 角色，请选择有权管理和快照 AMIs 以及描述实例的 IAM 角色。要使用 Amazon Data Lifecycle Manager 提供的默认角色，请选择默认角色。或者，要使用您之前创建的自定义 IAM 角色，请选择选择其他角色，然后选择要使用的角色。
7. 对于 Policy tags (策略标签)，选择要应用于生命周期策略的标签。您可以使用这些标签对策略进行标识和分类。
8. 对于创建后的策略状态，选择启用策略，以在下次计划时间启动策略运行，或者选择禁用策略，以禁止策略运行。如果您现在不启用该策略，则只有在创建后手动启用该策略后，它 AMIs 才会开始创建。
9. 在实例重启部分中，指明是否在创建 AMI 之前重启实例。为了防止目标实例重启，请选择否。选择否可能会导致数据一致性问题。要在创建 AMI 之前重启实例，请选择是。选择此选项可确保数据一致性，但可能导致多个目标实例同时重新启动。
10. 选择下一步。
11. 在 Configure schedule (配置计划) 页面配置策略计划。一个策略最多可以有四个计划。计划 1 是强制要求的计划。计划 2、3、4 是可选计划。对于您添加的每个策略计划，请执行以下操作：

    a. 在计划详细信息部分中，执行以下操作：

       i. 对于计划名称，请指定计划的描述性名称。

       ii. 在频率和相关字段中配置策略运行之间的间隔。

您可以按每日、每周、每月或每年计划配置策略运行。或者，选择自定义 cron 表达式以指定不超过一年的间隔时间。有关更多信息，请参阅 Amazon EventBridge 用户指南中的 Cron 和费率表达式。

iii. 对于开始时间，请指定策略开始运行策略的时间。第一次策略运行在计划时间之后的一小时内开始。您必须输入 hh:mm UTC 格式的时间。

iv. 对于 “保留类型”，请指定按计划 AMIs 创建的保留策略。

您可以 AMIs 根据他们的总人数或年龄来保留。

对于基于计数的保留，范围为 1 到 1000。在达到最大计数后，将在创建新 AMI 时注销最早 AMI。

对于基于存在时间的保留，范围是 1 天到 100 年。在每个 AMI 的保留期限过期后，会将其注销。

> **Note**
>
> 所有计划必须具有相同的保留类型。您只能为“计划 1”指定保留类型。计划 2、3、4 会继承计划 1 的保留类型。每个计划都可以有自己的保留计数或期限。

b. 为配置标记。 AMIs

在标记部分中，请执行以下操作：

i. 要将所有用户定义的标签从源实例复制到计划 AMIs 创建的标签，请选择从源实例复制标记。

ii. 默认情况下，由计划 AMIs 创建的会自动使用源实例的 ID 进行标记。要防止发生此自动标记，请在变量标签中，删除 instance-id:$(instance-id) 平铺。

iii. 要指定要分配给由此计划 AMIs 创建的其他标记，请选择添加标记。

c. 配置 AMI 弃用。

要在不应再使用 AMIs 时将其弃用，请在 AMI 弃用部分，选择为此计划启用 AMI 弃用，然后指定 AMI 弃用规则。AMI 弃用规则指定何 AMIs 时弃用。

如果计划使用基于计数的 AMI 保留期，则必须指定 AMIs 要弃用的最早保留的数量。弃用计数必须小于或等于计划的 AMI 保留计数，并且不能大于 1000。例如，如果将计划配置为最多保留 5 个 AMIs，则可以将计划配置为弃用最 AMIs旧的 5 个。

如果计划使用基于年龄的 AMI 保留期，则必须指定不推荐使用的期限。 AMIs 弃用计数必须小于或等于计划的 AMI 保留期限，并且不能超过 10 年（120 个月、520 周或 3650 天）。例如，如果计划配置 AMIs 为保留 10 天，则可以将计划配置为在创建 AMIs 后最多 10 天后弃用。

d. 配置跨区域复制。

要将计划 AMIs 创建的复制到不同的区域，请在跨区域复制部分中，选择启用跨区域复制。您最多可以复制 AMIs 到账户中的三个其他区域。您必须为每个目标区域指定单独的跨区域复制规则。

对于每个目标地区，您可以指定以下内容：

- AMI 副本的保留策略。保留期限过期后，将自动取消注册目标区域中的副本。
- AMI 副本的加密状态。如果源 AMI 已加密，或者默认启用了加密，则复制的 AMI 将始终 AMIs 处于加密状态。如果源 AMI 未加密，并且预设情况下禁用加密，则您可以选择启用加密。如果您未指定 KMS 密钥， AMIs 则在每个目标区域使用默认 KMS 密钥进行加密以进行 EBS 加密。如果您为目标区域指定 KMS 密钥，则选定的 IAM 角色必须具有对 KMS 密钥 的访问权限。
- AMI 副本的弃用规则。当弃用期限过期时，将自动弃用 AMI 副本。弃用期限必须小于或等于副本保留期限，并且不能超过 10 年。
- 是从源 AMI 复制所有标签还是不复制标签。

> **Note**
>
> 请勿超过每个区域的并发 AMI 副本数。

e. 要添加其他计划，请选择位于页面顶部的 Add another schedule (添加其他计划)。每个其他计划请按照本主题之前所述填写字段。

f. 添加所需计划之后，请选择查看策略。

12. 查看策略摘要，然后选择创建策略。

> **Note**
>
> 如果发生 `Role with name AWSDataLifecycleManagerDefaultRoleForAMIManagement already exists` 错误，请参阅 排查 Amazon Data Lifecycle Manager 问题 来了解更多信息。

Command line

使用create-lifecycle-policy命令创建 AMI 生命周期策略。对于 `PolicyType`，请指定 `IMAGE_MANAGEMENT`。

> **Note**
>
> 为简化语法，以下示例使用包含策略详细信息的 JSON 文件 `policyDetails.json`。

示例 1：基于存在时间的保留和 AMI 弃用

此示例创建了一个 AMI 生命周期策略，该策略在`production`不重启目标实例的情况下创建 AMIs 标签密钥为且值为的所有实例。`purpose`该策略包括一个每天可在 UTC `01:00` 创建 AMI 的计划。该政策将保留2数 AMIs 天，日复一日地将其弃用。1它还会将标签从源实例复制到 AMIs 其创建的。

```
aws dlm create-lifecycle-policy \
    --description "My AMI policy" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRoleForAMIManagement \
    --policy-details file://policyDetails.json
```

以下是 `policyDetails.json` 文件的示例。

```
{
    "PolicyType": "IMAGE_MANAGEMENT",
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key": "purpose",
```

```
        "Value": "production"
    }],
    "Schedules": [{
            "Name": "DailyAMIs",
            "TagsToAdd": [{
                "Key": "type",
                "Value": "myDailyAMI"
            }],
            "CreateRule": {
                "Interval": 24,
                "IntervalUnit": "HOURS",
                "Times": [
                    "01:00"
                ]
            },
            RetainRule":{
                "Interval" : 2,
                "IntervalUnit" : "DAYS"
            },
            DeprecateRule": {
                "Interval" : 1,
                "IntervalUnit" : "DAYS"
            },
            "CopyTags": true
        }
    ],
    "Parameters" : {
        "NoReboot":true
    }
}
```

如果请求成功，此命令将返回新创建的策略 ID。下面是示例输出。

```
{
   "PolicyId": "policy-9876543210abcdef0"
}
```

示例 2：基于计数的保留和使用跨区域复制的 AMI 弃用

此示例创建了一个 AMI 生命周期策略，该策略创建 AMIs 标签密钥为purpose且值为的所有实例，production并重新启动目标实例。该策略包括一个可在 UTC 17:30 起每 6 小时创建 AMI 的计划。该政策保留3 AMIs 并自动弃用最旧的。2 AMIs它还具有跨区域复制规则，可以复制到 AMI 副本 AMIs us-east-1、保留 2 AMI 副本并自动弃用最旧的 AMI。

```
aws dlm create-lifecycle-policy \
    --description "My AMI policy" \
    --state ENABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRoleForAMIManagement \
    --policy-details file://policyDetails.json
```

以下是 policyDetails.json 文件的示例。

```
{
    "PolicyType": "IMAGE_MANAGEMENT",
    "ResourceTypes" : [
        "INSTANCE"
    ],
    "TargetTags": [{
        "Key":"purpose",
        "Value":"production"
    }],
    "Parameters" : {
          "NoReboot": true
    },
    "Schedules" : [{
        "Name" : "Schedule1",
        "CopyTags": true,
        "CreateRule" : {
            "Interval": 6,
            "IntervalUnit": "HOURS",
            "Times" : ["17:30"]
        },
        "RetainRule":{
            "Count" : 3
        },
        "DeprecateRule":{
            "Count" : 2
        },
        "CrossRegionCopyRules": [{
            "TargetRegion": "us-east-1",
            "Encrypted": true,
            "RetainRule":{
                "IntervalUnit": "DAYS",
                "Interval": 2
            },
            "DeprecateRule":{
```

```
                "IntervalUnit": "DAYS",
                "Interval": 1
            },
            "CopyTags": true
        }]
    }]
}
```

AMI 生命周期策略的注意事项

创建 AMI 生命周期策略时应注意以下一般注意事项：

- AMI 生命周期策略仅针对与策略位于同一区域的实例。
- 第一个 AMI 创建操作将在指定开始时间之后的一小时内启动。后续 AMI 创建操作将在计划时间的一小时内开始。
- 当 Amazon Data Lifecycle Manager 注销 AMI 时，它会自动删除其支持的快照。
- 目标资源标签区分大小写。
- 如果您从策略所针对的实例中移除目标标签，Amazon Data Lifecycle Manager 将不再管理标准 AMIs 中的现有标签；如果不再需要它们，则必须手动将其删除。
- 您可以创建多个策略来备份实例。例如，如果一个实例有两个标签，其中标签 A 是策略 A 每隔 12 小时创建一个 AMI 的目标，标签 B 是策略 B 每隔 24 小时创建一个 AMI 的目标，则 Amazon Dat a Lifecycle Manager 会 AMIs 根据这两个策略的计划进行创建。或者，您可以通过创建包含多个计划的单个策略来实现相同的结果。例如，您可以创建仅针对标签 A 的单个策略，并指定两个计划，以分别用于每 12 小时和每 24 小时一次的策略。
- 在下次运行策略时，备份中将自动包含在创建策略后挂载到目标实例的新卷。策略运行时挂载到实例的所有卷都包括在内。
- 如果您创建了具有基于 cron 的自定义计划的策略，并且配置为仅创建一个 AMI，则该策略不会在达到保留阈值时自动注销该 AMI。如果不再需要该 AMI，则必须手动将其注销。
- 如果您创建基于存在时间的策略，其保留期短于创建频率，Amazon Data Lifecycle Manager 将始终保留最后一个 AMI，直到创建下一个 AMI。例如，如果基于存在时间的策略每月创建一个 AMI，保留期为七天，则 Amazon Data Lifecycle Manager 会将每个 AMI 保留一个月，即使保留期为七天。
- 对于基于计数的策略，Amazon Data Lifecycle Manager 在尝试 AMIs 根据保留政策注销最旧的 AMI 之前，始终根据创建频率进行创建。

- 成功取消注册 AMI 并删除其关联的备份快照可能需要几小时。如果 Amazon Data Lifecycle Manager 在成功注销先前创建的 AMI 之前创建了下一个 AMI AMIs ，则您可以暂时保留大于您的保留计数的数量。

终止策略针对的实例时应注意以下注意事项：

- 如果您终止了保留计划为基于计数的策略所针对的实例，则该策略将不再管理先前从 AMIs 已终止的实例中创建的实例。 AMIs 如果不再需要它们，则必须提前手动注销它们。
- 如果您终止了具有基于年龄的保留计划的策略所针对的实例，则该策略将继续取消注册 AMIs 之前按照定义的计划从已终止的实例创建的实例，直至但不包括最后一个 AMI。如果不再需要最后一个 AMI，则必须手动将其注销。

AMI 策略和 AMI 弃用应注意以下事项：

- 如果您增加具有基于计数的保留期的计划的 AMI 弃用次数，则更改将应用于该计划创建的所有 AMIs（现有和新的）。
- 如果您延长了保留期限为基于年龄的计划的 AMI 弃用期，则更改仅适用于新 AMIs 计划。现有 AMIs 不受影响。
- 如果您从计划中移除 AMI 弃用规则，Amazon Data Lifecycle Manager 将不会取消 AMIs 该计划之前已弃用的弃用规则。
- 如果您减少计划的 AMI 弃用次数或期限，Amazon Data Lifecycle Manager 将不会取消 AMIs 该计划之前已弃用的弃用次数。
- 如果您手动弃用由 AMI 策略创建的 AMI，则 Amazon Data Lifecycle Manager 将不会覆盖弃用操作。
- 如果您手动取消之前已被 AMI 策略弃用的 AMI 的弃用，则 Amazon Data Lifecycle Manager 将不会覆盖取消操作。
- 如果 AMI 由多个冲突的计划创建，并且其中一个或多个计划没有 AMI 弃用规则，则 Amazon Data Lifecycle Manager 将不会弃用该 AMI。
- 如果 AMI 由多个相互冲突的计划创建，并且其中所有计划都有 AMI 弃用规则，则 Amazon Data Lifecycle Manager 将会使用导致最新弃用日期的弃用规则。

以下注意事项适用于 AMI 策略和回收站：

- 如果 Amazon Data Lifecycle Manager 注销 AMI 并在达到策略的保留阈值时将其发送到回收站，并且您从回收站手动还原 AMI，则必须在不再需要该 AMI 时手动注销 AMI。Amazon Data Lifecycle Manager 将不再管理该 AMI。
- 如果您手动注销由策略创建的 AMI，并且该 AMI 在达到策略的保留阈值时位于回收站中，则 Amazon Data Lifecycle Manager 将不会注销该 AMI。AMIs 当它们在回收站中时，Amazon Data Lifecycle Manager 无法进行管理。

  如果在达到策略的保留阈值之前从回收站还原了 AMI，则 Amazon Data Lifecycle Manager 将在达到策略的保留阈值时注销 AMI。

  如果在达到策略的保留阈值之后从回收站还原了 AMI，则 Amazon Data Lifecycle Manager 将不再注销 AMI。如果不再需要 AMI，则必须手动将其删除。

以下注意事项适用于处于错误状态的 AMI 策略：

- 对于具有基于年龄的保留时间表的策略 AMIs ，如果设置为在策略处于该`error`状态时到期，则会无限期保留。您必须 AMIs 手动取消注册。重新启用策略后，Amazon Data Lifecycle Manager 将在保留期到期后恢复注销注册 AMIs 。
- 对于保留时间表基于计数的策略，该策略在状态下停止创建和取消注册 AMIs 。`error`当您重新启用策略时，Amazon Data Lifecycle Manager 会恢复创建 AMIs，并在达到保留阈值后恢复注销注册 AMIs 。

以下注意事项适用于 AMI 策略和禁用 AMIs：

- 如果您禁用了 Amazon Data Lifecycle Manager 创建的 AMI，并且在达到其保留阈值时该 AMI 被禁用，则 Amazon Data Lifecycle Manager 将注销该 AMI 并删除其关联的快照。
- 如果您禁用了 Amazon Data Lifecycle Manager 创建的 AMI，并手动归档了其关联的快照，并且这些快照在达到保留阈值时处于已归档状态，则 Amazon Data Lifecycle Manager 将不会删除这些快照，也不会再对其进行管理。

以下注意事项适用于 AMI 策略和 AMI 取消注册保护：

- 如果您手动为由 Amazon Data Lifecycle Manager 创建的 AMI 启用取消注册保护，并且在达到 AMI 保留阈值时该保护仍在启用，则 Amazon Data Lifecycle Manager 将不再管理该 AMI。如果不再需要 AMI，则必须手动取消注册并删除其底层快照。

其他资源

有关更多信息，请参阅使用 Amazon Data Lifecycle Manager Amazon 存储自动化 Amazon EBS 快照和 AMI 管理博客。

使用 Data Lifecycle Manager 自动化跨账户快照副本

通过自动执行跨账户快照副本，您可以将 Amazon EBS 快照复制到隔离账户中的特定区域，并使用加密密钥对这些快照进行加密。这样，您能够在账户遭到泄露时防止自己的数据丢失。

自动执行跨账户快照副本涉及两个账户：

- 源账户 – 源账户是创建快照并与目标账户共享快照的账户。在此账户中，您必须创建一个 EBS 快照策略，该策略以设定的时间间隔创建快照，然后与其他 Amazon 账户共享。
- 目标账户 – 目标账户是与之共享快照的目标账户，它也是创建共享快照副本的账户。在此账户中，您必须创建跨账户复制事件策略，以自动复制由一个或多个指定源账户共享的快照。

主题

- 创建跨账户快照复制策略
- 指定快照描述筛选条件
- 跨账户快照复制策略的注意事项
- 其他资源

创建跨账户快照复制策略

要为跨账户快照复制准备源账户和目标账户，您需要执行以下步骤：

步骤 1：创建 EBS 快照策略（源账户）

在源账户中，创建一个 EBS 快照策略，该策略将创建快照并与所需的目标账户共享。

创建策略时，请确保启用跨账户共享，并指定要与之共享快照的目标 Amazon 账户。这些是您要与之共享快照的账户。如果您要共享加密快照，则必须授予所选目标账户使用用于加密源卷的 KMS 密钥 的权限。有关更多信息，请参阅 步骤 2：共享客户托管密钥（源账户）。

> **Note**
>
> 您只能共享未加密的快照或使用 客户托管密钥 加密的快照。您无法共享使用默认 EBS 加密 KMS 密钥 加密的快照。如果您共享加密快照，则还必须与目标账户共享用于加密源卷的 KMS 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其他账户中的用户使用 KMS 密钥。

有关手动创建 EBS 快照策略的更多信息，请参阅 为 EBS 快照创建 Amazon Data Lifecycle Manager 自定义策略。

使用以下方法之一创建 EBS 快照策略。

步骤 2：共享客户托管密钥（源账户）

如果您要共享加密快照，则必须授予 IAM 角色和（您在上一步中选择的）目标 Amazon 账户使用用于加密源卷的客户托管密钥的权限。

> **Note**
>
> 仅在共享加密快照时执行此步骤。如果您正在共享的是未加密快照，请跳过此步骤。

Console

1. 在 https://console.aws.amazon.com/km Amazon KMS s 处打开控制台。
2. 要更改 Amazon Web Services 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择客户托管密钥，然后选择您需要与目标账户共享的 KMS 密钥。

   记下 KMS 密钥 ARN，稍后您将用到它。
4. 在密钥政策选项卡上，向下滚动到密钥用户部分。选择添加，输入您在上一步中选择的 IAM 角色的名称，然后选择添加。
5. 在密钥政策选项卡上，向下滚动到其他 Amazon 账户部分。选择 “添加其他 Amazon 帐户”，然后添加您在上一步中选择与之共享快照的所有目标 Amazon 帐户。
6. 选择保存更改。

Command line

使用get-key-policy命令检索当前附加到 KMS 密钥的密钥策略。

例如，以下命令检索 ID 为 9d5e2b3d-e410-4a27-a958-19e220d83a1e 的 KMS 密钥 的密钥策略，并将其写入名为 snapshotKey.json 的文件。

```
$ aws kms get-key-policy \
    --policy-name default \
    --key-id 9d5e2b3d-e410-4a27-a958-19e220d83a1e \
    --query Policy \
    --output text > snapshotKey.json
```

使用首选文本编辑器打开密钥策略。添加您在创建快照策略时指定的 IAM 角色的 ARN 以及要与 ARNs之共享 KMS 密钥的目标账户的 ARN。

例如，在以下策略中，我们添加了默认 IAM 角色的 ARN 以及目标账户 222222222222. 的根账户的 ARN

> **Tip**
>
> 为遵循最小特权原则，请不要允许对 kms:CreateGrant 拥有完全访问权限。相反，使用kms:GrantIsForAWSResource条件密钥允许用户仅在 Amazon 服务代表用户创建授权时才允许用户在 KMS 密钥上创建授权，如以下示例所示。

```
{
    "Sid" : "Allow use of the key",
    "Effect" : "Allow",
    "Principal" : {
        "AWS" : [
            "arn:aws:iam::111111111111:role/service-role/
AWSDataLifecycleManagerDefaultRole",
            "arn:aws:iam::222222222222:root"
        ]
    },
    "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
```

```
        "kms:DescribeKey"
    ],
    "Resource" : "*"
},
{
    "Sid" : "Allow attachment of persistent resources",
    "Effect" : "Allow",
    "Principal" : {
        "AWS" : [
            "arn:aws:iam::111111111111:role/service-role/
AWSDataLifecycleManagerDefaultRole",
            "arn:aws:iam::222222222222:root"
        ]
    },
    "Action" : [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
    ],
    "Resource" : "*",
    "Condition" : {
        "Bool" : {
          "kms:GrantIsForAWSResource" : "true"
        }
    }
}
```

保存并关闭文件。然后使用put-key-policy命令将更新的密钥策略附加到 KMS 密钥。

```
$ aws kms put-key-policy \
    --policy-name default \
    --key-id 9d5e2b3d-e410-4a27-a958-19e220d83a1e \
    --policy file://snapshotKey.json
```

第 3 步：创建跨账户复制事件策略（目标账户）

在目标账户中，您必须创建跨账户复制事件策略，该策略将自动复制由所需源账户共享的快照。

只有当指定的源账户之一与该账户共享快照时，此策略才会在目标账户中运行。

使用以下方法之一创建跨账户复制事件策略。

Console

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，依次选择 Elastic Block Store 和 Lifecycle Manager，然后选择创建生命周期策略。
3. 在选择策略类型屏幕上，选择跨账户复制事件策略，然后选择下一步。
4. 对于策略描述，输入策略的简短描述。
5. 对于 Policy tags (策略标签)，选择要应用于生命周期策略的标签。您可以使用这些标签对策略进行标识和分类。
6. 在事件设置部分中，定义将导致策略运行的快照共享事件。执行以下操作：

   a. 对于共享帐户，请指定要从中复制共享快照的源 Amazon 帐户。选择 “添加账户”，输入 12 位数的 Amazon 账户 ID，然后选择 “添加”。

   b. 对于按描述筛选，请使用正则表达式输入所需的快照描述。该策略仅复制由指定源账户共享且其描述与指定筛选条件匹配的快照。有关更多信息，请参阅指定快照描述筛选条件。

7. 对于 IAM 角色，请选择有权执行快照复制操作的 IAM 角色。要使用 Amazon Data Lifecycle Manager 提供的默认角色。请选择 Default role (默认角色)。或者，要使用您之前创建的自定义 IAM 角色，请选择 Choose another role (选择其他角色)，然后选择要使用的角色。

   如果您要复制加密快照，您必须授予所选 IAM 角色使用用于加密源卷的加密 KMS 密钥 的权限。同样，如果您使用不同的 KMS 密钥 对目标区域中的快照进行加密，则必须授予 IAM 角色使用目标 KMS 密钥 的权限。有关更多信息，请参阅步骤 4：允许 IAM 角色使用所需的 KMS 密钥（目标账户）。

8. 在复制操作部分中，定义激活策略时应执行的快照复制操作。该策略最多可以将快照复制到三个区域。您必须为每个目标区域指定单独的复制规则。对要添加的每个规则执行以下操作：

   a. 对于名称，为复制操作输入一个描述性名称。

   b. 对于目标区域，选择要将快照复制到的区域。

   c. 对于过期，请指定快照副本创建之后在目标区域中保留多长时间。

   d. 要加密快照副本，请在加密中选择启用加密。如果源快照已加密，或者预设情况下为您的账户启用了加密，则快照副本将始终加密，即使您在此处没有启用加密也一样。如果源快照未加密，并且默认情况下未为您的账户启用加密，则您可以选择启用或禁用加密。如果启用了加密但未指定 KMS 密钥，则快照在每个目标区域中都将使用默认加密 KMS 密钥进行加密。如果您为目标区域指定 KMS 密钥，则您必须具有对 KMS 密钥 的访问权限。

9. 要添加其他快照复制操作，请选择添加新区域。

10. 对于创建后的策略状态，选择启用策略，以在下次计划时间启动策略运行，或者选择禁用策略，以禁止策略运行。如果您现在不启用该策略，则该策略仅在创建后手动启用之后开始复制快照。
11. 选择 Create policy。

Command line

使用create-lifecycle-policy命令创建策略。要创建跨账户复制事件策略，请为 PolicyType 指定 EVENT_BASED_POLICY。

例如，以下命令可在目标账户 222222222222 中创建跨账户复制事件策略。该策略会复制由源账户 111111111111 共享的快照。该策略将快照复制到 sa-east-1 和 eu-west-2。复制到 sa-east-1 的快照未加密，它们将保留 3 天。复制到 eu-west-2 的快照使用 KMS 密钥 8af79514-350d-4c52-bac8-8985e84171c7 进行加密，它们将保留 1 个月。该策略使用默认 IAM 角色。

```
$ aws dlm create-lifecycle-policy \
    --description "Copy policy" \
    --state ENABLED \
    --execution-role-arn arn:aws:iam::222222222222:role/service-role/
AWSDataLifecycleManagerDefaultRole \
    --policy-details file://policyDetails.json
```

下面显示的是 policyDetails.json 文件的内容。

```
{
    "PolicyType" : "EVENT_BASED_POLICY",
    "EventSource" : {
        "Type" : "MANAGED_CWE",
        "Parameters": {
            "EventType" : "shareSnapshot",
            "SnapshotOwner": ["111111111111"]
        }
    },
    "Actions" : [{
        "Name" :"Copy Snapshot to Sao Paulo and London",
        "CrossRegionCopy" : [{
            "Target" : "sa-east-1",
             "EncryptionConfiguration" : {
                 "Encrypted" : false
             },
```

```
             "RetainRule" : {
             "Interval" : 3,
            "IntervalUnit" : "DAYS"
            }
        },
        {
            "Target" : "eu-west-2",
            "EncryptionConfiguration" : {
                 "Encrypted" : true,
                 "CmkArn" : "arn:aws:kms:eu-
west-2:222222222222:key/8af79514-350d-4c52-bac8-8985e84171c7"
            },
            "RetainRule" : {
                "Interval" : 1,
                "IntervalUnit" : "MONTHS"
            }
        }]
    }]
}
```

如果请求成功，此命令将返回新创建的策略 ID。下面是示例输出。

```
{
    "PolicyId": "policy-9876543210abcdef0"
}
```

步骤 4：允许 IAM 角色使用所需的 KMS 密钥（目标账户）

如果您要复制加密快照，则必须授予（您在上一步中选择的）IAM 角色使用用于加密源卷的 客户托管密钥 的权限。

> **Note**
>
> 仅在复制加密快照时执行此步骤。如果您要复制的是未加密快照，请跳过此步骤。

使用以下方法之一将所需策略添加到 IAM 角色。

Console

1. 使用 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。

2. 在导航窗格中，选择角色。搜索并选择您在上一步中创建跨账户复制事件策略时选择的 IAM 角色。如果您选择使用默认角色，则该角色的名称为AWSDataLifecycleManagerDefaultRole。
3. 选择添加内联策略，然后选择 JSON 选项卡。
4. 将现有策略替换为以下内容，然后指定用于加密源卷且源账户在步骤 2 中与您共享的 KMS 密钥的 ARN。

> **Note**
>
> 如果要从多个源账户复制，则必须从每个源账户中指定相应的 KMS 密钥 ARN。

在下面的示例中，策略授予该 IAM 角色所需的权限，以使用由源账户 111111111111 共享的 KMS 密钥 1234abcd-12ab-34cd-56ef-1234567890ab 和目标账户 222222222222 中存在的 KMS 密钥 4567dcba-23ab-34cd-56ef-0987654321yz。

> **Tip**
>
> 为遵循最小特权原则，请不要允许对 kms:CreateGrant 拥有完全访问权限。相反，使用kms:GrantIsForAWSResource条件密钥允许用户仅在 Amazon 服务代表用户创建授权时才允许用户在 KMS 密钥上创建授权，如以下示例所示。

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Effect": "Allow",
           "Action": [
               "kms:RevokeGrant",
               "kms:CreateGrant",
               "kms:ListGrants"
           ],
           "Resource": [
               "arn:aws:kms:us-
east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
               "arn:aws:kms:us-
east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
           ],
           "Condition": {
```

```
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-
east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
                "arn:aws:kms:us-
east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
            ]
        }
    ]
}
```

5. 选择查看策略
6. 对于名称，为策略输入描述性名称，然后选择创建策略。

Command line

使用首选文本编辑器，创建一个名为 `policyDetails.json` 的新 JSON 文件。添加以下策略并指定用于加密源卷且源账户在步骤 2 中与您共享的 KMS 密钥的 ARN。

> **Note**
>
> 如果要从多个源账户复制，则必须从每个源账户中指定相应的 KMS 密钥 ARN。

在下面的示例中，策略授予该 IAM 角色所需的权限，以使用由源账户 111111111111 共享的 KMS 密钥 1234abcd-12ab-34cd-56ef-1234567890ab 和目标账户 222222222222 中存在的 KMS 密钥 4567dcba-23ab-34cd-56ef-0987654321yz。

> **Tip**
>
> 为遵循最小特权原则，请不要允许对 kms:CreateGrant 拥有完全访问权限。相反，使用kms:GrantIsForAWSResource条件密钥允许用户仅在 Amazon 服务代表用户创建授权时才允许用户在 KMS 密钥上创建授权，如以下示例所示。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:RevokeGrant",
                "kms:CreateGrant",
                "kms:ListGrants"
            ],
            "Resource": [
                "arn:aws:kms:us-
east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
                "arn:aws:kms:us-
east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-
east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
```

```
                "arn:aws:kms:us-
east-1:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
            ]
        }
    ]
}
```

保存并关闭文件。然后使用put-role-policy命令将策略添加到 IAM 角色。

例如

```
$ aws iam put-role-policy \
    --role-name AWSDataLifecycleManagerDefaultRole \
    --policy-name CopyPolicy \
    --policy-document file://AdminPolicy.json
```

指定快照描述筛选条件

在目标账户中创建快照复制策略时，必须指定快照描述筛选条件。通过快照描述筛选条件，您可指定额外的筛选级别，从而控制策略应复制哪些快照。这意味着只有当快照由指定源账户之一共享，并且其快照描述与指定筛选条件匹配时，策略才会复制该快照。换句话说，如果快照由指定源账户之一共享，但其描述不符合指定的筛选条件，则策略不会复制该快照。

必须使用正则表达式指定快照描述筛选条件。使用控制台和命令行创建跨账户复制事件策略时，它是必填字段。下面是可以使用的示例正则表达式：

- `.*` – 此筛选条件匹配所有快照描述。如果使用此表达式，该策略将复制由指定源账户之一共享的所有快照。
- `Created for policy: policy-0123456789abcdef0.*` – 此筛选条件仅匹配由 ID 为 的策略创建的快照。`policy-0123456789abcdef0`如果您使用类似这样的表达式，则该策略仅复制由指定源账户之一与您的账户共享以及由具有指定 ID 的策略创建的快照。
- `.*production.*` – 此筛选条件匹配描述中任意位置包含词语 `production` 的任何快照。如果使用此表达式，该策略将复制由指定源账户之一共享且描述中包含指定文本的所有快照。

跨账户快照复制策略的注意事项

跨账户复制事件策略时需考虑以下事项：

- 您只能复制未加密的快照或使用 客户托管密钥 加密的快照。
- 您可以创建跨账户复制事件策略，用于复制在 Amazon Data Lifecycle Manager 外部共享的快照。
- 如果要加密目标账户中的快照，则为跨账户复制事件策略选择的 IAM 角色必须拥有使用所需 KMS 密钥 的权限。

其他资源

有关更多信息，请参阅跨 Amazon 账户 Amazon 存储自动复制加密的 Amazon EBS 快照博客。

修改 Amazon Data Lifecycle Manager 策略

修改 Amazon Data Lifecycle Manager 策略时请牢记以下事项：

- 如果您通过删除其目标标签来修改了 AMI 或快照策略，则具有这些标签的卷或实例将不再受此策略管理。
- 如果修改计划名称，则该策略将不再管理以旧计划名称 AMIs 创建的快照或使用旧计划名称创建的快照。
- 如果您修改基于年龄的保留计划以使用新的时间间隔，则新的时间间隔仅用于新快照或更改后 AMIs 创建的快照。新的计划不会影响快照的保留计划，也不会影响变更之前 AMIs 创建的快照的保留计划。
- 创建后，您无法将策略的保留计划从基于计数更改为基于存在时间。要进行该更改，您必须创建新的策略。
- 如果您禁用了具有基于年龄的保留时间表的策略，则该快照或在禁用 AMIs 该策略时设置为过期的快照将无限期保留。您必须 AMIs 手动删除快照或取消注册。当您重新启用策略时，Amazon Data Lifecycle Manager 会在快照的保留期到期后恢复删除快照或注销注册 AMIs 。
- 如果您使用基于计数的保留时间表禁用策略，则该策略将停止创建和删除快照或 AMIs。当您重新启用该策略时，Amazon Data Lifecycle Manager 会恢复创建快照 AMIs，并恢复删除快照，或者 AMIs 在达到保留阈值时恢复删除快照。
- 如果您禁用了某个具有已启用快照存档策略的策略，则禁用该策略时处于存档层中的快照将不再由 Amazon Data Lifecycle Manager 管理。您必须手动删除不再需要的快照。
- 如果您按某个基于计数的计划启用了快照存档，则存档规则适用于由该计划创建和存档的所有新快照，也适用于之前由该计划创建和存档的现有快照。
- 如果您按某个基于期限的计划启用了快照存档，则存档规则仅适用于启用快照存档后创建的新快照。对于在启用快照存档之前创建的现有快照，将继续根据最初创建和存档快照时设定的计划，从各自的存储层中删除。

- 如果您为某个基于计数的计划禁用了快照存档，则该计划会立即停止存档快照。之前由该计划存档的快照仍保留在存档层中，Amazon Data Lifecycle Manager 不会将其删除。
- 如果您为某个基于期限的计划禁用了快照存档，则由该策略创建并计划存档的快照将在 `aws:dlm:expirationTime` 系统标签注明发原定存档日期和时间永久删除。
- 如果您为某个计划禁用了快照存档，则该计划会立即停止存档快照。之前由该计划存档的快照仍保留在存档层中，Amazon Data Lifecycle Manager 不会将其删除。
- 如果您为基于计数的计划修改了存档保留计数，则新的保留计数将包括之前由该计划存档的现有快照。
- 如果您为基于期限的计划修改了存档保留期，则新的保留期仅适用于修改保留规则后存档的快照。

使用以下程序之一修改生命周期策略。

Console

修改生命周期策略

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，依次选择 Elastic Block Store 和生命周期管理器。
3. 从列表中选择生命周期策略。
4. 选择操作，然后选择修改生命周期策略。
5. 根据需要，修改策略设置。例如，您可以修改计划，添加或删除标签，或者启用或禁用策略。
6. 选择修改策略。

Command line

使用update-lifecycle-policy命令修改生命周期策略中的信息。为简化语法，此示例引用了包含策略详细信息的 JSON 文件 `policyDetailsUpdated.json`。

```
aws dlm update-lifecycle-policy \
    --state DISABLED \
    --execution-role-arn
 arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole" \
    --policy-details file://policyDetailsUpdated.json
```

以下是 `policyDetailsUpdated.json` 文件的示例。

```
{
```

```
    "ResourceTypes":[
       "VOLUME"
    ],
    "TargetTags":[
       {
          "Key": "costcenter",
          "Value": "120"
       }
    ],
    "Schedules":[
       {
          "Name": "DailySnapshots",
          "TagsToAdd": [
             {
                "Key": "type",
                "Value": "myDailySnapshot"
             }
          ],
          "CreateRule": {
             "Interval": 12,
             "IntervalUnit": "HOURS",
             "Times": [
                "15:00"
             ]
          },
          "RetainRule": {
             "Count" :5
          },
          "CopyTags": false
       }
    ]
}
```

要查看更新后的策略，请使用 `get-lifecycle-policy` 命令。您可以看到更改了状态、标签的值、快照时间间隔和快照开始时间。

删除 Amazon Data Lifecycle Manager 策略

在删除 Amazon Data Lifecycle Manager 策略时请牢记以下事项：

- 如果删除策略，则不会自动删除该策略 AMIs 创建的快照或快照。如果您不再需要快照或 AMIs，则必须手动将其删除。

- 如果您删除了某个具有已启用快照存档策略的策略，则删除该策略时处于存档层中的快照将不再由 Amazon Data Lifecycle Manager 管理。您必须手动删除不再需要的快照。
- 如果您删除了某个策略，并且该策略具有已启用存档并且基于期限的计划，则由该策略创建并计划存档的快照将在 `aws:dlm:expiretime` 系统标签注明发原定存档日期和时间永久删除。

使用以下程序之一删除生命周期策略。

Console

删除生命周期策略

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，依次选择 Elastic Block Store 和生命周期管理器。
3. 从列表中选择生命周期策略。
4. 选择操作，然后选择删除生命周期策略。
5. 在提示确认时，选择删除策略。

Command line

使用delete-lifecycle-policy命令删除生命周期策略并释放策略中指定的目标标签以供重复使用。

> **Note**
> 您可以仅删除由 Amazon Data Lifecycle Manager 创建的快照。

```
aws dlm delete-lifecycle-policy --policy-id policy-0123456789abcdef0
```

Amazon Data Lifecycle Manager API 参考提供了 Amazon Data Lifecycle Manager 查询 API 的各种操作和数据类型的描述和语法。

或者，您可以使用其中一个 Amazon SDKs 以针对您正在使用的编程语言或平台量身定制的方式访问 API。有关更多信息，请参阅 Amazon SDKs。

使用 IAM 控制对 Amazon Data Lifecycle Manager 的访问

Amazon Data Lifecycle Manager 的访问需要凭据。这些证书必须具有访问 Amazon 资源（例如实例、卷、快照和）的权限 AMIs。

使用 Amazon Data Lifecycle Manager 需要以下 IAM 权限。

> **Note**
>
> - 仅控制台用户需要 `ec2:DescribeAvailabilityZones`、`ec2:DescribeRegions`、`kms:ListAliases` 和 `kms:DescribeKey` 权限。如果不需要访问控制台，则可以删除权限。
> - AWSDataLifecycleManagerDefaultRole角色的 ARN 格式会有所不同，具体取决于它是使用控制台还是使用控制台创建的。 Amazon CLI如果使用控制台创建角色，则 ARN 格式为 `arn:aws:iam::account_id:role/service-role/AWSDataLifecycleManagerDefaultRole`。如果角色是使用创建的 Amazon CLI，则 ARN 格式为。`arn:aws:iam::account_id:role/AWSDataLifecycleManagerDefaultRole`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "dlm:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": [
                "arn:aws:iam::accound_id:role/AWSDataLifecycleManagerDefaultRole",
                "arn:aws:iam::accound_id:role/
AWSDataLifecycleManagerDefaultRoleForAMIManagement",
       "arn:aws:iam::accound_id:role/service-role/AWSDataLifecycleManagerDefaultRole",
                "arn:aws:iam::accound_id:role/service-role/
AWSDataLifecycleManagerDefaultRoleForAMIManagement"
                ]
```

```
        },
        {
            "Effect": "Allow",
            "Action": "iam:ListRoles",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeRegions",
                "kms:ListAliases",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        }
    ]
}
```

加密权限

使用 Amazon Data Lifecycle Manager 和加密资源时，请考虑以下情况。

- 如果源卷已加密，请确保 Amazon Data Lifecycle Manager 的默认角色（AWSDataLifecycleManagerDefaultRole和AWSDataLifecycleManagerDefaultRoleForAMIManagement）有权使用用于加密卷的 KMS 密钥。
- 如果您为未加密的快照启用跨区域复制或由未加密快照 AMIs 支持的跨区域复制，并选择在目标区域启用加密，请确保默认角色有权使用在目标区域执行加密所需的 KMS 密钥。
- 如果您为加密快照启用跨区域复制或由加密快照 AMIs 支持，请确保默认角色有权同时使用源和目标 KMS 密钥。
- 如果您为加密快照启用快照存档，请确保 Amazon Data Lifecycle Manager 的默认角色（AWSDataLifecycleManagerDefaultRole有权使用用于加密快照的 KMS 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其他账户中的用户使用 KMS 密钥。

有关更多信息，请参阅《IAM 用户指南》中的更改用户权限。

Amazon Amazon Data Lifecycle Manager 的托管策略

Amazon 托管策略是由创建和管理的独立策略 Amazon。 Amazon 托管策略旨在为许多常见用例提供权限。 Amazon 与必须自己编写策略相比，托管策略可以更有效地为用户、组和角色分配适当的权限。

但是，您无法更改 Amazon 托管策略中定义的权限。 Amazon 偶尔会更新 Amazon 托管策略中定义的权限。当发生此情况时，更新会影响策略附加到的所有委托人实体（用户、组和角色）。

Amazon Data Lifecycle Manager 为常见用例提供 Amazon 托管策略。通过这些策略可以更高效地定义适当的权限，并控制对资源的访问。Amazon Data Lifecycle Manager 提供的 Amazon 托管策略旨在附加到您传递给亚马逊数据生命周期管理器的角色。

主题

- AWSDataLifecycleManagerServiceRole
- AWSDataLifecycleManagerServiceRoleForAMIManagement
- AWSDataLifecycleManagerSSMFull访问权限
- Amazon 托管策略更新

AWSDataLifecycleManagerServiceRole

该AWSDataLifecycleManagerServiceRole政策为 Amazon Data Lifecycle Manager 提供了创建和管理亚马逊 EBS 快照策略和跨账户复制事件策略的相应权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots",
                "ec2:DeleteSnapshot",
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots",
                "ec2:EnableFastSnapshotRestores",
                "ec2:DescribeFastSnapshotRestores",
                "ec2:DisableFastSnapshotRestores",
                "ec2:CopySnapshot",
```

```
                "ec2:ModifySnapshotAttribute",
                "ec2:DescribeSnapshotAttribute",
                "ec2:ModifySnapshotTier",
                "ec2:DescribeSnapshotTierStatus",
                "ec2:DescribeAvailabilityZones"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "events:PutRule",
                "events:DeleteRule",
                "events:DescribeRule",
                "events:EnableRule",
                "events:DisableRule",
                "events:ListTargetsByRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/AwsDataLifecycleRule.managed-cwe.*"
        }
    ]
}
```

AWSDataLifecycleManagerServiceRoleForAMIManagement

该AWSDataLifecycleManagerServiceRoleForAMIManagement政策为亚马逊 Data Lifecycle Manager 提供了创建和管理由亚马逊 EBS 支持的 AMI 策略的相应权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
```

```
            "Resource": [
                "arn:aws:ec2:*::snapshot/*",
                "arn:aws:ec2:*::image/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeImageAttribute",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteSnapshot",
            "Resource": "arn:aws:ec2:*::snapshot/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ResetImageAttribute",
                "ec2:DeregisterImage",
                "ec2:CreateImage",
                "ec2:CopyImage",
                "ec2:ModifyImageAttribute"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:EnableImageDeprecation",
                "ec2:DisableImageDeprecation"
            ],
            "Resource": "arn:aws:ec2:*::image/*"
        }
    ]
}
```

AWSDataLifecycleManagerSSMFull访问权限

提供 Amazon Data Lifecycle Manager 权限，允许其执行在所有亚马逊 EC2 实例上运行预脚本和后置脚本所需的系统管理器操作。

> **Important**
>
> 使用前置和后置脚本时，该策略使用 `aws:ResourceTag` 条件键来限制对特定 SSM 文档的访问权限。要允许 Amazon Data Lifecycle Manager 访问 SSM 文档，您必须确保您的 SSM 文档带有 `DLMScriptsAccess:true` 标签。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSSMReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "ssm:GetCommandInvocation",
                "ssm:ListCommands",
                "ssm:DescribeInstanceInformation"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowTaggedSSMDocumentsOnly",
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
                "ssm:DescribeDocument",
                "ssm:GetDocument"
            ],
            "Resource": [
                "arn:aws:ssm:*:*:document/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/DLMScriptsAccess": "true"
                }
            }
        },
```

```
        {
            "Sid": "AllowSpecificAWSOwnedSSMDocuments",
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
                "ssm:DescribeDocument",
                "ssm:GetDocument"
            ],
            "Resource": [
                "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
                "arn:aws:ssm:*:*:document/AWSSystemsManagerSAP-
CreateDLMSnapshotForSAPHANA"
            ]
        },
        {
            "Sid": "AllowAllEC2Instances",
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ]
        }
    ]
}
```

Amazon 托管策略更新

Amazon 服务维护和更新 Amazon 托管策略。您无法更改 Amazon 托管策略中的权限。服务偶尔会向 Amazon 托管策略添加其他权限以支持新功能。此类更新会影响附加策略的所有身份（用户、组和角色）。当推出新功能或有新操作可用时，服务最有可能更新 Amazon 托管策略。服务不会从 Amazon 托管策略中移除权限，因此策略更新不会破坏您的现有权限。

下表详细介绍了 Amazon Data Lifecycle Manager Amazon 托管策略自该服务开始跟踪这些更改以来该服务所做的更新。要获得有关此页面更改的自动提示，请订阅 《Amazon EBS 用户指南》的文档历史记录 上的 RSS 源。

更改	描述	日期
AWSDataLifecycleMa	Amazon Data Lifec	2024 年 12 月 16 日

更改	描述	日期
nagerServiceRole— 更新了策略权限。	ec2:DescribeAvailabilityZones ycle Manager 添加了授予快照策略获取有关本地区域信息的权限的操作。	
AWSDataLifecycleManagerSSMFull访问权限-更新了策略权限。	使用 AWSSystemsManagerSAP-CreateDLMSnapshotForSAPHANA SSM 文档更新了政策，以支持 SAP HANA 的应用程序一致性快照。	2023 年 11 月 17 日
AWSDataLifecycleManagerSSMFull访问权限-添加了新的 Amazon 托管策略。	Amazon Data Lifecycle Manager 添加了 AWSDataLifecycleManagerSSMFull访问 Amazon 托管策略。	2023 年 11 月 7 日

更改	描述	日期
AWSDataLifecycleManagerServiceRole— 增加了支持快照存档的权限。	Amazon Data Lifecycle Manager 添加了 `ec2:ModifySnapshotTier` 和 `ec2:DescribeSnapshotTierStatus` 操作，以授予快照策略存档快照和检查快照存档状态的权限。	2022 年 9 月 30 日
AWSDataLifecycleManagerServiceRoleForAMIManagement— 增加了支持 AMI 弃用的权限。	Amazon Data Lifecycle Manager 添加了 `ec2:EnableImageDeprecation` 和 `ec2:DisableImageDeprecation` 操作以授予 EBS 支持的 AMI 策略权限，从而启用和禁用 AMI 弃用。	2021 年 8 月 23 日
Amazon Data Lifecycle Manager 已开启跟踪更改	Amazon Data Lifecycle Manager 开始跟踪其 Amazon 托管策略的变更。	2021 年 8 月 23 日

Amazon Data Lifecycle Manager 的 IAM 服务角色

Amazon Identity and Access Management (IAM) 角色与用户类似，因为它是一个具有权限策略的 Amazon 身份，该策略决定了该身份可以做什么和不能做什么 Amazon。但是，角色旨在让需要它的任何人代入，而不是唯一地与某个人员关联。服务角色是 Amazon 服务代替您执行操作的角色。作为代表您执行备份操作的服务，Amazon Data Lifecycle Manager 要求您在该服务代表您执行策略操作时将其传递给要代入的角色。有关 IAM 角色的更多信息，请参阅《IAM 用户指南》中的 IAM 角色。

您传递给 Amazon Data Lifecycle Manager 的角色必须具有 IAM 策略，该策略的权限使亚马逊数据生命周期管理器能够执行与策略操作相关的操作，例如创建快照和 AMIs、复制快照和 AMIs删除快照以及注销注册 AMIs。每种 Amazon Data Lifecycle Manager 策略类型需要不同的权限。该角色还必须将 Amazon Data Lifecycle Manager 列为可信实体，这使得 Amazon Data Lifecycle Manager 能够代入该角色。

主题

- Amazon Data Lifecycle Manager 的原定设置服务角色
- Amazon Data Lifecycle Manager 的自定义服务角色

Amazon Data Lifecycle Manager 的原定设置服务角色

Amazon Data Lifecycle Manager 使用以下原定设置的服务角色：

- AWSDataLifecycleManagerDefaultRole—管理快照的默认角色。它只信任 `dlm.amazonaws.com` 服务代入该角色，并允许 Amazon Data Lifecycle Manager 代表您执行快照和跨账户快照复制策略所需的操作。此角色使用 `AWSDataLifecycleManagerServiceRole` Amazon 托管策略。

  > **Note**
  >
  > 角色的 ARN 格式会有所不同，具体取决于使用控制台还是 Amazon CLI创建角色。如果使用控制台创建角色，则 ARN 格式为 `arn:aws:iam::account_id:role/service-role/AWSDataLifecycleManagerDefaultRole`。如果角色是使用创建的 Amazon CLI，则 ARN 格式为。`arn:aws:iam::account_id:role/AWSDataLifecycleManagerDefaultRole`

- AWSDataLifecycleManagerDefaultRoleForAMIManagement—用于管理 AMIs的默认角色。它只信任 `dlm.amazonaws.com` 服务代入该角色，并允许 Amazon Data Lifecycle Manager 代表您执行由 EBS 支持的 AMI 策略所需的操作。此角色使用`AWSDataLifecycleManagerServiceRoleForAMIManagement` Amazon 托管策略。

如果您使用的是 Amazon Data Lifecycle Manager 控制台，则在您首次创建快照或跨账户快照复制策略时，Amazon Data Lifecycle Manager 会自动创建AWSDataLifecycleManagerDefaultRoleForAMIManagement服务角色，并在您首次创建由 EBS 支持的 AMI 策略时自动创建服务角色。AWSDataLifecycleManagerDefaultRole

如果您不使用控制台，则可以使用create-default-role命令手动创建服务角色。对于`--resource-type`，请`snapshot`指定 “创建 AWSDataLifecycleManagerDefaultRole” 或 `image` “创建” AWSDataLifecycleManagerDefaultRoleFor AMIManagement。

```
$ aws dlm create-default-role --resource-type snapshot|image
```

如果您删除了原定设置服务角色，然后需要再次创建，则可以使用相同的流程在您的账户中重新创建它们。

Amazon Data Lifecycle Manager 的自定义服务角色

作为使用原定设置服务角色的替代方案，您可以在创建生命周期策略时创建具有所需权限的自定义 IAM 角色，然后选择它们。

创建自定义 IAM 角色

1. 创建具有以下权限的角色。

   - 管理快照生命周期策略所需的权限

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshot",
                "ec2:CreateSnapshots",
                "ec2:DeleteSnapshot",
                "ec2:DescribeInstances",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots",
                "ec2:EnableFastSnapshotRestores",
                "ec2:DescribeFastSnapshotRestores",
                "ec2:DisableFastSnapshotRestores",
                "ec2:CopySnapshot",
                "ec2:ModifySnapshotAttribute",
```

```
                "ec2:DescribeSnapshotAttribute",
                "ec2:ModifySnapshotTier",
                "ec2:DescribeSnapshotTierStatus",
                "ec2:DescribeAvailabilityZones"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "events:PutRule",
                "events:DeleteRule",
                "events:DescribeRule",
                "events:EnableRule",
                "events:DisableRule",
                "events:ListTargetsByRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/AwsDataLifecycleRule.managed-
cwe.*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetCommandInvocation",
                "ssm:ListCommands",
                "ssm:DescribeInstanceInformation"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
                "ssm:DescribeDocument",
                "ssm:GetDocument"
```

```
            ],
            "Resource": [
                "arn:aws:ssm:*:*:document/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/DLMScriptsAccess": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
                "ssm:DescribeDocument",
                "ssm:GetDocument"
            ],
            "Resource": [
                "arn:aws:ssm:*::document/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Condition": {
                "StringNotLike": {
                    "aws:ResourceTag/DLMScriptsAccess": "false"
                }
            }
        }
    ]
}
```

- 管理 AMI 生命周期策略所需的权限

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
                "arn:aws:ec2:*::snapshot/*",
                "arn:aws:ec2:*::image/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeImageAttribute",
                "ec2:DescribeVolumes",
                "ec2:DescribeSnapshots"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteSnapshot",
            "Resource": "arn:aws:ec2:*::snapshot/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ResetImageAttribute",
                "ec2:DeregisterImage",
                "ec2:CreateImage",
                "ec2:CopyImage",
                "ec2:ModifyImageAttribute"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:EnableImageDeprecation",
                "ec2:DisableImageDeprecation"
            ],
            "Resource": "arn:aws:ec2:*::image/*"
        }
    ]
```

```
}
```

有关更多信息，请参阅IAM 用户指南中的创建角色。

2. 向角色添加信任关系。

   a. 在 IAM 控制台中，选择角色。

   b. 选择您创建的角色，然后选择信任关系。

   c. 选择编辑信任关系，添加以下策略，然后选择更新信任策略。

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Effect": "Allow",
  "Principal": {
   "Service": "dlm.amazonaws.com"
  },
  "Action": "sts:AssumeRole"
 }]
}
```

建议您使用 aws:SourceAccount 和 aws:SourceArn 条件键来防止出现混淆代理人问题。例如，您可以将以下条件块添加到以前的信任策略。aws:SourceAccount 是生命周期策略的所有者，aws:SourceArn 是生命周期策略的 ARN。如果您不知道生命周期策略的 ID，可以用通配符（*）替换 ARN 的该部分，然后在创建生命周期策略后更新信任策略。

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account_id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:partition:dlm:region:account_id:policy/policy_id"
    }
}
```

监控 Amazon Data Lifecycle Manager 策略

您可以使用以下功能来监控快照的生命周期，以及 AMIs。

特征

- 控制台和 Amazon CLI
- Amazon CloudTrail
- 使用监控数据生命周期管理器策略 EventBridge
- 使用监控数据生命周期管理器策略 CloudWatch

控制台和 Amazon CLI

您可以使用 Amazon EC2 控制台或查看您的生命周期策略 Amazon CLI。策略创建的每个快照和 AMI 均具有时间戳以及与策略相关的标签。您可以筛选快照并 AMIs 使用这些标签来验证备份是否按预期创建。

Amazon CloudTrail

借 Amazon CloudTrail助，您可以跟踪用户活动和 API 使用情况，以证明其符合内部政策和监管标准。有关更多信息，请参阅 Amazon CloudTrail 《用户指南》。

使用监控数据生命周期管理器策略 EventBridge

Amazon EBS 和 Amazon Data Lifecycle Manager 发出与生命周期策略操作相关的事件。您可以使用 Amazon Lambda 和 Amazon CloudWatch Events 以编程方式处理事件通知。尽最大努力发出事件。有关更多信息，请参阅 Amazon EventBridge 用户指南。

提供的事件如下：

> **Note**
>
> AMI 生命周期策略操作不会触发任何事件。

- `createSnapshot` – 当 `CreateSnapshot` 操作成功或失败时发出的 Amazon EBS 事件。有关更多信息，请参阅 亚马逊 EBS 的亚马逊 EventBridge 活动。
- `DLM Policy State Change` – 当生命周期策略进入错误状态时发出的 Amazon Data Lifecycle Manager 事件。此事件包含有关导致错误的问题的描述。

  下面是在 IAM 角色授予的权限不足时发出的事件的示例。

```
{
    "version": "0",
    "id": "01234567-0123-0123-0123-0123456789ab",
    "detail-type": "DLM Policy State Change",
    source": "aws.dlm",
    "account": "123456789012",
    "time": "2018-05-25T13:12:22Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:dlm:us-east-1:123456789012:policy/policy-0123456789abcdef"
    ],
    "detail": {
        "state": "ERROR",
        "cause": "Role provided does not have sufficient permissions",
        "policy_id": "arn:aws:dlm:us-east-1:123456789012:policy/
policy-0123456789abcdef"
    }
}
```

下面是在超过限制时发出的事件的示例。

```
{
    "version": "0",
    "id": "01234567-0123-0123-0123-0123456789ab",
    "detail-type": "DLM Policy State Change",
    "source": "aws.dlm",
    "account": "123456789012",
    "time": "2018-05-25T13:12:22Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:dlm:us-east-1:123456789012:policy/policy-0123456789abcdef"
    ],
    "detail":{
        "state": "ERROR",
        "cause": "Maximum allowed active snapshot limit exceeded",
        "policy_id": "arn:aws:dlm:us-east-1:123456789012:policy/
policy-0123456789abcdef"
    }
}
```

- `DLM Pre Post Script Notification` – 前置或后置脚本启动、成功或失败时发出的事件。

以下是 VSS 备份成功时的示例事件。

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "DLM Pre Post Script Notification",
    "source": "aws.dlm",
    "account": "123456789012",
    "time": "2023-10-27T22:04:52Z",
    "region": "us-east-1",
    "resources": ["arn:aws:dlm:us-east-1:123456789012:policy/
policy-01234567890abcdef"],
    "detail": {
        "script_stage": "",
        "result": "success",
        "cause": "",
        "policy_id": "arn:aws:dlm:us-east-1:123456789012:policy/
policy-01234567890abcdef",
        "execution_handler": "AWS_VSS_BACKUP",
        "source": "arn:aws:ec2:us-east-1:123456789012:instance/i-01234567890abcdef",
        "resource_type": "EBS_SNAPSHOT",
        "resources": [{
            "status": "pending",
            "resource_id": "arn:aws:ec2:us-east-1::snapshot/snap-01234567890abcdef",
            "source": "arn:aws:ec2:us-east-1:123456789012:volume/
vol-01234567890abcdef"
        }],
        "request_id": "a1b2c3d4-a1b2-a1b2-a1b2-a1b2c3d4e5f6",
        "start_time": "2023-10-27T22:03:29.370Z",
        "end_time": "2023-10-27T22:04:51.370Z",
        "timeout_time": ""
    }
}
```

使用监控数据生命周期管理器策略 CloudWatch

您可以使用监控您的 Amazon Data Lifecycle Manager 生命周期策略 CloudWatch，该策略收集原始数据并将其处理为可读的近乎实时的指标。您可以使用这些指标来准确查看您的策略在一段时间内创建、删除和复制了多少 Amazon EBS 快照和 EBS 支持的 AMIs 快照。还可以设置特定阈值监视警报，在达到对应阈值时发送通知或采取行动。

指标的保留期限为 15 个月，以便您可以访问历史信息，并更好地了解生命周期策略在较长时间内的表现。

有关亚马逊的更多信息 CloudWatch，请参阅亚马逊 CloudWatch 用户指南。

主题

- 受支持的指标
- 查看您的政策 CloudWatch 指标
- 绘制策略的指标图表
- 为策略创建 CloudWatch 警报
- 使用案例示例
- 管理报告失败操作的策略

受支持的指标

AWS/EBS命名空间中包含以下 Amazon Data Lifecycle Manager 指标。这些指标因策略类型而异。

所有指标都可以在 DLMPolicyId 维度上衡量。最有用的统计工具为 sum 和 average，并且度量单位为 count。

选择选项卡以查看该策略类型支持的指标。

EBS snapshot policies

指标	描述
Resources Targeted	在快照或 EBS 支持的 AMI 策略中所指定标签针对的资源数量。
Snapshots CreateStarted	快照策略启动的快照创建操作数。即使有多次后续重试，每个操作也只记录一次。 如果快照创建操作失败，Amazon Data Lifecycle Manager 会发送 SnapshotsCreateFailed 指标。
Snapshots CreateCompleted	快照策略创建的快照数量。这包括在计划时间后 60 分钟内的成功重试。

指标	描述
SnapshotsCreateFailed	不能由快照策略创建的快照数量。这包括在计划时间后 60 分钟内的不成功重试。
SnapshotsSharedCompleted	快照策略跨账户共享的快照数量。
SnapshotsDeleteCompleted	快照或 EBS 支持的 AMI 策略删除的快照数量。此指标仅适用于策略创建的快照。它不适用于策略创建的跨区域快照副本。 该指标包括在 EBS 支持的 AMI 策略注销注册时删除的快照。AMIs
SnapshotsDeleteFailed	不能由快照或 EBS 支持的 AMI 策略删除的快照数量。此指标仅适用于策略创建的快照。它不适用于策略创建的跨区域快照副本。 该指标包括在 EBS 支持的 AMI 策略注销注册时删除的快照。 AMIs
SnapshotsCopiedRegionStarted	快照策略启动的跨区域快照复制操作数。
SnapshotsCopiedRegionCompleted	快照策略创建的跨区域快照副本数量。这包括在计划时间的 24 小时内的成功重试。
SnapshotsCopiedRegionFailed	不能由快照策略创建的跨区域快照副本的数量。这包括在计划时间后 24 小时内的不成功重试。
SnapshotsCopiedRegionDeleteCompleted	快照策略删除的跨区域快照副本的数量，由保留规则指定。

指标	描述
SnapshotsCopiedRegionDeleteFailed	不能由快照策略删除的跨区域快照副本的数量，由保留规则指定。
snapshotsArchiveDeletionFailed	不能由快照策略从存档层中删除的存档快照数量。
snapshotsArchiveScheduled	计划由快照策略存档的快照数量。
snapshotsArchiveCompleted	成功由快照策略存档的快照数量。
snapshotsArchiveFailed	不能由快照策略存档的快照数量。
snapshotsArchiveDeletionCompleted	成功由快照策略从存档层中删除的存档快照数量。
PreScriptStarted	前置脚本成功启动的实例数。 如果启用了脚本重试，则每次策略运行时可以多次发出此指标。
PreScriptCompleted	前置脚本成功完成的实例数。即使前置脚本在指定的超时期间之外完成，也会发出该指标。 如果启用了脚本重试，则每次策略运行时可以多次发出此指标。

指标	描述
PreScript Failed	前置脚本未能成功完成的实例数。即使前置脚本在指定的超时期间之外完成，也会发出该指标。 如果启用了脚本重试，则每次策略运行时可以多次发出此指标。
PostScript tStarted	后置脚本成功启动的实例数。 如果启用了脚本重试，则每次策略运行时可以多次发出此指标。
PostScriptCompleted	后置脚本成功完成的实例数。即使后置脚本在指定的超时期间之外完成，也会发出该指标。 如果启用了脚本重试，则每次策略运行时可以多次发出此指标。
PostScriptFailed	后置脚本未能成功完成的实例数。即使后置脚本在指定的超时期间之外完成，也会发出该指标。 如果启用了脚本重试，则每次策略运行时可以多次发出此指标。
VSSBackup Started	VSS 备份成功启动的实例数。 如果启用了脚本重试，则每次策略运行时可以多次发出此指标。
VSSBackup Completed	VSS 备份成功完成的实例数。即使 VSS 备份在超时期间之外完成，也会发出该指标。 如果启用了脚本重试，则每次策略运行时可以多次发出此指标。
VSSBackup Failed	VSS 备份未能成功完成的实例数。即使 VSS 备份在超时期间之外完成，也会发出该指标。 如果启用了脚本重试，则每次策略运行时可以多次发出此指标。

EBS-backed AMI policies

以下指标可与 EBS 支持的 AMI 策略一起使用：

指标	描述

指标	描述
Resources Targeted	在快照或 EBS 支持的 AMI 策略中所指定标签针对的资源数量。
Snapshots DeleteCompleted	快照或 EBS 支持的 AMI 策略删除的快照数量。此指标仅适用于策略创建的快照。它不适用于策略创建的跨区域快照副本。 该指标包括在 EBS 支持的 AMI 策略注销注册时删除的快照。AMIs
Snapshots DeleteFailed	不能由快照或 EBS 支持的 AMI 策略删除的快照数量。此指标仅适用于策略创建的快照。它不适用于策略创建的跨区域快照副本。 该指标包括在 EBS 支持的 AMI 策略注销注册时删除的快照。 AMIs
Snapshots CopiedRegionDelete Completed	快照策略删除的跨区域快照副本的数量，由保留规则指定。
Snapshots CopiedRegionDelete Failed	不能由快照策略删除的跨区域快照副本的数量，由保留规则指定。
ImagesCreateStarted	由 EBS 支持的 AMI 策略启动的CreateImage操作数量。
ImagesCreateCompleted	由 EBS 支持的 AMI 策略 AMIs 创建的数量。
ImagesCreateFailed	其中的数量 AMIs 无法由 EBS 支持的 AMI 策略创建。

指标	描述
ImagesDeregisterCompleted	由 EBS 支持的 AMI 策略注 AMIs 销的数量。
ImagesDeregisterFailed	EBS支持的AMI政策无法注销其中的数量。 AMIs
ImagesCopiedRegionStarted	由 EBS 支持的 AMI 策略启动的跨区域复制操作的数量。
ImagesCopiedRegionCompleted	由 EBS 支持的 AMI 策略创建的跨区域 AMI 副本的数量。
ImagesCopiedRegionFailed	不能由 EBS 支持的 AMI 策略创建的跨区域 AMI 副本的数量。
ImagesCopiedRegionDeregisterCompleted	由 EBS 支持的 AMI 策略取消注册的跨区域 AMI 副本数量，由保留规则指定。
ImagesCopiedRegionDeregisteredFailed	不能由 EBS 支持的 AMI 策略取消注册的跨区域 AMI 副本数量，由保留规则指定。

指标	描述
EnableImageDeprecationCompleted	EBS 支持 AMIs 的 AMI 政策将其中数量标记为弃用。
EnableImageDeprecationFailed	EBS 支持 AMIs 的 AMI 策略无法将其中的数量标记为弃用。
EnableCopiedImageDeprecationCompleted	由 EBS 支持的 AMI 策略标记为弃用的跨区域 AMI 副本数量。
EnableCopiedImageDeprecationFailed	不能由 EBS 支持的 AMI 策略标记为弃用的跨区域 AMI 副本数量。

Cross-account copy event policies

跨账户复制事件策略可以使用以下指标：

指标	描述
SnapshotsCopiedAccountStarted	跨账户复制事件策略启动的跨账户快照复制操作的数量。
SnapshotsCopiedAccountCompleted	跨账户复制事件策略从另一个账户复制的快照数量。这包括在计划时间的 24 小时内的成功重试。

指标	描述
SnapshotsCopiedAccountFailed	不能由跨账户复制事件策略从另一个账户复制的快照数量。这包括在计划时间的 24 小时内的不成功重试。
SnapshotsCopiedAccountDeleteCompleted	跨账户复制事件策略删除的跨区域快照副本的数量，由保留规则指定。
SnapshotsCopiedAccountDeleteFailed	不能由跨账户复制事件策略删除的跨区域快照副本的数量，由保留规则指定。

查看您的政策 CloudWatch 指标

您可以使用 Amazon Web Services Management Console 或命令行工具列出 Amazon Data Lifecycle Manager 发送给亚马逊的指标 CloudWatch。

Amazon EC2 console

使用 Amazon EC2 控制台查看指标

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Lifecycle Manager（生命周期管理器）。
3. 在网格中选择一个策略，然后选择 Monitoring（监控）选项卡。

CloudWatch console

使用 Amazon CloudWatch 控制台查看指标

1. 打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，选择指标。

3. 选择 EBS 命名空间，然后选择 Data Lifecycle Manager metrics（数据生命周期管理器指标）。

Amazon CLI

列出 Amazon Data Lifecycle Manager 的所有可用指标

使用 list-metrics 命令。

```
$ C:\> aws cloudwatch list-metrics \
    --namespace AWS/EBS
```

列出特定策略的所有指标

使用 list-metrics 命令并指定 DLMPolicyId 维度。

```
$ C:\> aws cloudwatch list-metrics \
    --namespace AWS/EBS \
    --dimensions Name=DLMPolicyId,Value=policy-abcdef01234567890
```

列出所有策略的单个指标

使用 list-metrics 命令并指定 --metric-name 选项。

```
$ C:\> aws cloudwatch list-metrics \
    --namespace AWS/EBS \
    --metric-name SnapshotsCreateCompleted
```

绘制策略的指标图表

创建策略后，您可以打开 Amazon EC2 控制台并在 “监控” 选项卡上查看该策略的监控图表。每个图表都基于一项可用的 Amazon EC2 指标。

可供使用图表指标如下：

- 资源目标已确定（基于 ResourcesTargeted）
- 快照创建已启动（基于 SnapshotsCreateStarted）
- 快照创建已完成（基于 SnapshotsCreateCompleted）

- 快照创建已失败（基于 SnapshotsCreateFailed）
- 快照共享已完成（基于 SnapshotsSharedCompleted）
- 快照删除已完成（基于 SnapshotsDeleteCompleted）
- 快照删除已失败（基于 SnapshotsDeleteFailed）
- 快照跨区域复制已启动（基于 SnapshotsCopiedRegionStarted）
- 快照跨区域复制已完成（基于 SnapshotsCopiedRegionCompleted）
- 快照跨区域复制已失败（基于 SnapshotsCopiedRegionFailed）
- 快照跨区域复制删除已完成（基于 SnapshotsCopiedRegionDeleteCompleted）
- 快照跨区域复制删除已失败（基于 SnapshotsCopiedRegionDeleteFailed）
- 快照跨账户复制已启动（基于 SnapshotsCopiedAccountStarted）
- 快照跨账户复制已完成（基于 SnapshotsCopiedAccountCompleted）
- 快照跨账户复制已失败（基于 SnapshotsCopiedAccountFailed）
- 快照跨账户复制删除已完成（基于 SnapshotsCopiedAccountDeleteCompleted）
- 快照跨账户复制删除已失败（基于 SnapshotsCopiedAccountDeleteFailed）
- AMI 创建已开始（基于ImagesCreateStarted）
- AMI 创建已完成（基于 ImagesCreateCompleted）
- AMI 创建已失败（基于 ImagesCreateFailed）
- AMI 取消注册已完成（基于 ImagesDeregisterCompleted）
- AMI 取消注册已失败（基于 ImagesDeregisterFailed）
- AMI 跨区域复制已启动（基于 ImagesCopiedRegionStarted）
- AMI 跨区域复制已完成（基于 ImagesCopiedRegionCompleted）
- AMI 跨区域复制已失败（基于 ImagesCopiedRegionFailed）
- AMI 跨区域取消注册已完成（基于 ImagesCopiedRegionDeregisterCompleted）
- AMI 跨区域复制取消注册已失败（基于 ImagesCopiedRegionDeregisteredFailed）
- AMI 启用弃用已完成（基于 EnableImageDeprecationCompleted）
- AMI 启用弃用已失败（基于 EnableImageDeprecationFailed）
- AMI 跨区域复制启用弃用已完成（基于 EnableCopiedImageDeprecationCompleted）
- AMI 跨区域复制启用弃用已失败（基于 EnableCopiedImageDeprecationFailed）

为策略创建 CloudWatch 警报

您可以创建用于监控策略 CloudWatch 指标的 CloudWatch 警报。 CloudWatch 当指标达到您指定的阈值时，将自动向您发送通知。您可以使用 CloudWatch 控制台创建 CloudWatch 警报。

有关使用 CloudWatch 控制台创建警报的更多信息，请参阅 Amazon CloudWatch 用户指南中的以下主题。

- 基于静态阈值创建 CloudWatch 警报
- 基于异常检测创建 CloudWatch 警报

使用案例示例

以下是使用案例示例：

主题

- 示例 1： ResourcesTargeted 指标
- 示例 2： SnapshotDeleteFailed 指标
- 示例 3： SnapshotsCopiedRegionFailed 指标

示例 1： ResourcesTargeted 指标

您可以使用 `ResourcesTargeted` 指标来监控特定策略每次运行时所针对的资源总数。这使您能够在目标资源的数量低于或高于预期阈值时触发告警。

例如，如果您希望每日策略创建不超过 50 卷的备份，可以创建告警，该告警会在 `ResourcesTargeted` 的 sum 大于 50 超过 1 小时时发送电子邮件通知。通过这种方式，您可以确保没有从已错误标记的卷意外创建任何快照。

可以使用以下命令创建此告警：

```
$ C:\> aws cloudwatch put-metric-alarm \
    --alarm-name resource-targeted-monitor \
    --alarm-description "Alarm when policy targets more than 50 resources" \
    --metric-name ResourcesTargeted \
    --namespace AWS/EBS \
    --statistic Sum \
    --period 3600 \
```

```
    --threshold 50 \
    --comparison-operator GreaterThanThreshold \
    --dimensions "Name=DLMPolicyId,Value=policy_id" \
    --evaluation-periods 1 \
    --alarm-actions sns_topic_arn
```

示例 2： SnapshotDeleteFailed 指标

您可以使用 SnapshotDeleteFailed 指标，以根据策略的快照保留规则来监控删除快照的故障情况。

例如，如果您已创建应每 12 小时自动删除一次快照的策略，则可以创建一个告警，该告警会在 SnapshotDeletionFailed 的 sum 大于 0 超过 1 小时通知您的工程团队。这有助于调查不正确的快照保留，并确保您的存储成本不会因不必要的快照而增加。

可以使用以下命令创建此告警：

```
$ C:\> aws cloudwatch put-metric-alarm \
    --alarm-name snapshot-deletion-failed-monitor \
    --alarm-description "Alarm when snapshot deletions fail" \
    --metric-name SnapshotsDeleteFailed \
    --namespace AWS/EBS \
    --statistic Sum \
    --period 3600 \
    --threshold 0 \
    --comparison-operator GreaterThanThreshold \
    --dimensions "Name=DLMPolicyId,Value=policy_id" \
    --evaluation-periods 1 \
    --alarm-actions sns_topic_arn
```

示例 3： SnapshotsCopiedRegionFailed 指标

使用 SnapshotsCopiedRegionFailed 指标以确定您的策略何时无法将快照复制到其他区域。

例如，如果您的策略每天跨区域复制快照，则可以创建告警，该告警会在 SnapshotCrossRegionCopyFailed 的 sum 大于 0 超过 1 小时时向您的工程团队发送 SMS。这对于验证策略是否成功复制了谱系中的后续快照非常有用。

可以使用以下命令创建此告警：

```
$ C:\> aws cloudwatch put-metric-alarm \
```

```
    --alarm-name snapshot-copy-region-failed-monitor \
    --alarm-description "Alarm when snapshot copy fails" \
    --metric-name SnapshotsCopiedRegionFailed \
    --namespace AWS/EBS \
    --statistic Sum \
    --period 3600 \
    --threshold 0 \
    --comparison-operator GreaterThanThreshold \
    --dimensions "Name=DLMPolicyId,Value=policy_id" \
    --evaluation-periods 1 \
    --alarm-actions sns_topic_arn
```

管理报告失败操作的策略

有关当您的某项政策报告操作失败指标出现意外非零值时该怎么办的更多信息，请参阅文章如果 Amazon Data Lifecycle Manager 报告 CloudWatch 指标中的失败操作该怎么办？

亚马逊 Data Lifecycle Manager 的服务终端节点

端点是用作 Amazon Web 服务入口点的 URL。Amazon Data Lifecycle Manager 支持以下终端节点类型：

- IPv4 端点
- 同时 IPv4 支持和的双栈端点 IPv6

当您发出请求时，您可以指定要使用的端点和区域。如果您未指定终端节点，则默认使用该 IPv4 终端节点。要使用不同的端点类型，您必须在请求中指定。有关如何执行此操作的示例，请参阅指定端点。

有关终端节点列表，请参阅终端节点和中国的 ARNs 终 Amazon端节点。

主题

- IPv4 端点
- 双栈（IPv4 和 IPv6）端点
- 指定端点

IPv4 端点

IPv4 端点仅支持 IPv4 流量。 IPv4 终端节点适用于所有区域。

您必须将区域指定为端点名称的一部分。端点名称使用以下命名约定：

- dlm。 *region*.amazonaws.com.cn

例如，北京区域的 IPv4 终端节点是dlm.cn-north-1.amazonaws.com.cn。

双栈（IPv4 和 IPv6）端点

双栈端点同时支持 IPv4 和 IPv6 流量。双堆栈端点适用于所有区域。

要使用 IPv6，必须使用双堆栈终端节点。当您向双栈终端节点发出请求时，终端节点 URL 会解析为 IPv6 或 IPv4 地址，具体取决于您的网络和客户端使用的协议。

您必须将区域指定为端点名称的一部分。双堆栈端点名称使用以下命名约定：

- dlm.*region*.api.amazonwebservices.com.cn

例如，北京区域的双栈终端节点是dlm.cn-cn-north-1.api.amazonwebservices.com.cn。

指定端点

以下示例显示如何使用 Amazon CLI为北京区域指定端点。

- 双堆栈

```
aws dlm create-default-role \
--resource-type snapshot \
--endpoint-url https://dlm.cn-north-1.api.amazonwebservices.com.cn
```

- IPv4

```
aws dlm create-default-role \
--resource-type snapshot \
--endpoint-url https://dlm.cn-north-1.amazonaws.com.cn
```

在 VPC 和 Amazon EBS 之间创建私有连接

您可以通过创建由提供支持的接口 VPC 终端节点在您的 VPC 和 Amazon EBS 之间建立私有连接。Amazon PrivateLink您可以像在您的 VPC 中一样访问 Amazon EBS，无需使用互联网网关、NAT

设备、VPN 连接或 Amazon Direct Connect 连接。您的 VPC 中的实例不需要公有 IP 地址即可与 Amazon EBS 通信。

我们将在您为接口端点启用的每个子网中创建一个端点网络接口。

有关更多信息，请参阅Amazon PrivateLink 指南 Amazon PrivateLink中的Amazon Web Services 服务通过访问。

> **Note**
>
> Amazon Data Lifec IPv4 ycle Manager 支持所有商业和 Amazon GovCloud (US) 区域的 IPv6 接口 VPC 终端节点，仅支持商业区域的接口 VPC 终端节点。

亚马逊 EBS VPC 终端节点的注意事项

在为 Amazon EBS 设置接口 VPC 终端节点之前，请查看Amazon PrivateLink 指南中的注意事项。

默认情况下，允许通过终端节点对 Amazon EBS 进行完全访问。您可以使用 VPC 端点策略控制对接口端点的访问。您可以将终端节点策略附加到控制对 Amazon EBS 的访问权限的 VPC 终端节点。该策略指定以下信息：

- 可执行操作的主体。
- 可执行的操作。
- 可对其执行操作的资源。

有关更多信息，请参阅 Amazon VPC 用户指南中的使用 VPC 终端节点控制对服务的访问。

以下是 Amazon EBS 的终端节点策略示例。当连接到终端节点时，该政策授予所有用户获取有关 Amazon Data Lifecycle Manager 政策摘要信息的权限。

```
{
  "Statement": [{
    "Action": "dlm:GetLifecyclePolicies",
    "Effect": "Allow",
    "Principal": "*",
    "Resource": "*"
  }]
}
```

为 Amazon EBS 创建接口 VPC 终端节点

您可以使用亚马逊 VPC 控制台或 Amazon Command Line Interface (Amazon CLI) 为 Amazon EBS 创建 VPC 终端节点。有关更多信息，请参阅 Amazon PrivateLink 指南中的创建 VPC 终端节点。

使用以下服务名称为 Amazon EBS 创建 VPC 终端节点：

- `cn.com.amazonaws.region.dlm`

例如，如果您为终端节点启用私有 DNS，则可以使用该区域的默认 DNS 名称向 Amazon EBS 发出 API 请求。`dlm.us-east-1.amazonaws.com`

排查 Amazon Data Lifecycle Manager 问题

以下文档可以帮助排查可能遇到的问题。

主题

- 错误：Role with name already exists

错误：**Role with name already exists**

描述

您在尝试使用控制台创建策略时收到了 `Role with name AWSDataLifecycleManagerDefaultRole already exists` 或 `Role with name AWSDataLifecycleManagerDefaultRoleForAMIManagement already exists` 错误。

原因

默认角色的 ARN 格式会有所不同，具体取决于使用控制台还是 Amazon CLI创建角色。虽然 ARNs 它们不同，但角色使用相同的角色名称，这会导致控制台和之间出现角色命名冲突 Amazon CLI。

解决方案

要解决此问题，请执行以下操作：

1. （仅适用于为预脚本和后脚本启用的快照策略）手动将 A AWSDataLifecycleManagerSSMFullcces s Amazon 托管策略附加到 AWSDataLifecycleManagerDefaultRoleIAM 角色。有关更多信息，请参阅添加 IAM 身份权限。

2. 在创建 Amazon Data Lifecycle Manager 策略时，对于 IAM 角色，选择选择其他角色，然后选择 AWSDataLifecycleManagerDefaultRole（对于快照策略）或 AWSDataLifecycleManagerDefaultRoleForAMIManagement（对于 AMI 策略）。
3. 像往常一样继续创建策略。

使用 EBS 直接 APIs 访问快照的内容

您可以 APIs 直接使用 Amazon Elastic Block Store (Amazon EBS) 创建 EBS 快照、直接向快照写入数据、读取快照上的数据，以及识别两个快照之间的区别或变化。如果您是为 Amazon EBS 提供备份服务的独立软件供应商 (ISV)，那么 EBS Direct APIs 可以提高通过快照跟踪 EBS 卷的增量更改的效率和成本效益。无需使用快照创建新卷，然后使用亚马逊弹性计算云 (Amazon EC2) 实例来比较差异，即可完成此操作。

您可以从本地数据直接创建增量快照到 EBS 卷和云中，以用于快速灾难恢复。通过写入和读取快照的功能，您可以在发生灾难时将本地数据写入 EBS 快照。然后，恢复后，您可以将其恢复到快照 Amazon 或从快照恢复到本地。您不再需要构建和维护复杂的机制来将数据复制到 Amazon EBS 或从中复制数据。

本用户指南概述了构成 EBS direct 的元素 APIs，并提供了如何有效使用它们的示例。有关操作、数据类型、参数和错误的更多信息 APIs，请参阅 EBS 直接 APIs 参考。有关 EBS direct 支持的 Amazon 区域、终端节点和服务配额的更多信息 APIs，请参阅中的 Amazon EBS 终端节点和配额。Amazon Web Services 一般参考

主题

- EBS direct 的定价 APIs
- EBS 直接版的概念 APIs
- APIs 使用 IAM 直接控制对 EBS 的访问权限
- 直接使用 EBS 读取 Amazon EBS 快照 APIs
- 使用 EBS Direct 写入亚马逊 EBS 快照 APIs
- EBS Direct 的加密结果 APIs
- 使用 EBS 直接 APIs 校验和来验证快照数据
- 确保 API 请求中的等性 StartSnapshot
- EBS direct 的错误重试次数 APIs
- 优化 EBS Direct 的性能 APIs
- EBS Direct 的服务端点 APIs
- Amazon EBS Direct 的 SDK 代码示例 APIs
- 在 VPC 和 EBS Direct 之间创建私有连接 APIs
- 使用记录 EBS 直接 APIs 呼叫 Amazon CloudTrail

- EBS direct 的常见问题解答 APIs

EBS direct 的定价 APIs

的定价 APIs

您直接使用EBS所支付的价格 APIs 取决于您提出的请求。有关更多信息，请参阅 Amazon EBS 定价。

- ListChangedBlocks并 ListSnapshotBlocks APIs 按请求收费。例如，如果您在某个地区发出 100,000 ListSnapshotBlocks 个 API 请求，且该地区每 1,000 个请求收费 0.0006 美元，则将向您收取 0.06 美元的费用（每 1,000 个请求 0.0006 美元 x 100）。
- GetSnapshotBlock按返回的区块收费。例如，如果您在某个地区发出 100,000 GetSnapshotBlock 个 API 请求，且每返回 1,000 个区块收费 0.003 美元，则将支付 0.30 美元（每返回 1,000 个区块 0.003 美元 x 100）。
- PutSnapshotBlock按写入的区块收费。例如，如果您在某个地区发出 100,000 PutSnapshotBlock 个 API 请求，且每写入 1,000 个区块收费 0.006 美元，则将支付 0.60 美元的费用（每写入 1,000 个区块 0.006 美元 x 100）。

联网成本

数据传输成本

使用非 FIPS 终端节点时，直接在同一 Amazon 区域的 EBS Di rect APIs 和 Amazon EC2 实例之间传输的数据是免费的。有关更多信息，请参阅Amazon 服务端点。如果您的数据传输途中还有其他 Amazon 服务，则将向您收取相关的数据处理费用。这些服务包括但不限于 PrivateLink 终端节点、NAT 网关和 Transit Gateway。

VPC 接口终端节点

如果您直接 APIs 使用 Amazon EC2 实例的 EBS 或私有子网中的 Amazon Lambda 函数，则可以使用 VPC 接口终端节点，而不使用 NAT 网关，以降低网络数据传输成本。有关更多信息，请参阅 在 VPC 和 EBS Direct 之间创建私有连接 APIs。

EBS 直接版的概念 APIs

以下是在开始使用 EBS direc APIs t 之前应了解的关键概念。

快照

快照是备份 EBS 卷中的数据的主要方式。借助 EBS Direct APIs，您还可以将本地磁盘中的数据备份到快照。为节省存储成本，连续快照为增量快照，只包含自上一个快照以来更改的卷数据。有关更多信息，请参阅 Amazon EBS 快照。

> **Note**
>
> EBS Direct APIs 不支持开启的公共快照和本地快照。 Amazon Outposts

数据块

数据块是快照中的数据片段。每个快照可以包含数千个数据块。快照中的所有数据块都具有固定大小。

数据块索引

数据块索引是以 512 KiB 数据块为单位的逻辑索引。若要确定数据块索引，请用逻辑卷中数据的逻辑偏移量除以数据块大小（数据的逻辑偏移量/524288）。数据的逻辑偏移量必须与 512 KiB 一致。

数据块令牌

数据块令牌是快照中的数据块的标识哈希，它用于查找数据块数据。EBS Direct 返回的区块代币 APIs 是临时的。它们会在为其指定的到期时间戳时发生变化，或者如果您运行另一个快照 ListSnapshotBlocks 或 ListChangedBlocks 请求相同的快照。

校验和

校验和是从数据块中派生的大小很小的基准值，用于检测其传输或存储过程中引入的错误。EBS 直接 APIs 使用校验和来验证数据的完整性。当您从 EBS 快照中读取数据时，该服务会为传输的每个数据块提供 Base64 编码的 SHA256 校验和，您可以将其用于验证。向 EBS 快照写入数据时，必须为每个传输的数据块提供 Base64 编码的 SHA256 校验和。服务使用提供的校验和验证接收的数据。有关更多信息，请参阅本指南下文中的使用 EBS 直接 APIs 校验和来验证快照数据。

加密

通过加密，您的数据将转换为无法读取的代码，只能由有权访问加密数据所用 KMS 密钥 的人员破译这些代码，从而为数据提供保护。您可以使用 EBS Direc APIs t 来读取和写入加密快照，但有一些限制。有关更多信息，请参阅本指南下文中的EBS Direct 的加密结果 APIs。

API 操作

EBS direc APIs t 由六个操作组成。包含三个读取操作和三个写入操作。读取操作包括：

- ListSnapshotBlocks— 返回指定快照中区块的区块索引和区块标记
- ListChangedBlocks— 返回同一卷和快照谱系的两个指定快照之间不同的区块索引和区块令牌。
- GetSnapshotBlock— 返回区块中指定快照 ID、区块索引和区块令牌的数据。

写入操作包括：

- StartSnapshot— 启动快照，可以是现有快照的增量快照，也可以是新快照。在使用 CompleteSnapshot 操作完成之前，已启动的快照将保持待处理状态。
- PutSnapshotBlock— 以单个块的形式向已启动的快照添加数据。必须为传输的数据块指定 Base64 编码的 SHA256 校验和。该服务会在传输完成以后验证校验和。若该服务计算的校验和与您指定值的不匹配，请求将会失败。
- CompleteSnapshot— 完成处于待处理状态的已启动快照。然后，该快照的状态会更改为“已完成”。

签名版本 4 签名

签名版本 4 是向 HTTP 发送的 Amazon 请求添加身份验证信息的过程。为了安全起见，对的大多数请求都 Amazon 必须使用访问密钥进行签名，访问密钥由访问密钥 ID 和私有访问密钥组成。这两个密钥通常称为您的安全凭证。有关如何获取账户凭证的信息，请参阅 Amazon 安全凭证。

如果您打算手动创建 HTTP 请求，则必须了解如何对其签名。当您使用 Amazon Command Line Interface (Amazon CLI) 或其中一个 Amazon SDKs 向发出请求时 Amazon，这些工具会自动使用您在配置工具时指定的访问密钥为您签署请求。当您使用这些工具时，您不必了解如何亲自签署这些请求。

有关更多信息，请参阅 I AM 用户指南中的签署 Amazon API 请求。

APIs 使用 IAM 直接控制对 EBS 的访问权限

用户必须遵循以下策略才能直接 APIs使用 EBS。有关更多信息，请参阅更改用户权限。

有关用于 IAM 权限策略的 EBS 直接 APIs 资源、操作和条件上下文密钥的更多信息，请参阅服务授权参考中的 A mazon Elastic Block Store 的操作、资源和条件密钥。

> **Important**
>
> 向 用户分配以下策略时请小心谨慎。通过分配这些策略，您可以向被拒绝通过 Amazon 访问相同资源的用户授予访问权限 EC2 APIs，例如 CopySnapshot 或 CreateVolume 操作。

读取快照的权限

以下策略允许在特定 Amazon 区域的所有快 APIs 照上使用直接读取 EBS。在策略中，*<Region>*替换为快照的区域。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ebs:GetSnapshotBlock"
            ],
            "Resource": "arn:aws:ec2:<Region>::snapshot/*"
        }
    ]
}
```

以下策略允许在带有特定键值标签 APIs 的快照上使用直接读取 EBS。在策略中，*<Key>*替换为标签的键值和*<Value>*标签的值。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ebs:GetSnapshotBlock"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*",
            "Condition": {
                "StringEqualsIgnoreCase": {
```

```
                    "aws:ResourceTag/<Key>": "<Value>"
                }
            }
        }
    ]
}
```

以下策略仅允许在特定时间范围内对账户中的所有快照使用所有读取 EBS direc APIs t。此策略授权 APIs 根据aws:CurrentTime全局条件密钥直接使用 EBS。在策略中，请务必将显示的日期和时间范围替换为适用于您的策略的日期和时间范围。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:ListSnapshotBlocks",
                "ebs:ListChangedBlocks",
                "ebs:GetSnapshotBlock"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*",
            "Condition": {
                "DateGreaterThan": {
                    "aws:CurrentTime": "2018-05-29T00:00:00Z"
                },
                "DateLessThan": {
                    "aws:CurrentTime": "2020-05-29T23:59:59Z"
                }
            }
        }
    ]
}
```

有关更多信息，请参阅《IAM 用户指南》中的更改用户权限。

写入快照的权限

以下策略允许在特定 Amazon 区域的所有快 APIs 照上直接写入 EBS。在策略中，<Region>替换为快照的区域。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:StartSnapshot",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot"
            ],
            "Resource": "arn:aws:ec2:<Region>::snapshot/*"
        }
    ]
}
```

以下策略允许在带有特定键值标签的快照上使用写入 EBS direc APIs t。在策略中，*<Key>*替换为标签的键值和*<Value>*标签的值。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:StartSnapshot",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*",
            "Condition": {
                "StringEqualsIgnoreCase": {
                    "aws:ResourceTag/<Key>": "<Value>"
                }
            }
        }
    ]
}
```

以下策略允许使用所有 EBS Dire APIs ct。只有在指定了父快照 ID 时，它才允许执行 `StartSnapshot` 操作。因此，此策略会阻止在不使用父快照的情况下开始新快照的功能。

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ebs:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ebs:ParentSnapshot": "arn:aws:ec2:*::snapshot/*"
                }
            }
        }
    ]
}
```

以下策略允许使用所有 EBS Dire APIs ct。它还允许只为新快照创建 `user` 标签键。此策略还确保用户有权创建标签。`StartSnapshot` 操作是唯一可以指定标签的操作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ebs:*",
            "Resource": "*",
            "Condition": {
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "user"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

以下策略仅允许在特定时间范围内对账户中的所有快照使用所有写入 EBS direc APIs t。此策略授权 APIs 根据`aws:CurrentTime`全局条件密钥直接使用 EBS。在策略中，请务必将显示的日期和时间范围替换为适用于您的策略的日期和时间范围。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ebs:StartSnapshot",
                "ebs:PutSnapshotBlock",
                "ebs:CompleteSnapshot"
            ],
            "Resource": "arn:aws:ec2:*::snapshot/*",
            "Condition": {
                "DateGreaterThan": {
                    "aws:CurrentTime": "2018-05-29T00:00:00Z"
                },
                "DateLessThan": {
                    "aws:CurrentTime": "2020-05-29T23:59:59Z"
                }
            }
        }
    ]
}
```

有关更多信息，请参阅《IAM 用户指南》中的更改用户权限。

使用权限 Amazon KMS keys

以下策略授予使用特定 KMS 密钥解密已加密快照的权限。该策略还授予使用 EBS 加密的默认 KMS 密钥来加密新快照的权限。在策略中，*<Region>*替换为 KMS 密钥的区域、*<AccountId>* KMS 密钥的 Amazon 账户 ID 和 *<KeyId>* KMS 密钥的 ID。

> **Note**
>
> 默认情况下，账户中的所有委托人都可以访问用于 Amazon EBS 加密的默认 Amazon 托管 KMS 密钥，并且可以将其用于 EBS 加密和解密操作。如果您使用的是客户托管式密钥，则必须创建新的密钥策略或修改客户托管式密钥的现有密钥策略，以便授予主体对客户托管式密钥的访问权限。有关更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的在 Amazon KMS中使用密钥策略。

> **Tip**
>
> 为遵循最小特权原则，请不要允许对 kms:CreateGrant 拥有完全访问权限。相反，使用kms:GrantIsForAWSResource条件密钥允许用户仅在 Amazon 服务代表用户创建授权时才允许用户在 KMS 密钥上创建授权，如以下示例所示。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:GenerateDataKey",
                "kms:GenerateDataKeyWithoutPlaintext",
                "kms:ReEncrypt*",
                "kms:CreateGrant",
                "ec2:CreateTags",
                "kms:DescribeKey"
            ],
            "Resource": "arn:aws:kms:<Region>:<AccountId>:key/<KeyId>",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

有关更多信息，请参阅《IAM 用户指南》中的更改用户权限。

直接使用 EBS 读取 Amazon EBS 快照 APIs

以下步骤介绍如何使用 EBS 直接读 APIs 取快照：

1. 使用 ListSnapshotBlocks 操作可查看快照中区块的所有区块索引和区块标记。或者使用 ListChangedBlocks 操作仅查看同一卷和快照谱系的两个快照之间不同的区块索引和区块令牌。这些操作可帮助您标识可能希望获取其数据的数据块的数据块令牌和数据块索引。
2. 使用 GetSnapshotBlock 操作，并指定要获取其数据的区块的区块索引和区块标记。

> **Note**
>
> 您不能将 EBS 直接 APIs 用于存档快照。

以下示例说明如何使用 EBS Dire APIs ct 读取快照。

主题

- 列出快照中的数据块
- 列出两个快照之间存在不同的数据块
- 从快照获取数据块数据

列出快照中的数据块

Amazon CLI

以下list-snapshot-blocks示例命令返回快照中区块的区块索引和区块标记snap-0987654321。--starting-block-index 参数将结果限制为索引大于 1000 的数据块，并且 --max-results 参数将结果限制为前 100 个数据块。

```
aws ebs list-snapshot-blocks --snapshot-id snap-0987654321 --starting-block-index 1000 --max-results 100
```

以下为上一个命令的示例响应，其中列出了快照中的数据块索引和数据块令牌。使用 get-snapshot-block 命令，请指定要获取其数据的数据块的数据块索引和数据块令牌。数据块令牌在列出的过期时间之前有效。

```
{
      "Blocks": [
          {
              "BlockIndex": 1001,
```

```
                "BlockToken": "AAABAV3/
PNhXOynVdMYHUpPsetaSvjLB1dtIGfbJv5OJ0sX855EzGTWos4a4"
            },
            {
                "BlockIndex": 1002,
                "BlockToken": "AAABATGQIgwr0WwIuqIMjCA/Sy7e/
YoQFZsHejzGNvjKauzNgzeI13YHBfQB"
            },
            {
                "BlockIndex": 1007,
                "BlockToken": "AAABAZ9CTuQtUvp/
dXqRWw4d07eOgTZ3jvn6hiW30W9duM8MiMw6yQayzF2c"
            },
            {
                "BlockIndex": 1012,
                "BlockToken": "AAABAQdzxhw0rVV6PNmsfo/
YRIxo9JPR85XxPf1BLjg0Hec6pygYr6laE1p0"
            },
            {
                "BlockIndex": 1030,
                "BlockToken": "AAABAaYvPax6mv+iGWLdTUjQtFWouQ7Dqz6nSD9L
+CbXnvpkswA6iDID523d"
            },
            {
                "BlockIndex": 1031,
                "BlockToken": "AAABATgWZC0XcFwUKvTJbUXMiSPg59KVxJGL
+BWBClkw6spzCxJVqDVaTskJ"
            },
            ...
        ],
        "ExpiryTime": 1576287332.806,
        "VolumeSize": 32212254720,
        "BlockSize": 524288
    }
```

Amazon API

以下ListSnapshotBlocks示例请求返回快照中区块的区块索引和区块标记snap-0acEXAMPLEcf41648。startingBlockIndex 参数将结果限制为索引大于 1000 的数据块，并且 maxResults 参数将结果限制为前 100 个数据块。

```
GET /snapshots/snap-0acEXAMPLEcf41648/blocks?maxResults=100&startingBlockIndex=1000
 HTTP/1.1
```

```
  Host: ebs.us-east-2.amazonaws.com
  Accept-Encoding: identity
  User-Agent: <User agent parameter>
  X-Amz-Date: 20200617T231953Z
  Authorization: <Authentication parameter>
```

以下为上一个请求的示例响应，其中列出了快照中的数据块索引和数据块令牌。使用 GetSnapshotBlock 操作并指定要获取其数据的区块的区块索引和区块标记。数据块令牌在列出的过期时间之前有效。

```
HTTP/1.1 200 OK
  x-amzn-RequestId: d6e5017c-70a8-4539-8830-57f5557f3f27
  Content-Type: application/json
  Content-Length: 2472
  Date: Wed, 17 Jun 2020 23:19:56 GMT
  Connection: keep-alive

  {
      "BlockSize": 524288,
      "Blocks": [
          {
              "BlockIndex": 0,
              "BlockToken": "AAUBAcuWqOCnDNuKle11s7IIX6jp6FYcC/q8oT93913HhvLvA
+3JRrSybp/0"
          },
          {
              "BlockIndex": 1536,
              "BlockToken":
 "AAUBAWudwfmofcrQhGVlLwuRKm2b8ZXPiyrgoykTRC6IU1NbxKWDY1pPjvnV"
          },
          {
              "BlockIndex": 3072,
              "BlockToken":
 "AAUBAV7p6pC5fKAC7TokoNCtAnZhqq27u6YEXZ3MwRevBkDjmMx6iuA6tsBt"
          },
          {
              "BlockIndex": 3073,
              "BlockToken":
 "AAUBAbqt9zpqBUEvtO2HINAfFaWToOwlPjbIsQOlx6JUN/0+iMQl0NtNbnX4"
          },
          ...
      ],
      "ExpiryTime": 1.59298379649E9,
```

```
    "VolumeSize": 3
}
```

列出两个快照之间存在不同的数据块

在发出分页请求以列出两个快照之间发生更改的块时应注意以下几点：

- 响应可能包含一个或多个空的 ChangedBlocks 数组。例如：
  - 快照 1 – 1000 个块的完整快照，带块索引 0 – 999。
  - 快照 2 – 仅包含一个发生更改的块，块索引为 999 的增量快照。

  使用 StartingBlockIndex = 0 和 MaxResults = 100 列出这些快照发生更改的块时，将返回一个空的 ChangedBlocks 数组。您必须使用 nextToken 请求剩余的结果，直到第十个结果集（其中包括块索引为 900 - 999 的块）返回发生更改的块为止。
- 响应可能回跳过快照中未写入的块。例如：
  - 快照 1 – 1000 个块的完整快照，带块索引 2000 – 2999。
  - 快照 2 – 仅包含一个发生更改的块，块索引为 2000 的增量快照。

  使用 StartingBlockIndex = 0 和 MaxResults = 100 列出这些快照中发生更改的块时，响应将跳过块索引 0 - 1999 并将包含块索引 2000。响应不会包含空的 ChangedBlocks 数组。

Amazon CLI

以下list-changed-blocks示例命令返回快照和之间不同的区块的区块索引snap-1234567890和区块标记snap-0987654321。--starting-block-index 参数将结果限制为索引大于 0 的数据块，并且 --max-results 参数将结果限制为前 500 个数据块。

```
aws ebs list-changed-blocks --first-snapshot-id snap-1234567890 --second-snapshot-
id snap-0987654321 --starting-block-index 0 --max-results 500
```

以下为上一个命令的示例响应，其中显示了两个快照的数据块索引 0、6000、6001、6002 和 6003 存在不同。此外，数据块索引 6001、6002 和 6003 仅存在于指定的第一个快照 ID 中，而不存在于第二个快照 ID 中，因为响应中没有列出第二个数据块令牌。

使用 get-snapshot-block 命令，请指定要获取其数据的数据块的数据块索引和数据块令牌。数据块令牌在列出的过期时间之前有效。

```
{
      "ChangedBlocks": [
          {
              "BlockIndex": 0,
              "FirstBlockToken": "AAABAVahm9SO60Dyi0ORySzn2ZjGjW/
KN3uygGlS0QOYWesbzBbDnX2dGpmC",
              "SecondBlockToken":
 "AAABAf8o0o6UFi1rDbSZGIRaCEdDyBu9TlvtCQxxoKV8qrUPQP7vcM6iWGSr"
          },
          {
              "BlockIndex": 6000,
              "FirstBlockToken": "AAABAbYSiZvJ0/
R9tz8suI8dSzecLjN4kkazK8inFXVintPkdaVFLfCMQsKe",
              "SecondBlockToken":
 "AAABAZnqTdzFmKRpsaMAsDxviVqEI/3jJzI2crq2eFDCgHmyNf777elD9oVR"
          },
          {
              "BlockIndex": 6001,
              "FirstBlockToken": "AAABASBpSJ2UAD3PLxJnCt6zun4/
T4sU25Bnb8jB5Q6FRXHFqAIAqE04hJoR"
          },
          {
              "BlockIndex": 6002,
              "FirstBlockToken": "AAABASqX4/
NWjvNceoyMUljcRd0DnwbSwNnes1UkoP62CrQXvn47BY5435aw"
          },
          {
              "BlockIndex": 6003,
              "FirstBlockToken":
 "AAABASmJ0O5JxAOce25rF4P1sdRtyIDsX12tFEDunnePYUKOf4PBROuICb2A"
          },
          ...
      ],
      "ExpiryTime": 1576308931.973,
      "VolumeSize": 32212254720,
      "BlockSize": 524288,
      "NextToken": "AAADARqElNng/sV98CYk/bJDCXeLJmLJHnNSkHvLzVaO0zsPH/QM3Bi3zF//
O6Mdi/BbJarBnp8h"
  }
```

Amazon API

以下ListChangedBlocks示例请求返回快照和之间不同的区块的区块索引snap-0acEXAMPLEcf41648和区块标记snap-0c9EXAMPLE1b30e2f。startingBlockIndex 参数将结果限制为索引大于 0 的数据块，并且 maxResults 参数将结果限制为前 500 个数据块。

```
GET /snapshots/snap-0c9EXAMPLE1b30e2f/changedblocks?
firstSnapshotId=snap-0acEXAMPLEcf41648&maxResults=500&startingBlockIndex=0 HTTP/1.1
  Host: ebs.us-east-2.amazonaws.com
  Accept-Encoding: identity
  User-Agent: <User agent parameter>
  X-Amz-Date: 20200617T232546Z
  Authorization: <Authentication parameter>
```

以下为上一个请求的示例响应，其中显示了两个快照的数据块索引 0、3072、6002 和 6003 存在不同。此外，数据块索引 6002 和 6003 仅存在于指定的第一个快照 ID 中，而不存在于第二个快照 ID 中，因为响应中没有列出第二个数据块令牌。

使用 GetSnapshotBlock 操作，请指定要获取其数据的数据块的数据块索引和数据块令牌。数据块令牌在列出的过期时间之前有效。

```
HTTP/1.1 200 OK
  x-amzn-RequestId: fb0f6743-6d81-4be8-afbe-db11a5bb8a1f
  Content-Type: application/json
  Content-Length: 1456
  Date: Wed, 17 Jun 2020 23:25:47 GMT
  Connection: keep-alive

  {
      "BlockSize": 524288,
      "ChangedBlocks": [
          {
              "BlockIndex": 0,
              "FirstBlockToken": "AAUBAVaWqOCnDNuKle11s7IIX6jp6FYcC/
tJuVT1GgP23AuLntwiMdJ+OJkL",
              "SecondBlockToken": "AAUBASxzy0Y0b33JVRLoYm3NOresCxn5RO+HVFzXW3Y/
RwfFaPX2Edx8QHCh"
          },
          {
              "BlockIndex": 3072,
```

```
                "FirstBlockToken":
 "AAUBAcHp6pC5fKAC7TokoNCtAnZhqq27u6fxRfZOLEmeXLmHBf2R/Yb24MaS",
                "SecondBlockToken":
 "AAUBARGCaufCqBRZC8tEkPYGGkSv3vqvOjJ2xKDi3ljDFiytUxBLXYgTmkid"
            },
            {
                "BlockIndex": 6002,
                "FirstBlockToken": "AAABASqX4/
NWjvNceoyMUljcRd0DnwbSwNnes1UkoP62CrQXvn47BY5435aw"
            },
            {
                "BlockIndex": 6003,
                "FirstBlockToken":
 "AAABASmJ0O5JxAOce25rF4P1sdRtyIDsX12tFEDunnePYUKOf4PBROuICb2A"
            },
            ...
        ],
        "ExpiryTime": 1.592976647009E9,
        "VolumeSize": 3
    }
```

从快照获取数据块数据

Amazon CLI

以下get-snapshot-block示例命令以快照形式返回区块索引中6001带有区块令牌AAABASBpSJ2UAD3PLxJnCt6zun4/T4sU25Bnb8jB5Q6FRXHFqAIAqE04hJoR的数据snap-1234567890。在 Windows 计算机上，二进制数据将输出到 data 目录中的 C:\Temp 文件。如果您在 Linux 或 Unix 计算机上运行该命令，请将输出路径替换为 /tmp/data 以将数据输出到 data 目录中的 /tmp 文件。

```
aws ebs get-snapshot-block --snapshot-id snap-1234567890 --block-index 6001 --block-
token AAABASBpSJ2UAD3PLxJnCt6zun4/T4sU25Bnb8jB5Q6FRXHFqAIAqE04hJoR C:/Temp/data
```

以下为上一个命令的示例响应，其中显示了返回的数据的大小、用于验证数据的校验和以及校验和的算法。二进制数据会自动保存到您在请求命令中指定的目录和文件中。

```
{
      "DataLength": "524288",
      "Checksum": "cf0Y6/Fn0oFa4VyjQPOa/iD0zhTflPTKzxGv2OKowXc=",
      "ChecksumAlgorithm": "SHA256"
```

```
  }
```

Amazon API

以下GetSnapshotBlock示例请求以快照形式返回区块索引中3072带有区块令牌AAUBARGCaufCqBRZC8tEkPYGGkSv3vqvOjJ2xKDi3ljDFiytUxBLXYgTmkid的数据snap-0c9EXAMPLE1b30e2f。

```
GET /snapshots/snap-0c9EXAMPLE1b30e2f/blocks/3072?
blockToken=AAUBARGCaufCqBRZC8tEkPYGGkSv3vqvOjJ2xKDi3ljDFiytUxBLXYgTmkid HTTP/1.1
  Host: ebs.us-east-2.amazonaws.com
  Accept-Encoding: identity
  User-Agent: <User agent parameter>
  X-Amz-Date: 20200617T232838Z
  Authorization: <Authentication parameter>
```

以下为上一个请求的示例响应，其中显示了返回的数据的大小、用于验证数据的校验和以及用于生成校验和的算法。二进制数据在响应正文中传输，如下例所BlockData示。

```
HTTP/1.1 200 OK
  x-amzn-RequestId: 2d0db2fb-bd88-474d-a137-81c4e57d7b9f
  x-amz-Data-Length: 524288
  x-amz-Checksum: Vc0yY2j3qg8bUL9I6GQuI2orTudrQRBDMIhcy7bdEsw=
  x-amz-Checksum-Algorithm: SHA256
  Content-Type: application/octet-stream
  Content-Length: 524288
  Date: Wed, 17 Jun 2020 23:28:38 GMT
  Connection: keep-alive

  BlockData
```

使用 EBS Direct 写入亚马逊 EBS 快照 APIs

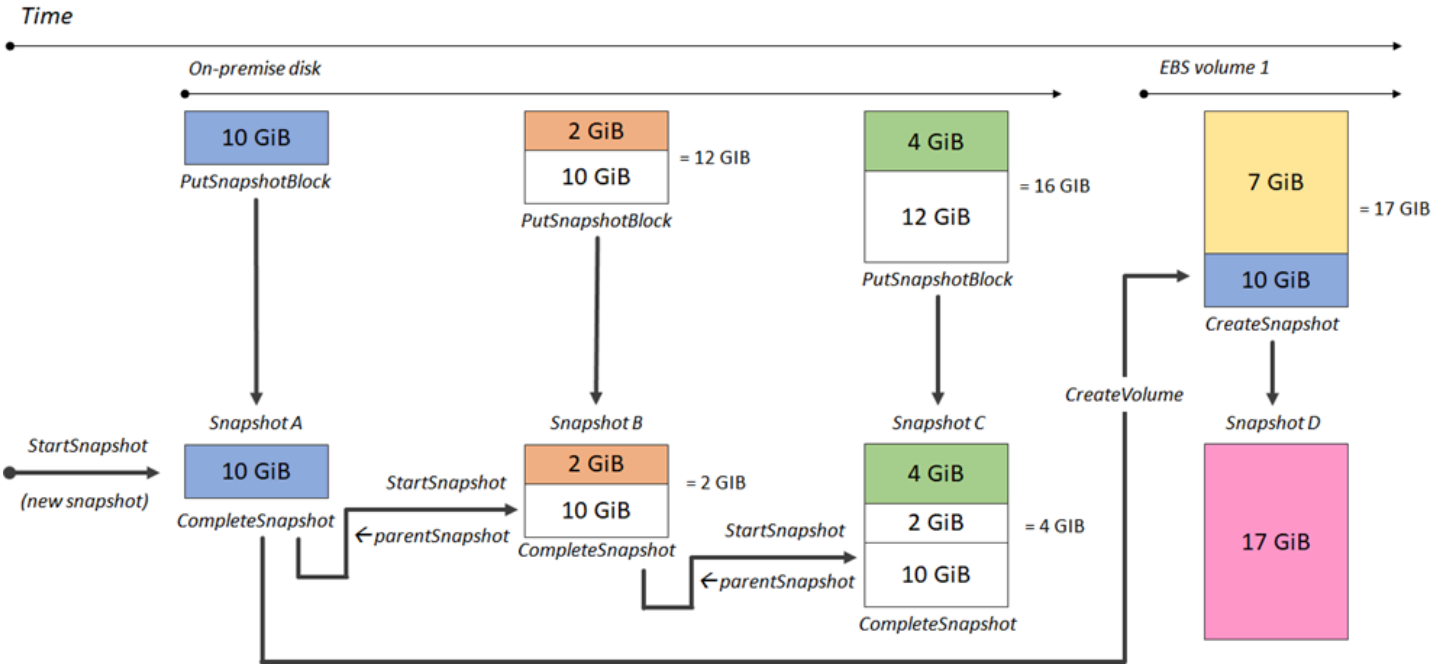
以下步骤介绍如何使用 EBS Direct 写入 APIs 增量快照：

1. 使用 StartSnapshot 操作并指定父快照 ID 将快照作为现有快照的增量快照启动，或者省略父快照 ID 以启动新快照。此操作返回处于“待处理”状态的新快照 ID。
2. 使用 PutSnapshotBlock 操作并指定待处理快照的 ID，以单个块的形式向其中添加数据。必须为传输的数据块指定 Base64 编码的 SHA256校验和。服务将计算接收到的数据的校验和，并使用您指定的校验和对其进行验证。如果校验和不匹配，则操作失败。

3. 向待处理快照添加数据后，使用 CompleteSnapshot操作启动异步工作流程，该工作流程将快照封存起来并将其移至已完成状态。

重复这些步骤，使用之前创建的快照作为父级创建新的增量快照。

例如，在下图中，快照 A 是启动的第一个新快照。快照 A 用作父快照来启动快照 B。快照 B 用作父快照来启动和创建快照 C。快照 A、B 和 C 均为增量快照。快照 A 用于创建 EBS 卷 1。快照 D 创建自 EBS 卷 1。快照 D 是 A 的增量快照；它不是 B 或 C 的增量快照。



以下示例说明如何使用 EBS Dire APIs ct 写入快照。

主题

- 启动快照
- 将数据放入快照
- 完成快照

启动快照

Amazon CLI

以下 start-snapshot 示例命令启动 8 GiB 快照，使用快照 snap-123EXAMPLE1234567 作为父快照。新快照将是父快照的增量快照。如果在指定的 60 分钟超时期限内，没有针对快照发出放置或

完成请求，则快照将转为错误状态。550e8400-e29b-41d4-a716-446655440000 客户端令牌确保请求的幂等性。如果省略了客户端令牌， Amazon SDK 会自动为您生成一个。有关幂等性的更多信息，请参阅 确保 API 请求中的等性 StartSnapshot 。

```
aws ebs start-snapshot --volume-size 8 --parent-snapshot snap-123EXAMPLE1234567 --
timeout 60 --client-token 550e8400-e29b-41d4-a716-446655440000
```

以下为上一个命令的示例响应，其中显示了快照 ID、 Amazon 账户 ID、状态、卷大小（以 GiB 为单位）以及快照中数据块的大小。快照以 pending 状态启动。在后续 put-snapshot-block 命令中指定快照 ID 以将数据写入快照，然后使用 complete-snapshot 命令完成快照并将其状态更改为 completed。

```
{
    "SnapshotId": "snap-0aaEXAMPLEe306d62",
    "OwnerId": "111122223333",
    "Status": "pending",
    "VolumeSize": 8,
    "BlockSize": 524288
}
```

Amazon API

以下StartSnapshot示例请求使用快照snap-123EXAMPLE1234567作为父快照启动 8 GiB 快照。新快照将是父快照的增量快照。如果在指定的 60 分钟超时期限内，没有针对快照发出放置或完成请求，则快照将转为错误状态。550e8400-e29b-41d4-a716-446655440000 客户端令牌确保请求的幂等性。如果省略了客户端令牌， Amazon SDK 会自动为您生成一个。有关幂等性的更多信息，请参阅 确保 API 请求中的等性 StartSnapshot 。

```
POST /snapshots HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T040724Z
Authorization: <Authentication parameter>

{
    "VolumeSize": 8,
    "ParentSnapshot": snap-123EXAMPLE1234567,
    "ClientToken": "550e8400-e29b-41d4-a716-446655440000",
    "Timeout": 60
```

```
}
```

以下为上一个请求的示例响应，其中显示了快照 ID、 Amazon 账户 ID、状态、卷大小（以 GiB 为单位）以及快照中数据块的大小。快照以“待处理”状态开始。在后续 PutSnapshotBlocks 请求中指定快照 ID，以将数据写入快照。

```
HTTP/1.1 201 Created
x-amzn-RequestId: 929e6eb9-7183-405a-9502-5b7da37c1b18
Content-Type: application/json
Content-Length: 181
Date: Thu, 18 Jun 2020 04:07:29 GMT
Connection: keep-alive

{
    "BlockSize": 524288,
    "Description": null,
    "OwnerId": "138695307491",
    "Progress": null,
    "SnapshotId": "snap-052EXAMPLEc85d8dd",
    "StartTime": null,
    "Status": "pending",
    "Tags": null,
    "VolumeSize": 8
}
```

将数据放入快照

Amazon CLI

以下put-snapshot-block示例命令将524288字节的数据写入快照1000上的块索引snap-0aaEXAMPLEe306d62。Base64 编码的 QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM= 校验和使用 SHA256 算法生成。传输的数据位于 /tmp/data 文件中。

```
aws ebs put-snapshot-block --snapshot-id snap-0aaEXAMPLEe306d62
 --block-index 1000 --data-length 524288 --block-data /tmp/data --
checksum QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM= --checksum-algorithm SHA256
```

以下为上一个命令的示例响应，其中确认服务接收的数据的数据长度、校验和以及校验和算法。

```
{
    "DataLength": "524288",
    "Checksum": "QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM=",
    "ChecksumAlgorithm": "SHA256"
}
```

Amazon API

以下PutSnapshot示例请求将524288字节的数据写入快照1000上的块索引snap-052EXAMPLEc85d8dd。Base64 编码的 QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM= 校验和使用 SHA256 算法生成。数据在请求正文中传输，如下*BlockData*例所示。

```
PUT /snapshots/snap-052EXAMPLEc85d8dd/blocks/1000 HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
x-amz-Data-Length: 524288
x-amz-Checksum: QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM=
x-amz-Checksum-Algorithm: SHA256
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T042215Z
X-Amz-Content-SHA256: UNSIGNED-PAYLOAD
Authorization: <Authentication parameter>

          BlockData
```

以下为上一个请求的示例响应，其中确认服务接收的数据的数据长度、校验和以及校验和算法。

```
HTTP/1.1 201 Created
x-amzn-RequestId: 643ac797-7e0c-4ad0-8417-97b77b43c57b
x-amz-Checksum: QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM=
x-amz-Checksum-Algorithm: SHA256
Content-Type: application/json
Content-Length: 2
Date: Thu, 18 Jun 2020 04:22:12 GMT
Connection: keep-alive

{}
```

完成快照

Amazon CLI

以下 complete-snapshot 示例命令完成快照 snap-0aaEXAMPLEe306d62。该命令指定将 5 数据块写入快照。6D3nmwi5f2F0wlh7xX8QprrJBFzDX8aacdOcA3KCM3c= 校验和表示写入快照的完整数据集的校验和。有关校验和的更多信息，请参阅本指南前文中的使用 EBS 直接 APIs 校验和来验证快照数据。

```
aws ebs complete-snapshot --snapshot-id snap-0aaEXAMPLEe306d62 --changed-blocks-count 5 --checksum 6D3nmwi5f2F0wlh7xX8QprrJBFzDX8aacdOcA3KCM3c= --checksum-algorithm SHA256 --checksum-aggregation-method LINEAR
```

以下为上一个命令的示例响应。

```
{
    "Status": "pending"
}
```

Amazon API

以下CompleteSnapshot示例请求完成快照snap-052EXAMPLEc85d8dd。该命令指定将 5 数据块写入快照。6D3nmwi5f2F0wlh7xX8QprrJBFzDX8aacdOcA3KCM3c= 校验和表示写入快照的完整数据集的校验和。

```
POST /snapshots/completion/snap-052EXAMPLEc85d8dd HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
x-amz-ChangedBlocksCount: 5
x-amz-Checksum: 6D3nmwi5f2F0wlh7xX8QprrJBFzDX8aacdOcA3KCM3c=
x-amz-Checksum-Algorithm: SHA256
x-amz-Checksum-Aggregation-Method: LINEAR
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T043158Z
Authorization: <Authentication parameter>
```

以下为上一个请求的示例响应。

```
HTTP/1.1 202 Accepted
x-amzn-RequestId: 06cba5b5-b731-49de-af40-80333ac3a117
Content-Type: application/json
```

```
Content-Length: 20
Date: Thu, 18 Jun 2020 04:31:50 GMT
Connection: keep-alive

{"Status":"pending"}
```

EBS Direct 的加密结果 APIs

使用启动新快照时 StartSnapshot，加密状态取决于您为已加密、和指定的值 KmsKeyArnParentSnapshotId，以及您的 Amazon 账户是否在默认情况下启用了加密功能。

> **Note**
>
> - 您可能需要额外的 IAM 权限才能直接使用 APIs 带加密功能的 EBS。有关更多信息，请参阅使用权限 Amazon KMS keys。
> - 如果您的 Amazon 账户默认启用 Amazon EBS 加密，则无法创建未加密的快照。
> - 如果您的 Amazon 账户默认启用 Amazon EBS 加密，则无法使用未加密的父快照启动新快照。您必须首先通过复制父快照来对其进行加密。有关更多信息，请参阅 复制 Amazon EBS 快照。

主题

- 加密结果：未加密父快照
- 加密结果：已加密父快照
- 加密结果：无父快照

加密结果：未加密父快照

下表描述了指定未加密父快照时每种可能的设置组合的加密结果。

ParentSnapshotId	已加密	KmsKeyArn	默认加密	结果
未加密	已忽略	已忽略	已启用	请求失败并显示 `ValidationException` 。

ParentSnapshotId	已加密	KmsKeyArn	默认加密	结果
			已禁用	快照未加密。
		指定	已启用	
			已禁用	
未加密	True	已忽略	已启用	请求失败并显示 `ValidationException` 。
			已禁用	
		指定	已启用	
			已禁用	
未加密	False	已忽略	已启用	请求失败并显示 `ValidationException` 。
			已禁用	
		指定	已启用	
			已禁用	

加密结果：已加密父快照

下表描述了指定已加密父快照时每种可能的设置组合的加密结果。

ParentSnapshotId	已加密	KmsKeyArn	默认加密	结果
已加密	已忽略	已忽略	已启用	已使用与父快照相同的 KMS 密钥对快照进行加密。
			已禁用	
		指定	已启用	请求失败并显示 `ValidationException` 。
			已禁用	

ParentSnapshotId	已加密	KmsKeyArn	默认加密	结果
已加密	True	已忽略	已启用	请求失败并显示 `ValidationException` 。
			已禁用	
		指定	已启用	
			已禁用	
已加密	False	已忽略	已启用	请求失败并显示 `ValidationException` 。
			已禁用	
		指定	已启用	
			已禁用	

加密结果：无父快照

下表描述了未使用父快照时每种可能的设置组合的加密结果。

ParentSnapshotId	已加密	KmsKeyArn	默认加密	结果
已忽略	True	已忽略	已启用	已使用账户的默认 KMS 密钥对快照进行加密。*
			已禁用	
		指定	已启用	快照使用为指定的 KMS 密钥进行加密KmsKeyArn。
			已禁用	
已忽略	False	已忽略	已启用	请求失败并显示 `ValidationException` 。
			已禁用	快照未加密。

ParentSnapshotId	已加密	KmsKeyArn	默认加密	结果
		指定	已启用	请求失败并显示 `ValidationException` 。
			已禁用	
已忽略	已忽略	已忽略	已启用	已使用账户的默认 KMS 密钥对快照进行加密。*
			已禁用	快照未加密。
		指定	已启用	快照使用为指定的 KMS 密钥进行加密KmsKeyArn。
			已禁用	

* 此默认 KMS 密钥可以是客户托管密钥，也可以是用于 Amazon EBS 加密的默认 Amazon 托管 KMS 密钥。

使用 EBS 直接 APIs 校验和来验证快照数据

该 GetSnapshotBlock 操作返回快照块中的数据，该 PutSnapshotBlock 操作将数据添加到快照中的区块中。传输的数据块数据不在签名版本 4 签名流程中进行签名。因此，使用校验和来验证数据的完整性，如下所示：

- 当您使用 GetSnapshotBlock 操作时，响应会使用 X-amz-checkSum 标头为区块数据提供 Base64 编码的 SHA256 校验和，并使用 x-amz-checksum 算法标头为校验和算法提供校验和算法。使用返回的校验和验证数据的完整性。如果生成的校验和与 Amazon EBS 提供的校验和不匹配，您应将数据视为无效，然后重试请求。
- 使用 PutSnapshotBlock 操作时，您的请求必须使用 X-amz-checkSum 标头为区块数据提供 Base64 编码的 SHA256 校验和，以及使用 x-amz-checksum 算法标头的校验和算法。您提供的校验和将根据 Amazon EBS 生成的校验和进行验证，以验证数据的完整性。如果校验和不相符，请求将失败。
- 使用 CompleteSnapshot 操作时，您的请求可以选择为添加到快照的完整数据集提供 Base64 编码的汇 SHA256 总校验和。使用 x-amz-Checksum 标头提供校验和，使用 x-amz-Checksum-Algorithm 标头提供校验和算法，并使用 x-amz-Checksum-Aggregation-Method 标头提供校验和聚合方法。要使用线性聚合方法生成聚合校验和，请按区块索引的升序排列每个写入区块的校验和，将它们连接成单个字符串，然后使用算法生成整个字符串的校验和。 SHA256

这些操作中的校验和是签名版本 4 签名流程的一部分。

确保 API 请求中的等性 StartSnapshot

幂等性确保 API 请求仅完成一次。对于幂等请求，如果原始请求成功完成，则后续重试将返回原始成功请求的结果，它们不会有额外的影响。

StartSnapshotAPI 使用客户端令牌支持等性。客户端令牌是您在发出 API 请求时指定的唯一字符串。如果在某个 API 请求成功完成后，您使用相同的客户端令牌和相同的请求参数重试该请求，则返回原始请求的结果。如果使用相同的客户端令牌重试请求，但更改了一个或多个请求参数，则返回 `ConflictException` 错误。

如果您未指定自己的客户端令牌，则会 Amazon SDKs 自动为请求生成客户端令牌，以确保该令牌是等效的。

客户端令牌可以是包含最多 64 个 ASCII 字符的任意字符串。您不应为不同的请求重复使用相同的客户端令牌。

使用 API 使用您自己的客户端令牌发出等效 StartSnapshot 请求

指定 `ClientToken` 请求参数。

```
POST /snapshots HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T040724Z
Authorization: <Authentication parameter>

{
    "VolumeSize": 8,
    "ParentSnapshot": snap-123EXAMPLE1234567,
    "ClientToken": "550e8400-e29b-41d4-a716-446655440000",
    "Timeout": 60
}
```

要使用您自己的客户端令牌发出等效 StartSnapshot 请求，请使用 Amazon CLI

指定 `client-token` 请求参数。

```
$ C:\> aws ebs start-snapshot --region us-east-2 --volume-size 8 --parent-
snapshot snap-123EXAMPLE1234567 --timeout 60 --client-token 550e8400-e29b-41d4-
a716-446655440000
```

EBS direct 的错误重试次数 APIs

为返回错误响应的请求Amazon SDKs实现自动重试逻辑。您可以为配置重试设置。 Amazon SDKs有关更多信息，请参阅 SDK 文档。

Amazon CLI 可以配置为自动重试部分失败的请求。有关为配置重试次数的更多信息 Amazon CLI，请参阅《Amazon Command Line Interface 用户指南》中的Amazon CLI 重试。

Amazon 查询 API 不支持失败的请求的重试逻辑。如果您使用的是 HTTP 或 HTTPS 请求，则必须在客户端应用程序中实现重试逻辑。

下表显示了可能的 API 错误响应。部分 API 错误是可重试的。客户端应用程序始终可以重试收到可重试错误的失败请求。

错误	响应代码	描述	由以下对象引发	可重试？
`InternalServerException`	500	由于网络或 Amazon 服务器端问题，请求失败。	全部 APIs	是
`ThrottlingException`	400	API 请求的数量已超过账户允许的最大 API 请求节流限制。	全部 APIs	是
`RequestThrottleException`	400	API 请求的数量已超过快照允许的最大 API 请求节流限制。	GetSnapshotBlock | PutSnapshotBlock	是
显示消息“`Failed to read`	400	提供的数据块不可读。	PutSnapshotBlock	是

错误	响应代码	描述	由以下对象引发	可重试？
block data”的 ValidationException				
显示任何其他消息的 ValidationException	400	请求语法格式错误，或输入不满足 Amazon Web Services 服务规定的约束。	全部 APIs	否
ResourceNotFoundException	404	指定的快照 ID 不存在。	全部 APIs	否
ConflictException	409	指定的客户端令牌曾在具有不同请求参数的类似请求中使用过。有关更多信息，请参阅 确保 API 请求中的等性 StartSnapshot 。	StartSnapshot	否
AccessDeniedException	403	您无权执行请求的操作。	全部 APIs	否
ServiceQuotaExceededException	402	请求失败，因为执行请求将超出您账户的一项或多项相关服务限额。	全部 APIs	否

错误	响应代码	描述	由以下对象引发	可重试？
InvalidSignatureException	403	请求授权签名已过期。必须刷新授权签名才能重试请求。	全部 APIs	否

优化 EBS Direct 的性能 APIs

您可以并发运行 API 请求。假设 PutSnapshotBlock 延迟为 100 毫秒，则一个线程可以在一秒钟内处理 10 个请求。此外，假设您的客户端应用程序创建多个线程和连接（例如 100 个连接），那么它每秒可以发出 1000（10 * 100）个请求。这对应于大约每秒 500 MB 的吞吐量。

以下列表包含在您应用程序中需要了解的几点：

- 每个线程是否使用单独的连接？ 如果应用程序上的连接受限制，则多线程将等待可用连接，而您会发现吞吐量较低。
- 应用程序的两个放置请求之间是否有任何等待时间？ 这将降低线程的有效吞吐量。
- 实例的带宽限制-如果实例上的带宽由其他应用程序共享，则可能会限制 PutSnapshotBlock请求的可用吞吐量。

请确保注意账户中可能运行的其他工作负载，以避免瓶颈。您还应该在 EBS 直接 APIs 工作流程中构建重试机制，以处理限制、超时和服务不可用。

查看 EBS 直接 APIs 服务配额，确定每秒可以运行的最大 API 请求数。有关更多信息，请参阅 Amazon 一般参考 中的 Amazon Elastic Block Store 终端节点和配额。

EBS Direct 的服务端点 APIs

端点是用作 Amazon Web 服务入口点的 URL。EBS Direct APIs 支持以下终端节点类型：

- IPv4 端点
- 同时 IPv4 支持和的双栈端点 IPv6

当您发出请求时，您可以指定要使用的端点和区域。如果您未指定终端节点，则默认使用该 IPv4 终端节点。要使用不同的端点类型，您必须在请求中指定。有关如何执行此操作的示例，请参阅指定端点。

有关区域的更多信息，请参阅 Amazon EC2 用户指南中的区域和可用区。有关 EBS direct 的终端节点列表 APIs，请参阅 APIs中的 EBS 直接终端节点。Amazon Web Services 一般参考

主题

- IPv4 端点
- 双栈（IPv4 和 IPv6）端点
- 指定端点

IPv4 端点

IPv4 端点仅支持 IPv4 流量。 IPv4 终端节点适用于所有区域。

EBS Direct 仅 APIs 支持可用于发出请求的区域 IPv4 终端节点。您必须将区域指定为端点名称的一部分。端点名称使用以下命名约定：

- `ebs.region.amazonaws.com.cn`

例如，北京区域的 IPv4 终端节点名称为`ebs.cn-northwest-1.amazonaws.com.cn`。

定价

您无需为使用同一地区的 IPv4 终端节点在 EBS Direct APIs 和 Amazon EC2 实例之间直接传输数据付费。但是，如果有中间服务，例如 Amazon PrivateLink 终端节点、NAT 网关或 Amazon VPC 传输网关，则需要向您收取相关费用。

双栈（IPv4 和 IPv6）端点

双栈端点同时支持 IPv4 和 IPv6 流量。双堆栈端点适用于所有区域。

要使用 IPv6，必须使用双堆栈终端节点。当您向双栈终端节点发出请求时，终端节点 URL 会解析为 IPv6 或 IPv4 地址，具体取决于您的网络和客户端使用的协议。

EBS Direct 仅 APIs 支持区域双栈终端节点，这意味着您必须在终端节点名称中指定区域。双堆栈端点名称使用以下命名约定：

- `ebs.region.api.amazonwebservices.com.cn`

例如，北京区域的双堆栈端点名称为 `ebs.cn-northwest-1.api.aws`。

定价

对于在同一区域使用双堆栈终端节点在 EBS Direct APIs 和 Amazon EC2 实例之间直接传输数据，您无需支付任何费用。但是，如果有中间服务，例如 Amazon PrivateLink 终端节点、NAT 网关或 Amazon VPC 传输网关，则需要向您收取相关费用。

指定端点

本节提供了一些在发出请求时如何指定端点的示例。

Amazon CLI

以下示例显示如何使用 Amazon CLI为北京区域指定端点。

- 双堆栈

```
aws ebs list-snapshot-blocks --snapshot-id snap-0987654321 --starting-block-index
 1000 --endpoint-url https://ebs.cn-northwest-1.api.amazonwebservices.com.cn
```

- IPv4

```
aws ebs list-snapshot-blocks --snapshot-id snap-0987654321 --starting-block-index
 1000 --endpoint-url https://ebs.cn-northwest-1.amazonaws.com.cn
```

Amazon SDK for Java 2.x

以下示例显示如何使用 Amazon SDK for Java 2.x为北京区域指定端点。

- 双堆栈

```
AwsClientBuilder.EndpointConfiguration config = new
 AwsClientBuilder.EndpointConfiguration("https://ebs.cn-
northwest-1.api.amazonwebservices.com.cn", "cn-northwest-1");
AmazonEBS ebs = AmazonEBSClientBuilder.standard()
    .withEndpointConfiguration(config)
    .build();
```

- IPv4

```
AwsClientBuilder.EndpointConfiguration config = new
 AwsClientBuilder.EndpointConfiguration("https://ebs.cn-
northwest-1.amazonaws.com.cn", "cn-northwest-1");
AmazonEBS ebs = AmazonEBSClientBuilder.standard()
    .withEndpointConfiguration(config)
    .build();
```

Amazon SDK for Go

以下示例显示如何使用 适用于 Go 的 Amazon SDK为北京区域指定端点。

- 双堆栈

```
sess := session.Must(session.NewSession())
svc := ebs.New(sess, &aws.Config{
    Region: aws.String(endpoints.CnNorth1RegionID),
    Endpoint: aws.String("https://ebs.cn-
northwest-1.api.amazonwebservices.com.cn")
})
```

- IPv4

```
sess := session.Must(session.NewSession())
svc := ebs.New(sess, &aws.Config{
    Region: aws.String(endpoints.CnNorth1RegionID),
    Endpoint: aws.String("https://ebs.cn-northwest-1.amazonaws.com.cn")
})
```

Amazon EBS Direct 的 SDK 代码示例 APIs

以下代码示例演示如何将 EBS 直接 APIs 与 Amazon 软件开发套件 (SDK) 配合使用。

操作

- StartSnapshot与 Amazon SDK 或 CLI 配合使用
- PutSnapshotBlock与 Amazon SDK 或 CLI 配合使用
- CompleteSnapshot与 Amazon SDK 或 CLI 配合使用

`StartSnapshot`与 Amazon SDK 或 CLI 配合使用

以下代码示例演示如何使用 `StartSnapshot`。

Rust

适用于 Rust 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
async fn start(client: &Client, description: &str) -> Result<String, Error> {
    let snapshot = client
        .start_snapshot()
        .description(description)
        .encrypted(false)
        .volume_size(1)
        .send()
        .await?;

    Ok(snapshot.snapshot_id.unwrap())
}
```

- 有关 API 的详细信息，请参阅适用StartSnapshot于 Rust 的Amazon SDK API 参考。

`PutSnapshotBlock`与 Amazon SDK 或 CLI 配合使用

以下代码示例演示如何使用 `PutSnapshotBlock`。

Rust

适用于 Rust 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
async fn add_block(
    client: &Client,
    id: &str,
    idx: usize,
    block: Vec<u8>,
    checksum: &str,
) -> Result<(), Error> {
    client
        .put_snapshot_block()
        .snapshot_id(id)
        .block_index(idx as i32)
        .block_data(ByteStream::from(block))
        .checksum(checksum)
        .checksum_algorithm(ChecksumAlgorithm::ChecksumAlgorithmSha256)
        .data_length(EBS_BLOCK_SIZE as i32)
        .send()
        .await?;

    Ok(())
}
```

- 有关 API 的详细信息，请参阅适用PutSnapshotBlock于 Rust 的Amazon SDK API 参考。

`CompleteSnapshot`与 Amazon SDK 或 CLI 配合使用

以下代码示例演示如何使用 `CompleteSnapshot`。

Rust

适用于 Rust 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。查找完整示例，学习如何在 Amazon 代码示例存储库中进行设置和运行。

```
async fn finish(client: &Client, id: &str) -> Result<(), Error> {
    client
        .complete_snapshot()
        .changed_blocks_count(2)
        .snapshot_id(id)
        .send()
        .await?;

    println!("Snapshot ID {}", id);
    println!("The state is 'completed' when all of the modified blocks have been
 transferred to Amazon S3.");
    println!("Use the get-snapshot-state code example to get the state of the
 snapshot.");

    Ok(())
}
```

- 有关 API 的详细信息，请参阅适用CompleteSnapshot于 Rust 的Amazon SDK API 参考。

在 VPC 和 EBS Direct 之间创建私有连接 APIs

您可以通过创建由提供支持的接口 VPC 终端节点在您的 VPC 和 Amazon EBS 之间建立私有连接。Amazon PrivateLink您可以像在您的 VPC 中一样访问 Amazon EBS，无需使用互联网网关、NAT 设备、VPN 连接或 Amazon Direct Connect 连接。您的 VPC 中的实例不需要公有 IP 地址即可与 Amazon EBS 通信。

我们将在您为接口端点启用的每个子网中创建一个端点网络接口。

有关更多信息，请参阅Amazon PrivateLink 指南 Amazon PrivateLink中的Amazon Web Services 服务通过访问。

亚马逊 EBS VPC 终端节点的注意事项

在为 Amazon EBS 设置接口 VPC 终端节点之前，请查看Amazon PrivateLink 指南中的注意事项。

默认情况下，允许通过终端节点对 Amazon EBS 进行完全访问。您可以使用 VPC 端点策略控制对接口端点的访问。您可以将终端节点策略附加到控制对 Amazon EBS 的访问权限的 VPC 终端节点。该策略指定以下信息：

- 可执行操作的主体。
- 可执行的操作。
- 可对其执行操作的资源。

有关更多信息，请参阅 Amazon VPC 用户指南中的使用 VPC 终端节点控制对服务的访问。

以下是 Amazon EBS 的终端节点策略示例。当连接到终端节点时，此策略允许访问所有资源上的所有 Amazon EBS 操作，但标有密钥`Environment`和值`Test`的快照除外。

```
{
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "ebs:*",
            "Principal": "*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Environment": "Test"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ebs:*",
            "Principal": "*",
            "Resource": "*"
        }
    ]
```

```
}
```

为 Amazon EBS 创建接口 VPC 终端节点

您可以使用亚马逊 VPC 控制台或 Amazon Command Line Interface (Amazon CLI) 为 Amazon EBS 创建 VPC 终端节点。有关更多信息，请参阅 Amazon PrivateLink 指南中的创建 VPC 终端节点。

使用以下服务名称为 Amazon EBS 创建 VPC 终端节点：

- `com.amazonaws.region.ebs`

例如，如果您为终端节点启用私有 DNS，则可以使用该区域的默认 DNS 名称向 Amazon EBS 发出 API 请求。`ebs.us-east-1.amazonaws.com`

使用记录 EBS 直接 APIs 呼叫 Amazon CloudTrail

Amazon EBS 与 Amazon CloudTrail一项服务集成，可记录用户、角色或 Amazon 服务所采取的操作。 CloudTrail 将拨打 Amazon EBS 的呼叫记录为事件。捕获的呼叫包括来自的调用 Amazon Web Services Management Console 和对 Amazon EBS 的代码调用。使用收集的信息 CloudTrail，您可以确定向 Amazon EBS 发出的请求、发出请求的 IP 地址、发出请求的时间以及其他详细信息。

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。

CloudTrail 在您创建账户 Amazon Web Services 账户 时在您的账户中处于活动状态，并且您自动可以访问 CloudTrail 活动历史记录。 CloudTrail 事件历史记录提供了过去 90 天中记录的管理事件的可查看、可搜索、可下载且不可变的记录。 Amazon Web Services 区域有关更多信息，请参阅《Amazon CloudTrail 用户指南》中的 “使用 CloudTrail 事件历史记录”。查看活动历史记录不 CloudTrail收取任何费用。

要持续记录 Amazon Web Services 账户 过去 90 天内的事件，请创建跟踪或 CloudTrailLake 事件数据存储。

CloudTrail 步道

跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。使用创建的所有跟踪 Amazon Web Services Management Console 都是多区域的。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，因为您可以捕获账户 Amazon Web Services 区域 中的所有活动。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，您可以免费将正在进行的管理事件的一份副本传送到您的 Amazon S3 存储桶，但是，会收取 Amazon S3 存储费用。 CloudTrail 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 湖泊事件数据存储

CloudTrail L@@ ak e 允许你对自己的事件运行基于 SQL 的查询。 CloudTrail Lake 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 湖泊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。

中的 Amazon EBS 数据事件 CloudTrail

数据事件提供有关对在资源上或资源内执行的资源操作的信息。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 控制台或 CloudTrail API 操作记录 Amazon EBS 资源类型的数据事件。Amazon CLI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。

您可以将以下 Amazon EBS 操作记录为数据事件。

- ListSnapshotBlocks
- ListChangedBlocks
- GetSnapshotBlock
- PutSnapshotBlock

> **Note**
>
> 如果您对与您共享的快照执行操作，则不会将数据事件发送到拥有该快照的 Amazon 账户。

中的 Amazon EBS 管理事件 CloudTrail

管理事件提供有关对中的资源执行的管理操作的信息 Amazon Web Services 账户。这些也称为控制面板操作。默认情况下， CloudTrail 记录管理事件。

Amazon EBS 服务将以下控制平面操作记录 CloudTrail 为管理事件。

- StartSnapshot
- CompleteSnapshot

亚马逊 EBS 事件示例

事件代表来自任何来源的单个请求，包括有关所请求的 API 操作、操作的日期和时间、请求参数等的信息。 CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此事件不会按任何特定顺序出现。

以下是 EBS direc APIs t 的示例 CloudTrail 事件。

StartSnapshot

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
```

```
    },
    "eventTime": "2020-07-03T23:27:26Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "StartSnapshot",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "PostmanRuntime/7.25.0",
    "requestParameters": {
        "volumeSize": 8,
        "clientToken": "token",
        "encrypted": true
    },
    "responseElements": {
        "snapshotId": "snap-123456789012",
        "ownerId": "123456789012",
        "status": "pending",
        "startTime": "Jul 3, 2020 11:27:26 PM",
        "volumeSize": 8,
        "blockSize": 524288,
        "kmsKeyArn": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "requestID": "be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",
    "eventID": "6e12345-2a4e-417c-aa78-7594fEXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```

CompleteSnapshot

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2020-07-03T23:28:24Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "CompleteSnapshot",
    "awsRegion": "eu-west-1",
```

```
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "PostmanRuntime/7.25.0",
    "requestParameters": {
        "snapshotId": "snap-123456789012",
        "changedBlocksCount": 5
    },
    "responseElements": {
        "status": "completed"
    },
    "requestID": "be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",
    "eventID": "6e12345-2a4e-417c-aa78-7594fEXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```

ListSnapshotBlocks

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAT4HPB2AO3JEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2021-06-03T00:32:46Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "ListSnapshotBlocks",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "111.111.111.111",
    "userAgent": "PostmanRuntime/7.28.0",
    "requestParameters": {
        "snapshotId": "snap-abcdef01234567890",
        "maxResults": 100,
        "startingBlockIndex": 0
    },
    "responseElements": null,
    "requestID": "example6-0e12-4aa9-b923-1555eexample",
    "eventID": "example4-218b-4f69-a9e0-2357dexample",
    "readOnly": true,
    "resources": [
```

```
        {
            "accountId": "123456789012",
            "type": "AWS::EC2::Snapshot",
            "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-SHA",
        "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
    }
}
```

ListChangedBlocks

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAT4HPB2AO3JEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2021-06-02T21:11:46Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "ListChangedBlocks",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "111.111.111.111",
    "userAgent": "PostmanRuntime/7.28.0",
    "requestParameters": {
        "firstSnapshotId": "snap-abcdef01234567890",
        "secondSnapshotId": "snap-9876543210abcdef0",
        "maxResults": 100,
        "startingBlockIndex": 0
    },
    "responseElements": null,
    "requestID": "example0-f4cb-4d64-8d84-72e1bexample",
```

```
    "eventID": "example3-fac4-4a78-8ebb-3e9d3example",
    "readOnly": true,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::EC2::Snapshot",
            "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
        },
       {
            "accountId": "123456789012",
            "type": "AWS::EC2::Snapshot",
            "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-9876543210abcdef0"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-SHA",
        "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
    }
}
```

GetSnapshotBlock

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAT4HPB2AO3JEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2021-06-02T20:43:05Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "GetSnapshotBlock",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "111.111.111.111",
    "userAgent": "PostmanRuntime/7.28.0",
```

```
    "requestParameters": {
        "snapshotId": "snap-abcdef01234567890",
        "blockIndex": 1,
        "blockToken": "EXAMPLEiL5E3pMPFpaDWjExM2/mnSKh1mQfcbjwe2mM7EwhrgCdPAEXAMPLE"
    },
    "responseElements": null,
    "requestID": "examplea-6eca-4964-abfd-fd9f0example",
    "eventID": "example6-4048-4365-a275-42e94example",
    "readOnly": true,
    "resources": [
        {
          "accountId": "123456789012",
          "type": "AWS::EC2::Snapshot",
          "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-SHA",
        "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
    }
}
```

PutSnapshotBlock

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAT4HPB2AO3JEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2021-06-02T21:09:17Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "PutSnapshotBlock",
    "awsRegion": "us-east-1",
```

```
    "sourceIPAddress": "111.111.111.111",
    "userAgent": "PostmanRuntime/7.28.0",
    "requestParameters": {
        "snapshotId": "snap-abcdef01234567890",
        "blockIndex": 1,
        "dataLength": 524288,
        "checksum": "exampleodSGvFSb1e3kxWUgbOQ4TbzPurnsfVexample",
        "checksumAlgorithm": "SHA256"
    },
    "responseElements": {
        "checksum": "exampleodSGvFSb1e3kxWUgbOQ4TbzPurnsfVexample",
        "checksumAlgorithm": "SHA256"
    },
    "requestID": "example3-d5e0-4167-8ee8-50845example",
    "eventID": "example8-4d9a-4aad-b71d-bb31fexample",
    "readOnly": false,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::EC2::Snapshot",
            "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-SHA",
        "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
    }
}
```


有关 CloudTrail 录音内容的信息，请参阅《Amazon CloudTrail 用户指南》中的CloudTrail录制内容。

EBS direct 的常见问题解答 APIs

APIs 如果快照处于待处理状态，能否使用 EBS Direct 访问该快照？

不可以。仅当快照具有已完成状态时，才能访问该快照。

EBS 直接 APIs 返回的区块索引是否按数字顺序排列？

是。返回的数据块索引是唯一的，并按数字顺序排列。

我能否提交 MaxResults 参数值低于 100 的请求？

不是。 您可以使用的最小 MaxResult 参数值为 100。如果您提交的请求 MaxResult 参数值低于 100，并且快照中有超过 100 个区块，则 API 将返回至少 100 个结果。

我是否可以并发运行 API 请求？

您可以并发运行 API 请求。请确保注意账户中可能运行的其他工作负载，以避免瓶颈。您还应该在 EBS 直接 APIs 工作流程中构建重试机制，以处理限制、超时和服务不可用。有关更多信息，请参阅 优化 EBS Direct 的性能 APIs。

查看 EBS 直接 APIs 服务配额以确定每秒可以运行的 API 请求。有关更多信息，请参阅 Amazon 一般参考 中的 Amazon Elastic Block Store 终端节点和配额。

运行 ListChangedBlocks 操作时，即使快照中有块，是否也可能得到空响应？

是。如果快照中几乎没有更改的数据块，则响应可能为空，但 API 将返回下一页令牌值。使用下一页令牌值来继续转到下一页结果。当 API 返回的下一页令牌值为 null 时，您可以确认已到达最后一页结果。

如果 NextToken 参数与参数一起指定，则使用两者中的哪一个 StartingBlockIndex ？

使用 NextToken 了，而忽略 StartingBlockIndex 了。

数据块令牌和下一个令牌的有效期是多久？

数据块令牌的有效期为七天，下一个令牌的有效期为 60 分钟。

是否支持已加密快照？

是。可以使用 EBS 直接 APIs访问加密快照。

要访问加密快照，用户必须有权访问用于加密快照的 KMS 密钥和 Amazon KMS 解密操作。有关分配给用户的 Amazon KMS 策略，请参阅本指南前 APIs 使用 IAM 直接控制对 EBS 的访问权限面的部分。

是否支持公有快照？

不支持公有快照。

是否 Amazon Outposts 支持开启 Amazon EBS 本地快照？

不支持开启 Amazon Outposts 的 Amazon EBS 本地快照。

list snapshot block 是返回快照中的所有数据块索引和数据块令牌，还是仅返回那些写入数据的数据块索引和数据块令牌？

它只返回写入数据的数据块索引和令牌。

我能否直接在我的账户 APIs 上获取 EBS 调用的历史记录，用于安全分析和操作故障排除？

是。要接收使用您的账户进行的 EBS 直接 APIs API 调用的历史记录，请打开 Amazon CloudTrail 。 Amazon Web Services Management Console有关更多信息，请参阅 使用记录 EBS 直接 APIs 呼叫 Amazon CloudTrail。

使用回收站恢复已删除的 Amazon EBS 快照和 EBS 支持的 AMIs 快照

回收站是一项数据恢复功能，可让您恢复意外删除的 Amazon EBS 快照和 E AMIs BS 支持的快照。使用回收站时，如果资源被删除，回收站功能将在您指定的时间段内保留快照，而后永久删除资源。

在资源保留期到期之前，您可以随时从回收站还原资源。从回收站还原资源后，资源将从回收站中删除，您可以像使用账户中任何该类型的其他资源的一样使用此资源。如果保留期过期且资源未还原，则资源将从回收站中永久删除，并且不再可用于恢复。

使用回收站可以保护业务关键型数据免遭意外删除，从而确保业务连续性。

主题

- 支持的资源
- 回收站是如何运作的？
- 回收站的注意事项
- 限额
- 相关服务
- 定价
- 使用 IAM 控制对回收站的访问
- 创建回收站保留规则
- 更新现有回收站保留规则
- 锁定回收站保留规则以防止其被更新或删除
- 解锁回收站保留规则以允许更新或删除它
- 为回收站保留规则添加标签
- 删除回收站保留规则以阻止其保留资源
- 从回收站恢复已删除的快照
- 恢复 AMIs 从回收站中删除的内容
- 使用 Amazon 监控回收站 EventBridge
- 使用监控回收站 Amazon CloudTrail
- 回收站的服务端点
- 在 VPC 和回收站之间创建私有连接

支持的资源

回收站支持以下资源类型：

- Amazon EBS 快照

> **Important**
>
> 回收站保留规则也适用于归档存储层中的已归档快照。如果删除与回收站保留规则匹配的已归档快照，则该快照将在保留规则定义的保留期内保留在回收站中。归档的快照在回收站中时，按归档快照的费率计费。

- 亚马逊 EBS 支持的亚马逊机器映像 () AMIs

> **Note**
>
> 保留规则也适用于禁用 AMIs。

回收站是如何运作的？

要启用和使用回收站，您必须在要保护资源的 Amazon 区域中创建保留规则。保留规则指定以下内容：

- 您要保护的资源类型（快照或 AMIs）。
- 保留规则的类型：
  - 标签级保留规则-这些保留规则使用资源标签来标识要保护的资源。对于每个保留规则，您可以指定一个或多个标签键和值对。至少具有其中一个标签键和值对的资源（指定类型）将在删除后自动保留在回收站中。使用这种类型的保留规则，根据标签保护您账户中的特定资源。
  - 区域级保留规则-默认情况下，这些保留规则适用于该区域中的所有资源（指定类型），即使这些资源未被标记。但是，您可以指定排除标签来排除具有特定标签的资源。使用这种类型的保留规则来保护区域中特定类型的所有资源。
- 资源被删除后保留的保留期。在此期限到期后，资源将从回收站中永久删除。

如果资源在回收站中，您可以随时将其还原以供使用。资源会保留在回收站中，直到发生以下情况之一：

- 您手动还原它以供使用。从回收站还原资源时，该资源将从回收站中删除，并立即可供使用。您可以像使用账户中该类型的任何其他资源一样，使用还原的资源。
- 保留期到期。如果保留期过期且资源未从回收站中还原，则资源将从回收站中永久删除，并且不再可查看或还原。

回收站的注意事项

使用回收站和保留规则时，需要考虑以下注意事项。

一般注意事项

- 只有当已删除的资源符合现有保留规则时，才会将其移至回收站。如果您删除的资源与保留规则不符，或者您当时没有任何保留规则，则该资源将被永久删除；它不会被移到回收站。
-

> **Important**
>
> 创建首个保留规则时，规则最多需要 30 分就能生效并开始保留资源。创建首个保留规则后，后续保留规则几乎立即会生效并开始保留资源。

- 如果资源在删除时与多个保留规则匹配，则保留期最长的保留规则优先。
- 您无法手动从回收站中删除资源。资源会在其保留期过期时自动删除。
- 如果资源在回收站中，您只能查看、还原或修改其标签。要以任何方式使用资源，您必须首先将其还原。
- 如果有任何 Amazon Web Services 服务资源（例如 Amazon Backup 或 Amazon Data Lifecycle Manager）删除了符合保留规则的资源，则回收站会自动保留该资源。如果需要，您可以通过标记这些资源，然后将这些标签作为排除标签添加到保留规则中，来防止这些资源在删除后进入回收站。
- 将资源发送到回收站时，将为该资源分配以下系统生成标签：
  - 标签键：`aws:recycle-bin:resource-in-bin`
  - 标签值：`true`

  您无法手动编辑或删除此标签。从回收站还原资源时，标签将自动删除。

快照注意事项

- > **Important**
  >
  > 如果您对 AMIs 关联的快照制定了保留规则，请使快照的保留期等于或长于的保留期 AMIs。这可确保回收站在删除 AMI 之前不会删除与 AMI 关联的快照，避免 AMI 无法恢复。

- 如果在删除快照时启用了快速快照还原功能，则在快照发送到回收站后不久将自动禁用快照还原。
  - 如果您在快速快照还原被禁用前还原快照，则该快照将保持启用状态。
  - 如果您在快速快照还原被禁用后还原快照，则该快照将保持禁用状态。如果有需要，您必须手动重新启用快速快照还原。
- 如果在删除时共享快照，则将在发送到回收站时自动取消共享。如果还原快照，则会自动恢复以前的所有共享权限。
- 如果将由其他 Amazon 服务创建的快照（例如 Amazon Backup ）发送到回收站，而您随后从回收站恢复了该快照，则该快照将不再由创建该快照的 Amazon 服务管理。如果不再需要快照，则必须手动删除该快照。

的注意事项 AMIs

- 仅支持 Amazon EBS 支持 AMIs 。
- > **Important**
  >
  > 如果您对 AMIs 关联的快照制定了保留规则，请使快照的保留期等于或长于的保留期 AMIs。这可确保回收站在删除 AMI 之前不会删除与 AMI 关联的快照，避免 AMI 无法恢复。

- 如果在删除时共享 AMI，则将在发送到回收站时自动取消共享。如果还原 AMI，则会自动恢复以前的所有共享权限。
- 您必须首先从回收站还原所有与 AMI 关联的快照，并确保其处于 `available` 状态，然后才可以从回收站还原 AMI。
- 如果将与 AMI 关联的快照从回收站中删除，则 AMI 将无法恢复。保留期到期后，AMI 将被删除。
- 如果由其他 Amazon 服务（例如 Amazon Backup）创建的 AMI 被发送到回收站，而您随后又从回收站恢复了该 AMI，则该AMI将不再由创建它的 Amazon 服务管理。如果不再需要 AMI，则必须手动将其删除。

Amazon Data Lifecycle Manager 快照策略注意事项

- 如果 Amazon Data Lifecycle Manager 删除与保留规则匹配的快照，则该快照将由回收站自动保留。
- 如果 Amazon Data Lifecycle Manager 删除快照并在达到策略的保留阈值时将其发送到回收站，并且您从回收站手动还原快照，则必须在不再需要该快照时手动删除它。Amazon Data Lifecycle Manager 将不再管理该快照。
- 如果您手动删除由策略创建的快照，并且该快照在达到策略的保留阈值时位于回收站中，则 Amazon Data Lifecycle Manager 将不会删除该快照。当快照存储在回收站中时，Amazon Data Lifecycle Manager 不管理快照。

  如果在达到策略的保留阈值之前从回收站还原了快照，那么当达到策略的保留阈值时，Amazon Data Lifecycle Manager 将删除快照。

  如果在达到策略的保留阈值之前从回收站还原了快照，则 Amazon Data Lifecycle Manager 将不再删除快照。如果不再需要快照，则必须手动删除该快照。

Amazon Backup 的注意事项

- 如果 Amazon Backup 删除了符合保留规则的快照，则回收站会自动保留该快照。

已归档快照的注意事项

- 回收站保留规则也适用于归档存储层中的已归档快照。如果删除与回收站保留规则匹配的已归档快照，则该快照将在保留规则定义的保留期内保留在回收站中。

  归档的快照在回收站中时，按归档快照的费率计费。

  如果按照某保留规则，在最短期限 90 天之前从回收站中删除了归档的快照，则需要为剩余天数付费。有关更多信息，请参阅 Archived snapshot pricing and billing。

  若要使用回收站中的已归档快照，您必须首先从回收站中恢复快照，然后将其从归档层中还原到标准层。

限额

以下配额适用于回收站。

配额	默认配额			
每个区域的保留规则	250			
为每个保留规则标记密钥和值对	50			

相关服务

回收站适用于以下服务。

- Amazon CloudTrail – 使您能够记录回收站中发生的事件。有关更多信息，请参阅 使用监控回收站 Amazon CloudTrail。

定价

使用回收站和保留规则不会产生额外费用。有关更多信息，请参阅 Amazon EBS 定价。

- Amazon EBS 快照 — 回收站中快照的计费费率与您账户中的常规快照相同。
- EBS-b AMIs acked — AMIs 在回收站中不会产生任何额外费用。

> **Note**
>
> 有些资源在保留期到期 Amazon CLI 并被永久删除后，可能仍会在短时间内出现在回收站控制台或和 API 输出中。您无需为这些资源付费。保留期到期后，账单立即停止。

使用时，您可以使用以下 Amazon 生成的成本分配标签进行成本跟踪和分配 Amazon 账单与成本管理。

- 键：`aws:recycle-bin:resource-in-bin`
- 值：`true`

有关更多信息，请参阅《Amazon 账单与成本管理 用户指南》中的 Amazon生成的成本分配标签。

使用 IAM 控制对回收站的访问

默认情况下，用户没有权限使用回收站、保留规则或回收站中的资源。要允许用户使用这些资源，您必须创建 IAM policy，以授予使用特定资源和 API 操作的权限。创建策略后，必须向您的用户、组或角色添加权限。

主题

- 使用回收站和保留规则的权限
- 使用回收站中的资源的权限
- 回收站的条件键

使用回收站和保留规则的权限

要使用回收站和保留规则，用户需要以下权限。

- `rbin:CreateRule`
- `rbin:UpdateRule`
- `rbin:GetRule`
- `rbin:ListRules`
- `rbin:DeleteRule`
- `rbin:TagResource`
- `rbin:UntagResource`
- `rbin:ListTagsForResource`
- `rbin:LockRule`
- `rbin:UnlockRule`

要使用回收站控制台，用户需要 `tag:GetResources` 权限。

以下是包含控制台用户 `tag:GetResources` 权限的示例 IAM policy。如果不需要某些上述权限，您可以从策略中将其删除。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "rbin:CreateRule",
            "rbin:UpdateRule",
            "rbin:GetRule",
            "rbin:ListRules",
            "rbin:DeleteRule",
            "rbin:TagResource",
            "rbin:UntagResource",
            "rbin:ListTagsForResource",
            "rbin:LockRule",
            "rbin:UnlockRule",
            "tag:GetResources"
        ],
        "Resource": "*"
    }]
}
```

要提供访问权限，请为您的用户、组或角色添加权限：

- 通过身份提供商在 IAM 中托管的用户：

  创建适用于身份联合验证的角色。按照《IAM 用户指南》中针对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 用户：
  - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
  - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

使用回收站中的资源的权限

有关使用回收站中的资源所需的 IAM 权限的更多信息，请参阅以下内容：

- 使用回收站中的快照的权限
- 在回收站 AMIs 中使用的权限

回收站的条件键

回收站定义以下条件键，您可在 IAM policy 的 Condition 元素中将其用于控制适用策略语句的条件。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。

主题

- rbin:Request/ResourceType 条件键
- rbin:Attribute/ResourceType 条件键

rbin:Request/ResourceType 条件键

rbin:Request/ResourceType条件键可用于根据为ListRules请求参数指定的值筛选访问权限CreateRule和ResourceType请求。

示例 1- CreateRule

以下 IAM 策略示例，仅当为CreateRule请求参数指定的值为EBS_SNAPSHOT或EC2_IMAGE时，IAM 委托人才能ResourceType发出请求。这允许委托人 AMIs 仅为快照创建新的保留规则。

```
{
    "Version" : "2012-10-17",
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" :[
                "rbin:CreateRule"
            ],
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "rbin:Request/ResourceType" : ["EBS_SNAPSHOT", "EC2_IMAGE"]
                }
            }
        }
    ]
}
```

示例 2- ListRules

以下示例 IAM 策略允许 IAM 委托人仅在为ResourceType请求参数指定的值为时发出请求。ListRulesEBS_SNAPSHOT这使主体仅列出快照的保留规则，并防止它们列出任何其他资源类型的保留规则。

```
{
    "Version" : "2012-10-17",
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" :[
                "rbin:ListRules"
            ],
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "rbin:Request/ResourceType" : "EBS_SNAPSHOT"
                }
            }
        }
    ]
}
```

rbin:Attribute/ResourceType 条件键

rbin:Attribute/ResourceType条件键可用于根据保留规则ResourceType属性的值筛选对DeleteRuleGetRuleUpdateRuleLockRuleUnlockRuleTagResource、UntagResource、、、、、和ListTagsForResource请求的访问权限。

示例 1- UpdateRule

以下示例 IAM 策略仅在UpdateRule请求的保留规则的ResourceType属性为EBS_SNAPSHOT或EC2_IMAGE时允许 IAM 委托人发出请求。这允许委托人 AMIs 仅更新快照的保留规则。

```
{
    "Version" : "2012-10-17",
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" :[
                "rbin:UpdateRule"
            ],
```

```
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "rbin:Attribute/ResourceType" : ["EBS_SNAPSHOT", "EC2_IMAGE"]
                }
            }
        }
    ]
}
```

示例 2- DeleteRule

以下示例 IAM 策略允许 IAM 委托人仅在DeleteRule请求的保留规则的ResourceType属性为EBS_SNAPSHOT时才发出请求。这使主体能够仅为快照删除保留规则。

```
{
    "Version" : "2012-10-17",
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" :[
                "rbin:DeleteRule"
            ],
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "rbin:Attribute/ResourceType" : "EBS_SNAPSHOT"
                }
            }
        }
    ]
}
```

创建回收站保留规则

创建保留规则时，必须指定以下必要参数：

- 要保护的资源类型（快照或 AMIs）。
- 保留规则的类型（标签级别或区域级别）。标签级别的规则仅保护具有特定标签的资源。区域级规则保护区域中的所有资源，但可以排除带有特定标签的资源。
- 保留期，最长可为 1 年（365 天）。

您还可以选择指定规则名称和描述，每个规则名称和描述不超过 255 个字符，以及用于帮助您识别和组织规则的标签。我们建议您不要在姓名、描述或标签中包含个人身份、机密或敏感信息。

您也可以选择在创建时锁定区域级别的保留规则。如果您在创建时锁定保留规则，则还必须指定解锁延迟时间期，可以是 7 到 30 天。保留规则默认保持解锁状态，除非您明确将其锁定。

> **Note**
>
> 保留规则仅在创建它们的区域中有效。如果您打算在其它区域中使用回收站，则必须在这些区域中创建其它保留规则。

您可以使用以下方法创建回收站保留规则。

Recycle Bin console

创建标签级别的保留规则

1. 在家中打开回收站控制台 https://console.aws.amazon.com/rbin//
2. 在导航窗格中，选择 Retention rules（保留规则），然后选择 Create retention rule（创建保留规则）。
3. （可选）在 Retention rule name（保留规则名称）中，输入保留规则的描述性名称。
4. （可选）在 Retention rule description（保留规则描述）中，输入保留规则的简单描述。
5. 在资源类型中，选择保留规则要保护的资源类型。保留规则将仅在回收站中保留此类资源。
6. 在 “选择要保留的资源” 中，选择 “保留具有特定标签的资源”。
7. 在资源标签中，输入标签键和值对，用于标识要保留在回收站中的资源。保留规则只会保留具有至少一个指定标签的指定类型的资源。
8. 在 “保留期” 中，输入在回收站中保留已删除资源的天数。
9. 选择 Create retention rule（创建保留规则）。

创建区域级保留规则

1. 在家中打开回收站控制台 https://console.aws.amazon.com/rbin//
2. 在导航窗格中，选择 Retention rules（保留规则），然后选择 Create retention rule（创建保留规则）。
3. （可选）在 Retention rule name（保留规则名称）中，输入保留规则的描述性名称。

4. （可选）在 Retention rule description（保留规则描述）中，输入保留规则的简单描述。
5. 在资源类型中，选择保留规则要保护的资源类型。保留规则将仅在回收站中保留此类资源。
6. 在 “选择要保留的资源” 中，选择 “保留所有资源”。
7. （可选）要排除具有特定标签的资源，请在排除标签中输入最多五个标签键和值对，用于标识要排除的资源。保留规则会忽略带有任何这些标签的资源。
8. 在 “保留期” 中，输入在回收站中保留已删除资源的天数。
9. （可选）若要锁定保留规则，对于 Rule lock settings（规则锁定设置），选择 Lock（锁定），然后对于 Unlock delay period（解锁延迟期），指定解锁延迟时间（以天为单位）。无法修改或删除锁定的保留规则。若要修改或删除规则，必须先将其解锁，然后等待解锁延迟期到期。有关更多信息，请参阅 锁定回收站保留规则以防止其被更新或删除。

   若要使保留规则保持解锁状态，对于 Rule lock settings（规则锁定设置），请保持 Unlock（解锁）处于选中状态。可以随时修改或删除已解锁的保留规则。

   > **Note**
   >
   > 您无法锁定带有排除标签的区域级保留规则。

10. 选择 Create retention rule（创建保留规则）。

Amazon CLI

创建保留规则

使用 create-rule Amazon CLI 命令。对于 `--retention-period`，请指定在回收站中保留已删除快照的天数。对于`--resource-type`，`EBS_SNAPSHOT`为快照指定或`EC2_IMAGE`为 AMIs。要创建标签级别保留规则，请在 `--resource-tags` 中指定用于标记要保留快照的标签。要创建区域级保留规则，请省略并可选择指定 `--resource-tags`或`--exclude-resource-tags`，以排除具有特定标签的资源。 要锁定区域级别的保留规则，请包括`--lock-configuration`并指定解锁延迟时间（以天为单位）。

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=number_of_days,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT|EC2_IMAGE \
--description "rule_description" \
--lock-configuration
 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=unlock_delay_in_days}' \
--resource-tags ResourceTagKey=tag_key,ResourceTagValue=tag_value \
```

```
--exclude-resource-tags ResourceTagKey=tag_key,ResourceTagValue=tag_value
```

示例 1

以下示例命令创建已解锁的区域级保留规则，该规则将所有已删除的快照保留 7 天。

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Match all snapshots"
```

示例 2

以下示例命令创建标签级保留规则，该规则将被 purpose=production 标记的所有已删除的快照保留 7 天。

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Match snapshots with a specific tag" \
--resource-tags ResourceTagKey=purpose,ResourceTagValue=production
```

示例 3

以下示例命令创建锁定的区域级保留规则，该规则将所有已删除的快照保留 7 天。保留规则已锁定，解锁延迟期为 7 天。

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Match all snapshots" \
--lock-configuration 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=7}'
```

示例 4

以下示例命令创建了一个未锁定的区域级保留规则，该规则将所有已删除的快照保留几天，但带有purpose:testing标签的7快照除外。

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
```

```
--description "Match only production snapshots" \
--exclude-resource-tags ResourceTagKey=purpose,ResourceTagValue=testing
```

更新现有回收站保留规则

创建后，您可以随时更新已解锁保留规则的说明、资源标签和保留期。您无法更新保留规则的资源类型或解锁延迟期，即使保留规则已解锁也是如此。

您无法以任何方式更新锁定的保留规则。如果您需要修改锁定的保留规则，则必须先将其解锁，然后等待解锁延迟期到期。

如果您需要修改锁定保留规则的解锁延迟期，则必须解锁保留规则，然后等待当前的解锁延迟期到期。解锁延迟期到期后，必须重新锁定保留规则并指定新的解锁延迟期。

> **Note**
>
> 我们建议您不要将个人身份识别、机密或敏感信息包括在留存规则描述中。

更新保留规则后，这些更改仅适用于其保留的新资源。这些更改不会影响之前发送到回收站的资源。例如，如果您更新了保留规则的保留期，则在新的保留期内只会保留更新后删除的快照。在更新之前发送到回收站的快照仍会在上一个（旧）保留期内保留。

您可以使用以下方法之一更新保留规则。

Recycle Bin console

更新保留规则

1. 在家中打开回收站控制台 https://console.aws.amazon.com/rbin//
2. 在导航窗格中，选择 Retention rules（保留规则）。
3. 在网格中，选择要更新的保留规则，然后选择 Actions（操作）、Edit retention rule（编辑保留规则）。
4. 在 Rule details（规则详细信息）部分中，根据需要更新 Retention rule name（保留规则名称）和 Retention rule description（保留规则描述）。
5. 在 Rule settings（规则设置）部分中，根据需要更新 Resource type（资源类型）、Resource tags to match（要匹配的资源标签）和 Retention period（保留期）。
6. 在 Tags（标签）部分，根据需要添加或删除保留规则标签。

7. 选择 Save retention rule（保存保留规则）。

Amazon CLI

更新保留规则

使用 update-rule Amazon CLI 命令。对于`--identifier`，请指定要更新的保留规则的 ID 为`--resource-types`、`EBS_SNAPSHOT`为快照指定或`EC2_IMAGE`为 AMIs。

```
aws rbin update-rule \
--identifier rule_ID \
--retention-period RetentionPeriodValue=number_of_days,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT|EC2_IMAGE \
--description "rule_description"
```

示例

以下示例命令更新了保留规则 `6lsJ2Fa9nh9`，以将所有快照保留 7 天，并更新其描述。

```
aws rbin update-rule \
--identifier 6lsJ2Fa9nh9 \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Retain for three weeks"
```

锁定回收站保留规则以防止其被更新或删除

回收站允许您随时锁定区域级别的保留规则。

即使拥有所需 IAM 权限的用户，也无法修改或删除锁定的保留规则。锁定保留规则以保护其免遭意外或恶意修改和删除。

锁定保留规则时，必须指定解锁延迟期。这是解锁保留规则后必须等待的时间，然后才能修改或删除该规则。在解锁延迟期内，您无法修改或删除保留规则。只有在解锁延迟期到期后，您才可修改或删除保留规则。

保留规则锁定后，您无法更改解锁延迟期。如果您的账户权限已外泄，则解锁延迟期会让您有更多时间检测和应对安全威胁。此期限的长度应长于您识别和应对安全漏洞所花费的时间。若要设置正确的持续时间，您可以查看以前的安全事件以及识别和修复账户漏洞所需的时间。

我们建议您使用 Amazon EventBridge 规则来通知您保留规则锁定状态的变化。有关更多信息，请参阅使用 Amazon 监控回收站 EventBridge。

注意事项

- 您无法锁定标签级别的保留规则，也无法锁定带有排除标签的区域级保留规则。
- 您可以随时锁定已解锁的保留规则。
- 解锁延迟期必须为 7 到 30 天。
- 您可以在解锁延迟期内重新锁定保留规则。重新锁定保留规则会重置解锁延迟期。

您可以使用以下方法之一锁定区域级别的保留规则。

Recycle Bin console

锁定保留规则

1. 在家中打开回收站控制台 https://console.aws.amazon.com/rbin//
2. 在导航面板中，选择 Retention rules（保留规则）。
3. 在网格中，选择要锁定的已解锁保留规则，然后选择 Actions（操作）、Edit retention rule lock（编辑保留规则锁定）。
4. 在编辑保留规则锁定屏幕上，选择 Lock（锁定），然后对于 Unlock delay period（解锁延迟期），指定解锁延迟期（以天为单位）。
5. 选择 I acknowledge that locking the retention rule will prevent it from being modified or deleted（我确认锁定保留规则将阻止其被修改或删除）复选框，然后选择 Save（保存）。

Amazon CLI

锁定已解锁的保留规则

使用 lock-rule Amazon CLI 命令。对于 `--identifier`，指定要锁定的保留规则 ID。对于 `--lock-configuration`，以天为单位指定解锁延迟期。

```
aws rbin lock-rule \
--identifier rule_ID \
--lock-configuration
 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=number_of_days}'
```

示例

以下示例命令锁定保留规则 6lsJ2Fa9nh9 并将解锁延迟期设置为 15 天。

```
aws rbin lock-rule \
--identifier 6lsJ2Fa9nh9 \
--lock-configuration 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=15}'
```

解锁回收站保留规则以允许更新或删除它

您无法修改或删除锁定的保留规则。如果您需要修改锁定的保留规则，则必须先将其解锁。解锁保留规则后，必须等待解锁延迟期到期，然后才能修改或删除该规则。在解锁延迟期内，您无法修改或删除保留规则。

拥有所需 IAM 权限的用户可以随时修改和删除已解锁的保留规则。让保留规则处于解锁状态，会使其遭受意外或恶意修改和删除的风险。

注意事项

- 您可以在解锁延迟期内重新锁定保留规则。
- 您可以在解锁延迟期到期后重新锁定保留规则。
- 您无法绕过解锁延迟期。
- 初始锁定后，您无法更改解锁延迟期。

我们建议您使用 Amazon EventBridge 规则来通知您保留规则锁定状态的变化。有关更多信息，请参阅使用 Amazon 监控回收站 EventBridge。

您可以使用以下方法之一解锁已锁定的区域级别保留规则。

Recycle Bin console

解锁保留规则

1. 在家中打开回收站控制台 https://console.aws.amazon.com/rbin//
2. 在导航面板中，选择 Retention rules（保留规则）。
3. 在网格中，选择要解锁的已锁定保留规则，然后选择 Actions（操作）、Edit retention rule lock（编辑保留规则锁定）。
4. 在编辑保留规则锁定屏幕上，选择 Unlock（解锁），然后选择 Save（保存）。

Amazon CLI

解锁已锁定的保留规则

使用 unlock-rule Amazon CLI 命令。对于 `--identifier`，指定要解锁的保留规则 ID。

```
aws rbin unlock-rule \
--identifier rule_ID
```

示例

以下示例命令解锁保留规则 `6lsJ2Fa9nh9`。

```
aws rbin unlock-rule \
--identifier 6lsJ2Fa9nh9
```

为回收站保留规则添加标签

可以给保留规则分配自定义标签，以便按不同的方式将它们分类，例如按用途、拥有者或环境分类。这有助于根据所分配的自定义标签高效查找特定保留规则。

您可以使用以下方法之一为保留规则分配标签。

Recycle Bin console

标记保留规则

1. 在家中打开回收站控制台 https://console.aws.amazon.com/rbin//
2. 在导航窗格中，选择 Retention rules（保留规则）。
3. 选择要标记的保留规则，选择 Tags（标签）选项卡，然后选择 Manage tags（管理标签）。
4. 选择 Add tag（添加标签）。对于 Key（键），输入标签建。对于 Value（值），输入键值。
5. 选择 Save（保存）。

Amazon CLI

标记保留规则

使用 tag-resou Amazon CLI rce 命令。对于 `--resource-arn`，请指定要标记的保留规则的 Amazon Resource Name (ARN)，并为 `--tags` 指定标签键值对。

```
aws rbin tag-resource \
--resource-arn retention_rule_arn \
--tags key=tag_key,value=tag_value
```

示例

以下示例命令使用标签 arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3 来标记保留规则 purpose=production。

```
aws rbin tag-resource \
--resource-arn arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3 \
--tags key=purpose,value=production
```

查看保留规则标签

您可以使用以下方法之一查看分配给保留规则的标签。

Recycle Bin console

查看保留规则的标签

1. 在家中打开回收站控制台 https://console.aws.amazon.com/rbin//
2. 在导航窗格中，选择 Retention rules（保留规则）。
3. 选择要查看标签的保留规则，然后选择 Tags（标签）选项卡。

Amazon CLI

查看分配给保留规则的标签

使用 list-tags-for-resource 命令。 Amazon CLI 对于 --resource-arn，请指定保留规则的 ARN。

```
aws rbin list-tags-for-resource \
--resource-arn retention_rule_arn
```

示例

以下示例命令列举保留规则 arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3 的标签。

```
aws rbin list-tags-for-resource \
--resource-arn arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3
```

从保留规则中删除标签

您可以使用以下方法之一从保留规则中删除标签。

Recycle Bin console

从保留规则中删除标签

1. 在家中打开回收站控制台 https://console.aws.amazon.com/rbin//
2. 在导航窗格中，选择 Retention rules（保留规则）。
3. 选择要从中删除标签的保留规则，选择 Tags（标签）选项卡，然后选择 Manage tags（管理标签）。
4. 在标签旁选择 Remove（移除），以移除标签。
5. 选择 Save（保存）。

Amazon CLI

从保留规则中删除标签

使用 untag-resource Amazon CLI 命令。对于 `--resource-arn`，请指定保留规则的 ARN。对于 `--tagkeys`，请指定要删除标签的标签键。

```
aws rbin untag-resource \
--resource-arn retention_rule_arn \
--tagkeys tag_key
```

示例

以下示例命令删除保留规则 `arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3` 的 标签键为 `purpose` 的标签。

```
aws rbin untag-resource \
--resource-arn arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3 \
--tagkeys purpose
```

删除回收站保留规则以阻止其保留资源

您可以随时删除保留规则。删除保留规则时，回收站内在删除完成后将不再保留删除的新资源。根据保留规则中定义的保留期限，在删除保留规则之前发送到回收站的资源将继续保留在回收站中。期限到期后，资源将从回收站中永久删除。

您可以使用以下方法之一删除保留规则。

Recycle Bin console

删除保留规则

1. 在家中打开回收站控制台 https://console.aws.amazon.com/rbin//
2. 在导航窗格中，选择 Retention rules（保留规则）。
3. 在表格中选择要删除的保留规则，然后选择 Actions（操作）、Delete retention rule（删除保留规则）。
4. 在系统提示时，输入确认消息并选择 Delete retention rule（删除保留规则）。

Amazon CLI

删除保留规则

使用 delete-rule Amazon CLI 命令。对于 `--identifier`，请指定要删除的保留规则的 ID。

```
aws rbin delete-rule --identifier rule_ID
```

示例

以下示例命令删除保留规则 `6lsJ2Fa9nh9`。

```
aws rbin delete-rule --identifier 6lsJ2Fa9nh9
```

从回收站恢复已删除的快照

主题

- 使用回收站中的快照的权限

- 在回收站中查看快照
- 从回收站中还原快照

使用回收站中的快照的权限

默认情况下，用户无权使用回收站中的快照。要允许用户使用这些资源，您必须创建 IAM policy，以授予使用特定资源和 API 操作的权限。创建策略后，必须向您的用户、组或角色添加权限。

要查看及恢复回收站中的快照，用户必须具有以下权限：

- `ec2:ListSnapshotsInRecycleBin`
- `ec2:RestoreSnapshotFromRecycleBin`

要管理回收站中快照的标签，用户需要以下额外权限。

- `ec2:CreateTags`
- `ec2:DeleteTags`

要使用回收站控制台，用户需要 `ec2:DescribeTags` 权限。

以下是 IAM policy 示例。其中包括控制台用户的 `ec2:DescribeTags` 权限，以及用于管理标签的 `ec2:CreateTags` 和 `ec2:DeleteTags` 权限。如果不需要上述权限，您可以从策略中将其删除。

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
            "ec2:ListSnapshotsInRecycleBin",
            "ec2:RestoreSnapshotFromRecycleBin"
        ],
        "Resource": "*"
      },
      {
        "Effect": "Allow",
        "Action": [
            "ec2:CreateTags",
            "ec2:DeleteTags",
```

```
            "ec2:DescribeTags"
        ],
        "Resource": "arn:aws:ec2:Region:account-id:snapshot/*"
      },

    ]
}
```

要提供访问权限，请为您的用户、组或角色添加权限：

- 通过身份提供商在 IAM 中托管的用户：

  创建适用于身份联合验证的角色。按照《IAM 用户指南》中针对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 用户：
  - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
  - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

有关使用回收站所需权限的更多信息，请参阅 使用回收站和保留规则的权限。

在回收站中查看快照

当快照在回收站中时，您可以查看有关该快照的有限信息，包括：

- 快照的 ID。
- 快照描述。
- 从中创建快照的卷的 ID。
- 快照被删除并进入回收站的日期和时间。
- 保留期到期的日期和时间。此时，快照将从回收站中永久删除。

您可以使用以下方法查看回收站中的快照。

Recycle Bin console

使用控制台查看回收站中的快照

1. 在家中打开回收站控制台 https://console.aws.amazon.com/rbin//

2. 在导航窗格中，选择 Recycle Bin（回收站）。
3. 该网格列出了当前在回收站中的所有快照。要查看特定快照的详细信息，请在网格中选择它，然后选择 Actions（操作）、View details（查看详细信息）。

Amazon CLI

要查看回收站中的快照，请使用 Amazon CLI

使用 list-snapshots-in-recycle-bin Amazon CLI 命令。加入 `--snapshot-id` 选项来查看特定快照。或者省略 `--snapshot-id` 选项以查看回收站中的所有快照。

```
aws ec2 list-snapshots-in-recycle-bin --snapshot-id snapshot_id
```

例如，以下命令提供有关回收站中的快照 `snap-01234567890abcdef` 的信息。

```
aws ec2 list-snapshots-in-recycle-bin --snapshot-id snap-01234567890abcdef
```

输出示例：

```
{
    "SnapshotRecycleBinInfo": [
        {
            "Description": "Monthly data backup snapshot",
            "RecycleBinEnterTime": "2021-12-01T13:00:00.000Z",
            "RecycleBinExitTime": "2021-12-15T13:00:00.000Z",
            "VolumeId": "vol-abcdef09876543210",
            "SnapshotId": "snap-01234567890abcdef"
        }
    ]
}
```

从回收站中还原快照

当快照在回收站中时，您不能以任何方式使用它。要使用快照，您必须首先还原它。从回收站还原快照时，该快照立即可供使用，回收站会将其删除。还原快照后，您可以像使用账户中任何其它快照一样使用它。

您可以使用以下方法之一从回收站中还原快照。

Recycle Bin console

使用控制台从回收站中还原快照

1. 在家中打开回收站控制台 https://console.aws.amazon.com/rbin//
2. 在导航窗格中，选择 Recycle Bin（回收站）。
3. 该网格列出了当前在回收站中的所有快照。选择要还原的快照，然后选择 Recover（还原）。
4. 系统提示时，选择 Recover（还原）。

Amazon CLI

要从回收站中恢复已删除的快照，请使用 Amazon CLI

使用 restore-snapshot-from-recycle-bin Amazon CLI 命令。对于 `--snapshot-id`，请指定需还原快照的 ID。

```
aws ec2 restore-snapshot-from-recycle-bin --snapshot-id snapshot_id
```

例如，以下命令将快照 `snap-01234567890abcdef` 从回收站中还原。

```
aws ec2 restore-snapshot-from-recycle-bin --snapshot-id snap-01234567890abcdef
```

输出示例：

```
{
    "SnapshotId": "snap-01234567890abcdef",
    "Description": "Monthly data backup snapshot",
    "Encrypted": false,
    "OwnerId": "111122223333",
    "Progress": "100%",
    "StartTime": "2021-12-01T13:00:00.000000+00:00",
    "State": "recovering",
    "VolumeId": "vol-ffffffff",
    "VolumeSize": 30
}
```

恢复 AMIs 从回收站中删除的内容

主题

- 在回收站 AMIs 中使用的权限
- AMIs 在回收站中查看
- AMIs 从回收站恢复

在回收站 AMIs 中使用的权限

默认情况下，用户无权使用 AMIs 回收站中的内容。要允许用户使用这些资源，您必须创建 IAM policy，以授予使用特定资源和 API 操作的权限。创建策略后，必须向您的用户、组或角色添加权限。

要查看和恢复 AMIs 回收站中的内容，用户必须具有以下权限：

- `ec2:ListImagesInRecycleBin`
- `ec2:RestoreImageFromRecycleBin`

要管理回收站 AMIs 中的标签，用户需要以下额外权限。

- `ec2:CreateTags`
- `ec2:DeleteTags`

要使用回收站控制台，用户需要 `ec2:DescribeTags` 权限。

以下是 IAM policy 示例。其中包括控制台用户的 `ec2:DescribeTags` 权限，以及用于管理标签的 `ec2:CreateTags` 和 `ec2:DeleteTags` 权限。如果不需要上述权限，您可以从策略中将其删除。

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
            "ec2:ListImagesInRecycleBin",
            "ec2:RestoreImageFromRecycleBin"
        ],
        "Resource": "*"
      },
      {
        "Effect": "Allow",
        "Action": [
```

```
            "ec2:CreateTags",
            "ec2:DeleteTags",
            "ec2:DescribeTags"
        ],
        "Resource": "arn:aws:ec2:Region::image/*"
      }
    ]
}
```

要提供访问权限，请为您的用户、组或角色添加权限：

- 通过身份提供商在 IAM 中托管的用户：

  创建适用于身份联合验证的角色。按照《IAM 用户指南》中针对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 用户：
  - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
  - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

有关使用回收站所需权限的更多信息，请参阅 使用回收站和保留规则的权限。

AMIs 在回收站中查看

如果 AMI 位于回收站中，则只能查看该 AMI 的有限信息，包括：

- AMI 的名称、描述和唯一 ID。
- AMI 被删除并放入回收站的日期和时间。
- 保留期到期的日期和时间。此后，系统会永久删除 AMI。

您可以使用以下方法之一 AMIs 在回收站中查看。

Recycle Bin console

使用控制台 AMIs 在回收站中查看已删除的内容

1. 在 conso le.aws.amazon 上打开回收站控制台。 com/rbin/home/。
2. 在导航窗格中，选择 Recycle Bin（回收站）。

3. 该表格列出了当前在回收站中的所有资源。要查看特定 AMI 的详细信息，请在表格中选择所需 AMI，然后选择 Actions（操作）、View details（查看详细信息）。

Amazon CLI

要在回收站 AMIs 中查看已删除的内容，请使用 Amazon CLI

使用 list-images-in-recycle-bin Amazon CLI 命令。要查看特定内容 AMIs，请添加`--image-id`选项并 IDs 指定 AMIs 要查看的。您最多可以在单个请求 IDs 中指定 20。

要查看回收站 AMIs 中的所有内容，请省略该`--image-id`选项。如果没有为 `--max-items` 指定值，命令默认每页将返回 1000 个项目。有关更多信息，请参阅 Amazon EC2 API 参考中的分页。

```
aws ec2 list-images-in-recycle-bin --image-id ami_id
```

例如，以下命令提供回收站中 AMI `ami-01234567890abcdef` 的相关信息。

```
aws ec2 list-images-in-recycle-bin --image-id ami-01234567890abcdef
```

输出示例：

```
{
    "Images": [
        {
            "ImageId": "ami-0f740206c743d75df",
            "Name": "My AL2 AMI",
            "Description": "My Amazon Linux 2 AMI",
            "RecycleBinEnterTime": "2021-11-26T21:04:50+00:00",
            "RecycleBinExitTime": "2022-03-06T21:04:50+00:00"
        }
    ]
}
```

Important

如果您收到以下错误，则可能需要更新您的 Amazon CLI 版本。有关更多信息，请参阅找不到命令错误。

```
aws.exe: error: argument operation: Invalid choice, valid choices are: ...
```

AMIs 从回收站恢复

当 AMI 在回收站中时，您不能以任何方式使用它。要使用该 AMI，您必须先还原它。从回收站还原 AMI 时，该 AMI 立即可供使用，回收站会将其删除。还原 AMI 后，您可以像使用账户中任何其他 AMI 一样使用它。

您可以使用以下方法之一从回收站还原 AMI。

Recycle Bin console

使用控制台从回收站还原 AMI

1. 在 conso le.aws.amazon 上打开回收站控制台。 com/rbin/home/。
2. 在导航窗格中，选择 Recycle Bin（回收站）。
3. 该表格列出了当前在回收站中的所有资源。选择要还原的 AMI，然后选择 Recover（恢复）。
4. 系统提示时，选择 Recover（还原）。

Amazon CLI

要从回收站中恢复已删除的 AMI，请使用 Amazon CLI

使用 restore-image-from-recycle-bin Amazon CLI 命令。对于 `--image-id`，指定需还原 AMI 的 ID。

```
aws ec2 restore-image-from-recycle-bin --image-id ami_id
```

例如，以下命令将 AMI `ami-01234567890abcdef` 从回收站中还原。

```
aws ec2 restore-image-from-recycle-bin --image-id ami-01234567890abcdef
```

命令成功后，不返回任何输出。

> **Important**
>
> 如果您收到以下错误，则可能需要更新您的 Amazon CLI 版本。有关更多信息，请参阅找不到命令错误。
>
> ```
> aws.exe: error: argument operation: Invalid choice, valid choices are: ...
> ```

使用 Amazon 监控回收站 EventBridge

回收站会向 Amazon 发送 EventBridge 针对保留规则执行操作的事件。使用 EventBridge，您可以建立规则，启动程序化操作以响应这些事件。例如，您可以创建一个 EventBridge 规则，当保留规则解锁并进入解锁延迟期限时，该规则会向您的电子邮件发送通知。有关更多信息，请参阅创建对事件做出反应的 Amazon EventBridge 规则。

中的 EventBridge 事件以 JSON 对象的形式表示。事件独有的字段包含在 JSON 对象的 `detail` 部分。`event` 字段包含事件名称。`result` 字段包含启动事件的操作的已完成状态。有关更多信息，请参阅《亚马逊 EventBridge 用户指南》中的亚马逊 EventBridge 事件模式。

有关亚马逊的更多信息 EventBridge，请参阅什么是亚马逊 EventBridge？ 在《亚马逊 EventBridge 用户指南》中。

事件

- RuleLocked
- RuleChangeAttempted
- RuleUnlockScheduled
- RuleUnlockingNotice
- RuleUnlocked

RuleLocked

以下是成功锁定保留规则时回收站生成的事件示例。此事件可以由CreateRule和LockRule请求生成。`api-name` 字段中注明了生成事件的 API。

```
{
 "version": "0",
 "id": "exampleb-b491-4cf7-a9f1-bf370example",
 "detail-type": "Recycle Bin Rule Locked",
 "source": "aws.rbin",
 "account": "123456789012",
 "time": "2022-08-10T16:37:50Z",
 "region": "us-west-2",
 "resources": [
 "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
 ],
 "detail":
```

```
 {
 "detail-version": " 1.0.0",
 "rule-id": "a12345abcde",
 "rule-description": "locked account level rule",
 "unlock-delay-period": "30 days",
 "api-name": "CreateRule"
 }
 }
```

RuleChangeAttempted

以下是回收站针对尝试修改或删除锁定规则失败生成的事件示例。此事件可以由DeleteRule和UpdateRule请求生成。api-name 字段中注明了生成事件的 API。

```
{
 "version": "0",
 "id": "exampleb-b491-4cf7-a9f1-bf370example",
 "detail-type": "Recycle Bin Rule Change Attempted",
 "source": "aws.rbin",
 "account": "123456789012",
 "time": "2022-08-10T16:37:50Z",
 "region": "us-west-2",
 "resources": [
 "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
 ],
 "detail":
 {
 "detail-version": " 1.0.0",
 "rule-id": "a12345abcde",
 "rule-description": "locked account level rule",
 "unlock-delay-period": "30 days",
 "api-name": "DeleteRule"
 }
 }
```

RuleUnlockScheduled

以下是在解锁保留规则并且其解锁延迟期开始时回收站生成的事件示例。

```
{
 "version": "0",
 "id": "exampleb-b491-4cf7-a9f1-bf370example",
```

```
 "detail-type": "Recycle Bin Rule Unlock Scheduled",
 "source": "aws.rbin",
 "account": "123456789012",
 "time": "2022-08-10T16:37:50Z",
 "region": "us-west-2",
 "resources": [
 "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
 ],
 "detail":
 {
 "detail-version": " 1.0.0",
 "rule-id": "a12345abcde",
 "rule-description": "locked account level rule",
 "unlock-delay-period": "30 days",
 "scheduled-unlock-time": "2022-09-10T16:37:50Z",
 }
 }
```

RuleUnlockingNotice

以下是保留规则处于解锁延迟期，直到解锁延迟期到期前一天，回收站每天生成的事件示例。

```
{
 "version": "0",
 "id": "exampleb-b491-4cf7-a9f1-bf370example",
 "detail-type": "Recycle Bin Rule Unlocking Notice",
 "source": "aws.rbin",
 "account": "123456789012",
 "time": "2022-08-10T16:37:50Z",
 "region": "us-west-2",
 "resources": [
 "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
 ],
 "detail":
 {
 "detail-version": " 1.0.0",
 "rule-id": "a12345abcde",
 "rule-description": "locked account level rule",
 "unlock-delay-period": "30 days",
 "scheduled-unlock-time": "2022-09-10T16:37:50Z"
 }
 }
```

RuleUnlocked

以下是保留规则的解锁延迟期到期且可对保留规则进行修改或删除时，回收站生成的事件示例。

```
{
 "version": "0",
 "id": "exampleb-b491-4cf7-a9f1-bf370example",
 "detail-type": "Recycle Bin Rule Unlocked",
 "source": "aws.rbin",
 "account": "123456789012",
 "time": "2022-08-10T16:37:50Z",
 "region": "us-west-2",
 "resources": [
 "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
 ],
 "detail":
 {
 "detail-version": " 1.0.0",
 "rule-id": "a12345abcde",
 "rule-description": "locked account level rule",
 "unlock-delay-period": "30 days",
 "scheduled-unlock-time": "2022-09-10T16:37:50Z"
 }
 }
```

使用监控回收站 Amazon CloudTrail

回收站服务已与集成 Amazon CloudTrail。 CloudTrail 是一项提供用户、角色或服务所执行操作记录的 Amazon 服务。 CloudTrail 捕获在回收站中执行的所有 API 调用作为事件。如果您创建了跟踪，则可以允许将 CloudTrail 事件持续传输到亚马逊简单存储服务 (Amazon S3) 存储桶。如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的事件历史记录中查看最新的管理事件。您可以使用收集的信息来确定 CloudTrail 向回收站发出的请求、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。

有关的更多信息 CloudTrail，请参阅《Amazon CloudTrail 用户指南》。

中的回收站信息 CloudTrail

CloudTrail 在您创建 Amazon 账户时已在您的账户上启用。当回收站中出现支持的事件活动时，该活动将与其他 Amazon 服务 CloudTrail 事件一起记录在事件历史记录中。您可以在自己的 Amazon 账

户中查看、搜索和下载最近发生的事件。有关更多信息，请参阅使用事件历史记录查看 CloudTrail 事件。

要持续记录 Amazon 账户中的事件，包括回收站的事件，请创建跟踪。跟踪允许 CloudTrail 将日志文件传送到 S3 存储桶。默认情况下，当您在控制台中创建跟踪时，该跟踪将应用于所有 Amazon 区域。跟踪记录 Amazon 分区中所有区域的事件，并将日志文件传送到您指定的 S3 存储桶。此外，您可以配置其他 Amazon 服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅 Amazon CloudTrail 用户指南中的创建跟踪记录概述部分。

支持的 API 操作

对于回收站，您可以使用 CloudTrail 将以下 API 操作记录为管理事件。

- CreateRule
- UpdateRule
- GetRules
- ListRule
- DeleteRule
- TagResource
- UntagResource
- ListTagsForResource
- LockRule
- UnlockRule

有关记录管理事件的更多信息，请参阅《CloudTrail 用户指南》中的记录跟踪的管理事件。

身份信息

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 服务发出。

有关更多信息，请参阅 CloudTrail userIdentityElement。

了解回收站日志文件条目

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 S3 存储桶。 CloudTrail 日志文件包含一个或多个日志条目。事件代表来自任何来源的单个请求，包括有关请求的操作、操作的日期和时间、请求参数等的信息。 CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此它们不会按任何特定的顺序出现。

以下是示例 CloudTrail 日志条目。

CreateRule


```
{
 "eventVersion": "1.08",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "123456789012",
 "arn": "arn:aws:iam::123456789012:root",
 "accountId": "123456789012",
 "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
 "sessionContext": {
   "sessionIssuer": {
     "type": "Role",
     "principalId": "123456789012",
     "arn": "arn:aws:iam::123456789012:role/Admin",
     "accountId": "123456789012",
     "userName": "Admin"
   },
   "webIdFederationData": {},
   "attributes": {
     "mfaAuthenticated": "false",
     "creationDate": "2021-08-02T21:43:38Z"
   }
 }
 },
 "eventTime": "2021-08-02T21:45:22Z",
 "eventSource": "rbin.amazonaws.com",
 "eventName": "CreateRule",
 "awsRegion": "us-west-2",
 "sourceIPAddress": "123.123.123.123",
 "userAgent": "aws-cli/1.20.9 Python/3.6.14
 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
 "requestParameters": {
 "retentionPeriod": {
```

```
    "retentionPeriodValue": 7,
    "retentionPeriodUnit": "DAYS"
  },
  "description": "Match all snapshots",
  "resourceType": "EBS_SNAPSHOT"
  },
  "responseElements": {
  "identifier": "jkrnexample"
  },
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
  "tlsVersion": "TLSv1.2",
  "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
  "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
  }
```

GetRule

```
{
  "eventVersion": "1.08",
  "userIdentity": {
  "type": "AssumedRole",
  "principalId": "123456789012",
  "arn": "arn:aws:iam::123456789012:root",
  "accountId": "123456789012",
  "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "sessionContext": {
    "sessionIssuer": {
      "type": "Role",
      "principalId": "123456789012",
      "arn": "arn:aws:iam::123456789012:role/Admin",
      "accountId": "123456789012",
      "userName": "Admin"
    },
    "webIdFederationData": {},
    "attributes": {
```

```
    "mfaAuthenticated": "false",
    "creationDate": "2021-08-02T21:43:38Z"
  }
 }
 },
 "eventTime": "2021-08-02T21:45:33Z",
 "eventSource": "rbin.amazonaws.com",
 "eventName": "GetRule",
 "awsRegion": "us-west-2",
 "sourceIPAddress": "123.123.123.123",
 "userAgent": "aws-cli/1.20.9 Python/3.6.14
 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
 "requestParameters": {
 "identifier": "jkrnexample"
 },
 "responseElements": null,
 "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
 "eventID": "714fafex-2eam-42pl-913e-926d4example",
 "readOnly": true,
 "eventType": "AwsApiCall",
 "managementEvent": true,
 "eventCategory": "Management",
 "recipientAccountId": "123456789012",
 "tlsDetails": {
 "tlsVersion": "TLSv1.2",
 "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
 "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
 }
 }
```

ListRules

```
{
 "eventVersion": "1.08",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "123456789012",
 "arn": "arn:aws:iam::123456789012:root",
 "accountId": "123456789012",
 "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
 "sessionContext": {
   "sessionIssuer": {
     "type": "Role",
```

```
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:role/Admin",
    "accountId": "123456789012",
    "userName": "Admin"
  },
  "webIdFederationData": {},
  "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2021-08-02T21:43:38Z"
  }
}
},
"eventTime": "2021-08-02T21:44:37Z",
"eventSource": "rbin.amazonaws.com",
"eventName": "ListRules",
"awsRegion": "us-west-2",
"sourceIPAddress": "123.123.123.123",
"userAgent": "aws-cli/1.20.9 Python/3.6.14
Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
"requestParameters": {
"resourceTags": [
  {
    "resourceTagKey": "test",
    "resourceTagValue": "test"
  }
]
},
"responseElements": null,
"requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
"eventID": "714fafex-2eam-42pl-913e-926d4example",
"readOnly": true,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012",
"tlsDetails": {
"tlsVersion": "TLSv1.2",
"cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
"clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
}
}
```

UpdateRule


```
{
 "eventVersion": "1.08",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "123456789012",
 "arn": "arn:aws:iam::123456789012:root",
 "accountId": "123456789012",
 "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
 "sessionContext": {
   "sessionIssuer": {
     "type": "Role",
     "principalId": "123456789012",
     "arn": "arn:aws:iam::123456789012:role/Admin",
     "accountId": "123456789012",
     "userName": "Admin"
   },
   "webIdFederationData": {},
   "attributes": {
     "mfaAuthenticated": "false",
     "creationDate": "2021-08-02T21:43:38Z"
   }
 }
 },
 "eventTime": "2021-08-02T21:46:03Z",
 "eventSource": "rbin.amazonaws.com",
 "eventName": "UpdateRule",
 "awsRegion": "us-west-2",
 "sourceIPAddress": "123.123.123.123",
 "userAgent": "aws-cli/1.20.9 Python/3.6.14
 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
 "requestParameters": {
 "identifier": "jkrnexample",
 "retentionPeriod": {
   "retentionPeriodValue": 365,
   "retentionPeriodUnit": "DAYS"
 },
 "description": "Match all snapshots",
 "resourceType": "EBS_SNAPSHOT"
 },
 "responseElements": null,
 "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
 "eventID": "714fafex-2eam-42pl-913e-926d4example",
```

```
 "readOnly": false,
 "eventType": "AwsApiCall",
 "managementEvent": true,
 "eventCategory": "Management",
 "recipientAccountId": "123456789012",
 "tlsDetails": {
 "tlsVersion": "TLSv1.2",
 "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
 "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
 }
 }
```


DeleteRule


```
{
 "eventVersion": "1.08",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "123456789012",
 "arn": "arn:aws:iam::123456789012:root",
 "accountId": "123456789012",
 "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
 "sessionContext": {
   "sessionIssuer": {
     "type": "Role",
     "principalId": "123456789012",
     "arn": "arn:aws:iam::123456789012:role/Admin",
     "accountId": "123456789012",
     "userName": "Admin"
   },
   "webIdFederationData": {},
   "attributes": {
     "mfaAuthenticated": "false",
     "creationDate": "2021-08-02T21:43:38Z"
   }
 }
 },
 "eventTime": "2021-08-02T21:46:25Z",
 "eventSource": "rbin.amazonaws.com",
 "eventName": "DeleteRule",
 "awsRegion": "us-west-2",
 "sourceIPAddress": "123.123.123.123",
```

```
"userAgent": "aws-cli/1.20.9 Python/3.6.14
Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
"requestParameters": {
"identifier": "jkrnexample"
},
"responseElements": null,
"requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
"eventID": "714fafex-2eam-42pl-913e-926d4example",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012",
"tlsDetails": {
"tlsVersion": "TLSv1.2",
"cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
"clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
}
}
```

TagResource

```
{
 "eventVersion": "1.08",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "123456789012",
 "arn": "arn:aws:iam::123456789012:root",
 "accountId": "123456789012",
 "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
 "sessionContext": {
   "sessionIssuer": {
     "type": "Role",
     "principalId": "123456789012",
     "arn": "arn:aws:iam::123456789012:role/Admin",
     "accountId": "123456789012",
     "userName": "Admin"
   },
   "webIdFederationData": {},
   "attributes": {
     "mfaAuthenticated": "false",
     "creationDate": "2021-10-22T21:38:34Z"
   }
```

```
 }
 },
 "eventTime": "2021-10-22T21:43:15Z",
 "eventSource": "rbin.amazonaws.com",
 "eventName": "TagResource",
 "awsRegion": "us-west-2",
 "sourceIPAddress": "123.123.123.123",
 "userAgent": "aws-cli/1.20.26 Python/3.6.14
Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 botocore/1.21.26",
 "requestParameters": {
 "resourceArn": "arn:aws:rbin:us-west-2:123456789012:rule/ABCDEF01234",
 "tags": [
   {
     "key": "purpose",
     "value": "production"
   }
 ]
 },
 "responseElements": null,
 "requestID": "examplee-7962-49ec-8633-795efexample",
 "eventID": "example4-6826-4c0a-bdec-0bab1example",
 "readOnly": false,
 "eventType": "AwsApiCall",
 "managementEvent": true,
 "eventCategory": "Management",
 "recipientAccountId": "123456789012",
 "tlsDetails": {
 "tlsVersion": "TLSv1.2",
 "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
 "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
 }
 }
```


UntagResource


```
{
 "eventVersion": "1.08",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "123456789012",
 "arn": "arn:aws:iam::123456789012:root",
 "accountId": "123456789012",
 "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
```

```
"sessionContext": {
  "sessionIssuer": {
    "type": "Role",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:role/Admin",
    "accountId": "123456789012",
    "userName": "Admin"
  },
  "webIdFederationData": {},
  "attributes": {
    "mfaAuthenticated": "false",
    "creationDate": "2021-10-22T21:38:34Z"
  }
}
},
"eventTime": "2021-10-22T21:44:16Z",
"eventSource": "rbin.amazonaws.com",
"eventName": "UntagResource",
"awsRegion": "us-west-2",
"sourceIPAddress": "123.123.123.123",
"userAgent": "aws-cli/1.20.26 Python/3.6.14
Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 botocore/1.21.26",
"requestParameters": {
"resourceArn": "arn:aws:rbin:us-west-2:123456789012:rule/ABCDEF01234",
"tagKeys": [
  "purpose"
]
},
"responseElements": null,
"requestID": "example7-6c1e-4f09-9e46-bb957example",
"eventID": "example6-75ff-4c94-a1cd-4d5f5example",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "123456789012",
"tlsDetails": {
"tlsVersion": "TLSv1.2",
"cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
"clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
}
}
```

ListTagsForResource


```
{
 "eventVersion": "1.08",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "123456789012",
 "arn": "arn:aws:iam::123456789012:root",
 "accountId": "123456789012",
 "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
 "sessionContext": {
   "sessionIssuer": {
     "type": "Role",
     "principalId": "123456789012",
     "arn": "arn:aws:iam::123456789012:role/Admin",
     "accountId": "123456789012",
     "userName": "Admin"
   },
   "webIdFederationData": {},
   "attributes": {
     "mfaAuthenticated": "false",
     "creationDate": "2021-10-22T21:38:34Z"
   }
 }
 },
 "eventTime": "2021-10-22T21:42:31Z",
 "eventSource": "rbin.amazonaws.com",
 "eventName": "ListTagsForResource",
 "awsRegion": "us-west-2",
 "sourceIPAddress": "123.123.123.123",
 "userAgent": "aws-cli/1.20.26 Python/3.6.14
Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 botocore/1.21.26",
 "requestParameters": {
 "resourceArn": "arn:aws:rbin:us-west-2:123456789012:rule/ABCDEF01234"
 },
 "responseElements": null,
 "requestID": "example8-10c7-43d4-b147-3d9d9example",
 "eventID": "example2-24fc-4da7-a479-c9748example",
 "readOnly": true,
 "eventType": "AwsApiCall",
 "managementEvent": true,
 "eventCategory": "Management",
 "recipientAccountId": "123456789012",
 "tlsDetails": {
```

```
 "tlsVersion": "TLSv1.2",
 "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
 "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
 }
 }
```

LockRule

```
{
 "eventVersion": "1.08",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "123456789012",
 "arn": "arn:aws:iam::123456789012:root",
 "accountId": "123456789012",
 "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
 "sessionContext": {
   "sessionIssuer": {
     "type": "Role",
     "principalId": "123456789012",
     "arn": "arn:aws:iam::123456789012:role/Admin",
     "accountId": "123456789012",
     "userName": "Admin"
   },
   "webIdFederationData": {},
   "attributes": {
     "creationDate": "2022-10-25T00:45:11Z",
     "mfaAuthenticated": "false"
   }
 }
 },
 "eventTime": "2022-10-25T00:45:19Z",
 "eventSource": "rbin.amazonaws.com",
 "eventName": "LockRule",
 "awsRegion": "us-west-2",
 "sourceIPAddress": "123.123.123.123",
 "userAgent": "python-requests/2.25.1",
 "requestParameters": {
 "identifier": "jkrnexample",
 "lockConfiguration": {
   "unlockDelay": {
     "unlockDelayValue": 7,
     "unlockDelayUnit": "DAYS"
```

```
  }
 }
 },
 "responseElements": {
 "identifier": "jkrnexample",
 "description": "",
 "resourceType": "EBS_SNAPSHOT",
 "retentionPeriod": {
   "retentionPeriodValue": 7,
   "retentionPeriodUnit": "DAYS"
 },
 "resourceTags": [],
 "status": "available",
 "lockConfiguration": {
   "unlockDelay": {
     "unlockDelayValue": 7,
     "unlockDelayUnit": "DAYS"
   }
 },
 "lockState": "locked"
 },
 "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
 "eventID": "714fafex-2eam-42pl-913e-926d4example",
 "readOnly": false,
 "eventType": "AwsApiCall",
 "managementEvent": true,
 "recipientAccountId": "123456789012",
 "eventCategory": "Management",
 "tlsDetails": {
 "tlsVersion": "TLSv1.2",
 "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
 "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
 }
 }
```


UnlockRule


```
{
 "eventVersion": "1.08",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "123456789012",
 "arn": "arn:aws:iam::123456789012:root",
```

```
"accountId": "123456789012",
"accessKeyId": "AKIAIOSFODNN7EXAMPLE",
"sessionContext": {
  "sessionIssuer": {
    "type": "Role",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:role/Admin",
    "accountId": "123456789012",
    "userName": "Admin"
  },
  "webIdFederationData": {},
  "attributes": {
    "creationDate": "2022-10-25T00:45:11Z",
    "mfaAuthenticated": "false"
  }
}
},
"eventTime": "2022-10-25T00:46:17Z",
"eventSource": "rbin.amazonaws.com",
"eventName": "UnlockRule",
"awsRegion": "us-west-2",
"sourceIPAddress": "123.123.123.123",
"userAgent": "python-requests/2.25.1",
"requestParameters": {
"identifier": "jkrnexample"
},
"responseElements": {
"identifier": "jkrnexample",
"description": "",
"resourceType": "EC2_IMAGE",
"retentionPeriod": {
  "retentionPeriodValue": 7,
  "retentionPeriodUnit": "DAYS"
},
"resourceTags": [],
"status": "available",
"lockConfiguration": {
  "unlockDelay": {
    "unlockDelayValue": 7,
    "unlockDelayUnit": "DAYS"
  }
},
"lockState": "pending_unlock",
"lockEndTime": "Nov 1, 2022, 12:46:17 AM"
```

```
},
"requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
"eventID": "714fafex-2eam-42pl-913e-926d4example",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
"tlsVersion": "TLSv1.2",
"cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
"clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
}
}
```


回收站的服务端点

端点是用作 Amazon Web 服务入口点的 URL。回收站支持以下端点类型：

- IPv4 端点
- 同时 IPv4 支持和的双栈端点 IPv6

当您发出请求时，您可以指定要使用的端点和区域。如果您未指定终端节点，则默认使用该 IPv4 终端节点。要使用不同的端点类型，您必须在请求中指定。有关如何执行此操作的示例，请参阅指定端点。

有关终端节点列表，请参阅终端节点和中国的 ARNs 终 Amazon端节点。

主题

- IPv4 端点
- 双栈（IPv4 和 IPv6）端点
- 指定端点

IPv4 端点

IPv4 端点仅支持 IPv4 流量。 IPv4 终端节点适用于所有区域。

您必须将区域指定为端点名称的一部分。端点名称使用以下命名约定：

- rbin。 *region*.amazonaws.com.cn

例如，北京区域的 IPv4 终端节点是rbin.cn-north-1.amazonaws.com.cn。

双栈（IPv4 和 IPv6）端点

双栈端点同时支持 IPv4 和 IPv6 流量。双堆栈端点适用于所有区域。

要使用 IPv6，必须使用双堆栈终端节点。当您向双栈终端节点发出请求时，终端节点 URL 会解析为 IPv6 或 IPv4 地址，具体取决于您的网络和客户端使用的协议。

您必须将区域指定为端点名称的一部分。双堆栈端点名称使用以下命名约定：

- rbin.*region*.api.amazonwebservices.com.cn

例如，北京区域的双栈终端节点是rbin.cn-north-1.api.amazonwebservices.com.cn。

指定端点

以下示例显示如何使用 Amazon CLI为北京区域指定端点。

- 双堆栈

```
aws rbin get-rule \
--identifier rule_id \
--endpoint-url https://rbin.cn-north-1.api.amazonwebservices.com.cn
```

- IPv4

```
aws rbin get-rule \
--identifier rule_id \
--endpoint-url https://rbin.cn-north-1.amazonaws.com.cn
```

在 VPC 和回收站之间创建私有连接

您可以通过创建由 Amazon PrivateLink 提供支持的接口 VPC 端点在 VPC 和回收站之间建立私有连接。您可以像访问您的 VPC 一样访问回收站，无需使用互联网网关、NAT 设备、VPN 连接或 Amazon Direct Connect 连接。VPC 中的实例不需要公有 IP 地址便可与回收站进行通信。

我们将在您为接口端点启用的每个子网中创建一个端点网络接口。

有关更多信息，请参阅Amazon PrivateLink 指南 Amazon PrivateLink中的通过访问 Amazon 服务。

为回收站创建接口 VPC 端点

您可以使用 Amazon VPC 控制台或 Amazon CLI为回收站创建 VPC 端点。有关更多信息，请参阅 Amazon PrivateLink 指南中的创建 VPC 终端节点。

使用以下服务名称为回收站创建 VPC 端点：`com.amazonaws.region.rbin`

如果为端点启用私有 DNS，则可以使用该区域的默认 DNS 名称（例如 `rbin.us-east-1.amazonaws.com`）向回收站发送 API 请求。

为回收站创建 VPC 端点策略

默认情况下，允许通过端点对回收站进行完全访问。您可以使用 VPC 端点策略控制对接口端点的访问。您可以将端点策略附加到控制回收站访问的 VPC 端点。该策略指定以下信息：

- 可执行操作的主体。
- 可执行的操作。
- 可对其执行操作的资源。

有关更多信息，请参阅 Amazon VPC 用户指南中的使用 VPC 终端节点控制对服务的访问。

```
{
    "Statement": [
    {
        "Effect": "Allow",
        "Action": "rbin:*",
        "Resource": "*",
        "Principal": "*"
    },
    {
        "Effect": "Deny",
        "Action": "rbin:DeleteRule",
        "Resource": "*",
        "Principal": "*",
        "Condition": {
            "StringEquals" : {
                "rbin:Attribute/ResourceType": "EBS_SNAPSHOT"
            }
        }
    }]
```

```
}
```

Amazon EBS 中的安全性

云安全 Amazon 是重中之重。作为 Amazon 客户，您可以从专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构中受益。

安全是双方共同承担 Amazon 的责任。责任共担模式将其描述为云的安全性和云中的安全性：

- 云安全 — Amazon 负责保护在云中运行 Amazon 服务的基础架构 Amazon Web Services 云。Amazon 还为您提供可以安全使用的服务。作为的一部分，第三方审计师定期测试和验证我们安全的有效性。要了解适用于 Amazon Elastic Block Store 的合规计划，请参阅按合规计划划分的范围内的服务。
- 云端安全-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、您公司的要求以及适用的法律法规。

该文档帮助您了解如何在使用 Amazon EBS 时应用责任共担模式。以下主题说明如何配置 Amazon EBS 以实现安全性和合规性目标。您还将学习如何使用其他 Amazon 服务来帮助您监控和保护您的 Amazon EBS 资源。

主题

- Amazon EBS 中的数据保护
- Amazon EBS 的身份和访问管理
- Amazon EBS 的合规性验证
- Amazon EBS 中的数据弹性

Amazon EBS 中的数据保护

责任共担模式 Amazon 分适用于 Amazon Elastic Block Store 中的数据保护。如本模型所述 Amazon ，负责保护运行所有内容的全球基础架构 Amazon Web Services 云。您负责维护对托管在此基础结构上的内容的控制。您还负责您所使用的 Amazon Web Services 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。

出于数据保护目的，我们建议您保护 Amazon Web Services 账户 凭证并使用 Amazon IAM Identity Center 或 Amazon Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证（MFA）。

- 使用 SSL/TLS 与资源通信。 Amazon 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 Amazon CloudTrail。有关使用 CloudTrail 跟踪捕获 Amazon 活动的信息，请参阅《Amazon CloudTrail 用户指南》中的使用跟 CloudTrail 踪。
- 使用 Amazon 加密解决方案以及其中的所有默认安全控件 Amazon Web Services 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 Amazon 通过命令行界面或 API 进行访问时需要经过 FIPS 140-3 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 140-3 版》。

强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括您 Amazon Web Services 服务 使用控制台、API 或与 Amazon EBS 或其他机构 Amazon CLI合作时。 Amazon SDKs在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供网址，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

主题

- Amazon EBS 数据安全
- 静态和动态加密
- KMS 密钥管理

Amazon EBS 数据安全

Amazon EBS 卷作为未格式化的原始块储存设备呈现。这些设备是在 EBS 基础设施上创建的逻辑设备；Amazon EBS 服务可确保在客户使用或重复使用之前，这些设备为逻辑空白（即，原始数据块被归零或包含加密伪随机数据）。

如果您有要求在使用后和/或使用前使用特定方法擦除所有数据的程序，例如 DoD 5220.22-M（美国《国家工业安全计划操作手册》）或 NIST 800-88（《存储介质清理指南》）中详细说明的程序，您可以在 Amazon EBS 上执行此操作。该数据块级活动将反映到 Amazon EBS 服务的底层存储介质中。

静态和动态加密

Amazon EBS 加密是一种加密解决方案，使您能够使用 Amazon Key Management Service 加密密钥对亚马逊 EBS 卷和亚马逊 EBS 快照进行加密。EBS 加密操作发生在托管 Amazon EC2 实例的服务

器上，从而确保两者的安全，data-at-rest以及实例及其附加卷与任何后续快照data-in-transit之间的安全。有关更多信息，请参阅 Amazon EBS 加密。

KMS 密钥管理

创建加密的 Amazon EBS 卷或快照时，需要指定 Amazon Key Management Service 密钥。默认情况下，亚马逊 EBS 在您的账户和区域（ ）aws/ebs中使用亚马逊 EBS 的 Amazon 托管 KMS 密钥。不过，您可以指定自己创建和管理的客户托管的 KMS 密钥。使用客户托管的 KMS 密钥可以提高灵活性，包括提供创建、轮换和禁用 KMS 密钥的能力。

要使用客户托管的 KMS 密钥，您必须向用户授予使用 KMS 密钥的权限。有关更多信息，请参阅 用户的权限。

> **Important**
>
> Amazon EBS 仅支持对称 KMS 密钥。不能使用非对称 KMS 密钥来加密 Amazon EBS 卷和快照。要帮助确定 KMS 密钥是对称密钥还是非对称密钥，请参阅识别非对称 KMS 密钥。

对于每个卷，Amazon EBS 会要求 Amazon KMS 生成一个使用您指定的 KMS 密钥加密的唯一数据密钥。Amazon EBS 使用该卷存储加密数据密钥。然后，当您将卷连接到 Amazon EC2 实例时，Amazon EBS 会调 Amazon KMS 用解密数据密钥。Amazon EBS 使用管理程序内存中的明文数据密钥来加密卷的所有 I/O。有关更多信息，请参阅 Amazon EBS 加密的工作原理。

Amazon EBS 的身份和访问管理

Amazon Identity and Access Management (IAM) Amazon Web Services 服务 可帮助管理员安全地控制对 Amazon 资源的访问权限。IAM 管理员控制谁可以通过身份验证（登录）和获得授权（具有权限）来使用 Amazon EBS 资源。您可以使用 IAM Amazon Web Services 服务 ，无需支付额外费用。

主题

- 受众
- 使用身份进行身份验证
- 使用策略管理访问
- Amazon EBS 如何与 IAM 配合使用
- Amazon EBS 的 IAM 策略示例

- 排查 Amazon EBS 授权问题

受众

您的使用方式 Amazon Identity and Access Management (IAM) 会有所不同，具体取决于您在 Amazon EBS 中所做的工作。

服务用户 – 如果使用 Amazon EBS 服务来完成任务，管理员会为您提供所需的凭证和权限。随着用来完成工作的 Amazon EBS 功能增多，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。如果无法访问 Amazon EBS 中的功能，请参阅排查 Amazon EBS 授权问题。

服务管理员 – 如果您在公司负责管理 Amazon EBS 资源，您可能对 Amazon EBS 具有完全访问权限。您有义务为服务用户确定可访问的 Amazon EBS 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 EBS 搭配使用的更多信息，请参阅Amazon EBS 如何与 IAM 配合使用。

IAM 管理员 – 如果您是 IAM 管理员，您可能需要详细了解如何编写策略以管理对 Amazon EBS 的访问。要查看您可在 IAM 中使用的 Amazon EBS 基于身份的策略示例，请参阅Amazon EBS 的 IAM 策略示例。

使用身份进行身份验证

身份验证是您 Amazon 使用身份凭证登录的方式。您必须以 IAM 用户身份或通过担 Amazon Web Services 账户根用户任 IAM 角色进行身份验证（登录 Amazon）。

如果您 Amazon 以编程方式访问，则会 Amazon 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 Amazon 工具，则必须自己签署请求。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 root 用户

创建时 Amazon Web Services 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 Amazon Web Services 服务 和资源。此身份被称为 Amazon Web Services 账户 root 用户，使用您创

建账户时使用的电子邮件地址和密码登录即可访问该身份。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）使用与身份提供商的联合身份验证 Amazon Web Services 服务 通过临时证书进行访问。

联合身份是指您的企业用户目录、Web 身份提供商、Identity C 或者任何使用 Amazon Web Services 服务 通过身份源提供的凭据进行访问的用户。 Amazon Directory Service当联合身份访问时 Amazon Web Services 账户，他们将扮演角色，角色提供临时证书。

IAM 用户和群组

I AM 用户是您 Amazon Web Services 账户 内部对个人或应用程序具有特定权限的身份。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，您可以拥有一个名为的群组，IAMAdmins并向该群组授予管理 IAM 资源的权限。

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

I AM 角色是您内部具有特定权限 Amazon Web Services 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。要在中临时担任 IAM 角色 Amazon Web Services Management Console，您可以从用户切换到 IAM 角色（控制台）。您可以通过调用 Amazon CLI 或 Amazon API 操作或使用自定义 URL 来代入角色。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，对于某些资源 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 — 有些 Amazon Web Services 服务 使用其他 Amazon Web Services 服务服务中的功能。例如，当您在服务中拨打电话时，该服务通常会在 Amazon 中运行应用程序 EC2 或在 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 用户或角色在中执行操作时 Amazon，您被视为委托人。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 使用调用委托人的权限以及 Amazon Web Services 服务 向下游服务发出请求的请求。 Amazon Web Services 服务只有当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-服务相关角色是一种与服务相关联的服务角色。 Amazon Web Services 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 Amazon Web Services 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 A@@ mazon 上运行的应用程序 EC2 — 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证书。这比在 EC2 实例中存储访问密钥更可取。要为 EC2 实例分配 Amazon 角色并使其可供其所有应用程序使用，您需要创建一个附加到该实例的实例配置文件。实例配置文件包含角色并允许在 EC2 实例上运行的程序获得临时证书。有关更多信息，请参阅 IAM 用户指南中的使用 IAM 角色向在 A mazon EC2 实例上运行的应用程序授予权限。

使用策略管理访问

您可以 Amazon 通过创建策略并将其附加到 Amazon 身份或资源来控制中的访问权限。策略是其中的一个对象 Amazon ，当与身份或资源关联时，它会定义其权限。 Amazon 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以 JSON 文档的 Amazon 形式存储在中。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。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。拥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。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 Amazon Web Services 账户。托管策略包括 Amazon 托管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。委托人可以包括账户、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 IAM 中的 Amazon 托管策略。

访问控制列表 (ACLs)

访问控制列表 (ACLs) 控制哪些委托人（账户成员、用户或角色）有权访问资源。 ACLs 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Amazon S3 和 Amazon VPC 就是支持的服务示例 ACLs。 Amazon WAF要了解更多信息 ACLs，请参阅《亚马逊简单存储服务开发者指南》中的访问控制列表 (ACL) 概述。

其他策略类型

Amazon 支持其他不太常见的策略类型。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 (SCPs)- SCPs 是指定组织或组织单位 (OU) 的最大权限的 JSON 策略 Amazon Organizations。 Amazon Organizations 是一项用于对您的企业拥有的多 Amazon Web Services 账户 项进行分组和集中管理的服务。如果您启用组织中的所有功能，则可以将服务控制策略 (SCPs) 应用于您的任何或所有账户。SCP 限制成员账户中的实体（包括每个 Amazon Web Services 账户根用户实体）的权限。有关 Organization SCPs s 和的更多信息，请参阅《Amazon Organizations 用户指南》中的服务控制策略。
- 资源控制策略 (RCPs) — RCPs 是 JSON 策略，您可以使用它来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 限制成员账户中资源的权限，并可能影响身份（包括身份）的有效权限 Amazon Web Services 账户根用户，无论这些身份是否属于您的组织。有关 Organizations 的更多信息 RCPs，包括 Amazon Web Services 服务 该支持的列表 RCPs，请参阅Amazon Organizations 用户指南中的资源控制策略 (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。要了解在涉及多种策略类型时如何 Amazon 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

Amazon EBS 如何与 IAM 配合使用

在使用 IAM 管理对 Amazon EBS 的访问权限之前，您应该了解哪些 IAM 功能可用于 Amazon EBS。

可与 Amazon Elastic Block Store 配合使用的 IAM 功能

IAM 特征	Amazon EBS 支持
基于身份的策略	是

IAM 特征	Amazon EBS 支持
基于资源的策略	否
策略操作	是
策略资源	是
策略条件键	是
ACLs	否
ABAC（策略中的标签）	部分
临时凭证	是
主体权限	是
服务角色	是
服务相关角色	否

要全面了解 Amazon EBS 和其他 Amazon 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中与 IAM 配合使用的Amazon 服务。

Amazon EBS 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 EBS 基于身份的策略示例

要查看 Amazon EBS 基于身份的策略示例，请参阅Amazon EBS 的 IAM 策略示例。

Amazon EBS 内基于资源的策略

支持基于资源的策略：否

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。委托人可以包括账户、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。当委托人和资源处于不同位置时 Amazon Web Services 账户，可信账户中的 IAM 管理员还必须向委托人实体（用户或角色）授予访问资源的权限。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 EBS 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。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。

要查看 Amazon EBS 操作列表，请参阅《服务授权参考》中的 Amazon 操作、资源 EC2和条件密钥以及 Amazon EBS 的操作、资源和条件密钥。

Amazon EBS 中的策略操作在操作前使用`ec2`或`ebs`前缀。

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
  "ec2:action1",
  "ec2:action2"
]
```

要查看 Amazon EBS 基于身份的策略示例，请参阅Amazon EBS 的 IAM 策略示例。

Amazon EBS 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。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 EBS API 操作支持多个资源。要在单个语句中指定多个资源，请 ARNs 用逗号分隔。例如，DescribeVolumes 访问 vol-01234567890abcdef 和 vol-09876543210fedcba，因此主体必须具有访问这两个资源的权限。

```
"Resource": [
  "arn:aws:ec2:us-east-1:123456789012:volume/vol-01234567890abcdef",
  "arn:aws:ec2:us-east-1:123456789012:volume/vol-09876543210fedcba"
]
```

Amazon EBS 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。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，则使用逻辑OR运算来 Amazon 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 支持全局条件密钥和特定于服务的条件密钥。要查看所有 Amazon 全局条件键，请参阅 IAM 用户指南中的Amazon 全局条件上下文密钥。

例如，以下条件允许主体仅在卷类型为 gp2 时才对卷执行操作。

```
"Condition":{
  "StringLikeIfExists":{
    "ec2:VolumeType":"gp2"
  }
}
```

要查看 Amazon EBS 条件键的列表，请参阅《服务授权参考》中的操作、资源和条件键。

ACLs 在 Amazon EBS 中

支持 ACLs：否

访问控制列表 (ACLs) 控制哪些委托人（账户成员、用户或角色）有权访问资源。 ACLs 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

ABAC 与 Amazon EBS

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。在中 Amazon，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）和许多 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）。

将临时凭证用于 Amazon EBS

支持临时凭证：是

当你使用临时证书登录时，有些 Amazon Web Services 服务 不起作用。有关更多信息，包括哪些 Amazon Web Services 服务 适用于临时证书，请参阅 IAM 用户指南中的Amazon Web Services 服务与 IAM 配合使用的信息。

如果您使用除用户名和密码之外的任何方法登录，则 Amazon Web Services Management Console 使用的是临时证书。例如，当您 Amazon 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。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 Amazon API 手动创建临时证书。然后，您可以使用这些临时证书进行访问 Amazon。 Amazon 建议您动态生成临时证书，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 EBS 的跨服务主体权限

支持转发访问会话（FAS）：是

当您使用 IAM 用户或角色在中执行操作时 Amazon，您被视为委托人。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 使用调用委托人的权限以及 Amazon Web Services 服务 向下游服务发出请求的请求。 Amazon Web Services 服务只有当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。

Amazon EBS 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 EBS 的功能。仅当 Amazon EBS 提供相关指导时才编辑服务角色。

Amazon EBS 的服务相关角色

支持服务相关角色：否

服务相关角色是一种与服务相关联的 Amazon Web Services 服务服务角色。服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 Amazon Web Services 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

有关创建或管理服务相关角色的详细信息，请参阅能够与 IAM 搭配使用的Amazon 服务。在表中查找服务相关角色列中包含 Yes 的表。选择是链接以查看该服务的服务相关角色文档。

Amazon EBS 的 IAM 策略示例

默认情况下，用户和角色没有创建或修改 Amazon EBS 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。

主题

- 策略最佳实践
- 允许用户使用 Amazon EBS 控制台
- 允许用户查看他们自己的权限
- 允许用户使用卷
- 允许用户使用快照

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 EBS 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：

- 开始使用 Amazon 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的Amazon 托管策略。它们在你的版本中可用 Amazon Web Services 账户。我们建议您通过定义针对您的用例的 Amazon 客户托管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。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 Amazon Web Services 服务，例如 Amazon CloudFormation。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 Amazon Web Services 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。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。

允许用户使用 Amazon EBS 控制台

要访问 Amazon Elastic Block Store 控制台，您必须具有一组最低权限。这些权限必须允许您列出和查看有关您 Amazon Web Services 账户的 Amazon EBS 资源的详细信息。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于仅调用 Amazon CLI 或 Amazon API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

为确保用户和角色仍然可以使用 Amazon EBS 控制台，还需要将亚马逊 EBS *ConsoleAccess* 或*ReadOnly* Amazon 托管策略附加到实体。有关更多信息，请参阅《IAM 用户指南》中的为用户添加权限。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上或使用 Amazon CLI 或 Amazon API 以编程方式完成此操作的权限。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

允许用户使用卷

示例

- 示例：附加和分离卷
- 示例：创建卷
- 示例：创建带有标签的卷
- 示例：使用 Amazon EC2 控制台处理卷

示例：附加和分离卷

在 API 操作需要发起人指定多种资源时，您必须创建一个策略语句，允许用户访问所需的所有资源。如果使用 Condition 元素时需要其中一种或多种资源，则必须创建多个语句，如本示例所示。

以下策略允许用户将带有 “volume_user= iam-user-name” 标签的卷连接到带有 department=dev “” 标签的实例，并将这些卷与这些实例分离。如果您将此策略添加到 IAM 组，aws:username 策略变量将授权组中的每位用户向具有 volume_user 标签（将用户的用户名作为值）的实例挂载卷，或从那些实例分离这些卷。

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:instance/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/department": "dev"
        }
      }
   },
   {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/volume_user": "${aws:username}"
        }
      }
   }
  ]
}
```

示例：创建卷

以下策略允许用户使用 CreateVolumeAPI 操作。系统只允许用户创建加密且大小不足 20 GiB 的卷。

```
{
  "Version": "2012-10-17",
  "Statement": [
         {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateVolume"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition":{
         "NumericLessThan": {
             "ec2:VolumeSize" : "20"
          },
          "Bool":{
              "ec2:Encrypted" : "true"
          }
       }
    }
  ]
}
```

示例：创建带有标签的卷

下面的策略包含 aws:RequestTag 条件键，该条件键要求用户标记其使用标签 costcenter=115 和 stack=prod 创建的任何卷。如果用户不传递这些特定标签，或者根本不指定任何标签，则请求失败。

对于应用标签的资源创建操作，用户还必须具有使用 CreateTags 操作的权限。第二个语句使用 ec2:CreateAction 条件键使用户只能在 CreateVolume 上下文中创建标签。用户无法标记现有卷或任何其他资源。

```
{
  "Version": "2012-10-17",
  "Statement": [
        {
      "Sid": "AllowCreateTaggedVolumes",
      "Effect": "Allow",
      "Action": "ec2:CreateVolume",
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
```

```
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/costcenter": "115",
          "aws:RequestTag/stack": "prod"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition": {
        "StringEquals": {
            "ec2:CreateAction" : "CreateVolume"
        }
      }
    }
  ]
}
```

下面的策略允许用户创建卷而无需指定标签。仅当用户在 CreateTags 请求中指定了标签时，系统才会评估 CreateVolume 操作。如果用户指定了标签，则标签必须为 purpose=test。请求中不允许使用任何其他标签。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVolume",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition": {
         "StringEquals": {
             "aws:RequestTag/purpose": "test",
```

```
            "ec2:CreateAction" : "CreateVolume"
          },
         "ForAllValues:StringEquals": {
            "aws:TagKeys": "purpose"
          }
       }
    }
  ]
}
```

示例：使用 Amazon EC2 控制台处理卷

以下策略向用户授予使用 Amazon EC2 控制台查看和创建卷以及将卷附加和分离到特定实例的权限。

用户可以将任何卷附加到具有标签“purpose=test”的实例，也可以从这些实例分离卷。要使用 Amazon EC2 控制台连接卷，用户拥有使用该ec2:DescribeInstances操作的权限会很有帮助，因为这允许他们从 “连接卷” 对话框中预先填充的列表中选择一个实例。但是，这也会允许用户在控制台的 Instances 页面上查看所有实例，因此，您可以省略此操作。

在第一条语句中，需要 ec2:DescribeAvailabilityZones 操作以确保用户可以在创建卷时选择可用区。

用户无法标记其创建的卷 (卷创建期间或之后)。

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVolumes",
        "ec2:DescribeAvailabilityZones",
        "ec2:CreateVolume",
        "ec2:DescribeInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource": "arn:aws:ec2:region:111122223333:instance/*",
```

```
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/purpose": "test"
        }
      }
   },
   {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource": "arn:aws:ec2:region:111122223333:volume/*"
   }
   ]
}
```

允许用户使用快照

以下是（EBS 卷的point-in-time快照）和 CreateSnapshotCreateSnapshots（多卷快照）的策略示例。

示例

- 示例：创建快照
- 示例：创建快照
- 示例：创建具有标签的快照
- 示例：创建带有标签的多卷快照
- 示例：复制快照
- 示例：修改快照的权限设置

示例：创建快照

以下政策允许客户使用 CreateSnapshotAPI 操作。仅当卷已加密并且卷大小不超过 20 GiB 时，客户才能创建快照。

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
```

```
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*"
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1:account-id:volume/*",
         "Condition":{
            "NumericLessThan":{
               "ec2:VolumeSize":"20"
            },
            "Bool":{
               "ec2:Encrypted":"true"
            }
         }
      }
   ]
}
```

示例：创建快照

以下政策允许客户使用 CreateSnapshotsAPI 操作。只有当实例上的所有卷均为类型时，客户才能创建快照 GP2。

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":[
"arn:aws:ec2:us-east-1::snapshot/*",
"arn:aws:ec2:*:*:instance/*"
   ]
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1:*:volume/*",
         "Condition":{
            "StringLikeIfExists":{
               "ec2:VolumeType":"gp2"
```

```
            }
      }

       }
   ]
}
```

示例：创建具有标签的快照

下面的策略包含 aws:RequestTag 条件键，该条件键要求客户将标签 costcenter=115 和 stack=prod 应用于任何新快照。如果用户不传递这些特定标签，或者根本不指定任何标签，则请求失败。

对于应用标签的资源创建操作，客户还必须具有使用 CreateTags 操作的权限。第三个语句使用 ec2:CreateAction 条件键使客户只能在 CreateSnapshot 上下文中创建标签。客户无法标记现有卷或任何其他资源。

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1:account-id:volume/*"
      },
      {
         "Sid":"AllowCreateTaggedSnapshots",
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/costcenter":"115",
               "aws:RequestTag/stack":"prod"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateTags",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
```

```
                "ec2:CreateAction":"CreateSnapshot"
            }
         }
      }
   ]
}
```

示例：创建带有标签的多卷快照

下面的策略包含 aws:RequestTag 条件键，该条件键要求客户在创建多卷快照集时应用标签 costcenter=115 和 stack=prod。如果用户不传递这些特定标签，或者根本不指定任何标签，则请求失败。

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":[
"arn:aws:ec2:us-east-1::snapshot/*",
"arn:aws:ec2:*:*:instance/*",
"arn:aws:ec2:*:*:volume/*"

   ]
      },
      {
         "Sid":"AllowCreateTaggedSnapshots",
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/costcenter":"115",
               "aws:RequestTag/stack":"prod"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateTags",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
```

```
            "StringEquals":{
               "ec2:CreateAction":"CreateSnapshots"
            }
         }
      }
   ]
}
```

下面的策略允许客户创建快照而无需指定标签。仅在 CreateTags 或 CreateSnapshot 请求中指定标签的情况下，系统才会评估 CreateSnapshots 操作。可以在请求中省略标签。如果指定一个标签，则该标签必须是 purpose=test。请求中不允许使用任何其他标签。

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateTags",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/purpose":"test",
               "ec2:CreateAction":"CreateSnapshot"
            },
            "ForAllValues:StringEquals":{
               "aws:TagKeys":"purpose"
            }
         }
      }
   ]
}
```

下面的策略允许客户创建多卷快照集而无需指定标签。仅在 CreateTags 或 CreateSnapshot 请求中指定标签的情况下，系统才会评估 CreateSnapshots 操作。可以在请求中省略标签。如果指定一个标签，则该标签必须是 purpose=test。请求中不允许使用任何其他标签。

```
{
```

```
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateTags",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/purpose":"test",
               "ec2:CreateAction":"CreateSnapshots"
            },
            "ForAllValues:StringEquals":{
               "aws:TagKeys":"purpose"
            }
         }
      }
   ]
}
```

以下策略仅允许在以下情况下创建快照：源卷已使用客户的 User:*username* 进行标记，并且快照本身已使用 Environment:Dev 和 User:*username* 进行标记。客户可向快照添加其他标签。

```
{
   "Version":"2012-10-17",
   "Statement": [
           {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1:account-id:volume/*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/User":"${aws:username}"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshot",
```

```
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/Environment":"Dev",
               "aws:RequestTag/User":"${aws:username}"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateTags",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*"
      }
   ]
}
```

CreateSnapshots 的以下策略仅允许在以下情况下创建快照：源卷已使用客户的 User:*username* 进行标记，并且快照本身已使用 Environment:Dev 和 User:*username* 进行标记。

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1:*:instance/*",
 },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1:account-id:volume/*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/User":"${aws:username}"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
```

```
                "aws:RequestTag/Environment":"Dev",
                "aws:RequestTag/User":"${aws:username}"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":"ec2:CreateTags",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*"
      }
   ]
}
```

以下策略仅允许在以下情况下删除快照：快照已使用客户的 User:username 进行标记。

```
{
   "Version":"2012-10-17",
   "Statement": [
            {
         "Effect":"Allow",
         "Action":"ec2:DeleteSnapshot",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/User":"${aws:username}"
            }
         }
      }
   ]
}
```

以下策略允许客户创建快照，但在要创建的快照具有标签键 value=stack 时拒绝操作。

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":[
            "ec2:CreateSnapshot",
            "ec2:CreateTags"
         ],
         "Resource":"*"
```

```
      },
      {
         "Effect":"Deny",
         "Action":"ec2:CreateSnapshot",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "ForAnyValue:StringEquals":{
               "aws:TagKeys":"stack"
            }
         }
      }
   ]
}
```

以下策略允许客户创建快照，但在要创建的快照具有标签键 value=stack 时拒绝操作。

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect":"Allow",
         "Action":[
            "ec2:CreateSnapshots",
            "ec2:CreateTags"
         ],
         "Resource":"*"
      },
      {
         "Effect":"Deny",
         "Action":"ec2:CreateSnapshots",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "ForAnyValue:StringEquals":{
               "aws:TagKeys":"stack"
            }
         }
      }
   ]
}
```

以下策略允许您将多个操作整合到单个策略中。您只能在快照在区域 us-east-1 中创建时创建快照（在 CreateSnapshots 的上下文稿中）。您只能在快照正在区域 CreateSnapshots 中创建时且实例类型为 us-east-1 时创建快照（在 t2* 的上下文中）。

```
{
   "Version":"2012-10-17",
   "Statement": [
          {
         "Effect":"Allow",
         "Action":[
            "ec2:CreateSnapshots",
            "ec2:CreateSnapshot",
            "ec2:CreateTags"
         ],
         "Resource": [
            "arn:aws:ec2:*:*:instance/*",
            "arn:aws:ec2:*:*:snapshot/*",
            "arn:aws:ec2:*:*:volume/*"
         ],
         "Condition":{
            "StringEqualsIgnoreCase": {
              "ec2:Region": "us-east-1"
            },
            "StringLikeIfExists": {
              "ec2:InstanceType": ["t2.*"]
            }
         }
      }
   ]
}
```

示例：复制快照

为CopySnapshot操作指定的资源级权限适用于新快照和源快照。

只有在使用标签键 purpose 和标签值 production (purpose=production) 创建新快照时，以下示例策略才允许委托人复制快照。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCopySnapshotWithTags",
            "Effect": "Allow",
            "Action": "ec2:CopySnapshot",
            "Resource": "arn:aws:ec2:*:account-id:snapshot/*",
            "Condition": {
```

```
                "StringEquals": {
                    "aws:RequestTag/purpose": "production"
                }
            }
        }
    ]
}
```

以下示例策略仅在源快照归 Amazon 账户123456789012所有时才允许委托人复制快照。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCopySnapshotByOwner",
            "Effect": "Allow",
            "Action": "ec2:CopySnapshot",
            "Resource": "arn:aws:ec2:*:account-id:snapshot/*",
            "Condition": {
                "StringEquals": {
                    "ec2:Owner": "123456789012"
                }
            }
        }
    ]
}
```

以下示例策略仅允许委托人仅在使用标签密钥创建源快照时复制快照。CSISnapshotName

```
{
    "Effect": "Allow",
    "Action": "ec2:CopySnapshot",
    "Resource": "arn:aws:ec2:*::snapshot/${*}",
    "Condition": {
        "StringLike": {
            "aws:RequestTag/CSISnapshotName": "*"
         }
     }
},

{
    "Effect": "Allow",
    "Action": "ec2:CopySnapshot",
```

```
    "Resource": "arn:aws:ec2:*::snapshot/snap-*"
}
```

示例：修改快照的权限设置

以下策略仅在快照标有（其中*username*是客户的 Amazon 账户用户名）时才允许修改快照。User:*username*如果未满足此条件，则请求将失败。

```
{
   "Version":"2012-10-17",
   "Statement": [
           {
         "Effect":"Allow",
         "Action":"ec2:ModifySnapshotAttribute",
         "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/user-name":"${aws:username}"
            }
         }
      }
   ]
}
```

排查 Amazon EBS 授权问题

使用以下信息可帮助您诊断和修复在使用 Amazon EBS 和 IAM 时可能遇到的常见问题。

事务

- 我无权在 Amazon EBS 中执行操作
- 我无权执行 iam：PassRole
- 我想允许我以外的人访问我 Amazon Web Services 账户 的 Amazon EBS 资源

我无权在 Amazon EBS 中执行操作

如果 Amazon Web Services Management Console 告诉您您无权执行某项操作，则必须联系管理员寻求帮助。管理员是向您提供登录凭证的人。

当不具有 ec2:DescribeVolumes 权限的 mateojackson IAM 用户尝试使用控制台查看有关卷的详细信息时，就会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ec2:DescribeVolumes on resource: volume-id
```

在这种情况下，Mateo 要求 Amazon 管理员允许他描述音量。

我无权执行 iam：PassRole

如果您收到一个错误，指明您无权执行 `iam:PassRole` 操作，则必须更新策略以允许您将角色传递给 Amazon EBS。

有些 Amazon Web Services 服务 允许您将现有角色传递给该服务，而不是创建新的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 EBS 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，请联系您的 Amazon 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人访问我 Amazon Web Services 账户 的 Amazon EBS 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 (ACLs) 的服务，您可以使用这些策略向人们授予访问您的资源的权限。

要了解更多信息，请参阅以下内容：

- 要了解 Amazon EBS 是否支持这些功能，请参阅Amazon EBS 如何与 IAM 配合使用。
- 要了解如何提供对您拥有的资源的访问权限 Amazon Web Services 账户 ，请参阅 IAM 用户指南中的向您拥有 Amazon Web Services 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 Amazon Web Services 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 Amazon Web Services 账户
- 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。

Amazon EBS 的合规性验证

要了解是否属于特定合规计划的范围，请参阅Amazon Web Services 服务 “” Amazon Web Services 服务 中的 “按合规计划划分的范围”，然后选择您感兴趣的合规计划。 Amazon Web Services 服务 有关一般信息，请参阅合规计划。

您可以使用下载第三方审计报告 Amazon Artifact。有关更多信息，请参阅中的 “下载报告” Amazon Artifact。

您在使用 Amazon Web Services 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。 Amazon 提供了以下资源来帮助实现合规性：

- Security & Compliance：这些解决方案实施指南讨论了架构考虑因素，并提供了部署安全性和合规性功能的步骤。
- 合规资源 — 此工作簿和指南集合可能适用于您的行业和所在地区。
- 使用Amazon Config 开发人员指南中的规则评估资源 — 该 Amazon Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- Amazon Security Hub— 这 Amazon Web Services 服务 可以全面了解您的安全状态 Amazon。Security Hub 通过安全控制措施评估您的 Amazon 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控制措施的列表，请参阅 Security Hub 控制措施参考。
- Amazon GuardDuty — 它通过监控您的 Amazon Web Services 账户环境中是否存在可疑和恶意活动，来 Amazon Web Services 服务 检测您的工作负载、容器和数据面临的潜在威胁。 GuardDuty 通过满足某些合规性框架规定的入侵检测要求，可以帮助您满足各种合规性要求，例如 PCI DSS。

Amazon EBS 中的数据弹性

Amazon 全球基础设施是围绕 Amazon Web Services 区域 可用区构建的。 Amazon Web Services 区域 提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络连接。利用可用区，您可以设计和操作在可用区之间无中断地自动实现失效转移的应用程序和数据库。与传统的单个或多个数据中心基础结构相比，可用区具有更高的可用性、容错性和可扩展性。

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 全球基础设施外，Amazon EBS 还提供多项功能来帮助支持您的数据弹性和备份需求。

- 使用 Amazon Data Lifecycle Manager 自动处理 EBS 快照
- 跨区域复制 EBS 快照

Amazon EBS 的监控工具

监控是维护 Amazon Elastic Block Store 和其他 Amazon 解决方案的可靠性、可用性和性能的重要组成部分。 Amazon 提供以下监控工具，用于监视 Amazon EBS，在出现问题时进行报告，并在适当时自动采取措施：

- Amazon CloudTrail捕获由您或代表您发起的 API 调用和相关事件， Amazon Web Services 账户 并将日志文件传输到您指定的 Amazon S3 存储桶。您可以识别哪些用户和帐户拨打了电话 Amazon、发出呼叫的源 IP 地址以及呼叫发生的时间。 APIs 用于管理您的 EBS 卷和快照是亚马逊 EC2 API 的一部分。有关 CloudTrail 和亚马逊 EC2 API 的更多信息，请参阅亚马逊 EC2 用户指南 Amazon CloudTrail中的使用记录亚马逊 EC2 API 调用。
- Amazon 会实时 CloudWatch监控您的 Amazon 资源和您运行 Amazon 的应用程序。您可以收集和跟踪指标，创建自定义的控制平面，以及设置警报以在指定的指标达到您指定的阈值时通知您或采取措施。例如，您可以 CloudWatch 跟踪您的 Amazon EC2 实例的 CPU 使用率或其他指标，并在需要时自动启动新实例。有关更多信息，请参阅 the section called “Amazon CloudWatch”。
- Amazon EventBridge 可用于实现 Amazon 服务自动化，并自动响应系统事件，例如应用程序可用性问题或资源更改。来自 Amazon 服务的事件几乎实时 EventBridge 地传送到。您可以编写简单的规则来指示您关注的事件，并指示要在事件匹配规则时执行的自动化操作。有关更多信息，请参阅 the section called “Amazon EventBridge”。
- Amazon EBS 的详细性能统计数据为连接到基于 Nitro 的亚马逊实例的 Amazon EBS 卷提供了实时 I/O 性能统计数据。 EC2 有关更多信息，请参阅 Amazon EBS 的详细绩效统计数据。
- Amazon GuardDuty 可帮助检测您的 EC2 实例中潜在的恶意活动。 GuardDuty 恶意软件防护用于 EC2 扫描连接到您的 EC2 实例的 EBS 卷。有关更多信息，请参阅 the section called “Amazon GuardDuty”。

亚马逊 EBS 的亚马逊 CloudWatch 指标

Amazon CloudWatch 指标是统计数据，可用于查看、分析卷的运行行为并设置警报。

数据在 1 分钟期间内自动可用，无需收费。

当您从中获取数据时 CloudWatch，可以包含一个`Period`请求参数来指定返回数据的粒度。这不同于我们收集数据时所用的时间（ 1 分钟时间 ）。我们建议您在请求中指定的时间大于等于收集时间，从而确保返回数据有效。

您可以使用 CloudWatch API 或 Amazon EC2 控制台获取数据。控制台从 CloudWatch API 中获取原始数据，并根据这些数据显示一系列图表。根据您的需要，您既可以选择使用从 API 中获得的数据也可以选择使用控制台中的图表。

主题

- Amazon EBS 卷的指标
- 亚马逊 EBS 快照的指标
- Nitro 实例的指标
- 快速快照还原的指标
- Amazon EC2 控制台图表

Amazon EBS 卷的指标

AWS/EBS 命名空间包括连接到所有实例类型的 EBS 卷的以下指标。所有 Amazon EBS 卷类型都会自动向其发送 1 分钟指标 CloudWatch，但前提是该卷已连接到实例。

要从实例上的操作系统获取有关可用磁盘空间的信息，请参阅查看可用磁盘空间。

> **Note**
>
> 某些指标在基于 Nitro 系统构建的实例上存在差异。有关这些实例类型的列表，请参阅基于 Nitro 系统构建的实例。

指标	描述	单位	Dimensions	有意义的统计数据
VolumeAvgReadLatency	**Note** 支持连接到 Nitro 实例的所有卷类型。未针对附加到 Amazon ECS 的卷和 Amazon Fargate 任务发布。	毫秒	VolumeId | InstanceId	Minimum | Maximum

指标	描述	单位	Dimensions	有意义的统计数据
	在一分钟内完成读取操作所花费的平均时间。使用此指标来监控连接到 Amazon EC2 实例的 EBS 卷的平均 I/O 延迟。平均值是根据最后一分钟完成的 I/O 操作计算得出的。如果在最后一分钟内没有完成任何操作，则该指标的值为零。 对于启用了多重连接的卷，请使用`InstanceId` 维度查看特定卷实例连接的平均延迟。			

指标	描述	单位	Dimensions	有意义的统计数据
VolumeAvgWriteLatency	**Note** 支持连接到 Nitro 实例的所有卷类型。未针对附加到 Amazon ECS 的卷和 Amazon Fargate 任务发布。 在一分钟内完成写入操作所花费的平均时间。使用此指标来监控连接到 Amazon EC2 实例的 EBS 卷的平均 I/O 延迟。平均值是根据最后一分钟完成的 I/O 操作计算得出的。如果在最后一分钟内没有完成任何操作，则该指标的值为零。 对于启用了多重连接的卷，请使用InstanceId 维度查看特定卷实例连接的平均延迟。	毫秒	VolumeId | InstanceId	Minimum | Maximum

指标	描述	单位	Dimensions	有意义的统计数据
VolumeIOPSExceededCheck	**Note** 支持连接到 Nitro 实例的所有卷类型，但磁性 (standard) 除外。启用多重挂载的卷不支持此指标。未针对附加到 Amazon ECS 的卷和 Amazon Fargate 任务发布。 报告应用程序是否在最后一分钟内持续尝试驱动超过卷预配置 IOPS 性能的 IOPS 性能。此指标可以是0（未超过预配置 IOPS）或1（已超出预配置 IOPS）。有关更多信息，请参阅 使用监控 I/O 特性 CloudWatch。	None（无）	VolumeId | InstanceId	• Sum • Average • Minimum | Maximum

指标	描述	单位	Dimensions	有意义的统计数据
VolumeThroughputExceededCheck	**Note** 支持连接到 Nitro 实例的所有卷类型，但磁性 (standard) 除外。启用多重挂载的卷不支持此指标。未针对附加到 Amazon ECS 的卷和 Amazon Fargate 任务发布。 报告应用程序是否在最后一分钟内持续尝试提高超过卷预配置吞吐量性能的吞吐量。该指标可以是0（未超过预配置吞吐量）或1（已超出预配置吞吐量）。有关更多信息，请参阅。使用监控 I/O 特性 CloudWatch	无	VolumeId | InstanceId	• Sum • Average • Minimum | Maximum

指标	描述	单位	Dimensions	有意义的统计数据
VolumeReadBytes	提供有关指定时间段内的读取操作的信息。 • Sum 统计数据将报告该时间段内传输的总字节数。 • 该Average统计数据报告在指定时间段内读取的平均字节数。 • SampleCount 统计数据表示统计计算中使用的数据点数量。 **Note** 对于 Xen 实例，只有在卷上有读取活动时才报告数据。	字节	VolumeId	• Average • Sum • SampleCount • Minimum | Maximum：仅适用于附加到基于 Nitro 实例的卷

指标	描述	单位	Dimensions	有意义的统计数据
VolumeWriteBytes	提供有关指定时间段内的写入操作的信息 • Sum 统计数据将报告该时间段内传输的总字节数。 • 该Average统计数据报告在指定时间段内写入的平均字节数。 • SampleCount 统计数据表示统计计算中使用的数据点数量。 Note 对于 Xen 实例，只有在卷上有写入活动时才报告数据。	字节	VolumeId	• Average • Sum • SampleCount • Minimum | Maximum：仅适用于附加到基于 Nitro 实例的卷
VolumeReadOps	在指定时间的读取操作总数。读取操作在完成时计数。要计算该时间段的平均每秒读取操作数（读取 IOPS），请将该时间段的总读取操作数除以秒数。	计数	VolumeId	• Average • Sum • Minimum | Maximum：仅适用于附加到基于 Nitro 实例的卷

指标	描述	单位	Dimensions	有意义的统计数据
VolumeWriteOps	在指定时间的写入操作总数。写入操作在完成时计数。要计算该时间段的平均每秒写入操作数（写入 IOPS），请将该时间段的总写入操作数除以秒数。	计数	VolumeId	• Average • Sum • Minimum | Maximum：仅适用于附加到基于 Nitro 实例的卷
VolumeTotalReadTime	**Note** 启用多重挂载的卷不支持此指标。对于 Xen 实例，只有在卷上有读取活动时才报告数据。 指定时间段中所有读取操作耗费的总秒数。如果同时提交多个请求，该总数可能大于时间段长度。例如，对于长度为 1 分钟（60 秒）的时间段：如果该时间段内完成了 150 个操作，每个操作耗时 1 秒，值便是 150 秒。	秒	VolumeId	• Average：与附加到基于 Nitro 实例的卷无关 • Sum • Minimum | Maximum：仅适用于附加到基于 Nitro 实例的卷

指标	描述	单位	Dimensions	有意义的统计数据
VolumeTotalWriteTime	**Note** 启用多重挂载的卷不支持此指标。对于 Xen 实例，只有在卷上有写入活动时才报告数据。 指定时间段中所有写入操作耗费的总秒数。如果同时提交多个请求，该总数可能大于时间段长度。例如，对于长度为 1 分钟（60 秒）的时间段：如果该时间段内完成了 150 个操作，每个操作耗时 1 秒，值便是 150 秒。	秒	VolumeId	• Average：与附加到基于 Nitro 实例的卷无关 • Sum • Minimum | Maximum：仅适用于附加到基于 Nitro 实例的卷

指标	描述	单位	Dimensions	有意义的统计数据
VolumeIdleTime	**Note** 启用多重挂载的卷不支持此指标。 未提交读取或写入操作的指定时间段中的总秒数。	秒	VolumeId	• Average：与附加到基于 Nitro 实例的卷无关 • Sum • Minimum | Maximum：仅适用于附加到基于 Nitro 实例的卷
VolumeQueueLength	指定时间段中等待完成的读取和写入操作请求的数量。	计数	VolumeId	• Average • Sum：与附加到 Nitro 实例的卷无关 • Minimum | Maximum：仅适用于附加到 Nitro 实例的卷

指标	描述	单位	Dimensions	有意义的统计数据
VolumeStalledIOCheck	**Note** 仅适用于 Nitro 实例。对附加到 Amazon ECS 和 Amazon Fargate 任务的卷未发布。 报告卷在最后一分钟内是通过还是未通过停滞的 IO 检查。此指标可以是0（通过）或1（失败）。有关更多信息，请参阅 使用监控 I/O 特性 CloudWatch。	None（无）	VolumeId | InstanceId	• 总和 • 平均值 • 最小值 • 最大值

指标	描述	单位	Dimensions	有意义的统计数据
VolumeThroughputPercentage	**Note** 仅限预调配 IOPS SSD 卷。启用多重挂载的卷不支持此指标。 每秒传输的 I/O 操作数（IOPS）在为 Amazon EBS 卷预置的总 IOPS 中所占的百分比。预置 IOPS SSD 卷在 99.9% 的时间里可提供预置性能。写入过程中，如果一分钟内没有其他待处理的 I/O 请求，指标值就会是 100%。此外，由于您采取的操作（例如，在使用高峰期创建卷快照、在 non-EBS-optimized实例上运行卷或首次访问卷上的数据），卷的 I/O 性能可能会暂时降低。	百分比	VolumeId	• Average • Minimum | Maximum

指标	描述	单位	Dimensions	有意义的统计数据
VolumeConsumedReadWriteOps	**Note** 仅限预调配 IOPS SSD 卷。 指定时间段内使用的读取和写入操作的总量（规格化为 256K 容量单位）。每个小于 256K 的 I/O 操作算作使用了 1 IOPS。大于 256K 的 I/O 操作按 256K 容量单位计算。例如，1024K I/O 算作使用了 4 IOPS。	计数	VolumeId	• Average • Sum • Minimum | Maximum

指标	描述	单位	Dimensions	有意义的统计数据
BurstBalance	**Note** 仅适用于 gp2、st1 和 sc1 卷。 提供有关突增存储桶中剩余的 I/O 积分百分比（对于 gp2）或吞吐量积分（对于 st1 和 sc1）的信息。只有当卷处于活动状态时， CloudWatch 才会向其报告数据。如果未附加卷，则不会报告任何数据。如果卷的基准性能超过了最大突发性能，则绝不会使用积分。如果卷附加到基于 Nitro 系统构建的实例，则不会报告突增余额。对于其他实例，报告的突增余额是 100%。有关更多信息，请参阅 gp2 卷性能。	百分比	VolumeId	• Average • Sum：与附加到 Nitro 实例的卷无关。 • Minimum | Maximum

亚马逊 EBS 快照的指标

AWS/EBS命名空间包括以下用于 Amazon EBS 快照的指标。

指标	描述	单位	Dimensions	有意义的统计数据
SnapshotCopyBytesTransferred	复制到某个 Amazon 区域的快照数据量。	字节	sourceRegion	Sum

Nitro 实例的指标

AWS/EC2 命名空间包括所添加的卷的基于 Nitro 的实例（非裸机实例）的其他 Amazon EBS 指标。

指标	描述	单位	有意义的统计数据
EBSReadOps	在指定时间段内在挂载到实例的所有 Amazon EBS 卷中完成的读取操作数。要计算该时间段的平均每秒读取 I/O 操作数 (读取 IOPS)，请将该时间段的总操作数除以秒数。如果使用基本 (5 分钟) 监控，您可以将该数字除以 300 以计算读取 IOPS。如果您使用的是详细 (1 分钟) 监控，请将其除以 60。您也可以使用 CloudWatch 公制数学函数DIFF_TIME 来查找每秒的运算次数。例如，如果您将图表绘EBSReadOps 制 CloudWatch 为m1，则指标数学公式会m1/(DIFF_TIME(m1)) 返回以运算/秒为单位的量度。有关DIFF_TIME 和其他指标数学函数的更多信息，请参阅 Amazon CloudWatch 用户指南中的使用公制数学。	计数	• 总和 • 平均值 • 最小值 • 最大值
EBSWriteOps	在指定时间段内在附加到实例的所有 EBS 卷中完成的写入操作数。要计算该时间段的平均每秒写入 I/O 操作数 (写入 IOPS)，请将该时间段的总操作数除以秒数。如果使用基本 (5 分钟) 监控，您可以将该数字除以 300 以计算写入 IOPS。如果您使用的是详细（1 分钟）监	计数	• 总和 • 平均值 • 最小值 • 最大值

指标	描述	单位	有意义的统计数据
	控，请将其除以 60。您也可以使用 CloudWatch 公制数学函数DIFF_TIME 来查找每秒的运算次数。例如，如果您将图表绘EBSWriteOps 制 CloudWatch 为m1，则指标数学公式会m1/(DIFF_TIME(m1)) 返回以运算/秒为单位的量度。有关DIFF_TIME 和其他指标数学函数的更多信息，请参阅 Amazon CloudWatch 用户指南中的使用公制数学。		
EBSReadBytes	在指定时间段内从附加到实例的所有 EBS 卷中读取的字节数。报告的数字是在该时间段内读取的字节数。如果使用基本 (5 分钟) 监控，您可以将该数字除以 300 以计算每秒读取的字节数。如果您使用的是详细（1 分钟）监控，请将其除以 60。您也可以使用 CloudWatch 公制数学函数DIFF_TIME 来查找每秒的字节数。例如，如果您将图形化EBSReadBytes CloudWatch 为m1，则指标数学公式将m1/(DIFF_TIME(m1)) 返回以字节/秒为单位的指标。有关DIFF_TIME 和其他指标数学函数的更多信息，请参阅 Amazon CloudWatch 用户指南中的使用公制数学。	字节	• 总和 • 平均值 • 最小值 • 最大值

指标	描述	单位	有意义的统计数据
EBSWriteBytes	在指定时间段内写入附加到实例的所有 EBS 卷的字节数。报告的数字是在该时间段内写入的字节数。如果使用基本 (5 分钟) 监控，您可以将该数字除以 300 以计算每秒写入的字节数。如果您使用的是详细（1 分钟）监控，请将其除以 60。您也可以使用 CloudWatch 公制数学函数DIFF_TIME 来查找每秒的字节数。例如，如果您将图形化EBSWriteBytes CloudWatch 为m1，则指标数学公式将m1/(DIFF_TIME(m1)) 返回以字节/秒为单位的指标。有关DIFF_TIME 和其他指标数学函数的更多信息，请参阅 Amazon CloudWatch 用户指南中的使用公制数学。	字节	• 总和 • 平均值 • 最小值 • 最大值
EBSIOBalance%	提供有关突增存储桶中剩余的 I/O 积分百分比的信息。此指标仅对基本监控可用。此指标仅适用于某些 *.4xlarge 大小和更小的实例，这样的实例仅需 30 分钟便可突增到最高性能，且至少每 24 小时发生一次。有关更多信息，请参阅默认为 EBS 优化。 Sum 统计数据不适用于该指标。	百分比	• 最小值 • 最大值
EBSByteBalance%	提供有关突增存储桶中剩余的吞吐量积分百分比的信息。此指标仅对基本监控可用。此指标仅适用于某些 *.4xlarge 大小和更小的实例，这样的实例仅需 30 分钟便可突增到最高性能，且至少每 24 小时发生一次。有关更多信息，请参阅默认为 EBS 优化。 Sum 统计数据不适用于该指标。	百分比	• 最小值 • 最大值

快速快照还原的指标

AWS/EBS 命名空间包含以下用于快速快照还原的指标。

指标	描述	单位	Dimensions	有意义的统计数据
FastSnapshotRestoreCreditsBucketSize	可以累积的最大卷创建积分数。将为每个可用区的每个快照报告该指标。	无	SnapshotId | AvailabilityZone	• Average • Minimum | Maximum **Note** 最有意义的统计数据是 Average。Minimum 和 Maximum 统计数据的结果与 Average 相同，可以替换使用。
FastSnapshotRestoreCreditsBalance	可用的卷创建积分数。将为每个可用区的每个快照报告该指标。	无	SnapshotId | AvailabilityZone	• Average • Minimum | Maximum **Note** 最有意义的统计数据是 Average。Minimum 和 Maximum 统计数据的结果与 Average 相同，可以替换使用。

Amazon EC2 控制台图表

创建卷后，您可以在 Amazon EC2 控制台中查看该卷的监控图表。在控制台的 Volumes 页面上选择一个卷，然后选择 Monitoring。下表列出了显示的图表。右边的列描述了如何使用 CloudWatch API 中的原始数据指标来生成每个图表。所有的图表周期都是 5 分钟。

图表	使用原始指标描述
读取吞吐量（KiB/s）	`Sum(VolumeReadBytes) / Period / 1024`
写入吞吐量（KiB/s）	`Sum(VolumeWriteBytes) / Period / 1024`
读取操作（Ops/s）	`Sum(VolumeReadOps) / Period`
写入操作（Ops/s）	`Sum(VolumeWriteOps) / Period`
平均队列长度（操作数）	`Avg(VolumeQueueLength)`
空闲花费时间（%）	`Sum(VolumeIdleTime) / Period × 100`

平均读取大小（KiB/op）	`Avg(VolumeReadBytes) / 1024`
	
	对于基于 Nitro 的实例，以下公式使用CloudWatch公式计算出平均读取大小：
	
	`(Sum(VolumeReadBytes) / Sum(VolumeReadOps)) / 1024`
	
	`VolumeReadBytes` 和`VolumeReadOps` 指标可在 EBS CloudWatch 控制台中找到。

平均写入大小（KiB/op）	`Avg(VolumeWriteBytes) / 1024`
	
	对于基于 Nitro 的实例，以下公式使用CloudWatch公式计算出平均写入大小：
	
	`(Sum(VolumeWriteBytes) / Sum(VolumeWriteOps)) / 1024`

图表	使用原始指标描述
	VolumeWriteBytes 和VolumeWriteOps 指标可在 EBS CloudWatch 控制台中找到。
平均读取延迟（ms/op）	Avg(VolumeTotalReadTime) × 1000 对于基于 Nitro 的实例，以下公式使用CloudWatch指标数学推导出平均读取延迟： (Sum(VolumeTotalReadTime) / Sum(VolumeReadOps)) × 1000 VolumeTotalReadTime 和VolumeReadOps 指标可在 EBS CloudWatch 控制台中找到。
平均写入延迟（ms/op）	Avg(VolumeTotalWriteTime) × 1000 对于基于 Nitro 的实例，以下公式使用CloudWatch指标数学推导出平均写入延迟： (Sum(VolumeTotalWriteTime) / Sum(VolumeWriteOps)) * 1000 VolumeTotalWriteTime 和VolumeWriteOps 指标可在 EBS CloudWatch 控制台中找到。

对于平均延迟图表和平均大小图表，平均值通过该期间内完成的操作（读取或写入，以适用于图表者为准）总数计算得出。

亚马逊 EBS 的亚马逊 EventBridge 活动

Amazon EBS 会向亚马逊发送 EventBridge 针对卷和快照执行的操作的事件。借 EventBridge助，您可以建立触发编程操作以响应这些事件的规则。例如，您可以创建一个规则，在启用快照以快速恢复快照时向您的电子邮件发送通知。

中的 EventBridge 事件以 JSON 对象的形式表示。该事件独有的字段包含在 JSON 对象的“详细信息”部分。“事件”字段包含事件名称。“结果”字段包含触发事件的操作的已完成状态。有关更多信息，请参阅亚马逊 EventBridge 用户指南中的亚马逊 EventBridge 事件模式。

有关更多信息，请参阅什么是亚马逊 EventBridge？ 在《亚马逊 EventBridge 用户指南》中。

事件

- EBS 卷事件
- EBS 卷初始化事件
- EBS 卷修改事件
- EBS 快照事件
- EBS 快照归档事件
- EBS 快速快照还原事件
- Amazon Lambda 用于处理 EventBridge 事件

EBS 卷事件

当发生以下卷事件 EventBridge 时，Amazon EBS 会向发送事件。

事件

- 创建卷（createVolume）
- 删除卷（deleteVolume）
- 卷附加或重新附加（attachVolume、reattachVolume）
- 分离卷（detachVolume）

创建卷（createVolume）

创建卷的操作完成后，该`createVolume`事件就会发送到您的 Amazon 账户。但是，它不会被保存、记录或存档。此事件的结果可能是 `available` 或 `failed`。如果提供的内容无效 Amazon KMS key ，则创建将失败，如下例所示。

事件数据

下面的列表是 EBS 为成功的 `createVolume` 事件发送的 JSON 对象示例。

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Volume Notification",
```

```
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": [
       "arn:aws:ec2:us-east-1:012345678901:volume/vol-01234567"
    ],
    "detail": {
       "result": "available",
       "cause": "",
       "event": "createVolume",
       "request-id": "01234567-0123-0123-0123-0123456789ab"
    }
}
```

下面的列表是 EBS 在 createVolume 事件失败后发送的 JSON 对象的示例。失败原因是 KMS 密钥被禁用。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "sa-east-1",
  "resources": [
    "arn:aws:ec2:sa-east-1:0123456789ab:volume/vol-01234567",
  ],
  "detail": {
    "event": "createVolume",
    "result": "failed",
    "cause": "arn:aws:kms:sa-
east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is disabled.",
    "request-id": "01234567-0123-0123-0123-0123456789ab",
  }
}
```

以下是 EBS 在 createVolume 事件失败后发送的 JSON 对象的示例。失败原因是 KMS 密钥 正等待导入。

```
{
```

```
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "sa-east-1",
  "resources": [
    "arn:aws:ec2:sa-east-1:0123456789ab:volume/vol-01234567",
  ],
  "detail": {
    "event": "createVolume",
    "result": "failed",
    "cause": "arn:aws:kms:sa-
east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is pending import.",
    "request-id": "01234567-0123-0123-0123-0123456789ab",
  }
}
```

删除卷（deleteVolume）

删除卷的操作完成后，该deleteVolume事件就会发送到您的 Amazon 账户。但是，它不会被保存、记录或存档。此事件具有 deleted 结果。如果删除操作未完成，绝不会发送此事件。

事件数据

下面的列表是 EBS 为成功的 deleteVolume 事件发送的 JSON 对象示例。

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Volume Notification",
   "source": "aws.ec2",
   "account": "012345678901",
   "time": "yyyy-mm-ddThh:mm:ssZ",
   "region": "us-east-1",
   "resources": [
      "arn:aws:ec2:us-east-1:012345678901:volume/vol-01234567"
   ],
   "detail": {
      "result": "deleted",
      "cause": "",
      "event": "deleteVolume",
```

```
      "request-id": "01234567-0123-0123-0123-0123456789ab"
   }
}
```

卷附加或重新附加（attachVolume、reattachVolume）

将卷附加attachVolume或重新附加到实例时，或reattachVolume事件将发送到您的 Amazon 账户。但是，它不会被保存、记录或存档。如果您使用 KMS 密钥 加密 EBS 卷并且该 KMS 密钥 变为无效，则日后使用该 KMS 密钥 将卷附加或重新附加到实例时，EBS 会发送一个事件，如以下示例所示。

事件数据

下面的列表是 EBS 在 attachVolume 事件失败后发送的 JSON 对象的示例。失败原因是 KMS 密钥处于待删除状态。

> **Note**
>
> Amazon 服务器例行维护后，可能会尝试重新连接到卷。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
  "arn:aws:ec2:us-east-1:0123456789ab:volume/vol-01234567",
  "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab"
  ],
  "detail": {
    "event": "attachVolume",
    "result": "failed",
    "cause": "arn:aws:kms:us-
east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is pending deletion.",
    "request-id": ""
  }
}
```

下面的列表是 EBS 在 reattachVolume 事件失败后发送的 JSON 对象的示例。失败原因是 KMS 密钥 处于待删除状态。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-0123456789ab",
  "detail-type": "EBS Volume Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
  "arn:aws:ec2:us-east-1:0123456789ab:volume/vol-01234567",
  "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab"
  ],
  "detail": {
    "event": "reattachVolume",
    "result": "failed",
    "cause": "arn:aws:kms:us-
east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is pending deletion.",
    "request-id": ""
  }
}
```

分离卷（detachVolume）

当卷与 Amazon EC2 实例分离时，该detachVolume事件将发送到您的 Amazon 账户。

事件数据

以下是成功 detachVolume 事件的示例。

```
{
  "version":"0",
  "id":"2ec37298-1234-e436-70fc-c96b1example",
  "detail-type":"AWS API Call via CloudTrail",
  "source":"aws.ec2",
  "account":"123456789012",
  "time":"2024-03-18T16:35:52Z",
  "region":"us-east-1",
  "resources":[],
  "detail":
  {
```

```
    "eventVersion":"1.09",
    "userIdentity":
    {
      "type":"IAMUser",
      "principalId":"AIDAJT12345SQ2EXAMPLE",
      "arn":"arn:aws:iam::123456789012:user/administrator",
      "accountId":"123456789012",
      "accessKeyId":"AKIAJ67890A6EXAMPLE",
      "userName":"administrator"
    },
    "eventTime":"2024-03-18T16:35:52Z",
    "eventSource":"ec2.amazonaws.com",
    "eventName":"DetachVolume",
    "awsRegion":"us-east-1",
    "sourceIPAddress":"12.12.123.12",
    "userAgent":"aws-cli/2.7.12 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
ec2.detach-volume",
    "requestParameters":
    {
      "volumeId":"vol-072577c46bexample",
      "force":false
    },
    "responseElements":
    {
      "requestId":"1234513a-6292-49ea-83f8-85e95example",
      "volumeId":"vol-072577c46bexample",
      "instanceId":"i-0217f7eb3dexample",
      "device":"/dev/sdb",
      "status":"detaching",
      "attachTime":1710776815000
    },
    "requestID":"1234513a-6292-49ea-83f8-85e95example",
    "eventID":"1234551d-a15a-43eb-9e69-c983aexample",
    "readOnly":false,
    "eventType":"AwsApiCall",
    "managementEvent":true,
    "recipientAccountId":"123456789012",
    "eventCategory":"Management",
    "tlsDetails":
    {
      "tlsVersion":"TLSv1.3",
      "cipherSuite":"TLS_AES_128_GCM_SHA256",
      "clientProvidedHostHeader":"ec2.us-east-1.amazonaws.com"
    }
```

```
  }
}
```

EBS 卷初始化事件

当您创建具有卷初始化率的 Amazon EBS 卷时，该initializeVolume事件将在初始化完成后的五分钟内发送到您的 Amazon 账户。有关更多信息，请参阅 使用 Amazon EBS 预配置速率进行卷初始化。

> **Important**
>
> completionTime反映了我们生成事件的时间。由于事件是在初始化完成后的 5 分钟内生成的，因此最多completionTime可以在初始化完成后的五分钟内生成。

以下是示例事件。

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Volume Notification",
   "source": "aws.ec2",
   "account": "012345678901",
   "time": "yyyy-mm-ddThh:mm:ssZ",
   "region": "us-east-1",
   "resources": [
      "arn:aws:ec2:us-east-1:012345678901:volume/vol-01234567890abcdef"
   ],
   "detail": {
      "event": " initializeVolume",
      "result": "succeeded",
      "completionTime": "yyyy-mm-ddThh:mm:ssZ",
      "request-id": "01234567-0123-0123-0123-0123456789ab"
   }
}
```

EBS 卷修改事件

修改卷 EventBridge 时，Amazon EBS 会向发送modifyVolume事件。但是，它不会被保存、记录或存档。

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Volume Notification",
   "source": "aws.ec2",
   "account": "012345678901",
   "time": "yyyy-mm-ddThh:mm:ssZ",
   "region": "us-east-1",
   "resources": [
      "arn:aws:ec2:us-east-1:012345678901:volume/vol-03a55cf56513fa1b6"
   ],
   "detail": {
      "result": "optimizing",
      "cause": "",
      "event": "modifyVolume",
      "request-id": "01234567-0123-0123-0123-0123456789ab"
   }
}
```

EBS 快照事件

当发生以下卷事件 EventBridge 时，Amazon EBS 会向发送事件。

事件

- 创建单个快照（createSnapshot）
- 创建多个快照（createSnapshots）
- 复制快照（copySnapshot）
- 共享快照（shareSnapshot）

创建单个快照（createSnapshot）

创建快照的操作完成后，该`createSnapshot`事件就会发送到您的 Amazon 账户。但是，它不会被保存、记录或存档。此事件的结果可能是 `succeeded` 或 `failed`。

事件数据

下面的列表是 EBS 为成功的 `createSnapshot` 事件发送的 JSON 对象示例。在 `detail` 部分，`source` 字段包含源卷的 ARN。`startTime` 和 `endTime` 字段表示快照的创建何时开始以及何时完成。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
     "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "createSnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::us-west-2:volume/vol-01234567",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ"  }
}
```

创建多个快照（createSnapshots）

创建多卷快照的操作完成后，该createSnapshots事件就会发送到您的 Amazon 账户。此事件的结果可能是 succeeded 或 failed。

事件数据

下面的列表是 EBS 为成功的 createSnapshots 事件发送的 JSON 对象示例。在该detail部分中，该source字段包含多卷快照集的源卷。 ARNs startTime 和 endTime 字段表示快照的创建何时开始以及何时完成。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Multi-Volume Snapshots Completion Status",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
```

```
    "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
    "arn:aws:ec2::us-east-1:snapshot/snap-012345678"
  ],
  "detail": {
    "event": "createSnapshots",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "snapshots": [
      {
        "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
        "source": "arn:aws:ec2::us-east-1:volume/vol-01234567",
        "status": "completed"
      },
      {
        "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-012345678",
        "source": "arn:aws:ec2::us-east-1:volume/vol-012345678",
        "status": "completed"
      }
    ]
  }
}
```

下面的列表是 EBS 在 `createSnapshots` 事件失败后发送的 JSON 对象的示例。失败的原因是多卷快照集的一个或多个快照未能完成。的值`snapshot_id`是失败快照 ARNs 的值。`startTime`并`endTime`表示创建快照操作的开始和结束时间。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Multi-Volume Snapshots Completion Status",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
    "arn:aws:ec2::us-east-1:snapshot/snap-012345678"
  ],
"detail": {
    "event": "createSnapshots",
```

```
    "result": "failed",
    "cause": "Snapshot snap-01234567 is in status error",
   "request-id": "",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "snapshots": [
      {
        "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
        "source": "arn:aws:ec2::us-east-1:volume/vol-01234567",
        "status": "error"
      },
      {
        "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-012345678",
        "source": "arn:aws:ec2::us-east-1:volume/vol-012345678",
        "status": "error"
      }
    ]
  }
}
```

复制快照（copySnapshot）

复制快照的操作完成后，该copySnapshot事件就会发送到您的 Amazon 账户。但是，它不会被保存、记录或存档。此事件的结果可能是 succeeded 或 failed。

在detail部分中，source是源快照的 ARN，snapshot_id也是快照副本的 ARN。startTime并endTime指明复制操作何时开始和结束。 incremental表示快照副本是增量快照 (true) 还是完整快照 (false)。 transferType表示快照复制操作是标准复制操作还是基于时间的复制操作。有关更多信息，请参阅 Amazon EBS 快照和 EBS 支持的基于时间的副本 AMIs。

如果您要跨区域复制快照，则事件将在目标区域中发出。

场景 1：标准快照复制操作完成

以下是标准快照复制操作成功完成时向您的账户发送的事件示例。请注意，transferType 为 standard 。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
```

```
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "copySnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::eu-west-1:snapshot/snap-76543210",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "incremental": "true",
    "transferType": "standard"
  }
}
```

场景 2：基于时间的快照复制操作在完成持续时间内完成

以下是基于时间的快照复制操作在其完成持续时间内完成时向您的账户发送的事件示例。请注意，这transferType表明这是一项基于时间的快照复制操作。time-based completionDurationStartTime表示完成持续时间何时开始。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "copySnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
```

```
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::eu-west-1:snapshot/snap-76543210",
    "incremental": "true",
    "completionDurationStartTime":"2024-11-16T06:27:33.816Z",
    "transferType": "time-based"
  }
}
```

场景 3：基于时间的快照复制操作已完成，但错过了请求的完成持续时间

当基于时间的快照复制操作完成但未能达到请求的完成持续时间时， CloudWatch 会向您的账户发送两个事件。以下是这些事件的示例。

- 即使复制操作仍在进行中，第一个事件也会在错过完成时长后立即发送到您的账户。对于此事件，detail-type是EBS Copy Snapshot Missed Completion Duration，并missedCompletionDurationCause提供了原因。

```
{
 "version":"0",
 "id":"fd90eb95-0938-e02c-cf55-b81363b8ac12",
 "detail-type":"EBS Copy Snapshot Missed Completion Duration",
 "source":"aws.ec2",
 "account":"123456789012",
 "time":"2024-11-19T18:17:08Z",
 "region":"us-east-1",
 "resources": ["arn:aws:ec2:us-east-1:123456789012:snapshot/snap-01234567890abcedf"],
 "detail":{
   "event":"copySnapshot",
   "missedCompletionDurationCause":"Snapshot copy was not able to meet the specified
 completion duration because your snapshot copy operation throughput quota was
 exceeded.",
   "snapshot_id":"arn:aws:ec2:us-
east-1:123456789012:snapshot/snap-01234567890abcedf",
   "source":"arn:aws:ec2:us-east-1:123456789012:snapshot/snap-00987654321fedcba",
   "startTime": "Sun Nov 24 22:32:55 UTC 2024",
   "transferType": "time-based"
   }
}
```

- 只有在快照完成后，第二个事件才会发送到您的账户。该事件包括missedCompletionDurationCause，这提供了原因。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "copySnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::eu-west-1:snapshot/snap-76543210",
    "incremental": "true",
    "completionDurationStartTime":"2024-11-16T06:27:33.816Z",
    "missedCompletionDurationCause":"Snapshot copy was not able to meet the specified
 completion duration because your snapshot copy operation throughput quota was
 exceeded.",
    "transferType": "time-based"
  }
}
```

场景 4：快照复制操作失败

以下是快照复制操作失败时向您的账户发送的事件示例。请注意`failed`，`result`这表示操作失败。

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
```

```
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "copySnapshot",
    "result": "failed",
    "cause": "Source snapshot ID is not valid",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": "arn:aws:ec2::eu-west-1:snapshot/snap-76543210",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

共享快照（shareSnapshot）

当另一个 Amazon 账户与其共享快照时，该shareSnapshot事件就会发送到您的账户。但是，它不会被保存、记录或存档。结果始终是 succeeded。

事件数据

下面是 EBS 在 shareSnapshot 事件完成后发送的 JSON 对象的示例。在该detail部分中，的值source是与您共享快照的用户的 Amazon 账号。 startTime并endTime表示共享快照操作的开始和结束时间。仅在与其他用户共享私有快照时，系统才会发送 shareSnapshot 事件。共享公有快照不会触发该事件。

```
{
  "version": "0",
  "id": "01234567-01234-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "012345678901",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2::us-west-2:snapshot/snap-01234567"
  ],
  "detail": {
    "event": "shareSnapshot",
    "result": "succeeded",
    "cause": "",
```

```
    "request-id": "",
    "snapshot_id": "arn:aws:ec2::us-west-2:snapshot/snap-01234567",
    "source": 012345678901,
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ"
  }
}
```

EBS 快照归档事件

Amazon EBS 发出与快照归档操作相关的事件。

EBS 快速快照还原事件

当快照的快速还原状态发生变化 EventBridge 时，Amazon EBS 会向发送事件。尽最大努力发出事件。

以下是此事件的示例数据。

```
{
   "version": "0",
   "id": "01234567-0123-0123-0123-012345678901",
   "detail-type": "EBS Fast Snapshot Restore State-change Notification",
   "source": "aws.ec2",
   "account": "123456789012",
   "time": "yyyy-mm-ddThh:mm:ssZ",
   "region": "us-east-1",
   "resources": [
      "arn:aws:ec2:us-east-1::snapshot/snap-03a55cf56513fa1b6"
   ],
   "detail": {
      "snapshot-id": "snap-1234567890abcdef0",
      "state": "optimizing",
      "zone": "us-east-1a",
      "message": "Client.UserInitiated - Lifecycle state transition",
   }
}
```

可能的 `state` 值为 `enabling`、`optimizing`、`enabled`、`disabling` 和 `disabled`。

`message` 的可能值如下所示：

`Client.InvalidSnapshot.InvalidState - The requested snapshot transitioned to an invalid state (Error)`

启用快速快照还原的请求失败，并且状态转换为 disabling 或 disabled。无法为该快照启用快速快照还原。

`Client.UserInitiated`

状态成功转换为 enabling 或 disabling。

`Client.UserInitiated - Lifecycle state transition`

状态成功转换为 optimizing、enabled 或 disabled。

`Server.InsufficientCapacity - There was insufficient capacity available to satisfy the request`

由于容量不足而导致启用快速快照还原的请求失败，并且状态转换为 disabling 或 disabled。等待，然后重试。

`Server.InternalError - An internal error caused the operation to fail`

由于内部错误而导致启用快速快照还原的请求失败，并且状态转换为 disabling 或 disabled。等待，然后重试。

`Client.InvalidSnapshot.InvalidState - The requested snapshot was deleted or access permissions were revoked`

快照的快速快照还原状态已转换为 disabling 或 disabled，因为快照已被快照所有者删除或取消共享。无法为已删除或不再与您共享的快照启用快速快照还原。

Amazon Lambda 用于处理 EventBridge 事件

您可以使用 Amazon EBS 和 Amazon EventBridge 来自动执行数据备份工作流程。这要求您创建 IAM 策略、处理事件的 Amazon Lambda 函数以及匹配传入事件并将其路由到 Lambda 函数的 EventBridge 规则。

以下过程使用 `createSnapshot` 事件自动将已完成的快照复制到其他区域，以用于灾难恢复。

将已完成的快照复制到其他区域

1. 创建一个 IAM 策略（如以下示例所示的策略），以提供使用该CopySnapshot操作和写入 EventBridge 日志的权限。将策略分配给将处理 EventBridge 事件的用户。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CopySnapshot"
      ],
      "Resource": "*"
    }
  ]
}
```

2. 在 Lambda 中定义一个可在控制台中使用的函数。 EventBridge 下面用 Node.js 编写的示例 Lambda 函数是在亚马逊 EBS 发出匹配`createSnapshot`的事件（表示快照已完成）EventBridge 时调用的。该函数被调用后，它会将快照从 `us-east-2` 复制到 `us-east-1`。

```
// Sample Lambda function to copy an EBS snapshot to a different Region

var AWS = require('aws-sdk');
var ec2 = new AWS.EC2();

// define variables
var destinationRegion = 'us-east-1';
var sourceRegion = 'us-east-2';
console.log ('Loading function');

//main function
exports.handler = (event, context, callback) => {

    // Get the EBS snapshot ID from the event details
    var snapshotArn = event.detail.snapshot_id.split('/');
    const snapshotId = snapshotArn[1];
```

```
    const description = `Snapshot copy from ${snapshotId} in ${sourceRegion}.`;
    console.log ("snapshotId:", snapshotId);

    // Load EC2 class and update the configuration to use destination Region to
 initiate the snapshot.
    AWS.config.update({region: destinationRegion});
    var ec2 = new AWS.EC2();

    // Prepare variables for ec2.modifySnapshotAttribute call
    const copySnapshotParams = {
        Description: description,
        DestinationRegion: destinationRegion,
        SourceRegion: sourceRegion,
        SourceSnapshotId: snapshotId
    };

    // Execute the copy snapshot and log any errors
    ec2.copySnapshot(copySnapshotParams, (err, data) => {
        if (err) {
            const errorMessage = `Error copying snapshot ${snapshotId} to Region
 ${destinationRegion}.`;
            console.log(errorMessage);
            console.log(err);
            callback(errorMessage);
        } else {
            const successMessage = `Successfully started copy of snapshot
 ${snapshotId} to Region ${destinationRegion}.`;
            console.log(successMessage);
            console.log(data);
            callback(null, successMessage);
        }
    });
};
```

为确保您的 Lambda 函数可在 EventBridge 控制台中使用，请在 EventBridge 事件发生的区域创建该函数。有关更多信息，请参见Amazon Lambda 开发人员指南。

3. 打开亚马逊 EventBridge 控制台，网址为https://console.aws.amazon.com/events/。
4. 在导航窗格中，选择规则，然后选择创建规则。
5. 对于 Step 1: Define rule detail（步骤 1：定义规则详细信息），请执行以下操作：

   a. 为 Name（名称）和 Description（描述）输入值。

b. 对于 Event bus（事件总线），保持 default（默认）。

c. 确保 Enable the rule on the selected event bus（在选定的事件总线上启用该规则）已开启。

d. 对于 Event type（事件类型），选择 Rule with an event pattern（具有事件模式的规则）。

e. 选择下一步。

6. 对于 Step 2: Build event pattern（步骤 2：构建事件模式），执行以下操作：

a. 在事件源中，选择Amazon 事件或 EventBridge 合作伙伴事件。

b. 在事件模式部分中，对于事件源，确保选择了Amazon 服务，对于Amazon 服务，请选择EC2。

c. 对于事件类型，选择 EBS 快照通知，选择特定事件，然后选择 createSnapshot。

d. 选择特定结果，然后选择已成功。

e. 选择下一步。

7. 对于 Step 3: Select targets（步骤 3：选择目标），请执行以下操作：

a. 对于目标类型，选择Amazon 服务。

b. 对于 Select target（选择目标），选择 Lambda function（Lambda 函数），对于 Function（函数），选择之前创建的函数。

c. 选择 Next（下一步）。

8. 对于 Step 4: Configure tags（步骤 4：配置标签），如果需要，为规则指定标签，然后选择 Next（下一步）。

9. 对于 Step 5: Review and create（步骤 5：查看并创建），查看规则，然后选择 Create rule（创建规则）。

现在，您的规则应该会显示在规则选项卡中。在所示的示例中，当您下次复制快照时，EBS 应该会发送您所配置的事件。

Amazon EBS 的详细绩效统计数据

Amazon EBS NVMe 区块设备为连接到基于 Nitro的亚马逊实例的 Amazon EBS 卷提供实时、高分辨率的 I/O 性能统计数据。 EC2 这些统计数据以聚合计数器的形式显示，这些计数器将在卷连接到实例的期间内保留。这些统计数据提供有关累积操作数、发送和接收的字节数以及读取和写入 I/O 操作所花费时间的详细信息。此外，统计数据还包括读取和写入 I/O 操作的直方图，以及您的应用程序超过 EBS 卷或附加实例的预配置 IOPS 或吞吐量限制的总时间。

您可以以最多 1 秒的间隔收集这些统计数据。如果发出请求的频率超过 1 秒，则 NVMe 驱动程序可能会将请求以及其他管理命令排入队列，以便稍后处理。

注意事项

- 所有 Amazon EBS 卷类型都支持统计数据。
- 只有连接到 Amazon Nitro System 上构建的实例的卷才支持统计数据。
- 这些统计数据适用于启用了多重连接的卷。在查看启用了多重连接的卷的统计数据时，统计数据特定于该实例的附件，并且仅反映该实例的使用情况。
- 统计数据无需额外费用即可获得。

统计信息

Amazon EBS NVMe 区块设备提供以下统计数据：

统计名称	全名	类型	描述
total_read_ops	读取操作总数	计数器	已完成的读取操作总数。
total_write_ops	写入操作总数	计数器	已完成的写入操作的总数。
total_read_bytes	读取的总字节数	计数器	传输的读取字节总数。
total_write_bytes	写入总字节数	计数器	传输的写入字节总数。
total_read_time	总读取时间	计数器	所有已完成的读取操作所花费的总时间，以微秒为单位。
total_write_time	总写入时间	计数器	所有已完成的写入操作所花费的总时间，以微秒为单位。
ebs_volume_performance_exce	需求总时间超过容量预配置 IOPS	计数器	IOPS 需求超过卷预配置 IOPS 性能的总时间（以微秒为单位）。

统计名称	全名	类型	描述
eded_iops			
ebs_volume_performance_exceeded_tp	总时间需求超过了容量预置吞吐量	计数器	吞吐量需求超过卷预配置吞吐量性能的总时间（以微秒为单位）。
ec2_instance_ebs_performance_exceeded_iops	总时间需求超过了 EC2 实例的 IOPS 性能	计数器	EBS 卷超过所连接的 Amazon EC2 实例的最大 IOPS 性能的总时间（以微秒为单位）。
ec2_instance_ebs_performance_exceeded_tp	总时间需求超过了 EC2 实例的吞吐量性能	计数器	EBS 卷超过所连接的 Amazon EC2 实例的最大吞吐量性能的总时间（以微秒为单位）。
volume_queue_length	卷队列长度	时间点	等待完成的读取和写入操作的数量。
read_io_latency_histogram	读取 I/O 直方图	直方图 *	在每个延迟 bin 内完成的读取操作数，以微秒为单位。
write_io_latency_histogram	写入 I/O 直方图	直方图 *	在每个延迟 bin 内完成的写入操作数，以微秒为单位。

> **Note**
>
> * 直方图统计数据仅表示成功完成的 I/O 操作。停滞或受损的 I/O 操作不包括在内，但会在统计数据中显而易见，`volume_queue_length`统计数据以 point-in-time统计数据形式呈现。

访问统计数据

必须直接从连接了 Amazon EBS 卷的实例访问统计数据。您可以使用以下方法之一访问统计信息。

Amazon CloudWatch

您可以将 Amazon CloudWatch 代理配置为从您的实例收集统计数据，并在中将其作为自定义指标提供 CloudWatch。然后，您可以使用中的指标 CloudWatch 来分析 I/O 模式、跟踪性能趋势、创建自定义仪表板以及根据性能阈值设置自动警报。

有关配置 CloudWatch 代理的更多信息，请参阅以下内容：

- 创建 CloudWatch 代理配置文件
- 收集 Amazon EBS NVMe 驱动程序指标

在 Amazon O CloudWatch bservability EKS 附加版本`4.1.0`及更高版本中，当启用 Amazon EBS CSI 驱动程序指标时，统计数据会自动收集。有关更多信息，请参阅 Amazon EBS NVMe 驱动程序指标。

ebsnvme script

该`ebsnvme`脚本可以在 ama zon-ec2- utils Github 存储库中找到。

访问统计数据

1. Connect 连接到该卷所连接的实例。
2. 从 `amazon-ec2-utils` Github 存储库下载`ebsnvme`脚本。

```
wget https://raw.githubusercontent.com/amazonlinux/amazon-ec2-utils/refs/heads/main/ebsnvme
```

3. 修改脚本的权限以使其可执行。

```
sudo chmod +x ./ebsnvme
```

4. 运行ebsnvme脚本并指定该卷的设备名称。

```
sudo ./ebsnvme stats /dev/nvme0n1
```

nvme-cli tool (Amazon Linux only)

访问统计数据

1. Connect 连接到该卷所连接的实例。
2. 2024 年 11 月 12 日之后 AMIs 发布的亚马逊 Linux 包含该nvme-cli工具的最新版本。如果您使用的是较旧的亚马逊 Linux AMI，请更新该nvme-cli工具。

```
sudo yum install nvme-cli
```

3. 运行以下命令并为该卷指定设备名称。

```
nvme amzn stats /dev/nvme0n1
```

Prometheus

您可以使用开源监控应用程序 Prometheus 和适用于 Prometheus 的亚马逊托管服务来监控统计数据。这使得跨容器和 Kubernetes 环境大规模监控 Amazon EBS 卷变得更加容易。在 Amazon EBS CSI 驱动程序版本 v1.37.0 及更高版本中，详细的性能统计数据将作为与 Prometheus 兼容的终端节点公开，用于导出到 Promethe /metrics us。

有关更多信息，请参阅《适用于 Promethe us 的亚马逊托管服务用户指南》中的 “向适用于 Prometheus 的亚马逊托管服务工作区提取指标”。

Amazon f GuardDuty or Amazon EBS

Amazon GuardDuty 是一项威胁检测服务，可帮助保护您的账户、容器、工作负载和 Amazon 环境中的数据。使用机器学习 (ML) 模型以及异常和威胁检测功能， GuardDuty 持续监控不同的日志源和运行时活动，以识别环境中的潜在安全风险和恶意活动并确定其优先级。

其中的恶意软件保护功能 GuardDuty 会扫描与您的 Amazon EC2 实例和容器工作负载关联的 Amazon EBS 卷，以检测潜在威胁。 GuardDuty 提供了两种方法来做到这一点：

- 启用恶意软件防护 — 当 GuardDuty 生成表明在 Amazon EC2 实例或容器工作负载中可能存在恶意软件的发现结果时，它将自动对可能受感染的资源启动恶意软件扫描。
- 在@@ 不启用恶意软件保护的情况下使用按需恶意软件扫描 — 提供您的亚马逊 EC2 实例的亚马逊资源名称 (ARN) 以启动按需扫描。

有关更多信息，请参阅 Amazon GuardDuty 用户指南。

Amazon EBS 的限额

您的每个配额 Amazon Web Services 账户 都有默认配额，以前称为限制 Amazon Web Services 服务。除非另有说明，否则，每个限额是区域特定的。您可以请求增加某些配额，但其他一些配额无法增加。

要查看 Amazon EBS 的限额，请打开“服务限额”控制台。在导航窗格中，选择 Amazon 服务，然后选择 Amazon Elastic Block Store（Amazon EBS）。要请求提高配额，请参阅《Service Quotas 用户指南》中的请求提高配额。

您 Amazon Web Services 账户 拥有以下与 Amazon EBS 相关的配额。

名称	默认值	可调整	描述
每卷的已归档快照	每个受支持的区域：25 个	是	每个卷的存档快照的最大数量。
CompleteSnapshot 每个账户的请求数	每个受支持的区域：每秒 10 个	否	每个账户允许的最大 CompleteSnapshot 请求数。
每个目标区域的并发快照副本	每个受支持的区域：20 个	否	针对单个目标区域的并发快照副本的最大数量。
每个 Cold HDD（sc1）卷的并发快照数	每个受支持的区域：1 个	否	此区域中每个冷 HDD (sc1) 卷的并发快照的最大数量。
每个通用型 SSD（gp2）卷的并发快照数	每个受支持的区域：5 个	否	此区域中每个通用型 SSD (gp2) 卷的并发快照的最大数量。
每个通用型 SSD（gp3）卷的并发快照数	每个受支持的区域：5 个	否	此区域中每个通用型 SSD (gp3) 卷的并发快照的最大数量。

名称	默认值	可调整	描述
每个磁介质（标准）卷的并发快照数	每个受支持的区域：5 个	否	此区域中每个磁介质（标准）卷的并发快照的最大数量。
每个预置 IOPS SSD（io1）卷的并发快照数	每个受支持的区域：5 个	否	此区域中每个预调配 IOPS SSD (io1) 卷的并发快照的最大数量。
每个预置 IOPS SSD（io2）卷的并发快照数	每个受支持的区域：5 个	否	此区域中每个预调配 IOPS SSD (io2) 卷的并发快照的最大数量。
每个吞吐量优化型 HDD（st1）卷的并发快照数	每个受支持的区域：1 个	否	此区域中每个吞吐量优化型 HDD (st1) 卷的并发快照的最大数量。

名称	默认值	可调整	描述
快速快照还原	us-east-1：5 个 us-east-2：5 个 us-west-1：5 个 us-west-2：5 个 af-south-1：5 个 ap-east-1：5 个 ap-northeast-1：5 个 ap-northeast-2：5 个 ap-northeast-3：5 个 ap-south-1：5 个 ap-southeast-1：5 个 ap-southeast-2：5 个 ap-southeast-3：5 个 ca-central-1：5 个 eu-central-1：5 个 eu-north-1：5 个	是	此区域中可为快速快照还原启用的快照的最大数量。

名称	默认值	可调整	描述
	eu-south-1：5 个 eu-west-1：5 个 eu-west-2：5 个 eu-west-3：5 个 me-south-1：5 个 sa-east-1：5 个 每个其他支持的区域：5 个		
GetSnapshotBlock 每个账户的请求数	us-east-1：每秒 5,000 us-east-2：每秒 5,000 us-west-2：每秒 5,000 ap-southeast-1：每秒 5,000 eu-west-1：每秒 5,000 每个其他支持的区域：每秒 1,000	是	每个账户允许的最大 GetSnapshotBlock 请求数。
GetSnapshotBlock 每个快照的请求数	每个受支持的区域：每秒 1000 个	否	每个快照允许的最大 GetSnapshotBlock 请求数。

名称	默认值	可调整	描述
预调配 IOPS SSD（io1）卷	每个受支持的区域：30 万个	是	此区域中可跨预调配 IOPS SDD (io1) 卷预调配的 IOPS 的最大聚合数量。
预置 IOPS SSD（io2）卷的 IOPS	每个受支持的区域：10 万个	是	此区域中可跨预调配 IOPS SDD (io2) 卷预调配的 IOPS 的最大聚合数量。
预置 IOPS SSD（io1）卷的 IOPS 修改	每个受支持的区域：50 万个	是	此区域中可跨预调配 IOPS SDD (io1) 卷在卷修改中请求的 IOPS 的最大聚合数量。
预置 IOPS SSD（io2）卷的 IOPS 修改	每个受支持的区域：10 万个	是	此区域中，跨预调配 IOPS SSD（io2）卷的卷修改请求中的最大当前（从）IOPS 值和请求的（到）IOPS 值。
每个账户正在进行的快照存档	每个受支持的区域：25 个	是	每个账户正在进行的快照存档的最大数量。
每个账户正在通过存档进行的快照还原	每个受支持的区域：5 个	是	每个账户正在通过存档进行的快照还原的最大数量。
ListChangedBlocks 每个账户的请求数	每个受支持的区域：每秒 50 个	否	每个账户允许的最大 ListChangedBlocks 请求数。

名称	默认值	可调整	描述
ListSnapshotBlocks 每个账户的请求数	每个受支持的区域：每秒 50 个	否	每个账户允许的最大 ListSnapshotBlocks 请求数。
每个区域并发卷创建请求之间的卷初始化预配置速率	每个受支持的区域：5000 个	是	可以在该区域的并发卷创建请求中请求的卷初始化的最大汇总预配置速率，以 MiB/s 为单位。
PutSnapshotBlock 每个账户的请求数	us-east-1：每秒 5,000 us-east-2：每秒 5,000 us-west-2：每秒 5,000 ap-southeast-1：每秒 5,000 eu-west-1：每秒 5,000 每个其他支持的区域：每秒 1,000	是	每个账户允许的最大 PutSnapshotBlock 请求数。
PutSnapshotBlock 每个快照的请求数	每个受支持的区域：每秒 1000 个	否	每个快照允许的最大 PutSnapshotBlock 请求数。
每个区域的快照数	每个受支持的区域：10 万个	是	每个区域的最大快照数。

名称	默认值	可调整	描述
StartSnapshot 每个账户的待处理快照	每个受支持的区域：100 个	否	每个账户可以使用 StartSnapshot API 创建的最大待处理快照数。
StartSnapshot 每个账户的请求数	每个受支持的区域：每秒 10 个	否	每个账户允许的最大 StartSnapshot 请求数。
Cold HDD（sc1）卷存储（单位 TiB）	af-south-1：300 个 ap-east-1：300 个 ap-northeast-3：300 ap-southeast-3：300 eu-south-1：300 个 me-south-1：300 个 每个其他支持的区域：50 个	是	此区域中可跨冷 HDD (sc1) 卷预调配的最大聚合存储容量（以 TiB 为单位）。

名称	默认值	可调整	描述
通用型 SSD（gp2）卷存储（单位 TiB）	af-south-1：300 个 ap-east-1：300 个 ap-northeast-3：300 ap-southeast-3：300 eu-south-1：300 个 me-south-1：300 个 每个其他支持的区域：50 个	是	此区域中可跨通用型 SSD (gp2) 卷预调配的最大聚合存储容量（以 TiB 为单位）。

名称	默认值	可调整	描述
通用型 SSD（gp3）卷存储（单位 TiB）	af-south-1：300 个 ap-east-1：300 个 ap-northeast-3：300 ap-southeast-3：300 eu-south-1：300 个 me-south-1：300 个 每个其他支持的区域：50 个	是	此区域中可跨通用型 SSD (gp3) 卷预调配的最大聚合存储容量（以 TiB 为单位）。

名称	默认值	可调整	描述
磁介质（标准）卷存储（单位 TiB）	af-south-1：300 个 ap-east-1：300 个 ap-northeast-3：300 ap-southeast-3：300 eu-south-1：300 个 me-south-1：300 个 每个其他支持的区域：50 个	是	此区域中可跨磁介质（标准）卷预调配的最大聚合存储容量（以 TiB 为单位）。

名称	默认值	可调整	描述
预置 IOPS SSD（io1）卷存储（单位 TiB）	af-south-1：300 个 ap-east-1：300 个 ap-northeast-3：300 ap-southeast-3：300 eu-south-1：300 个 me-south-1：300 个 每个其他支持的区域：50 个	是	此区域中可跨预调配 IOPS SDD (io1) 卷预调配的最大聚合存储容量（以 TiB 为单位）。
预置 IOPS SSD（io2）卷存储（单位 TiB）	每个受支持的区域：20 个	是	此区域中可跨预调配 IOPS SDD (io2) 卷预调配的最大聚合存储容量（以 TiB 为单位）。

名称	默认值	可调整	描述
吞吐量优化型 HDD（st1）卷存储（单位 TiB）	af-south-1：300 个 ap-east-1：300 个 ap-northeast-3：300 ap-southeast-3：300 eu-south-1：300 个 me-south-1：300 个 每个其他支持的区域：50 个	是	此区域中可跨吞吐量优化型 HDD (st1) 卷预调配的最大聚合存储容量（以 TiB 为单位）。
冷 HDD（sc1）卷存储修改（单位 TiB）	每个受支持的区域：500 个	是	此区域中可跨冷 HDD (sc1) 卷在卷修改中请求的最大聚合存储容量（以 TiB 为单位）。
通用型 SSD（gp2）卷存储修改（单位 TiB）	每个受支持的区域：500 个	是	此区域中可跨通用型 SSD (gp2) 卷在卷修改中请求的最大聚合存储容量（以 TiB 为单位）。
通用型 SSD（gp3）卷存储修改（单位 TiB）	每个受支持的区域：500 个	是	此区域中可跨通用型 SSD (gp3) 卷在卷修改中请求的最大聚合存储容量（以 TiB 为单位）。

名称	默认值	可调整	描述
磁介质（标准）卷存储修改（单位 TiB）	每个受支持的区域：500 个	是	此区域中可跨磁介质（标准）卷在卷修改中请求的最大聚合存储容量（以 TiB 为单位）。
预置 IOPS SSD（io1）卷存储修改（单位 TiB）	每个受支持的区域：500 个	是	此区域中可跨预调配 IOPS SDD (io1) 卷在卷修改中请求的最大聚合存储容量（以 TiB 为单位）。
预置 IOPS SSD（io2）卷存储修改（单位 TiB）	每个受支持的区域：20 个	是	此区域中可跨预调配 IOPS SDD (io2) 卷在卷修改中请求的最大聚合存储容量（以 TiB 为单位）。
吞吐量优化型 HDD（st1）卷存储修改（单位 TiB）	每个受支持的区域：500 个	是	此区域中可跨吞吐量优化型 HDD (st1) 卷在卷修改中请求的最大聚合存储容量（以 TiB 为单位）。
每个目标区域基于时间的快照副本吞吐量	每个支持的区域：2000 个	是	每个目标区域基于时间的快照复制操作的最大账户级别吞吐量，以 MiB/sec 为单位。

注意事项

- 限额可能会随时间而改变。Amazon EBS 将持续监控您在每个区域内的预调配存储和 IOPS 使用情况，并可能根据您的使用量自动增加您在每个区域内的配额。尽管 Amazon EBS 可以根据使用情况自动提高限额，您仍可以在需要时请求提高限额。例如，假设您计划在美国东部（弗吉尼亚州北部）使用超过当前限额的 gp3 存储量，则可以在计划的使用量基础上请求提高该区域对该卷类型的限额。

- 每个目标区域的并发快照副本限额无法使用服务限额进行调整。但是，您可以通过联系 Amazon Support 来申请增加此配额。
- IOPS 修改和存储修改限额适用于可并发进行修改的卷的当前聚合值（大小或 IOPS，具体取决于限额）。您可对当前总值（大小或 IOPS）不超过限额的卷提出并发修改请求。例如，如果预调配 IOPS SSD（io1）卷的 IOPS 修改的限额为 50,000，则可对任意数量的 io1 卷并发提出 IOPS 修改请求，前提是它们的当前 IOPS 总和等于或小于 50,000。如果您有三个 io1 卷，每个卷都预调配了 20,000 IOPS，则可并发请求对两个卷进行 IOPS 修改（20,000 * 2 < 50,000）。如果您并发提出第三个卷的 IOPS 修改请求，则超出了限额，该请求将失败（20,000 * 3 > 50,000）。
- Amazon EBS 对每个实例启动请求的 EBS 卷数量具有以下不可调整的限制。
  - 2500 — us-east-1、us-west-2、eu-west-1 和 ap-northeast-1
  - 500 — 所有其他区域

  此限制适用于您发出的实例启动请求以及 Amazon 服务（例如 Amazon EMR）代表您发出的实例启动请求。如果您的实例启动请求因超过此限制而失败，我们建议您在启动请求中调整 EBS 卷配置，以确保卷数低于限制，或者建议您与技术客户经理（TAM）合作，探索在不超过限制的情况下启动集群的其他方法。

《Amazon EBS 用户指南》的文档历史记录

下表介绍了 Amazon EBS 的文档版本。

变更	说明	日期
Local Zones 中的本地快照	现在，您可以在 Local Zones 中创建本地快照。	2025年5月15日
Amazon EBS 用于卷初始化的预配置速率	现在，您可以在创建 Amazon EBS 卷时指定卷初始化速率，以确保这些卷在可预测的时间内完全初始化。	2025年5月6日
基于时间的 AMI 复制	现在，您可以请求为 EBS 支持的 AMI 复制操作设置完成期限，以确保在特定的时间期限内完成 AMI 复制。	2025 年 2 月 25 日
完整快照大小	现在，您可以使用亚马逊 EC2 控制台和 Amazon CLI查看亚马逊 EBS 快照的完整大小。	2025年2月11日
Amazon Data Lifecycle Manager IPv6 支持	Amazon Data Lifecycle Manager 现在提供双栈终端节点，可同时支持 IPv4 和 IPv6 流量。	2025 年 2 月 7 日
回收站 IPv6 支持	回收站现在提供双堆栈端点，支持两者 IPv4 兼而有之 IPv6 。	2024 年 12 月 19 日
专用 Local Zones 中的本地快照	现在，您可以在 Dedicated Local Zones 中创建本地快照。	2024 年 12 月 16 日
AWSDataLifecycleManagerServiceRole Amazon 托管策略已更新	AWSDataLifecycleManagerServiceRole Amazon 托管策略已更新，包	2024 年 12 月 16 日

	括ec2:DescribeAvailabilityZones 操作权限。	
用于封锁 EBS 快照的公开访问的声明性策略	现在，您可以使用声明性策略应用账户级别的设置，以同时在多个地区和账户中阻止对快照的公开访问。有关更多信息，请参阅《Amazon Organizations User Guide》中的 Declarative policies。	2024 年 12 月 1 日
基于时间的快照副本	现在，您可以请求快照复制操作的完成持续时间，以确保快照副本在特定的时间范围内完成。	2024 年 11 月 26 日
回收站的排除标签	现在，您可以向区域级保留规则添加排除标签，以排除具有特定标签的资源。	2024 年 11 月 19 日
Amazon CloudFormation 支持回收站	现在，您可以使用创建和管理回收站保留规则 Amazon CloudFormation。	2024 年 11 月 18 日
Amazon EBS 的详细绩效统计数据	Amazon EBS NVMe 区块设备为连接到基于 Nitro的亚马逊实例的 Amazon EBS 卷提供实时、高分辨率的 I/O 性能统计数据。 EC2	2024 年 11 月 12 日

亚马逊 EBS 交易 CloudWatch 量的新指标	现在，您可以使用VolumeAvgReadLatency 、VolumeAvgWriteLatency VolumeIOPSExceededCheck 、和VolumeThroughputExceededCheck Amazon CloudWatch 指标来监控卷性能。	2024 年 10 月 30 日
跨账户启用 Amazon Data Lifecycle Manager 默认策略	您可以使用 Amazon CloudFormation StackSets 启用跨 Amazon 组织或特定 Amazon 账户的 Amazon Data Lifecycle Manager 默认策略。	2024 年 4 月 26 日
VolumeStalledIOCheck 指标	您可以使用 VolumeStalledIOCheck 指标来检查卷在最后一分钟是否通过停滞的 IO 检查。	2023 年 11 月 16 日
Amazon Data Lifecycle Manager 默认策略	现在，您可以为 EBS 快照创建 Amazon Data Lifecycle Manager 的默认策略和 EBS 支持的策略 AMIs ，以备份一个区域中的所有卷和实例。	2023 年 11 月 16 日
Amazon EBS 快照锁	您可以锁定 Amazon EBS 快照以保护其免受意外或恶意删除，或者将其以 WORM 格式存储一段特定的时间。	2023 年 11 月 15 日
屏蔽对快照的公共访问权限	现在，您可以屏蔽对快照的公共访问权限，以防止公开共享快照。	2023 年 11 月 9 日

Amazon Data Lifecycle Manager 前置和后置脚本	现在，您可以在 Amazon Data Lifecycle Manager 快照策略中使用前置和后置脚本来自动化应用程序一致快照的生命周期。	2023 年 11 月 7 日
NVMe 保留	支持多重连接的io2卷支持 NVMe 预留，这是一组行业标准的存储屏蔽协议。	2023 年 9 月 18 日
在 Amazon EBS 上进行故障测试	Amazon FIS 用于暂时停止 EBS 卷与其连接的实例之间的 I/O，以测试您的工作负载如何处理 I/O 中断。	2023 年 1 月 27 日
回收站保留规则锁定	您可以锁定保留规则，以保护其免遭意外或恶意修改和删除。	2022 年 11 月 23 日
回收站的条件键	您可以使用 `rbin:Request/ResourceType` 和 `rbin:Attribute/ResourceType` 条件键来筛选回收站访问权限请求。	2022 年 6 月 14 日
io2 Block Express 卷	您可以修改 io2 Block Express 卷的大小和预调配 IOPS，并为其启用快速快照还原。	2022 年 5 月 31 日
的回收站 AMIs	回收站允许您恢复意外删除的内容 AMIs。	2022 年 2 月 3 日
Amazon EBS 快照回收站	Amazon EBS 快照回收站是一项快照还原功能，能够使您还原意外删除的快照。	2021 年 11 月 29 日

Amazon Data Lifecycle Manager 的 AMI 弃用支持	EBS 支持的 Amazon Data Lifecycle Manager 的 AMI 策略可能会被弃用。 AMIs AWSDataLifecycleManagerServiceRoleForAMIManagement Amazon 托管策略已更新为支持此功能。	2021 年 8 月 23 日
CloudWatch Amazon Data Lifecycle Manager 的指标	您可以使用亚马逊监控您的 Amazon Data Lifecycle Manager 政策 CloudWatch。	2021 年 7 月 28 日
CloudTrail EBS Direct 的数据事件 APIs	ListSnapshotBlocks、ListChangedBlocks、GetSnapshotBlock、和 PutSnapshotBlock APIs 可以在中记录数据事件 CloudTrail。	2021 年 7 月 27 日
io2 Block Express 卷	io2 Block Express 卷现已正式发布。	2021 年 7 月 19 日
对 io2 卷的多重挂载支持	您现在可以为 Amazon EBS 多重挂载启用预置 IOPS SSD（io2）卷。	2020 年 12 月 18 日
Amazon Data Lifecycle Manager	使用 Amazon Data Lifecycle Manager 自动执行共享快照和跨 Amazon 账户复制快照的过程。	2020 年 12 月 17 日
gp3 卷	一种新 Amazon EBS 通用型 SSD 卷类型。您可以在创建或修改卷时指定预置 IOPS 和吞吐量。	2020 年 12 月 1 日

吞吐量优化型 HDD h 和 Cold HDD 卷大小	吞吐量优化 HDD (st1) 和冷 HDD (sc1) 卷的大小范围可为 125 GiB 到 16 TiB。	2020 年 11 月 30 日
Amazon Data Lifecycle Manager	您可以使用 Amazon Data Lifecycle Manager 自动创建、保留和删除 EBS 支持的 AMIs 内容。	2020 年 11 月 9 日
Amazon Data Lifecycle Manager	Amazon Data Lifecycle Manager 策略最多可配置四个计划。	2020 年 9 月 17 日
适用于 Amazon EBS 的预调配 IOPS SSD（io2）卷	预置 IOPS SSD（io2）卷旨在提供 99.999% 的容量耐用性且 AFR 不高于 0.001%。	2020 年 8 月 24 日
快速快照还原	您可以为与您共享的快照启用快速快照还原。	2020 年 7 月 21 日
Amazon EBS 快速快照还原	您可以在 EBS 快照上启用快速快照还原，以确保从快照创建的 EBS 卷在创建时已完全初始化，并立即交付所有预配置性能。	2019 年 11 月 20 日
Amazon EBS 多卷快照	您可以跨连接到实例的多个 EBS 卷拍摄精确 point-in-time、数据协调和崩溃一致的快照。 EC2	2019 年 5 月 29 日
Amazon EBS 默认加密	在区域中启用默认加密后，将使用用于 EBS 加密的默认 KMS 密钥 加密在区域中创建的所有新 EBS 卷。	2019 年 5 月 23 日

自动化快照生命周期	您可以使用 Amazon Data Lifecycle Manager 来自动创建和删除 EBS 卷的快照。	2018 年 7 月 12 日
在挂载的 EBS 卷上进行修改	由于大多数 EBS 卷已连接到大多数 EC2 实例，因此您可以修改卷大小、类型和 IOPS，而无需分离卷或停止实例。	2017 年 2 月 13 日
在两者之间复制加密的 Amazon EBS 快照 Amazon Web Services 账户	您现在可以在 Amazon Web Services 账户之间复制加密的 EBS 快照。	2016 年 6 月 21 日
吞吐量优化型 HDD 和 Cold HDD 卷类型	您现在可以创建经过吞吐量优化的 HDD (st1) 以及冷数据 HDD (sc1) 卷。	2016 年 4 月 19 日
通用型 SSD 卷类型	通用型 SSD 卷提供经济实惠的存储，是广泛工作负载的理想选择。这些卷可提供不超过 10 毫秒的延迟，能突增至 3000 IOPS 很长时间，基准性能为 3 IOPS/GiB。通用型 SSD 卷的大小范围为 1 GiB 到 1 TiB。	2014 年 6 月 16 日
Amazon EBS 加密	Amazon EBS 加密 提供 EBS 数据卷和快照的无缝加密，无需构建和维护安全密钥管理基础设施。通过使用 Amazon 托管式密钥加密数据，EBS 加密可保护静态数据的安全。加密发生在托管 EC2 实例的服务器上，从而在 EC2 实例和 EBS 存储之间移动时对数据进行加密。	2014 年 5 月 21 日
增量快照副本	您现在可以执行增量快照副本。	2013 年 6 月 11 日

EBS 快照副本	您可以使用快照副本来创建数据备份、创建新的 Amazon EBS 卷或创建亚马逊系统映像 (AMIs)。	2012 年 12 月 17 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。