亚马逊云科技

用户指南

Amazon Transfer Family

Amazon Transfer Family: 用户指南

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 Transfer Family？ 1
如何 Amazon Transfer Family 运作 3
与 Transfer Family 相关的博客文章 4
先决条件 8
区域、端点和限额 8
报名参加 Amazon 8
配置存储 9
配置 Amazon S3 存储桶 10
配置 Amazon EFS 文件系统 14
创建 IAM 角色和策略 17
创建用户角色 18
会话策略工作原理 21
read/write 访问策略示例 24
Transfer Family 教程 27
服务器端点入门 28
先决条件 28
步骤 1：登录到 Amazon Transfer Family 控制台 29
步骤 2：创建启用 SFTP 的服务器 29
步骤 3：添加服务托管用户 30
步骤 4：使用客户端传输文件 31
创建解密工作流程 33
步骤 2：配置执行角色 33
步骤 2：创建托管工作流程 35
步骤 3：将工作流程添加至服务器并创建用户 36
步骤 2：创建 PGP 密钥对 37
步骤 5：将 PGP 私有密钥存储在 Amazon Secrets Manager中 38
步骤 6：加密文件 39
步骤 7：运行工作流程并查看结果 39
创建和使用 SFTP 连接器 40
连接器出口类型 41
步骤 1：创建必要的支持资源 42
步骤 2：创建和测试 SFTP 连接器 48
步骤 3：使用 SFTP 连接器发送和检索文件 53
创建用作远程 SFTP 服务器的 Transfer Family 服务器的步骤 57

使用自定义身份提供商 60
先决条件 60
步骤 1：创建 CloudFormation 堆栈 60
步骤 2：检查服务器的 API Gateway 方法配置。 61
步骤 3：查看 Transfer Family 服务器详细信息 62
步骤 4：测试您的用户是否可以连接到服务器 64
步骤 5：测试 SFTP 连接和文件传输 64
步骤 6：限制对存储桶的访问权限 65
如果使用 Amazon EFS，请更新 Lambda 67
设置 AS2 配置 68
步骤 1：为创建证书 AS2 69
第 2 步：将证书作为 Transfer Family 证书资源导入 72
第 3 步：为您和您的贸易伙伴创建档案 74
步骤 4：创建使用该 AS2协议的 Transfer Family 服务器 74
第 5 步：创建您与合作伙伴之间的协议 77
第 6 步：创建您与合作伙伴之间的连接器 79
第 7 步：使用 Transfer Famil AS2 y 测试文件交换情况 80
设置基本的 Web 应用程序 82
先决条件 82
步骤 1：创建必要的支持资源 82
第 2 步：创建 Transfer Family 网络应用程序 83
步骤 3：为您的存储桶配置跨源资源共享 (CORS) 84
第 4 步：将用户添加到你的 Transfer Family 网络应用程序 85
步骤 5：在 Amazon S3 中注册营业地点并创建访问授权 86
第 6 步：以用户身份访问你的 Transfer Family 网络应用程序 88
后续步骤 89
将 Okta 整合为你的 Web 应用程序身份提供商 90
设置具有选择性多存储桶访问权限的 Web 应用程序 92
先决条件 92
第 1 步：创建 Transfer Family 网络应用程序 93
步骤 2：为 S3 访问权限配置 IAM 角色 93
步骤 3：设置 S3 访问授权 96
步骤 4：注册 S3 存储桶位置 96
步骤 5：创建访问授权 96
步骤 6：为 S3 存储桶配置 CORS 策略 97
步骤 7：测试配置 98

结论 98
Transfer Family 适用于 SFTP、FTPS、FTP 99
身份提供商选项 99
Amazon Transfer Family 端点类型矩阵 101
配置 Transfer Family 服务器端点 104
创建启用 SFTP 的服务器 105
创建启用 FTPS 的服务器 112
创建启用 FTP 的服务器 120
在 VPC 中创建服务器 127
使用自定义主机名 147
FTP/FTPS NLB 注意事项 151
通过服务器端点传输文件 151
可用SFTP/FTPS/FTP命令 154
查找您的 Amazon VPC 端点 155
避免 setstat 错误 157
使用 OpenSSH 32
使用 WinSCP 159
使用 Cyberduck 31
使用 FileZilla 162
使用 Perl 客户端 163
使用 LFTP 163
上传后处理 163
SFTP 消息 164
管理用户 166
Amazon EFS 与 Amazon S3 167
逻辑目录 167
活动目录组配额 168
服务托管用户 169
自定义身份提供者 177
适用于 MS AD 的目录服务 210
Entra ID 的目录服务 220
使用逻辑目录 226
了解 chroot 和目录结构 227
使用逻辑目录的规则 227
实现逻辑目录 229
配置逻辑目录示例 231

为 Amazon EFS 配置逻辑目录 233
自定义 Amazon Lambda 响应 234
Transfer Family 网络应用程序 235
Amazon Web Services 区域 适用于 Transfer Family 网络应用程序 235
Amazon Transfer Family Web 应用程序的浏览器兼容性 236
如何创建 Transfer Family 网络应用程序 236
配置您的身份提供商 238
配置 IAM 角色 240
配置 Transfer Family 网络应用程序 242
创建 Transfer Family 网络应用程序 243
在 VPC 中创建 Transfer Family 网络应用程序 244
创建 Transfer Family 网络应用程序 245
创建后步骤 247
跨源资源共享 (CORS) 政策 247
限制对特定 VPC 端点的访问 248
在 Transfer Family 网络应用中分配或添加用户或群组 249
为您的存储桶设置跨源资源共享 (CORS) 252
配置 Amazon S3 访问授权 254
使用自定义 URL 259
登录 Transfer Family 网络应用程序 262
启用 Amazon S3 数据事件 262
身份验证日志示例 265
查看日志条目 271
对 Web 应用程序进行故障排除 272
对网络错误进行故障排除 272
对配置的存储桶未显示进行故障排除 273
排查自定义 URL 错误 273
对其他错误进行故障排除 274
Web 应用程序中出现重复的 S3 存储桶 275
最终用户说明 275
Web 应用程序配额 275
IAM Identity Center 用户 276
第三方最终用户 277
Transfer Family 最终用户界面 278
可用操作 278
SFTP 连接器 281

创建 SFTP 连接器 281
选择 SFTP 连接器出口类型 282
在 Secrets Manager 中存储凭证 283
使用服务管理的出口创建一个 SFTP 连接器 284
使用基于 VPC 的出口创建一个 SFTP 连接器 293
测试 SFTP 连接器 303
VPC 连接 305
使用 SFTP 连接器 306
传输文件 306
列出远程目录的内容 308
在远程服务器上移动和删除文件 310
监控 SFTP 连接器 311
使用连接器 API 查询文件传输请求的状态 312
在亚马逊上查看 SFTP 连接器事件 EventBridge 312
在亚马逊上查看 SFTP 连接器日志 CloudWatch 312
监控 VPC 出口类型连接器 312
管理 SFTP 连接器 314
更新 SFTP 连接器 314
查看 SFTP 连接器详细信息 315
SFTP 连接器配额 316
SFTP 连接器配额 316
扩展您的 SFTP 连接器 318
参考架构 319
博客文章 319
研讨会 319
Solutions 319
VPC 参考架构 320
转移 Family for AS2 322
AS2 用例 323
AS2 CloudFormation 模板 327
自定义模板 AS2 327
测试您的 AS2 部署 327
AS2 模板部署的最佳实践 328
配置 AS2 329
AS2 配置 330
AS2 配额 331

AS2 特性和功能 334
管理 AS2 证书 336
导入 AS2 证书 336
AS2 证书轮换 338
创建 AS2 个人资料 340
创建 AS2 服务器 340
使用 Tran AS2 sfer Family 控制台创建服务器 341
使用模板创建 AS2 服务器 344
创建 AS2 协议 346
配置 AS2 连接器 348
创建 AS2 连接器 348
AS2 连接器算法 351
AS2 连接器的基本身份验证 352
为 AS2连接器启用基本身份验证 354
查看连接器详细信息 356
传输 AS2 消息 359
接收 AS2 消息 360
配置 HTTPS AS2 360
使用 AS2 连接器传输文件 365
文件名和位置 367
状态代码 370
示例 JSON 文件 370
的自定义 HTTP 标头 AS2 372
模板概述 373
工作方式 373
主要功能 373
实施详情 374
部署和使用 375
监视器 AS2 376
AS2 状态码 377
AS2 错误代码 378
证书到期监控 386
DaysUntilExpiry 指标 386
证书监控的最佳实践 387
警报配置示例 387
管理文件处理工作流程 389

创建工作流 391
配置和运行工作流程 392
查看工作流详细信息 394
使用预定义的步骤 397
复制文件 397
解密文件 402
标记文件 407
delete-file 408
工作流程的命名变量 409
标记和删除工作流程示例 409
使用自定义文件处理步骤 414
连续使用多个 Lambda 函数 415
在自定义处理后访问文件 416
文件上传 Amazon Lambda 时发送到的事件示例 417
自定义工作流程步骤的 Lambda 函数示例 418
自定义步骤的 IAM 权限 419
适用于工作流程的 IAM 策略 419
工作流程信任关系 421
执行角色示例：解密、复制和标记 421
执行角色示例：运行函数并删除 423
工作流程的异常处理 424
监控工作流程执行情况 425
CloudWatch 记录工作流程 425
CloudWatch 工作流程指标 428
通过模板创建工作流 428
从 Transfer Family 服务器中移除工作流 432
限额和限制 433
管理服务器 435
查看服务器列表 435
删除服务器 435
查看 SFTP 服务器的详细信息 437
查看 AS2 服务器详细信息 438
IPv6 支持 439
IPv6 局限性 440
IPv6 为服务器配置 440
将 ALB 用于双栈公共服务器 AS2 441

编辑服务器详细信息 442
编辑文件传输协议 445
编辑服务器端点 447
编辑日志记录 448
编辑安全策略 449
更改托管工作流程 450
更改服务器的显示横幅 451
将服务器联机或脱机 451
编辑身份提供商配置 452
更改为服务托管身份提供商 453
更改为“ Amazon 目录服务” 453
更改为自定义身份提供商 453
身份提供商过渡期间的用户保存 457
更改身份提供者时的重要注意事项 458
管理服务器主机密钥 458
何时导入主机密钥 459
添加其他的服务器主机密钥 460
删除服务器主机密钥 461
轮换服务器主机密钥 462
其他服务器主机密钥信息 463
在控制台中监控使用情况 464
管理访问控制 470
创建 S3 存储桶访问策略 470
创建会话策略 472
会话策略示例 473
会话策略的嵌套替换 475
动态权限管理 476
了解 Transfer Family 权限架构 476
两种权限管理方法 476
实施会话策略 477
按用户类型实现情况 478
示例：使用会话策略简化角色管理 478
CloudTrail 日志记录 481
启用 CloudTrail 日志记录 482
启用 Amazon S3 数据事件 483
创建服务器的日志条目示例 483

数据访问日志 485
成功访问数据的日志条目示例 485
常见的数据访问操作 487
CloudWatch 日志记录 488
Transfer Family 的 CloudWatch 登录类型 488
为服务器创建日志 490
为服务器创建日志 492
更新服务器的日志记录 493
查看服务器配置 496
管理工作流程的日志记录 498
为配置角色 CloudWatch 501
查看 Transfer Family 日志流 503
创建亚马逊 CloudWatch 警报 506
将 S3 API 调用记录到 S3 访问日志 507
混淆代理问题限制示例 507
CloudWatch Transfer Family 的日志结构 509
Transfer Family 的 JSON 结构化 509
Transfer Family 的旧日志 512
CloudWatch 日志条目示例 515
传输会话日志条目示例 515
SFTP 连接器的日志条目示例 516
VPC Lattice 连接器的日志条目示例 518
密钥交换算法失败的日志条目示例 519
使用 CloudWatch 指标 520
Transfer Family 维度 524
用户通知 524
CloudWatch 查询 525
使用管理事件 EventBridge 527
Transfer Family 事件 527
SFTP、FTPS 和 FTP 服务器事件 528
SFTP 连接器事件 530
AS2 事件 531
发送 Transfer Family 事件 532
创建事件模式 533
测试事件 Transfer Family 的事件模式 534
Permissions 534

其他资源 534
事件详细信息参考 535
服务器事件 535
连接器事件 542
AS2 事件 549
安全性 556
VPC 连接安全优势 557
VPC 莱迪思安全模型 557
VPC 连接的安全最佳实践 557
服务器的安全策略 558
加密算法 559
TransferSecurityPolicy-2024-01 569
TransferSecurityPolicy-SshAuditCompliant -2025-02 570
TransferSecurityPolicy-2023-05 572
TransferSecurityPolicy-2022-03 573
TransferSecurityPolicy-2020-06 和-Restricted-2020-06 TransferSecurityPolicy 574
TransferSecurityPolicy-2018-11 和-Restricted-2018-11 TransferSecurityPolicy 576
TransferSecurityPolicy-FIPS-2024-01/-FIPS-2024-05 TransferSecurityPolicy 577
TransferSecurityPolicy-FIPS-2023-05 579
TransferSecurityPolicy-FIPS-2020-06 580
TransferSecurityPolicy-AS2 限量版-2025-07 582
后量子安全策略 583
SFTP 连接器的安全策略 591
加密算法 591
SFTP 连接器安全策略详细信息 592
后量子安全策略 594
关于 SSH 中的后量子混合密钥交换 595
使用方法 595
测试方法 596
数据保护 599
Transfer Family 中的数据加密 600
静态加密 601
密钥管理 602
算法概述 602
SSH 身份验证 603
PGP 算法 604

生成 SSH 密钥 605
轮换 SSH 密钥 610
生成 PGP 密钥 613
管理 PGP 密钥 614
支持的 PGP 客户端 617
Identity and access management 619
受众 619
使用身份进行身份验证 619
使用策略管理访问 620
如何 Amazon Transfer Family 与 IAM 配合使用 622
基于身份的策略示例 626
基于标签的策略示例 628
排除 身份和访问问题 631
IAM 条件键 633
合规性验证 635
恢复能力 635
的 VPC 终端节点 APIs 636
使用 VPC 终端节点策略控制访问 637
创建 VPC 端点 637
基础结构安全性 638
NLB 和 NAT 注意事项 638
VPC 连接基础设施安全 639
Web 应用程序防火墙 640
防止跨服务混淆代理 641
Transfer 用户角色 643
Transfer Family 工作流程角色 644
Transfer Family 连接器角色 646
Transfer Family 日志记录/调用角色 647
Amazon 托管策略 648
AWSTransferConsoleFullAccess 649
AWSTransferFullAccess 649
AWSTransferLoggingAccessV3 649
AWSTransferReadOnlyAccess 650
策略更新 650
Transfer Family terraform 模块 652
SFTP 服务器 652

SFTP 连接器 652
AS2 652
B2B 数据交换 653
Transfer Family 故障排除 654
身份验证问题 654
身份验证失败 — SSH/SFTP 655
托管 AD 领域不匹配问题 655
已超出活动目录组限制 656
其他身份验证问题 656
对 Amazon API Gateway 问题进行故障排除 657
对测试您的身份提供商进行故障排除 658
在网络应用程序中重复亚马逊 S3 存储桶 275
SFTP 连接器问题 659
为您的 SFTP 连接器添加可信主机密钥进行故障排除 660
密钥协商失败 660
SFTP 连接器限制 661
优化 SFTP 连接器性能 661
排除 VPC 连接问题 662
其他 SFTP 连接器问题 665
SFTP 连接问题 665
对 SFTP 连接问题进行故障排除 665
对 SFTP 客户端问题进行故障排除 666
文件上传问题进行故障排除 666
排除 VPC 出口类型 SFTP 连接器问题 667
自定义身份提供商问题 669
对 API Gateway 集成错误进行故障排除 669
对 Lambda 函数超时进行故障排除 671
解决持续的 Lambda 超时问题 671
排除KeyError异常问题 672
工作流程问题 672
对托管工作流程问题进行故障排除 672
对工作流程解密问题进行故障排除 675
EFS 问题 679
对 Amazon EFS 问题进行故障排除 679
存储和加密问题 681
对加密 Amazon S3 存储桶的策略进行故障排除 681

对 ResourceNotFound 异常进行故障排除 682
监控和警报问题 682
对缺失或不完整的 CloudWatch 指标进行故障排除 682
解决丢失 EventBridge的事件 683
跨区域传输问题 684
解决跨区域转移权限问题 685
解决跨区域传输性能问题 686
Terraform 部署问题 687
对 Terraform 资源创建失败进行故障排除 687
对 Terraform 状态管理问题进行故障排除 688
WAF 集成问题 689
排除 WAF 屏蔽合法流量的故障 689
对 WAF 与自定义身份提供商的集成进行故障排除 690
服务管理的用户问题 691
对服务托管用户进行故障排除 691
AS2 问题 692
AS2 问题疑难解答 692
AS2 证书问题 692
AS2 MDN 收据问题 693
证书过期监控问题 693
API 参考资料 695
文档历史记录 697
..... dccviii

什么是 Amazon Transfer Family？

Amazon Transfer Family 是一种安全的传输服务，使您能够将文件传入和传出 Amazon 存储服务。Transfer Family 是该 Amazon Web Services 云 平台的一部分。 Amazon Transfer Family 为通过 SFTP、FTPS AS2、FTP 传输文件以及基于 Web 浏览器的文件直接传入和传出存储服务提供完全托管的支持。 Amazon 通过维护现有的客户端身份验证、访问和防火墙配置，您可以无缝迁移、自动化和监控文件传输工作流程，因此您的客户、合作伙伴和内部团队或其应用程序不会发生任何变化。Amazon要了解更多信息并开始使用 Amazon Web Services 构建云应用程序，请参阅入门。

Amazon Transfer Family 支持将数据从以下存储服务传输或传输到以下 Amazon 存储服务。

- Amazon Simple Storage Service (Amazon S3) 存储。有关 Amazon S3 的更多信息，请参阅 Amazon Simple Storage Service 入门。
- Amazon Elastic File System (Amazon EFS) Network File System (NFS) 系统。有关 Amazon EFS 的更多信息，请参阅什么是 Amazon Elastic File System？

Amazon Transfer Family 支持通过以下协议传输数据：

- 安全文件传输协议 (SFTP)：版本 3

  IETF 的官方文档在这里：SSH 文件传输协议 draft-ietf-secsh-filexfer -02.txt。
- 安全文件传输协议 (FTPS)
- 文件传输协议 (FTP)
- 适用性声明 2 (AS2)
- 基于浏览器的传输

> **Note**
>
> 对于 FTP 和 FTPS 数据连接，Transfer Family 用于建立数据通道的端口范围为 8192—8200。

File transfer 协议用于不同行业的数据交换工作流程，例如金融服务、医疗保健、广告和零售等。Transfer Family 简化了将文件传输工作流程迁移到 Amazon。

以下是 Amazon S3 的一些常见 Transfer Family 使用案例：

- 数据湖 Amazon 可供第三方上传，例如供应商和合作伙伴。
- 与客户进行基于订阅的数据分发。
- 组织内部传输。

以下是使用 Amazon EFS 的一些常见使用案例：

- 数据分布
- 供应链
- 内容管理
- Web 服务应用程序

以下是通过以下方式使用 Transfer Family 的一些常见用例 AS2：

- 具有合规性要求的工作流程依赖于在协议中内置数据保护和安全功能
- 供应链物流
- 付款工作流程
- Business-to-business (B2B) 交易
- 与企业资源规划 (ERP) 和客户关系管理 (CRM) 系统集成

以下是使用 Transfer Family 网络应用程序的一些常见用例：

- 更广泛和多样化的企业用户可以更轻松地访问 Amazon S3 中的数据
- 为员工提供集中式数据访问管理
- 通过托管界面可视化 Amazon S3 访问授权

使用 Transfer Family，您无需运行任何服务器基础架构，即可访问支持文件传输协议的服务器 Amazon（或托管文件传输网络界面）。您可以使用此服务将基于文件传输的工作流程迁移到，Amazon 同时保持最终用户的客户端和配置不变。对于服务器，首先要将主机名与服务器端点相关联，然后添加用户并为其配置适当的访问级别。执行此操作后，用户传输请求将直接从 Transfer Family 服务器端点获得服务。

对于 Transfer Family 网络应用程序，请确定您的配置设置并应用可选的自定义设置。完成此操作后，您的用户可以登录并直接在 Amazon S3 之间传输数据。

Transfer Family 提供以下优势：

- 一项完全托管的服务，可实时扩展以满足您的需求。
- 您无需修改应用程序或运行任何文件传输协议基础设施。
- 将您的数据存储在持久的 Amazon S3 存储空间中，您可以使用原生存储 Amazon Web Services 服务 进行处理、分析、报告、审计和存档功能。
- 使用 Amazon EFS 作为数据存储，您将获得一个完全托管的弹性文件系统，用于 Amazon Web Services 云 服务和本地资源。Amazon EFS 可在不中断应用程序的情况下按需扩展到 PB 级，并可在您添加和删除文件时自动增加和缩减。这有助于无需预调配和管理容量来满足容量增长需求。
- 一项完全托管的无服务器文件传输工作流服务，可轻松设置、运行、自动化和监控使用 Amazon Transfer Family上传的文件的处理。
- 没有预付费用，您仅需支付服务使用费。

在以下各节中，您可以找到对 Transfer Family 不同功能的描述、入门教程、有关如何设置不同协议服务器的详细说明、如何使用不同类型的身份提供程序以及该服务的 API 参考。

要开始使用 Transfer Family，请参阅：

- 如何 Amazon Transfer Family 运作
- 先决条件
- Amazon Transfer Family 服务器端点入门
- Transfer Family 网络应用程序

如何 Amazon Transfer Family 运作

Amazon Transfer Family 是一项完全托管的 Amazon 服务，您可以使用它通过以下协议或网络浏览器将文件传入和传出亚马逊简单存储服务 (Amazon S3) Simple S3 存储或亚马逊弹性文件系统 (Amazon EFS) 文件系统：

- 安全文件传输协议 (SFTP)：版本 3

  IETF 的官方文档在这里：SSH 文件传输协议 draft-ietf-secsh-filexfer -02.txt。
- 安全文件传输协议 (FTPS)
- 文件传输协议 (FTP)
- 适用性声明 2 (AS2)
- 基于浏览器的传输

Amazon Transfer Family 最多支持 3 个可用区，并由 auto Scaling 的冗余队列提供支持，用于处理您的连接和传输请求。有关如何使用基于延迟的路由来构建更高的冗余并最大限度地减少网络延迟的示例，请参阅博客文章 SFTP 服务器Amazon 传输时最大限度地减少网络延迟。

Transfer Family 托管文件传输工作流程 (MFTW) 是一项完全托管的无服务器文件传输工作流程服务，可轻松设置、运行、自动化和监控使用 Amazon Transfer Family上传的文件的处理。客户可以使用 MFTW 自动执行各种处理步骤，例如复制、标记、扫描、筛选，以及使用 Transf compressing/decompressing, and encrypting/decrypting er Family 传输的数据。这为跟踪和可审核性提供了端到端的可见性。有关更多详细信息，请参阅Amazon Transfer Family 托管工作流程。

Amazon Transfer Family 支持任何标准文件传输协议客户端。一些常用的客户端如下：

- OpenSSH — Macintosh 和 Linux 命令行实用工具。
- WinSCP — 仅 Windows 图形客户端。
- Cyberduck — Linux、Macintosh 和 Microsoft Windows 图形客户端。
- FileZilla— Linux、Macintosh 和 Windows 图形客户端。

Amazon 提供以下 Transfer Family 研讨会。

- 构建一个文件传输解决方案，利用托管 SFTP/FTPS 终 Amazon Transfer Family 端节点，利用 Amazon Cognito 和 DynamoDB 进行用户管理。您可以在此处查看本次研讨会的详细信息。
- 在 AS2 启用状态下构建 Transfer Family 端点和 Transfer Family AS2 连接器您可以在此处查看本次研讨会的详细信息。
- 构建一个解决方案，提供规范性指导和动手实验，说明如何在无需修改现有应用程序或管理服务器基础架构 Amazon 的情况下构建可扩展且安全的文件传输架构。您可以在此处查看本次研讨会的详细信息。

与 Transfer Family 相关的博客文章

下表列出了包含对Transfer Family客户有用信息的博客文章。该表按时间倒序排列，因此最近的帖子位于表的开头。

博客文章标题和链接	日期
将 Okta 部署为自定义身份提供商 Amazon Transfer Family	2025 年 8 月 11 日

博客文章标题和链接	日期
使用实现 paper-to-electronic医疗保健索赔处理的自动化 Amazon	2025 年 5 月 29 日
如何使用 Amazon Transfer Family 和 GuardDuty 进行恶意软件防护	2025 年 4 月 30 日
FICO如何使用ETL自动化实现文件传输的现代化 Amazon Transfer Family	2025 年 4 月 24 日
宣布推出适用于完全托管的 Amazon S3 文件传输的 Amazon Transfer Family 网络应用程序	2024 年 12 月 1 日
提高 Amazon Transfer Family 服务器安全性的六个技巧	2024 年 9 月 24 日
使用自定义身份提供商简化 Active Directory 身份验证 Amazon Transfer Family	2024 年 8 月 12 日
使用 Amazon Transfer Family SFTP 连接器和 PGP 加密架构安全且合规的托管文件传输	2024 年 5 月 16 日
使用 Amazon Cognito 作为身份提供者 Amazon Transfer Family 和 Amazon S3	2024 年 5 月 14 日
Transfer Family 如何帮助您构建安全、合规的托管文件传输解决方案	2024 年 1 月 3 日
使用检测恶意软件威胁 Amazon Transfer Family	2023 年 7 月 20 日
使用扩展 SAP 工作负载 Amazon Transfer Family	2023 年 7 月 13 日
使用 PGP 加密和解密文件 Amazon Transfer Family	2023 年 6 月 21 日
使用 Azure 活动目录 Amazon Transfer Family 进行身份验证和 Amazon Lambda	2022 年 12 月 15 日

博客文章标题和链接	日期
使用 Amazon Transfer Family 托管工作流程自定义文件传送通知	2022 年 10 月 14 日
使用 Amazon Transfer Family 工作流程构建云原生文件传输平台	2022 年 1 月 5 日
使用 A Amazon Transfer Family 和，启用用户自助密钥管理 Amazon Lambda。	2021 年 12 月 17 日
使用 Amazon Transfer Family 和 Amazon S3 增强数据访问控制	2021 年 10 月 5 日
使用 Amazon Global Accelerator 和 Amazon Transfer Family 服务提高面向互联网的文件传输的吞吐量	2021 年 6 月 7 日
Amazon Transfer Family 使用 Amazon Web 应用程序防火墙和 Amazon API Gateway 确保安全	2021 年 5 月 5 日
Amazon Transfer Family 使用 Amazon Web 应用程序防火墙和 Amazon API Gateway 确保安全	2021 年 1 月 15 日
Amazon Transfer Family 支持 Amazon Elastic File System	2021 年 1 月 7 日
启用密码身份验证以供 Amazon Transfer Family 使用 Amazon Secrets Manager	2020 年 11 月 5 日
使用 Amazon Transfer Family 和集中数据访问 Amazon Storage Gateway	2020 年 6 月 22 日
Amazon Lambda 在您的无服务器应用程序中使用 Amazon EFS	2020 年 6 月 18 日

博客文章标题和链接	日期
使用 IP 允许列表来保护您的 Amazon Transfer Family 服务器	2020 年 4 月 8 日
通过 SFTP 服务器 Amazon 传输最大限度地减少网络延迟	2020 年 2 月 19 日
将 SFTP 服务器迁移到 Amazon	2020 年 2 月 12 日
使用 chroot 和逻辑目录简化你的 Amazon SFTP 结构	2019 年 9 月 26 日
使用 Okta 作为身份提供商 Amazon Transfer Family	2019 年 5 月 30 日

先决条件

以下各节描述了使用该 Amazon Transfer Family 服务所需的先决条件。您至少需要创建一个亚马逊简单存储服务 (Amazon S3) 存储桶，并通过 (IAM) 角色提供对该存储桶 Amazon Identity and Access Management 的访问权限。您的角色还需要建立信任关系。此信任关系允许 Transfer Family 代入 IAM 角色来访问存储桶，以便能为用户的文件传输请求提供服务。

有关 Amazon Transfer Family 服务器 IPv6 支持的信息，请参阅 “管理服务器” 一章IPv6 支持 Transfer Family 服务器中的。

主题

- Transfer Family 服务器支持的 Amazon 区域、终端节点和配额
- 报名参加 Amazon
- 配置用于 Amazon Transfer Family 服务器的存储
- 创建 IAM 角色和策略

Transfer Family 服务器支持的 Amazon 区域、终端节点和配额

要以编程方式连接到 Amazon 服务，请使用终端节点。例如，美国东部（俄亥俄州）地区客户的终端节点 (us-east-2) 是`transfer.us-east-2.amazonaws.com`。服务限额（也称为限制）是 Amazon Web Services 账户使用的服务资源或操作的最大数量。在本指南中，您可以在AS2 配额和中找到配额SFTP 连接器配额。

有关支持的 Amazon 区域、终端节点和服务配额的更多信息，请参阅中的Amazon Transfer Family 终端节点和配额Amazon Web Services 一般参考。

对于 Transfer Family 网络应用程序，中列出了支持的区域Amazon Web Services 区域 适用于 Transfer Family 网络应用程序。有关与 Transfer Family 网络应用程序相关的配额，请参阅Web 应用程序配额。

报名参加 Amazon

当您注册 Amazon Web Services (Amazon) 时，您的 Amazon 账户会自动注册使用中的所有服务 Amazon，包括 Amazon Transfer Family。您只需为使用的服务付费。

如果您已经有一个 Amazon 帐户，请跳到下一个任务。如果您还没有 Amazon 账户，请按照以下步骤创建。

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

要注册 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，将接到电话或收到短信，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。

有关定价以及用于估算使用 Amazon 定价计算器 Transfer Family 的成本的信息，请参阅Amazon Transfer Family 定价。

有关 Amazon 区域可用性的信息，请参阅中的Amazon Transfer Family 终端节点和配额Amazon Web Services 一般参考。

配置用于 Amazon Transfer Family 服务器的存储

本主题介绍可以与配合使用的存储选项 Amazon Transfer Family。你可以使用 Amazon S3 或 Amazon EFS 作为 Transfer Family 服务器的存储。

目录

- 配置 Amazon S3 存储桶
  - Amazon S3 接入点
  - 亚马逊 S3 的 HeadObject 行为
    - 授予仅写入和列出文件的权限
    - 大量零字节对象导致延迟问题
- 配置 Amazon EFS 文件系统
  - Amazon EFS 文件所有权
  - 为 Transfer Family 设置 Amazon EFS 用户
    - 在 Amazon EFS 上配置 Transfer Family 用户
    - 创建 Amazon EFS 根用户
  - 受支持的 Amazon EFS 命令

配置 Amazon S3 存储桶

Amazon Transfer Family 访问您的 Amazon S3 存储桶以处理用户的传输请求，因此在设置支持文件传输协议的服务器时，您需要提供 Amazon S3 存储桶。您可以使用现有存储桶或新建一个存储桶。

> **Note**
>
> 您不必使用位于相同 Amazon 区域中的服务器和 Amazon S3 存储桶，但是我们建议将此作为最佳实践。

在设置用户时，您可以为每个用户分配一个 IAM 角色。此角色决定了用户对 Amazon S3 存储桶的访问级别。

有关创建新存储桶的更多信息，请参阅 Amazon Simple Storage Service 用户指南中的如何创建 S3 存储桶？。

> **Note**
>
> 您可以使用 Amazon S3 对象锁定在固定的时间段内或无限期内阻止对象被覆盖。Transfer Family 的工作方式与其他服务相同。如果对象存在且受保护，则不允许写入或删除该文件。有关 Amazon S3 对象锁定的更多详细信息，请参阅 Amazon 简单存储服务用户指南中的使用 Amazon S3 对象锁定。

Amazon S3 接入点

Amazon Transfer Family 支持 Amazon S3 接入点，这是 Amazon S3 的一项功能，可让您轻松管理对共享数据集的精细访问。您可以在任何使用 S3 存储桶名称的地方使用 S3 接入点别名。您可以在 Amazon S3 中为拥有不同权限的用户创建数百个访问点，以访问 Amazon S3 存储桶中的共享数据。

例如，您可以使用接入点允许三个不同的团队访问同一个共享数据集，其中一个团队可以从 S3 读取数据，第二个团队可以将数据写入 S3，第三个团队可以从 S3 读取、写入和删除数据。要实现如上所述的精细访问控制，您可以创建一个 S3 接入点，该接入点包含向不同团队提供非对称访问权限的策略。您可以将 S3 接入点与 Transfer Family 服务器配合使用来实现精细的访问控制，而无需创建涵盖数百个用例的复杂 S3 存储桶策略。要详细了解如何在 Transfer Family 服务器上使用 S3 接入点，请参阅使用Amazon Transfer Family 和 Amazon S3 增强数据访问控制博客文章。

> **Note**
>
> Amazon Transfer Family 目前不支持 Amazon S3 多区域接入点。

亚马逊 S3 的 HeadObject 行为

> **Note**
>
> 在创建或更新 Transfer Family 服务器时，您可以优化 Amazon S3 目录的性能，从而消除`HeadObject`调用。

在 Amazon S3 中，存储桶和对象是主要资源，并且对象存储在存储桶中。Amazon S3 可以模仿分层文件系统，但有时行为可能与典型文件系统不同。例如，在 Amazon S3 中，目录不是头等概念，而是基于对象密钥。 Amazon Transfer Family 推断出目录路径的方法是：用正斜杠字符 (/) 分割对象的密钥，将最后一个元素视为文件名，然后将具有相同前缀的文件名分组到同一路径下。当您使用`mkdir`或使用 Amazon S3 控制台创建空目录时，创建零字节对象是为了表示文件夹的路径。这些对象的密钥以尾随的正斜杠结尾。Amazon S3 用户指南中的使用文件夹在 Amazon S3 控制台中组织对象中描述了这些零字节对象。

当您运行`ls`命令时，如果某些结果是 Amazon S3 零字节对象（这些对象的密钥以正斜杠字符结尾），Transfer Family 会针对每个对象`HeadObject`发出请求（详情请参阅《亚马逊简单存储服务 API 参考》HeadObject中）。使用 Amazon S3 作为 Transfer Family 的存储空间时，这可能会导致以下问题。

授予仅写入和列出文件的权限

在某些情况下，您可能只想提供对 Amazon S3 对象的写入权限。例如，您可能希望提供写入（或上传）和列出存储桶中对象的权限，但不提供读取（下载）对象的权限。要使用文件传输客户端执行`ls`和`mkdir`命令，您必须拥有 Amazon S3 `ListObjects` 和`PutObject`权限。但是，当 Transfer Family 需要`HeadObject`调用写入文件或列出文件时，呼叫失败并显示拒绝访问的错误，因为此调用需要`GetObject`权限。

> **Note**
>
> 在创建或更新 Transfer Family 服务器时，您可以优化 Amazon S3 目录的性能，从而消除`HeadObject`调用。

在这种情况下，您可以通过添加 Amazon Identity and Access Management (IAM) 策略条件来授予访问`GetObject`权限，该条件仅为以斜杠 (/) 结尾的对象添加权限。此条件可防止`GetObject`调用文件（因此无法读取文件），但允许用户列出和遍历文件夹。以下示例策略仅提供对您的 Amazon S3 存储桶的写入和列出权限。要使用此策略，请*`amzn-s3-demo-bucket`*替换为存储桶的名称。

> **Note**
>
> 要解决 WinSCP 的上传行为，请务必添加以下示例策略中列出的`"arn:aws:s3:::amzn-s3-demo-bucket/*.filepart"`行。此行可确保正确处理.filepart 对象以防止出现故障。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowListing",
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
        },
        {
            "Sid": "AllowReadWrite",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
         },
      {
            "Sid": "DenyIfNotFolder",
            "Effect": "Deny",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "NotResource": [
                "arn:aws:s3:::amzn-s3-demo-bucket/*/",
                "arn:aws:s3:::amzn-s3-demo-bucket/*.filepart"
```

```
            ]
         }
      ]
}
```

> **Note**
>
> 此策略不允许用户追加文件。换句话说，分配了此策略的用户无法打开文件来向其添加内容或修改文件。此外，如果您的用例要求在上传文件之前进行HeadObject调用，则此策略对您不起作用。

大量零字节对象导致延迟问题

如果您的 Amazon S3 存储桶包含大量这样的零字节对象，Transfer Family 会发出大量HeadObject调用，这可能会导致处理延迟。此问题的推荐解决方案是启用优化目录以减少延迟。

例如，假设您进入主目录，并且有 10,000 个子目录。换句话说，您的亚马逊 S3 存储桶有 10,000 个文件夹。在这种情况下，如果您运行 `ls` (list) 命令，则列表操作需要六到八分钟。但是，如果您优化目录，则此操作只需要几秒钟。在服务器创建或更新过程中，您可以在 “配置其他详细信息” 屏幕中设置此选项。这些程序将在该配置 SFTP、FTPS 或 FTP 服务器端点主题下详细介绍。

> **Note**
>
> GUI 客户端可能会发出超出您控制范围的ls命令，因此，如果可以，请务必启用此设置。

如果您不优化或无法优化目录，则此问题的另一种解决方案是删除所有零字节对象。注意以下几点：

- 空目录将不再存在。只有当目录的名称位于对象的密钥中时，才会存在目录。
- 不会阻止某人再次调用mkdir并破坏事务处理。您可以通过制定阻止目录创建的策略来缓解这种情况。
- 有些场景会使用这些 0 字节的对象。例如，您有一个像 /inboxes/customer1000 这样的结构，每天都会清理收件箱目录。

最后，还有一种可能的解决方案是限制通过策略条件可见的对象数量，以减少HeadObject调用次数。要使之成为可行的解决方案，您需要接受这样一个事实，即您可能只能查看有限的一组子目录。

配置 Amazon EFS 文件系统

Amazon Transfer Family 访问亚马逊 Elastic File System (Amazon EFS)，为用户的传输请求提供服务。因此，在设置支持文件传输协议的服务器时，您必须提供 Amazon EFS 文件系统。您可以使用现有文件系统或新建一个文件系统。

注意以下几点：

- 当您使用 Transfer Family 服务器和 Amazon EFS 文件系统时，服务器和文件系统必须处于同一位置 Amazon Web Services 区域。
- 服务器和文件系统不必位于同一个账户中。如果服务器和文件系统不在同一个账户中，则文件系统策略必须为用户角色提供明确的权限。

  有关如何设置多个账户的信息，请参阅《Amazon Organizations 用户指南》中的管理组织中的 Amazon 账户。
- 在设置用户时，您可以为每个用户分配一个 IAM 角色。此角色决定了用户对 Amazon EFS 文件系统的访问级别。
- 有关挂载 Amazon EFS 文件系统的详细信息，请参阅挂载 Amazon EFS 文件系统。

有关如何 Amazon Transfer Family 与 Amazon EFS 协同工作的更多详细信息，请参阅《亚马逊弹性文件系统用户指南》中的 “使用 Amazon Transfer Family 访问您的 Amazon E FS 文件系统中的文件”。

Amazon EFS 文件所有权

Amazon EFS 使用便携式操作系统接口 (POSIX) 文件权限模型来表示文件所有权。

在 POSIX 中，系统中的用户分为三个不同的权限类别：当您允许用户使用访问存储在 Amazon EFS 文件系统中的文件时 Amazon Transfer Family，必须为他们分配一个 “POSIX 配置文件”。此配置文件用于确定他们对 Amazon EFS 文件系统中文件和目录的访问权限。

- 用户 (u)：文件或目录的所有者。通常，文件或目录的创建者也是所有者。
- 组 (g)：一组需要对他们共享的文件和目录具有相同访问权限的用户。
- 其他 (o)：除所有者和群组成员外，有权访问系统的所有其他用户。此权限类别也称为“公有”类别。

在 POSIX 权限模型中，每个文件系统对象（文件、目录、符号链接、命名管道和套接字）都与前面提到的三组权限相关联。Amazon EFS 对象具有关联的 Unix 风格模式。此模式值定义了对该对象执行操作的权限。

此外，在 Unix 风格的系统上，用户和组被映射到数字标识符，Amazon EFS 使用这些标识符来表示文件所有权。对于 AmazonEFS，对象由单个所有者和单个组所有。当用户尝试访问文件系统对象时 IDs ，Amazon EFS 使用映射的数字来检查权限。

为 Transfer Family 设置 Amazon EFS 用户

设置 Amazon EFS 用户之前，您可以执行以下操作之一：

- 您可以在 Amazon EFS 中创建用户并设置他们的主文件夹。有关详细信息，请参阅 在 Amazon EFS 上配置 Transfer Family 用户。
- 如果您愿意添加根用户，则可以创建 Amazon EFS 根用户。

> **Note**
>
> Transfer Family 服务器不支持 Amazon EFS 接入点来设置 POSIX 权限。Transfer Family 用户的 POSIX 配置文件（如上一节所述）提供了设置 POSIX 权限的功能。这些权限是在用户级别设置的，用于基于 UID、GID 和辅助权限的精细访问。 GIDs

在 Amazon EFS 上配置 Transfer Family 用户

Transfer Family 会将用户映射到您指定的 UID/GID 和目录。如果 EFS 中尚UID/GID/directories不存在，则应先创建它们，然后再在 Transfer 中将其分配给用户。有关创建 Amazon EFS 用户的详细信息，请参阅 Amazon Elastic File System 用户指南中的在网络文件系统 (NFS) 级别处理用户、组和权限。

在 Transfer Family 中设置亚 Amazon EFS 用户的步骤

1. 使用 `PosixProfile` 字段在 Transfer Family 中为用户映射 EFS UID 和 GID。
2. 如果您希望用户在登录时在特定文件夹中启动，则可以在`HomeDirectory`字段下指定 EFS 目录。

您可以使用 CloudWatch 规则和 Lambda 函数自动执行该过程。有关与 EFS 交互的 Lambda 函数示例，请参阅Amazon Lambda 在您的无服务器应用程序中使用 Amazon EFS。

此外，您还可以为 Transfer Family 用户配置逻辑目录。有关详细信息，请参阅 为 Amazon EFS 配置逻辑目录 章节中的 使用逻辑目录简化您的 Transfer Family 目录结构 主题。

创建 Amazon EFS 根用户

如果您的组织愿意通过 SFTP/FTPS 为用户配置启用根用户访问权限，则可以创建一个 UID 和 GID 为 0 的用户（根用户），然后使用该根用户创建文件夹，并为其余用户分配 POSIX ID 所有者。此选项的优点是，无需挂载 Amazon EFS 文件系统。

执行添加 Amazon EFS 服务托管用户中描述的步骤，为用户 ID 和组 ID 输入 0（零）。

> **Tip**
>
> 不要让这个超级用户帐户存在的时间超过必要的时间。或者，如果您确实保留了 root 用户帐户，请确保对其进行良好的保护。

受支持的 Amazon EFS 命令

对于 Amazon Transfer Family，Amazon EFS 支持以下命令。

- `cd`
- `ls/dir`
- `pwd`
- `put`
- `get`
- `rename`
- `chown`: 只有根用户（即 uid 为 0 的用户）可以更改文件和目录的所有权和权限。
- `chmod`：只有根用户可以更改文件和目录的所有权和权限。
- `chgrp`：根用户或只能将文件组更改为次要组之一的文件所有者支持。
- `ln -s/symlink`
- `mkdir`
- `rm/delete`
- `rmdir`
- `chmtime`

创建 IAM 角色和策略

本主题介绍可与之配合使用的策略和角色类型 Amazon Transfer Family，并介绍创建用户角色的过程。它还描述了会话策略的工作原理，并提供了一个用户角色示例。

Amazon Transfer Family 使用以下类型的角色：

- 用户角色-允许服务管理的用户访问必要的 Transfer Family 资源。 Amazon Transfer Family 在 Transfer Family 用户 ARN 的背景下担任此角色。
- 访问角色 - 仅提供对正在传输的 Amazon S3 文件的访问权限。对于入站 AS2 转移，访问角色使用协议的 Amazon 资源名称 (ARN)。对于出站 AS2 传输，访问角色使用连接器的 ARN。
- 调用角色 – 用于作为服务器自定义身份提供程序的 Amazon API Gateway。Transfer Family 在 Transfer Family 服务器 ARN 的背景下扮演这个角色。
- 日志角色-用于将条目登录到 Amazon CloudWatch。Transfer Family 使用此角色记录成功和失败的详细信息以及有关文件传输的信息。Transfer Family 在 Transfer Family 服务器 ARN 的背景下扮演这个角色。对于出站 AS2 传输，日志角色使用连接器 ARN。
- 执行角色 - 允许 Transfer Family 用户调用和启动工作流程。Transfer Family 在 Transfer Family 工作流程 ARN 的背景下担任此角色。

除了这些角色之外，您还可以使用会话策略。会话策略用于在必要时限制访问权限。请注意，这些策略是独立的：也就是说，您不会将这些策略添加到角色中。相反，您可以直接向 Transfer Family 用户添加会话策略。

> **Note**
>
> 创建服务管理的 Transfer Family 用户时，可以选择基于主文件夹自动生成策略。如果您想限制用户访问自己的文件夹，这是一个有用的快捷方式。此外，您还可以在会话策略工作原理中查看有关会话策略的详细信息以及示例。您还可以在《IAM 用户指南》的会话策略中找到有关会话策略的更多信息。

主题

- 创建用户角色
- 会话策略工作原理
- read/write 访问策略示例

创建用户角色

在创建用户时，您会做出大量有关用户访问权限的决定。这些决定包括用户可以访问哪些 Amazon S3 存储桶或 Amazon EFS 文件系统、每个 Amazon S3 存储桶的哪些部分和文件系统中的哪些文件可以访问，以及用户拥有哪些权限（例如PUT或GET）。

要设置访问权限，您需要创建基于身份 Amazon Identity and Access Management (IAM) 的策略和角色来提供该访问信息。作为此过程的一部分，您为用户提供对 AmazonS3 存储桶或 Amazon EFS 文件系统的访问权限，这些文件系统是文件操作的目标或源。为此，请执行以下简要步骤（稍后将详细介绍）：

创建用户角色

1. 为创建 IAM 策略 Amazon Transfer Family。为 Amazon Transfer Family创建 IAM policy中对此进行了描述。
2. 创建 IAM 角色并附加新的 IAM policy。有关示例，请参阅 read/write 访问策略示例。
3. 在和 IAM 角色 Amazon Transfer Family 之间建立信任关系。建立信任关系中对此进行了描述。

以下过程介绍如何创建 IAM policy 和角色。

为 Amazon Transfer Family创建 IAM policy

1. 使用 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
2. 在导航窗格中，选择 策略，然后选择 创建策略。
3. 在创建策略页面上，选择 JSON 选项卡。
4. 在显示的编辑器中，将编辑器的内容替换为要附加到 IAM 角色的 IAM policy。

   您可以授予 read/write 访问权限或限制用户访问其主目录。有关更多信息，请参阅 read/write 访问策略示例。
5. 选择查看策略，并提供策略的名称和描述，然后选择创建策略。

接下来，您将创建一个 IAM 角色并向该角色附加新的 IAM 策略。

为创建 IAM 角色 Amazon Transfer Family

1. 在导航窗格中，选择角色，然后选择创建角色。

   在创建角色页面上，确保已选择Amazon 服务。

2. 从服务列表中选择转移，然后选择下一步：权限。这在 Amazon Transfer Family 和之间建立了信任关系 Amazon。
3. 在附加权限策略部分中，找到并选择刚刚创建的策略，然后选择下一步：标签。
4. （可选）输入标签的键和值，然后选择下一步：审核。
5. 在审核页面上，输入新角色的名称和描述，然后选择创建角色。

接下来，在 Amazon Transfer Family 和之间建立信任关系 Amazon。

建立信任关系

> **Note**
>
> 在我们的示例中，我们同时使用 `ArnLike` 和 `ArnEquals`。它们在功能上是相同的，因此您可以在制定策略时使用其中任何一个。Transfer Family 文档在条件包含通配符时使用`ArnLike`，`ArnEquals`用于表示完全匹配的条件。

1. 在 IAM 控制台中，选择您刚创建的角色。
2. 在 Summary (摘要) 页面上，选择 Trust relationships (信任关系)，然后选择 Edit trust relationship (编辑信任关系)。
3. 在编辑信任关系编辑器中，确保服务是`"transfer.amazonaws.com"`。编辑后的访问策略如下所示。

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.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。源账户是域的所有者，并且源 ARN 是域的 ARN。例如：

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account_id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:transfer:region:account_id:user/*"
    }
}
```

如果您希望限制到特定的服务器而不是用户账户中的任何服务器，也可以使用ArnLike条件。例如：

```
"Condition": {
    "ArnLike": {
        "aws:SourceArn": "arn:aws:transfer:region:account-id:user/server-id/*"
    }
}
```

> **Note**
>
> 在上面的示例中，用您自己的信息替换每个*user input placeholder*示例。

有关混淆代理人问题的详细信息以及更多示例，请参阅 防止跨服务混淆代理。

4. 选择更新信任策略以更新访问策略。

现在，您已经创建了一个 IAM 角色， Amazon Transfer Family 允许您代表您调用 Amazon 服务。您已将创建的 IAM policy 附加到该角色，以授予对用户的访问权限。在Amazon Transfer Family 服务器端点入门部分中，此角色和策略将分配给您的用户或用户。

另请参阅

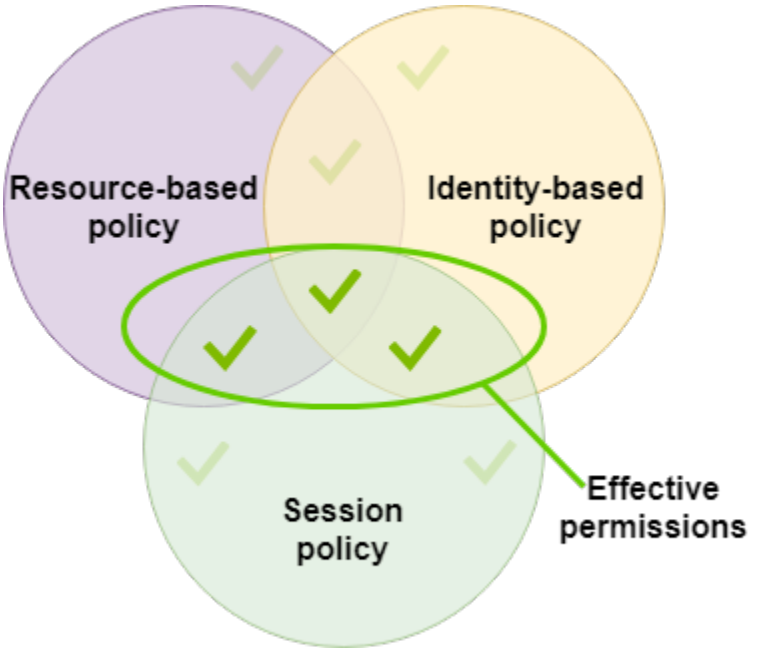
- 有关 IAM 角色的更多一般信息，请参阅 I A M 用户指南中的创建角色以向 Amazon 服务委派权限。

- 要详细了解 Amazon S3 资源基于身份的策略，请参阅 Amazon 简单存储服务用户指南中的 Amazon S3 中的身份和访问管理。
- 要了解有关 Amazon EFS 资源基于身份的策略的更多信息，请参阅 Amazon 弹性文件系统用户指南中的使用 IAM 控制文件系统数据访问。

会话策略工作原理

管理员创建角色时，该角色通常包含涵盖多个用例或团队成员的广泛权限。如果管理员配置了控制台 URL，则他们可以使用会话策略来减少对生成的会话的权限。例如，如果您创建具有读/写访问权限的角色，则可以设置一个 URL，限制用户只能访问其主目录。

会话策略是当您以编程方式为角色或用户创建临时会话时作为参数传递的高级策略。会话策略对于锁定用户非常有用，这样他们就只能访问存储桶中包含其用户名的对象前缀的部分。下图显示了会话策略的权限是会话策略和基于资源的策略的交集，以及会话策略和基于身份策略的交集。



有关更多详细信息，请参阅 IAM 用户指南中的会话策略。

在中 Amazon Transfer Family，只有当您向 Amazon S3 传输或从 Amazon S3 传输数据时，才支持会话策略。以下示例策略是一个会话策略，它仅限制用户访问其 home 目录。注意以下几点：

- 只有当您需要启用跨账户存取时，才需要`GetObjectACL`和`PutObjectACL`语句。也就是说，您的 Transfer Family 服务器需要访问其他账户中的存储桶。
- 会话策略的最大长度为 2048 个字符。有关更多详细信息，请参阅 API 参考中 `CreateUser` 操作的策略请求参数。

- 如果您的 Amazon S3 存储桶使用 Amazon Key Management Service (Amazon KMS) 进行加密，则必须在策略中指定其他权限。有关更多信息，请参阅 数据保护和加密。
- 要使用会话策略根据用户属性创建访问权限，而不必为每个用户创建单独的 IAM 角色，请参阅动态权限管理方法。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowListingOfUserFolder",
            "Action": [
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::${transfer:HomeBucket}"
            ],
            "Condition": {
                "StringLike": {
                    "s3:prefix": [
                        "${transfer:HomeFolder}/*",
                        "${transfer:HomeFolder}"
                    ]
                }
            }
        },
        {
            "Sid": "HomeDirObjectAccess",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetObjectVersion",
                "s3:GetObjectACL",
                "s3:PutObjectACL"
            ],
            "Resource": "arn:aws:s3:::${transfer:HomeDirectory}/*"
        }
    ]
```

```
}
```

> **Note**
>
> 前面的策略示例假设用户的主目录设置为包含尾部斜杠，以表示它是一个目录。另一方面，如果您设置的用户 HomeDirectory 不带尾部的斜杠，则应将其作为策略的一部分。

在前面的示例策略中，请注意使用transfer:HomeFolder、transfer:HomeBucket和transfer:HomeDirectory策略参数。这些参数是为用户配置的设置的，如HomeDirectory和中所述实施您的 API Gateway 方法。HomeDirectory这些参数具有以下定义：

- transfer:HomeBucket参数将替换为的HomeDirectory第一个组件。
- transfer:HomeFolder 参数将替换为 HomeDirectory 参数的其余部分。
- transfer:HomeDirectory参数删除了前导正斜杠 (/)，因此可以在Resource语句中将其用作 S3 Amazon 资源名称 (ARN) 的一部分。

> **Note**
>
> 如果您使用的是逻辑目录（即用户的homeDirectoryType是LOGICAL），则不支持这些策略参数（HomeBucket、HomeDirectory和HomeFolder）。

例如，假设为 Transfer Family 用户配置的 HomeDirectory 参数是 /home/bob/amazon/stuff/。

- transfer:HomeBucket 设置为 /home。
- transfer:HomeFolder 设置为 /bob/amazon/stuff/。
- transfer:HomeDirectory 变为 home/bob/amazon/stuff/。

第一个"Sid"允许用户列出从/home/bob/amazon/stuff/开始的所有目录。

第二个 "Sid" 限制用户对同一路径 /home/bob/amazon/stuff/ 的 put 和 get 访问权限。

read/write 访问策略示例

授予 read/write 对 Amazon S3 存储桶的访问权限

以下示例策略 Amazon Transfer Family 授予对您的 Amazon S3 存储桶中对象的 read/write 访问权限。

注意以下几点：

- 将 `amzn-s3-demo-bucket` 替换为您的 Amazon S3 存储桶的名称。
- 只有当您需要启用跨账户存取时，才需要 `GetObjectACL` 和 `PutObjectACL` 语句。也就是说，您的 Transfer Family 服务器需要访问其他账户中的存储桶。
- 只有在正在访问的 Amazon S3 存储桶上启用版本控制时，才需要使用`GetObjectVersion`和`DeleteObjectVersion`语句。

> **Note**
>
> 如果您曾经为存储桶启用过版本控制，则需要这些权限，因为您只能在 Amazon S3 中暂停版本控制，而不能完全将其关闭。有关详细信息，请参阅未版本化、启用版本控制和已暂停版本控制的存储桶。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowListingOfUserFolder",
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket"
            ]
        },
        {
            "Sid": "HomeDirObjectAccess",
            "Effect": "Allow",
            "Action": [
```

```
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetObjectTagging",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetObjectVersion",
                "s3:GetObjectVersionTagging",
                "s3:GetObjectACL",
                "s3:PutObjectACL"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
        }
    ]
}
```

授予文件系统访问 Amazon EFS 文件系统中文件的权限

> **Note**
>
> 除了策略外，您还必须确保您的 POSIX 文件权限授予了相应的访问权限。有关更多信息，请参阅 Amazon Elastic File System 用户指南中的在网络文件系统 (NFS) 级别处理用户、组和权限。

以下示例策略允许根文件系统访问您的 Amazon EFS 文件系统中的文件。

> **Note**
>
> 在以下示例中，*region*替换为您所在的地区、*account-id*文件所在的账户以及*file-system-id*您的亚马逊弹性文件系统 (Amazon EFS) 的 ID。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "RootFileSystemAccess",
            "Effect": "Allow",
            "Action": [
```

```
                "elasticfilesystem:ClientRootAccess",
                "elasticfilesystem:ClientMount",
                "elasticfilesystem:ClientWrite"
            ],
            "Resource": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-
system/file-system-id"
        }
    ]
}
```

以下示例策略授予用户文件系统访问您的 Amazon EFS 文件系统中文件的权限。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "UserFileSystemAccess",
            "Effect": "Allow",
            "Action": [
                "elasticfilesystem:ClientMount",
                "elasticfilesystem:ClientWrite"
            ],
            "Resource": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-
system/file-system-id"
        }
    ]
}
```

Transfer Family 教程

该 Amazon Transfer Family 用户指南提供了多个用例的详细演练。

- Amazon Transfer Family 服务器端点入门-使用服务管理用户创建 SFTP Transfer Family 服务器并使用客户端传输文件。
- 设置和使用 SFTP 连接器-设置 SFTP 连接器以在 Amazon S3 存储和 SFTP 服务器之间传输文件。
- 将 Amazon API Gateway 方法设置为自定义身份提供商 -将 Amazon API Gateway 方法配置为用于将文件上传到 Amazon Transfer Family 服务器的自定义身份提供商。
- 设置用于解密文件的托管工作流程-创建托管工作流程来解密文件、将加密文件上传到 Amazon S3 以及查看解密的内容。
- 设置 AS2 配置-设置 Trans AS2 fer Family 服务器，包括证书导入、配置文件和协议创建、可选 AS2 连接器配置和测试。
- 以下教程将指导您创建和配置 Transfer Family 网络应用程序。选择最适合你需求的教程：

  教程：设置基本的 Transfer Family 网络应用程序-学习如何创建和配置 Transfer Family 网络应用程序。

  教程：设置具有选择性多存储桶访问权限的 Amazon Transfer Family Web 应用程序-配置 Transfer Family 网络应用程序，为单个用户提供精细的 Amazon S3 存储桶权限。

主题

- Amazon Transfer Family 服务器端点入门
- 设置用于解密文件的托管工作流程
- 设置和使用 SFTP 连接器
- 将 Amazon API Gateway 方法设置为自定义身份提供商
- 设置 AS2 配置
- 教程：设置基本的 Transfer Family 网络应用程序
- 教程：设置具有选择性多存储桶访问权限的 Amazon Transfer Family Web 应用程序

Amazon Transfer Family 服务器端点入门

使用本教程开始使用 Amazon Transfer Family （ Transfer Family ）。您将学习如何使用 Amazon S3 存储创建具有可公开访问端点的启用 SFTP 的服务器，如何添加具有服务托管身份验证的用户，以及如何使用 Cyberduck 传输文件。

主题

- 先决条件
- 步骤 1：登录到 Amazon Transfer Family 控制台
- 步骤 2：创建启用 SFTP 的服务器
- 步骤 3：添加服务托管用户
- 步骤 4：使用客户端传输文件

先决条件

开始之前，请确保完成 先决条件 中的要求。在此设置中，您将创建一个亚马逊简单存储服务 (Amazon S3) 存储桶和 Amazon Identity and Access Management 一个 (IAM) 用户角色。

使用 Amazon Transfer Family 控制台需要权限，也需要权限才能配置 Transfer Family 使用的其他 Amazon 服务，例如亚马逊简单存储服务 Amazon Certificate Manager、亚马逊弹性文件系统和亚马逊 Route 53。例如，对于 Amazon 使用 Transfer Family 传入和传出文件的用户，AmazonS3 会FullAccess授予设置和使用 Amazon S3 存储桶的权限。创建 Amazon S3 存储桶需要此策略中的一些权限。

要使用 Transfer Family 控制台，您需要满足以下条件：

- AWSTransferConsoleFullAccess向您的 SFTP 用户授予创建 Transfer Family 资源的权限。
- IAMFull只有当您希望 Transfer Family 在 Amazon CloudWatch Logs 中自动为您的服务器创建日志角色或为登录服务器的用户创建用户角色时，才需要@@ 访问权限（或者具体来说是允许创建 IAM 角色的策略）。
- 要创建和删除 VPC 服务器类型，您需要在策略中添加操作 ec2: CreateVpcEndpoint 和 ec2: DeleteVpcEndpoints。有关出于安全目的限制 VPC 终端节点访问的信息，请参阅限制 Transfer Family 服务器的 VPC 终端节点访问权限。

> **Note**
>
> 一般IAMFull使用并不需要 AmazonS3 FullAccess 和 Access 政策。 Amazon Transfer Family 此处将它们作为一种简单的方法来确保您需要的所有权限都得到满足。此外，这些是 Amazon 托管策略，它们是可供所有 Amazon 客户使用的标准策略。您可以查看这些策略中的个人权限，并确定实现您的目的所需的最低权限集。

步骤 1：登录到 Amazon Transfer Family 控制台

要登录 Transfer Family

1. 登录 Amazon Web Services 管理控制台 并打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 对于账户 ID 或别名，请输入您的 Amazon Web Services 账户 ID。
3. 对于IAM 用户名，输入您为 Transfer Family 创建的用户角色名称。
4. 在“密码”中，输入您的 Amazon 帐户密码。
5. 选择登录。

步骤 2：创建启用 SFTP 的服务器

Secure Shell (SSH) 文件传输协议 (SFTP) 是一种用于通过互联网安全传输数据的网络协议。该协议支持 SSH 的完整安全和身份验证功能。它被广泛应用于金融服务、医疗保健、零售和广告等各行各业的业务合作伙伴之间交换数据，包括敏感信息。

要创建启用 SFTP 的服务器

1. 从导航窗格中选择服务器，然后选择创建服务器。
2. 在选择协议中，选择 SFTP，然后选择下一步。
3. 在选择身份提供商中，选择服务托管，在 Transfer Family 中存储用户身份和密钥，然后选择下一步。
4. 在选择端点中，执行以下操作：
   a. 对于端点类型，选择可公开访问的端点类型。
   b. 对于自定义主机名，选择无。
   c. 选择下一步。

5. 在选择域名中，选择 Amazon S3。
6. 在配置其他详细信息中，对于加密算法选项，选择包含允许服务器使用的加密算法的安全策略。我们的最新安全策略是默认策略：有关详细信息，请参阅Amazon Transfer Family 服务器的安全策略。

   > **Note**
   >
   > 只有在为服务器添加托管工作流程时，才选择创建新的CloudWatch日志记录角色。要记录服务器事件，您无需创建 IAM 角色。

7. 在审核并创建中，选择创建服务器。您将进入服务器页面。

您的新服务器状态更改为在线可能需要几分钟时间。此时，您的服务器可以执行文件操作，但您需要先创建一个用户。有关创建用户的详细信息，请参阅管理服务器端点的用户。

步骤 3：添加服务托管用户

要向启用 SFTP 的服务器添加用户

1. 在“服务器”页面上，选择要向其添加用户的服务器。
2. 选择添加用户。
3. 在用户配置部分的用户名中，输入用户名。此用户名长度最少为 3 个字符，最多为 100 个字符你可以在用户名中使用以下字符：a—z、A-Z、0—9、下划线 '_'、连字符 '-'、句点 '.' 和 at 符号 '@'。用户名不能以连字符 “-”、“句点” 或 “@” 开头。
4. 对于访问权限，请选择您在中创建的 IAM 角色创建 IAM 角色和策略。此 IAM 角色包括一个 IAM 策略，该策略包含访问您的 Amazon S3 存储桶的权限，以及与该 Amazon Transfer Family 服务的信任关系。中概述的程序建立信任关系显示了如何建立适当的信任关系。
5. 对于策略，选择无。
6. 在主目录中，选择要用来存储传输的数据的 Amazon S3 存储桶 Amazon Transfer Family。输入home目录的路径。这是您的用户使用客户端登录时看到的目录。

   我们建议使用包含用户名的目录路径，以便您可以选择使用会话策略。会话策略限制用户在 Amazon S3 存储桶中访问该用户的home目录。有关使用会话策略的更多信息，请参阅会话策略工作原理。

   如果您愿意，可以将此参数保留为空以使用您的 Amazon S3 存储桶的`root`目录。如果您选择此选项，请确保您的 IAM 角色提供对`root`目录的访问权限。

7. 选中 “受限” 复选框可防止您的用户访问其home目录之外的任何内容。这还可以防止用户看到 Amazon S3 存储桶名称或文件夹名称。
8. 对于 SSH 公钥，请按`ssh-rsa <string>`格式输入 SSH 密钥对的 SSH 公钥部分。

   您的密钥必须经过服务验证，然后才能添加新用户。有关如何生成 SSH 密钥对的更多信息，请参阅为服务托管用户生成 SSH 密钥。
9. （可选）对于键和值，输入一个或多个标记作为键-值对，然后选择添加标记。
10. 选择 Add (添加) 可将您的新用户添加到所选服务器。

    新用户将出现在服务器详细信息页面的用户部分。

步骤 4：使用客户端传输文件

通过在客户端中指定传输操作，您可以通过 Amazon Transfer Family 服务传输文件。 Amazon Transfer Family 支持多个客户端。有关详细信息，请参阅 使用客户端通过服务器端点传输文件

本部分包含使用 Cyberduck 和 OpenSSH 的过程。

主题

- 使用 Cyberduck
- 使用 OpenSSH

使用 Cyberduck

Amazon Transfer Family 使用 Cyberduck 传输文件

1. 打开 Cyberduck 客户端。
2. 选择打开连接。
3. 在打开连接对话框中，选择 SFTP（SSH 文件传输协议）。
4. 对于服务器，输入您的服务器端点。服务器端点位于服务器详细信息页面上，请参阅 查看 SFTP、FTPS 和 FTP 服务器的详细信息。
5. 在端口号中，输入**22** SFTP。
6. 对于用户名，输入您在管理服务器端点的用户中创建的用户的名称。
7. 对于SSH 私有密钥，请选择或输入 SSH 私有密钥。
8. 选择连接。

9. 执行文件传输。

   根据您的文件所在的位置，执行以下操作之一：

   - 在您的本地目录（源）中，选择您要传输的文件，然后将这些文件拖放到 Amazon S3 目录（目标）中。
   - 在 Amazon S3 目录（源）中，选择您要传输的文件，然后将这些文件拖放到您的本地目录（目标）中。

使用 OpenSSH

按照下文中的说明，使用 OpenSSH 从命令行传输文件。

> **Note**
>
> 此客户端仅适用于启用 SFTP 的服务器。

Amazon Transfer Family 使用 OpenSSH 命令行实用程序传输文件

1. 在 Linux 或 Macintosh 上，打开命令终端。
2. 在提示符中，输入以下命令：`% sftp -i transfer-key sftp_user@service_endpoint`

   在前面的命令中，`sftp_user` 是用户名，`transfer-key` 是 SSH 私有密钥。此处`service_endpoint`是服务器的终端节点，如所选服务器的 Amazon Transfer Family 控制台中所示。

   此时应显示 `sftp` 提示符。
3. （可选）要查看用户的主目录，请在`sftp`提示符下输入以下命令：`sftp> pwd`
4. 在下一行上，输入以下文本：`sftp> cd /amzn-s3-demo-bucket/home/sftp_user`

   在本入门练习中，将此 Amazon S3 存储桶作为文件传输的目标。
5. 在下一行上，输入以下命令：`sftp> put filename.txt`

   `put` 命令将文件传输到 Amazon S3 存储桶中。

   此时将显示类似于下文的消息，指示文件传输正在进行或者已完成。

```
Uploading filename.txt to /amzn-s3-demo-bucket/home/sftp_user/
filename.txt

some-file.txt 100% 127 0.1KB/s 00:00
```

设置用于解密文件的托管工作流程

本教程说明如何设置包含解密步骤的托管工作流程。本教程还展示了如何将加密文件上传到 Amazon S3 存储桶，然后在同一存储桶中查看解密后的文件。

> **Note**
>
> Amazon 存储博客上有一篇文章描述了如何使用 Transfer Family Managed 工作流程、使用 PGP 加密和解密文件以及，无需编写任何代码即可简单地解密文件。 Amazon Transfer Family

主题

- 步骤 2：配置执行角色
- 步骤 2：创建托管工作流程
- 步骤 3：将工作流程添加至服务器并创建用户
- 步骤 2：创建 PGP 密钥对
- 步骤 5：将 PGP 私有密钥存储在 Amazon Secrets Manager中
- 步骤 6：加密文件
- 步骤 7：运行工作流程并查看结果

步骤 2：配置执行角色

创建一个 Amazon Identity and Access Management (IAM) 执行角色，Transfer Family 可以使用该角色来启动工作流程。适用于工作流程的 IAM 策略 中描述了创建执行角色的过程。

> **Note**
>
> 在创建执行角色时，请务必在执行角色和 Transfer Family 之间建立信任关系，如 建立信任关系 中所述。

以下执行角色策略包含启动您在本教程中创建的工作流程所需的所有权限。要使用此示例策略，请将 *user input placeholders* 替换为您自己的信息。amzn-s3-demo-bucket替换为您上传加密文件的 Amazon S3 存储桶的名称。

> **Note**
>
> 并非每个工作流程都需要此示例中列出的每个权限。您可以根据特定工作流程中的步骤类型来限制权限。使用预定义的步骤 中描述了每种预定义步骤类型所需的权限。自定义步骤的 IAM 权限 中描述了每种自定义步骤所需的权限。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "WorkflowsS3Permissions",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:PutObject",
                "s3:PutObjectTagging",
                "s3:ListBucket",
                "s3:PutObjectTagging",
                "s3:PutObjectVersionTagging",
                "s3:DeleteObjectVersion",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket/*",
                "arn:aws:s3:::amzn-s3-demo-bucket"
            ]
        },
        {
            "Sid": "DecryptSecret",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
```

```
            "Resource": "arn:aws:secretsmanager:us-east-1:123456789012:secret:aws/
transfer/*"
        }
    ]
}
```

步骤 2：创建托管工作流程

现在，您需要创建一个包含解密步骤的工作流程。

创建一个包含解密步骤的工作流程。

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在左侧的导航窗格中，选择工作流程，然后选择创建工作流程。
3. 输入以下详细信息：
   - 例如，输入描述 **Decrypt workflow example**。
   - 在标称步骤部分中，选择添加步骤。
4. 对于选择步骤类型，选择解密文件，然后选择下一步。
5. 在配置参数对话框中，指定以下内容：
   - 例如，输入描述性步骤名称 **decrypt-step**。步骤名称中不允许使用空格。
   - 对于解密文件的目标，请选择 Amazon S3。
   - 对于目标存储桶名称，请选择您在步骤 1 中创建的 IAM 策略 amzn-s3-demo-bucket 中指定的相同的 Amazon S3 存储桶。
   - 在目标密钥前缀中，输入要在目标存储桶中存储解密文件的前缀（文件夹）的名称，例如，**decrypted-files/**。

     > **Note**
     >
     > 请务必在前缀中添加一个尾部斜杠 (**/**)。

   - 在本教程中，请清除覆盖现有文件。清除此设置后，如果您尝试解密与现有文件同名的文件，则工作流处理将停止，并且不会处理新文件。

   选择下一步，进入下一个审核屏幕。

6. 审核该步骤的详细信息。如果一切正确，请选择创建步骤。
7. 您的工作流程只需要单个解密步骤，因此无需配置其他步骤。选择创建工作流程以创建新工作流程。

记下新工作流程的工作流程 ID。下一步骤中，您需要用到此 ID。本教程使用 *w-1234abcd5678efghi* 作为示例工作流程 ID。

步骤 3：将工作流程添加至服务器并创建用户

现在您已经有了带有解密步骤的工作流程，您必须将其与 Transfer Family 服务器相关联。本教程介绍如何将工作流程附加至现有 Transfer Family 服务器。或者，您可以创建新的服务器以用于您的工作流程。

将工作流程附加到服务器后，必须创建一个可以通过 SFTP 连接到服务器并触发工作流程运行的用户。

配置 Transfer Family 服务器以运行工作流程

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在左侧导航窗格中，选择服务器，然后从列表中选择服务器。确保此服务器支持 SFTP 协议。
3. 在服务器的详细信息页面上，向下滚动到其他详细信息部分，然后选择编辑。
4. 在编辑其他详细信息页面的托管工作流程部分，选择您的工作流程，然后选择相应的执行角色。
   - 对于完成文件上传的工作流程，请选择您在 步骤 2：创建托管工作流程 中创建的工作流程，例如 **w-1234abcd5678efghi**。
   - 对于托管工作流程执行角色，选择您在 步骤 2：配置执行角色 中创建的 IAM 角色。
5. 滚动到页面底部并选择保存以保存您的更改。

记下您正在使用的服务器的 ID。用于存储 PGP Amazon Secrets Manager 密钥的密钥的名称部分基于服务器 ID。

添加可以触发工作流程的用户

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在左侧导航窗格中，选择服务器，然后选择您要用于解密工作流程的服务器。
3. 在服务器的详细信息页面上，向下滚动到用户部分，然后选择添加用户。

4. 对于您的新用户，请输入以下详细信息：

   - 对于用户名，输入 **decrypt-user**。
   - 对于角色，请选择可以访问您的服务器的用户角色。
   - 对于主目录，选择您之前使用的 Amazon S3 存储桶，例如 amzn-s3-demo-bucket。
   - 对于 SSH 公有密钥，请粘贴与您拥有的私有密钥相对应的公有密钥。有关更多信息，请参阅 为服务托管用户生成 SSH 密钥。

5. 选择添加以保存您的新用户。

记下您在这台服务器上的 Transfer Family 用户的名称。该密钥部分基于用户的名称。为简单起见，本教程使用了服务器的任何用户均可使用的默认密钥。

步骤 2：创建 PGP 密钥对

使用支持的 PGP 客户端之一以生成 PGP 密钥对。有关此过程的详细介绍，请参阅 生成 PGP 密钥。

生成 PGP 密钥对

1. 在本教程中，您可以使用 gpg (GnuPG) 版本 2.0.22 客户端生成使用 RSA 作为加密算法的 PGP 密钥对。对于此客户端，运行如下命令，并提供电子邮件地址和密码。您可以使用任何您喜欢的姓名或电子邮件地址。请务必记住所使用的值，因为本教程稍后需要输入这些值。

   ```
   gpg --gen-key
   ```

   > **Note**
   >
   > 如果您使用的版本是 GnuPG 2.3.0 或以上，则必须运行 gpg --full-gen-key。当提示输入要创建的密钥类型时，请选择 RSA 或 ECC。如果选择 ECC，则可以选择BrainPool和Curve25519作为椭圆曲线。NIST

2. 通过运行以下命令导出私有密钥。将 *user@example.com* 替换为生成密钥时使用的电子邮件地址。

   ```
   gpg --output workflow-tutorial-key.pgp --armor --export-secret-key user@example.com
   ```

   此命令将私有密钥导出到 **workflow-tutorial-key.pgp** 文件中。您可以随意命名输出文件。您也可以在将私有密钥文件添加到 Amazon Secrets Manager后删除该文件。

步骤 5：将 PGP 私有密钥存储在 Amazon Secrets Manager中

您需要以非常具体的方式将私有密钥存储在 Secrets Manager 中，以便工作流程在对上传的文件运行解密步骤时可以找到私有密钥。

> **Note**
>
> 当你在 Secret Amazon Web Services 账户 s Manager 中存储密钥时，会产生费用。有关定价的信息，请参阅Amazon Secrets Manager 定价。

在 Secrets Manager 中存储 PGP 私有密钥

1. 登录 Amazon Web Services 管理控制台 并打开 Amazon Secrets Manager 控制台，网址为https://console.aws.amazon.com/secretsmanager/。
2. 在左侧导航窗格中，选择密钥。
3. 在密钥页面，选择存储新密钥。
4. 在选择密钥类型页面上，对于密钥类型，选择其他类型密钥。
5. 在键/值对部分，选择键/值选项卡。
   - 键 — 输入 **PGPPrivateKey**。
   - 值 — 将您的私有密钥文本粘贴至值字段。
6. 选择添加行，然后在密钥/值对部分选择密钥/值选项卡。
   - 键 — 输入 **PGPPassphrase**。
   - 值 — 输入您在 步骤 2：创建 PGP 密钥对 中生成 PGP 密钥对时使用的密码。
7. 选择下一步。
8. 在配置密钥页面，输入密钥的名称和描述。您可以为特定用户创建密钥，也可以创建可供所有用户使用的密钥。如果您的服务器 ID 是*s-11112222333344445*，则按如下方式命名密钥。
   - 要为所有用户创建默认密钥，请为该密钥命名**aws/transfer/*s-11112222333344445*/@pgp-default**。
   - 要仅为之前创建的用户创建密钥，请为该密钥命名 **aws/transfer/*s-11112222333344445*/decrypt-user**。
9. 选择下一步，接受配置轮换页面的默认设置。然后选择下一步。
10. 在审核页面，选择存储以创建和存储密钥。

有关将 PGP 私钥添加到 Secrets Manager 的更多信息，请参阅用于 Amazon Secrets Manager 存储 PGP 密钥。

步骤 6：加密文件

使用该 gpg 程序对文件进行加密，以便在工作流程中使用。要加密文件，请运行以下命令：

```
gpg -e -r marymajor@example.com --openpgp testfile.txt
```

在运行此命令之前，请注意以下事项：

- 对于 `-r` 参数，请 *marymajor@example.com* 替换为创建 PGP 密钥对时使用的电子邮件地址。
- `--openpgp` 标记是可选的。此标志使加密文件符合 OpenPGP RFC488 0 标准。
- 此命令将创建一个名为 **testfile.txt.gpg** 的文件，其位置与 **testfile.txt** 相同。

> **Important**
>
> 加密用于 Amazon Transfer Family 工作流程的文件时，请务必使用参数指定非匿名收件人。`-r`匿名加密（不指定收件人）可能会导致工作流程中的解密失败，因为系统无法识别要使用哪个密钥进行解密。有关此问题的调试信息，请访问解决匿名收件人加密问题。

步骤 7：运行工作流程并查看结果

要运行工作流程，您需要使用在步骤 3 中创建的用户连接到 Transfer Family 服务器。然后，您可以查看您在步骤 2.5 中指定的 Amazon S3 存储桶，配置目标参数以查看解密后的文件。

运行解密工作流程

1. 打开命令终端。
2. 运行以下命令，替换 *your-endpoint* 为实际端点和 *transfer-key* 为用户的 SSH 私有密钥：

   ```
   sftp -i transfer-key decrypt-user@your-endpoint
   ```

   例如，如果私有密钥存储在 `~/.ssh/decrypt-user` 中，而您的端点存储在 `s-11112222333344445.server.transfer.us-east-2.amazonaws.com` 中，则命令如下所示：

```
sftp -i  ~/.ssh/decrypt-user decrypt-user@s-11112222333344445.server.transfer.us-
east-2.amazonaws.com
```

3. 运行 pwd 命令。如果成功，此命令将返回以下内容：

```
Remote working directory: /amzn-s3-demo-bucket/decrypt-user
```

   您的目录反映了 Amazon S3 存储桶的名称。

4. 运行如下命令来上传文件并触发要运行的工作流程：

```
put testfile.txt.gpg
```

5. 对于解密文件的目标，您在创建工作流程时指定了 `decrypted-files/` 文件夹。现在，您可以导航到该文件夹并列出内容。

```
cd ../decrypted-files/
ls
```

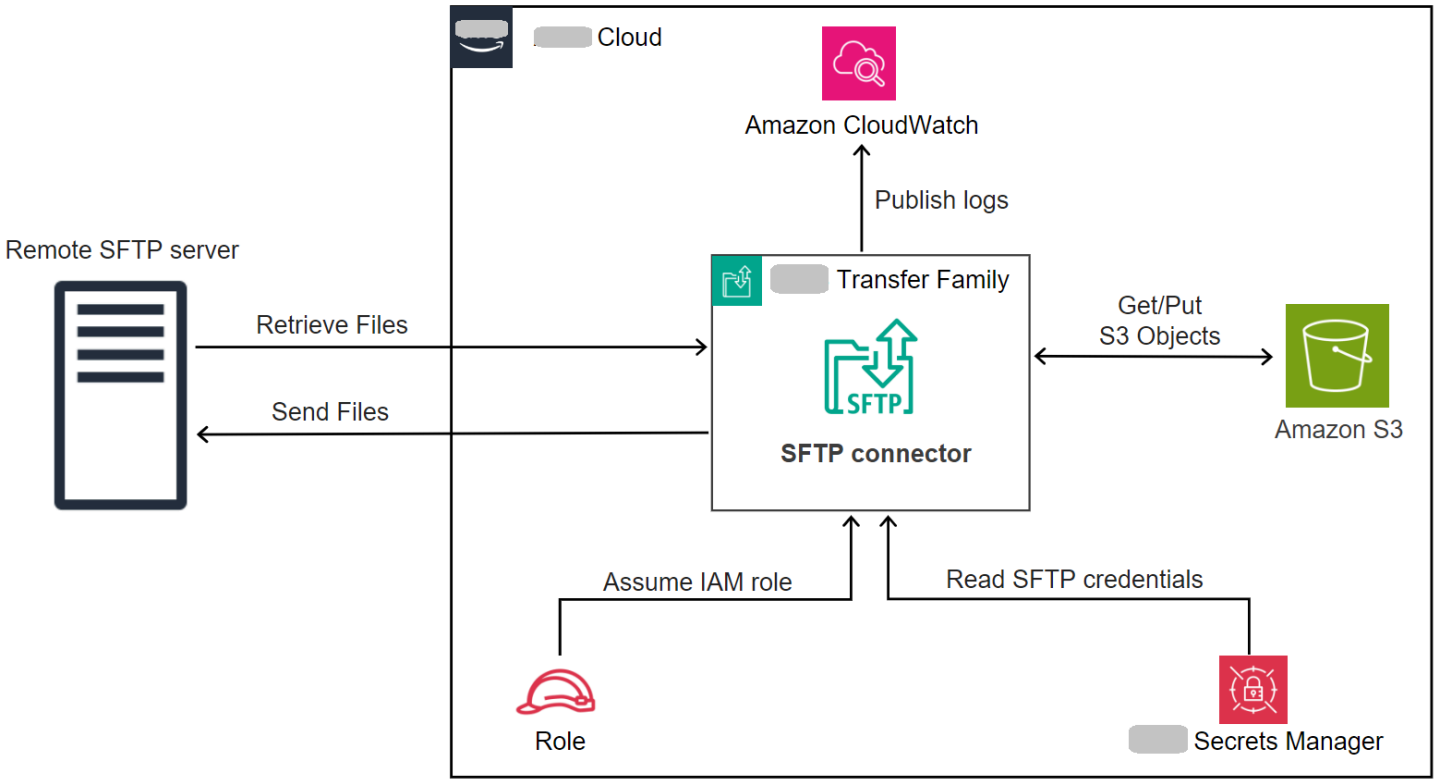
   如果成功，则 `ls` 命令将列出 `testfile.txt` 文件。您可以下载此文件并验证它是否与之前加密的原始文件相同。

设置和使用 SFTP 连接器

连接器的目的是在您的 Amazon 存储设备和合作伙伴的 SFTP 服务器之间建立关系。您可以将文件从 Amazon S3 发送到合作伙伴拥有的外部目的地。您也可以使用 SFTP 连接器从合作伙伴的 SFTP 服务器检索文件。

本教程演示了如何使用服务托管和 VPC_LATTICE 出口类型设置 SFTP 连接器，然后在 Amazon S3 存储和 SFTP 服务器之间传输文件。

SFTP 连接器从中检索 SFTP 凭据 Amazon Secrets Manager ，以便对远程 SFTP 服务器进行身份验证并建立连接。连接器向远程服务器发送文件或从远程服务器检索文件，并将文件存储在 Amazon S3 中。您可以在服务托管出口（使用托 Amazon 管基础设施）或 VPC 出口（使用跨VPC资源访问通过您的 VPC 路由）之间进行选择。IAM 角色用于允许访问 Amazon S3 存储桶和存储在 Secrets Manager 中的证书。而且你可以登录到亚马逊 CloudWatch。



以下博客文章提供了使用 SFTP 连接器构建 MFT 工作流程的参考架构，包括在使用 SFTP 连接器将文件发送到远程 SFTP 服务器之前使用 PGP 加密文件：使用 SFTP 连接器和 PGP 加密架构安全且合规的托管文件传输。 Amazon Transfer Family

连接器出口类型

SFTP 连接器支持两种输出类型，它们决定了您的连接器如何将流量路由到远程 SFTP 服务器：

- SERVICE_MAN AGED（默认）：使用 Amazon 带有静态 IP 地址的 Transfer Family 托管基础设施进行出站连接。
- VPC：使用跨虚拟私有网络资源访问通过您的 VPC 路由流量，启用私有终端节点连接并使用您自己的 NAT 网关。

本教程涵盖了两种出口类型。需要时，选择 VPC 出口类型：

- 连接到您的 VPC 中的私有 SFTP 服务器（私有 IP 地址）
- 通过 Direct Connect 或 VPN 连接到本地 SFTP 服务器
- 通过您的 VPC 路由公有终端节点流量以实现安全控制
- 使用您自己的弹性 IP 地址进行出站连接

主题

- 步骤 1：创建必要的支持资源
- 步骤 2：创建和测试 SFTP 连接器
- 步骤 3：使用 SFTP 连接器发送和检索文件
- 创建用作远程 SFTP 服务器的 Transfer Family 服务器的步骤

步骤 1：创建必要的支持资源

您可以使用 SFTP 连接器在 Amazon S3 和任何远程 SFTP 服务器之间复制文件。在本教程中，我们使用 Amazon Transfer Family 服务器作为远程 SFTP 服务器。我们需要创建和配置以下资源：

- 创建 Amazon S3 存储桶以在您的 Amazon 环境中存储文件，以及从远程 SFTP 服务器发送和检索文件：。创建 Amazon S3 存储桶
- 在 Secrets Manager 中创建用于访问 Amazon S3 存储空间和我们的密钥的 Amazon Identity and Access Management 角色：创建具有必要权限的 IAM 角色。
- 创建使用 SFTP 协议的 Transfer Family 服务器，以及使用 SFTP 连接器在 SFTP 服务器之间传输文件或从 SFTP 服务器传输文件的服务管理用户：。创建 Transfer Family SFTP 服务器和一个用户
- 创建一个 Amazon Secrets Manager 密钥来存储 SFTP 连接器用于登录远程 SFTP 服务器的凭据：。创建密钥并将其存储在 Amazon Secrets Manager

对于 VPC 出口类型连接器，您还需要：

- 具有相应子网和安全组的 VPC
- 资源网关（至少需要 2 个可用区）：创建资源网关（仅限 VPC 出口类型）。
- 指向您的 SFTP 服务器的资源配置：创建资源配置（仅限 VPC 出口类型）。有关更多信息，请参阅《Amazon VPC Lattice User Guide》中的 Resource configurations。

创建 Amazon S3 存储桶

创建 Amazon S3 存储桶

1. 登录 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/s3/。
2. 选择一个地区并输入名称。

在本教程中，我们的存储桶位于中**US East (N. Virginia) us-east-1**，名称为**sftp-server-storage-east**。

3. 接受默认值并选择创建存储桶。

有关创建 Amazon S3 存储桶的完整详细信息，请参阅如何创建 S3 存储桶？ 在 Amazon 简单存储服务用户指南中。

创建具有必要权限的 IAM 角色

对于访问角色，创建具有以下权限的策略。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
        "Sid": "AllowListingOfUserFolder",
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket"
        ]
    },
    {
        "Sid": "HomeDirObjectAccess",
        "Effect": "Allow",
        "Action": [
            "s3:PutObject",
            "s3:GetObject",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion",
            "s3:GetObjectVersion",
            "s3:GetObjectACL",
            "s3:PutObjectACL"
        ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
```

```
    },
    {
        "Sid": "GetConnectorSecretValue",
        "Effect": "Allow",
        "Action": [
            "secretsmanager:GetSecretValue"
        ],
        "Resource": "arn:aws:secretsmanager:us-west-2:111122223333:secret:aws/
transfer/SecretName-6RandomCharacters"
    }
  ]
}
```

按如下方式替换项目：

- 对于amzn-s3-demo-bucket，本教程使用**sftp-server-storage-east**。
- 对于*region*，本教程使用**us-east-1**。
- 对于*account-id*，请使用您的 Amazon Web Services 账户 身份证。
- 因为*SecretName-6RandomCharacters*，我们**using sftp-connector1**支持这个名字（你将有自己的六个随机字符作为你的秘密）。

您还必须确保此角色包含信任关系，允许连接器在处理用户的转移请求时访问您的资源。有关建立信任关系的详细信息，请参阅 建立信任关系。

> **Note**
>
> 要查看我们在本教程中使用的角色的详细信息，请参阅用户和访问角色的组合。

创建密钥并将其存储在 Amazon Secrets Manager

我们需要在 Secrets Manager 中存储一个密钥来存储你的 SFTP 连接器的用户凭证。您可以使用密码、SSH 私钥或两者兼而有之。在本教程中，我们使用的是私钥。

> **Note**
>
> 当你在 Secret Amazon Web Services 账户 s Manager 中存储密钥时，会产生费用。有关定价的信息，请参阅Amazon Secrets Manager 定价。

在开始存储密钥的过程之前，请检索并格式化您的私钥。私钥必须与在远程 SFTP 服务器上为用户配置的公钥相对应。在本教程中，私钥必须对应于我们用作远程服务器的 Transfer Family SFTP 服务器上为测试用户存储的公钥。

为此，请运行以下命令：

```
jq -sR . path-to-private-key-file
```

例如，如果您的私钥文件位于中`~/.ssh/sftp-testuser-privatekey`，则命令如下所示。

```
jq -sR . ~/.ssh/sftp-testuser-privatekey
```

这会将正确格式的密钥（带有嵌入的换行符）输出到标准输出。将此文本复制到某个地方，因为您需要将其粘贴到以下步骤中（在步骤 6 中）。

若要在 Secrets Manager 中存储 SFTP 连接器的用户凭证

1. 登录 Amazon Web Services 管理控制台 并打开 Amazon Secrets Manager 控制台，网址为https://console.aws.amazon.com/secretsmanager/。
2. 在左侧导航窗格中，选择密钥。
3. 在密钥页面，选择存储新密钥。
4. 在选择密钥类型页面上，对于密钥类型，选择其他类型密钥。
5. 在键/值对部分，选择键/值选项卡。
   - 密钥-输入**`Username`**。
   - valu e — 输入我们的用户名**`sftp-testuser`**。
6. 要输入密钥，我们建议您使用纯文本选项卡。
   a. 选择添加行，然后输入**`PrivateKey`**。
   b. 选择纯文本选项卡。该字段现在包含以下文本：

      ```
      {"Username":"sftp-testuser","PrivateKey":""}
      ```

   c. 在空双引号 (“”) 之间粘贴私钥文本（之前保存）。

      屏幕应如下所示（关键数据显示为灰色）。

7. 选择下一步。
8. 在配置密钥页面上，输入您的密钥的名称。在本教程中，我们命名了秘密**aws/transfer/sftp-connector1**。
9. 选择下一步，接受配置轮换页面的默认设置。然后选择下一步。
10. 在审核页面，选择存储以创建和存储密钥。

创建资源网关（仅限 VPC 出口类型）

对于 VPC 出口类型连接器，您需要在 VPC 中创建资源网关。资源网关充当跨VPC资源访问的入口点。

创建资源网关

1. 运行以下命令创建资源网关（将 VPC ID 和子网 IDs 替换为您的值）：

```
aws vpc-lattice create-resource-gateway \
    --name my-sftp-resource-gateway \
    --vpc-identifier vpc-12345678 \
    --subnet-ids subnet-12345678 subnet-87654321
```

> **Note**
>
> 资源网关要求子网位于至少 2 个可用区。

2. 记下响应中的资源网关 ID，以便在下一步中使用。

创建资源配置（仅限 VPC 出口类型）

创建指向您的 SFTP 服务器的资源配置。这可以是您的 VPC 中服务器的私有 IP 地址，也可以是外部服务器的公有 DNS 名称。有关资源配置的更多信息，请参阅 Amazon VPC Lattice 用户指南中的资源配置。

创建资源配置

1. 对于私有 SFTP 服务器，请运行：

```
aws vpc-lattice create-resource-configuration \
    --name my-sftp-resource-config \
    --port-ranges 22 \
    --type SINGLE \
    --resource-gateway-identifier rgw-12345678 \
    --resource-configuration-definition ipResource={ipAddress="10.0.1.100"}
```

2. 对于公共 SFTP 服务器（仅限 DNS 名称），请运行：

```
aws vpc-lattice create-resource-configuration \
    --name my-public-sftp-resource-config \
    --port-ranges 22 \
    --type SINGLE \
    --resource-gateway-identifier rgw-12345678 \
    --resource-configuration-definition dnsResource={domainName="sftp.example.com"}
```

> **Note**
>
> 公共端点必须使用 DNS 名称，而不是 IP 地址。

3. 记下响应中的资源配置 ARN，以便在创建连接器时使用。

步骤 2：创建和测试 SFTP 连接器

在本节中，我们将创建一个使用我们之前创建的所有资源的 SFTP 连接器。有关更多详细信息，请参阅创建 SFTP 连接器。

若要创建 SFTP 连接器

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在左侧导航窗格中，选择 SFTP 连接器，然后选择创建 SFTP 连接器。
3. 对于 Egress 类型，请选择以下选项之一：

   - 服务托管（默认）：使用 Amazon 带有静态 IP 地址的 Transfer Family 托管基础设施进行出站连接。
   - VPC Lattice：使用跨虚拟私有云资源访问通过您的 VPC 路由流量。选择此选项进行私有终端节点连接或使用您自己的 NAT 网关。

   > **Important**
   >
   > 创建连接器后，您无法更改出口类型。请根据您的连接要求谨慎选择。

4. 在连接器配置部分中，提供以下信息：

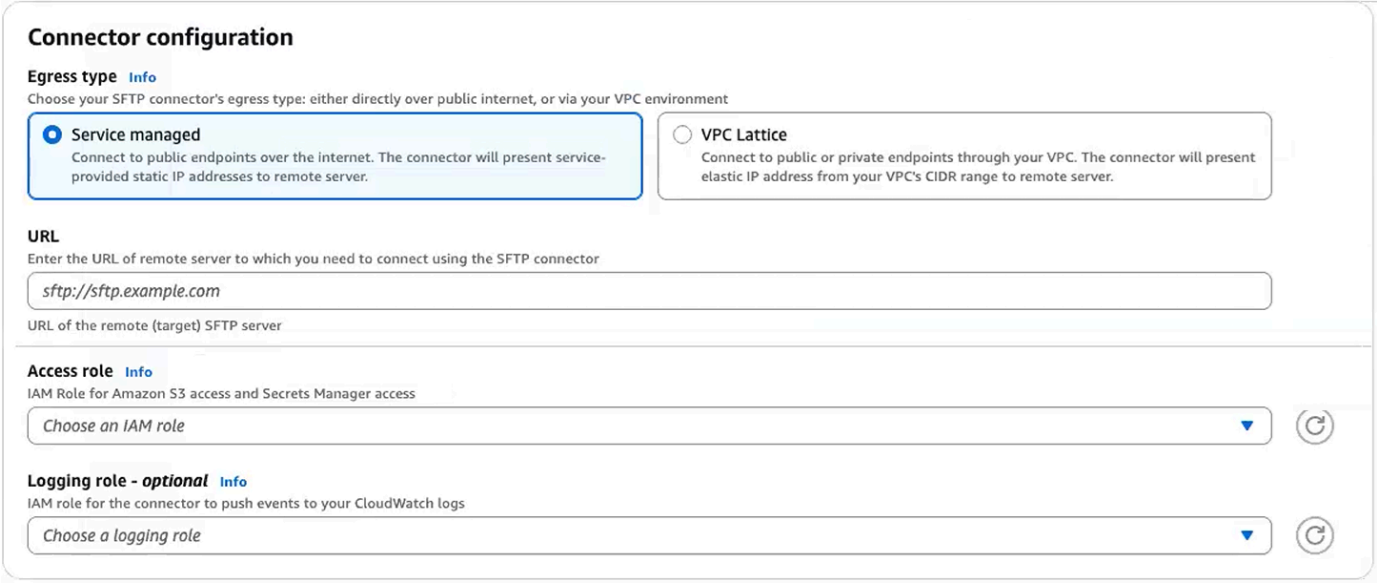
   - 在 URL 中，输入远程 SFTP 服务器的 URL。在本教程中，我们输入用作远程 SFTP 服务器的 Transfer Family 服务器的 URL。

     ```
     sftp://s-1111aaaa2222bbbb3.server.transfer.us-east-1.amazonaws.com
     ```

     *1111aaaa2222bbbb3*替换为您的 Transfer Family 服务器 ID。
   - 对于访问角色，请输入我们之前创建的角色**sftp-connector-role**。
   - 对于资源配置 ARN（仅限 VPC Lattice 出口类型），请输入您之前创建的资源配置的 ARN：

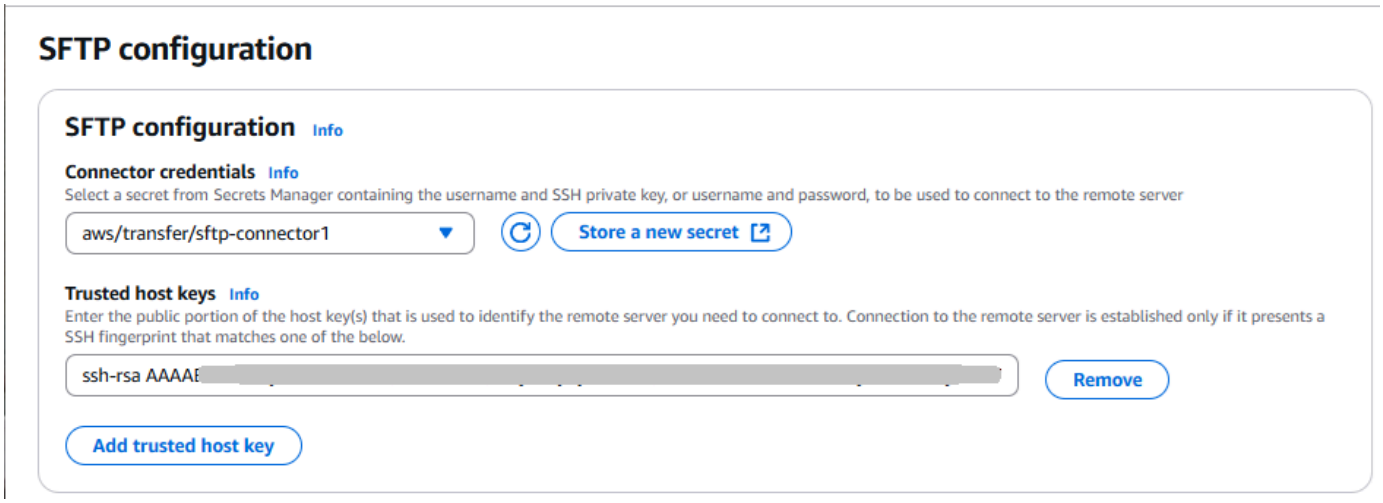
     ```
     arn:aws:vpc-lattice:us-east-1:account-id:resourceconfiguration/rcfg-12345678
     ```
   - 对于日志记录角色，请选择一个在 Principal 元素`transfer.amazonaws.com`中包含信任策略的角色。

提示：除了将 Transfer Family 添加为可信实体外，您还可以将 AWSTransferLoggingAccessV3 Amazon 托管策略添加到角色中。中详细介绍了该政策Amazon 托管策略：AWSTransferLoggingAccessV3。



5. 在 SFTP 配置面板中提供以下信息：

   - 对于连接器凭据，请选择包含 SFTP 凭据的 Secrets Manager 资源的名称。在本教程中，选择**`aws/transfer/sftp-connector1`**。
   - 对于受信任的主机密钥，请粘贴主机密钥的公共部分。您可以通过`ssh-keyscan`为 SFTP 服务器运行来检索此密钥。有关如何格式化和存储可信主机密钥的详细信息，请参阅SftpConnectorConfig数据类型文档。
   - 在“最大并发连接数”中，选择 1 到 5 之间的整数值：默认值为 5。



6. 确认所有设置后，选择创建连接器以创建 SFTP 连接器。

您也可以使用创建连接器 Amazon Command Line Interface。

- 要创建具有服务管理出口的 SFTP 连接器，请运行以下命令：

```
aws transfer create-connector \
    --url "sftp://s-1111aaaa2222bbbb3.server.transfer.us-east-1.amazonaws.com" \
    --access-role "arn:aws::iam::account-id:role/sftp-connector-role" \
    --sftp-config UserSecretId="aws/transfer/sftp-connector1",TrustedHostKeys="ssh-
rsa AAAAB3NzaC..."
```

- 要使用基于 VPC 的出口创建 SFTP 连接器，请运行以下命令：

```
aws transfer create-connector \
   --url "sftp://my.sftp.server.com:22" \
   --access-role "arn:aws::iam::account-id:role/sftp-connector-role" \
   --sftp-config UserSecretId="aws/transfer/sftp-connector1",TrustedHostKeys="ssh-rsa
 AAAAB3NzaC..." \
   --egress-config VpcLattice={ResourceConfigurationArn="arn:aws:vpc-lattice:us-
east-1:account-id:resourceconfiguration/rcfg-12345678",PortNumber=22}
```

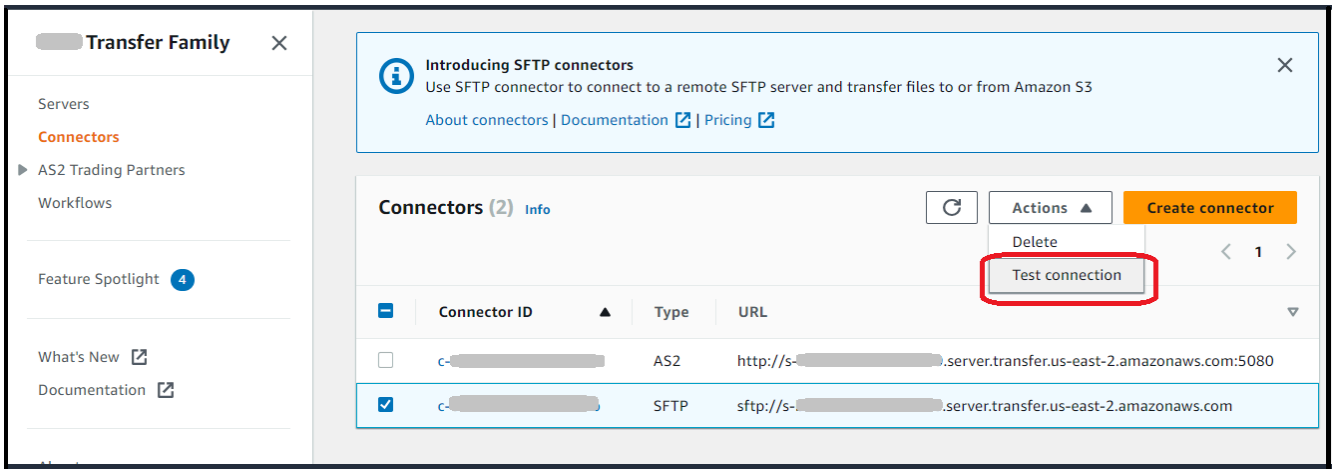
创建 SFTP 连接器后，我们建议您在尝试使用新连接器传输任何文件之前对其进行测试。

> **Note**
>
> 对于 VPC 出口类型连接器，DNS 解析在创建后可能需要几分钟时间。在此期间，连接器状态将为，PENDINGTestConnection并将返回 “连接器不可用”。等待状态变为ACTIVE后再尝试文件传输。

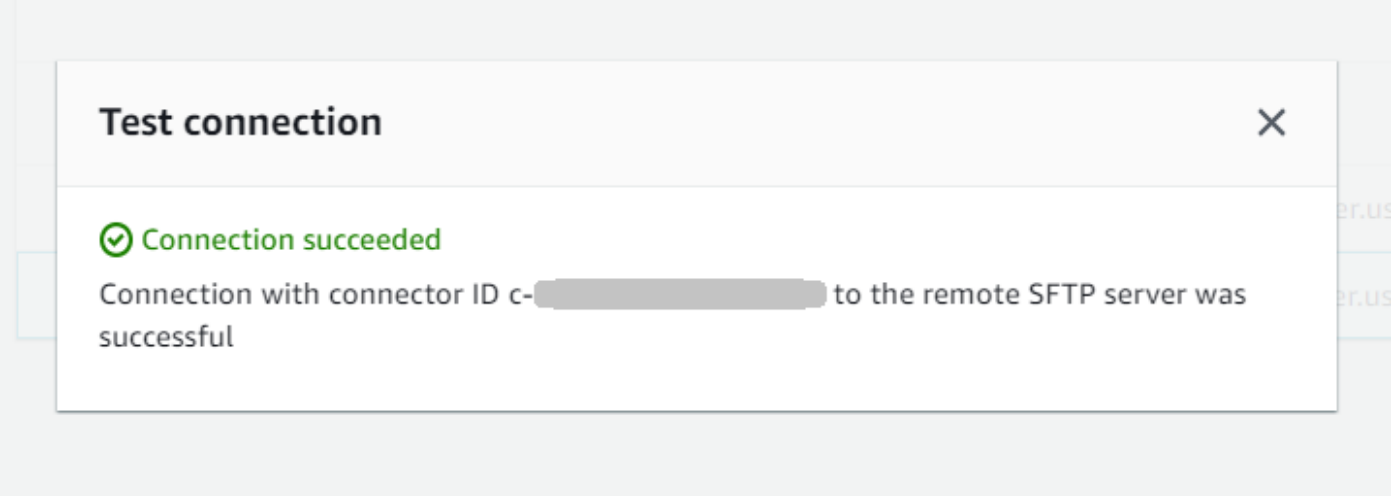
Test a connector using the console

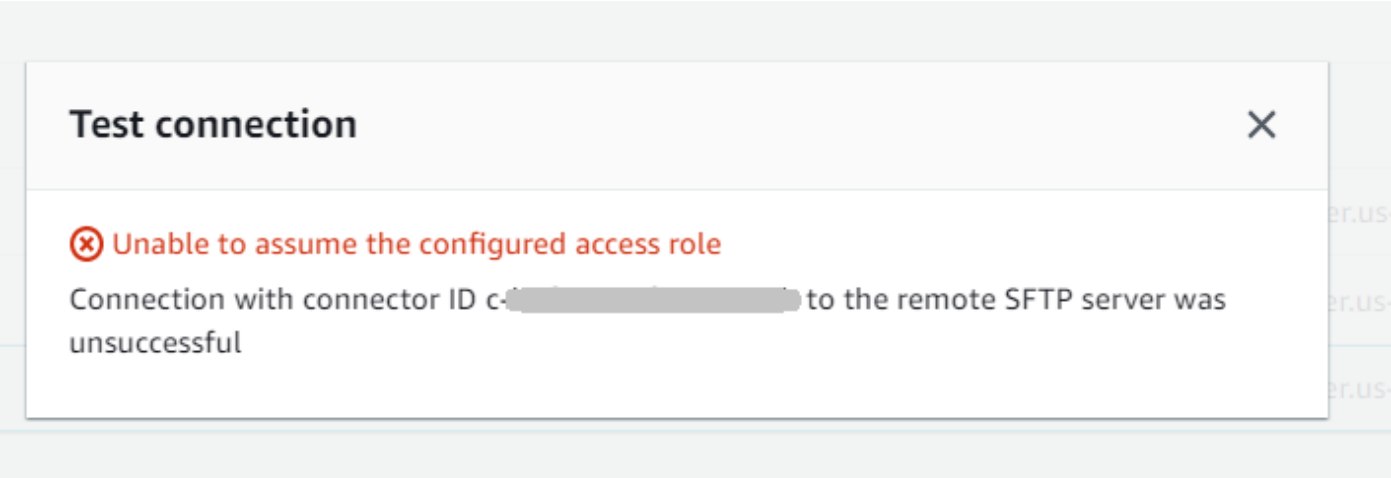
若要测试 SFTP 连接器

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在左侧导航窗格中，选择 SFTP 连接器，然后选择一个连接器。
3. 从操作菜单中选择测试连接。



系统会返回一条消息，指示测试是通过还是失败。如果测试失败，系统会根据测试失败的原因提供错误消息。





Test a connector using the CLI

要使用测试连接器 Amazon Command Line Interface，请在命令提示符下运行以下命令（*connector-id*替换为实际的连接器 ID）：

```
aws transfer test-connection --connector-id c-connector-id
```

如果测试成功，则返回以下几行：

```
{
   "Status": "OK",
   "StatusMessage": "Connection succeeded"
}
```

如果测试失败，您会收到一条描述性错误消息，例如：

```
{
```

```
    "Status": "ERROR",
    "StatusMessage": "Unable to assume the configured access role"
}
```

当您描述 VPC 出口类型连接器时，响应将包含新字段：

```
{
   "Connector": {
      "AccessRole": "arn:aws:iam::219573224423:role/sftp-connector-role",
      "Arn": "arn:aws:transfer:us-east-1:219573224423:connector/c-5dfa309ccabf40759",
      "ConnectorId": "c-5dfa309ccabf40759",
      "Status": "ACTIVE",
      "EgressConfig": {
        "ResourceConfigurationArn": "arn:aws:vpc-lattice:us-
east-1:025066256552:resourceconfiguration/rcfg-079259b27a357a190"
      },
      "EgressType": "VPC",
      "ServiceManagedEgressIpAddresses": null,
      "SftpConfig": {
         "TrustedHostKeys": [ "ssh-rsa AAAAB3NzaC..." ],
         "UserSecretId": "aws/transfer/sftp-connector1"
      },
      "Url": "sftp://my.sftp.server.com:22"
   }
}
```

请注意，`ServiceManagedEgressIpAddresses`对于 VPC 出口类型连接器，该值为空，因为流量通过您的 VPC 而不是 Amazon 托管基础设施路由。

步骤 3：使用 SFTP 连接器发送和检索文件

为简单起见，我们假设您的 Amazon S3 存储桶中已经有文件。

> **Note**
>
> 本教程使用了 Amazon S3 存储桶作为源存储位置和目标存储位置。如果您的 SFTP 服务器不使用 Amazon S3 存储，那么无论您在以下命令`sftp-server-storage-east`中看到的任何地方，都可以将路径替换为可从 SFTP 服务器访问的文件位置的路径。

- 我们将名为 Amazon S3 存储的文件发送`SEND-to-SERVER.txt`到 SFTP 服务器。

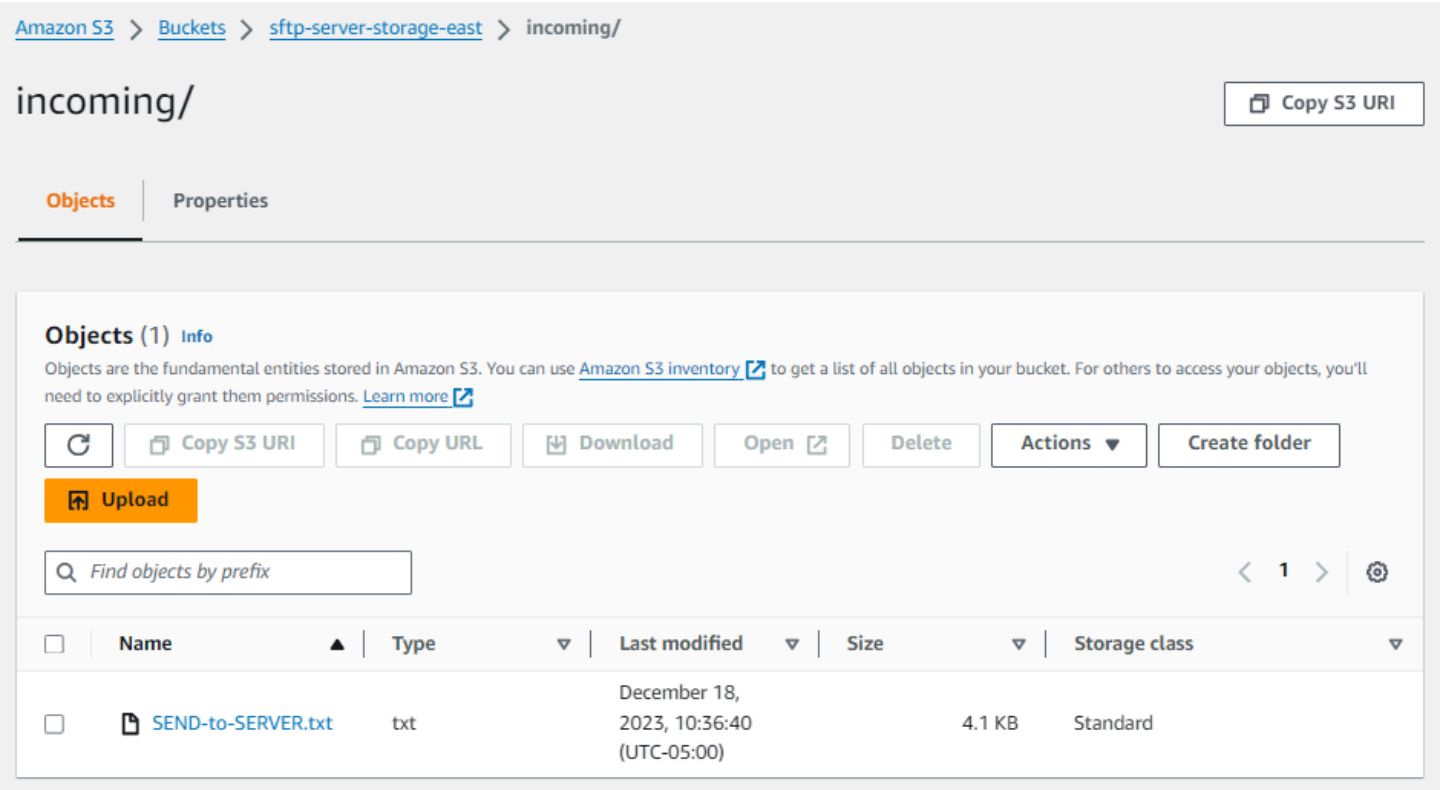
- 我们将名为的文件RETRIEVE-to-S3.txt从 SFTP 服务器检索到 Amazon S3 存储空间。

> **Note**
>
> 在以下命令中，*connector-id*替换为您的连接器 ID。

首先，我们将文件从 Amazon S3 存储桶发送到远程 SFTP 服务器。在命令提示符下，运行以下命令：

```
aws transfer start-file-transfer --connector-id c-connector-id --send-file-paths "/
sftp-server-storage-east/SEND-to-SERVER.txt" /
   --remote-directory-path "/sftp-server-storage-east/incoming"
```

你的sftp-server-storage-east存储桶现在应该是这样的。



如果您未按预期看到该文件，请检查您的 CloudWatch 日志。

查看您的 CloudWatch 日志

1. 打开亚马逊 CloudWatch 控制台，网址为 https://console.aws.amazon.com/cloudwatch/
2. 从左侧导航菜单中选择“日志组”。

3. 在搜索栏中输入您的连接器 ID 以查找您的日志。
4. 选择从搜索中返回的日志流。
5. 展开最新的日志条目。

如果成功，则日志条目如下所示：

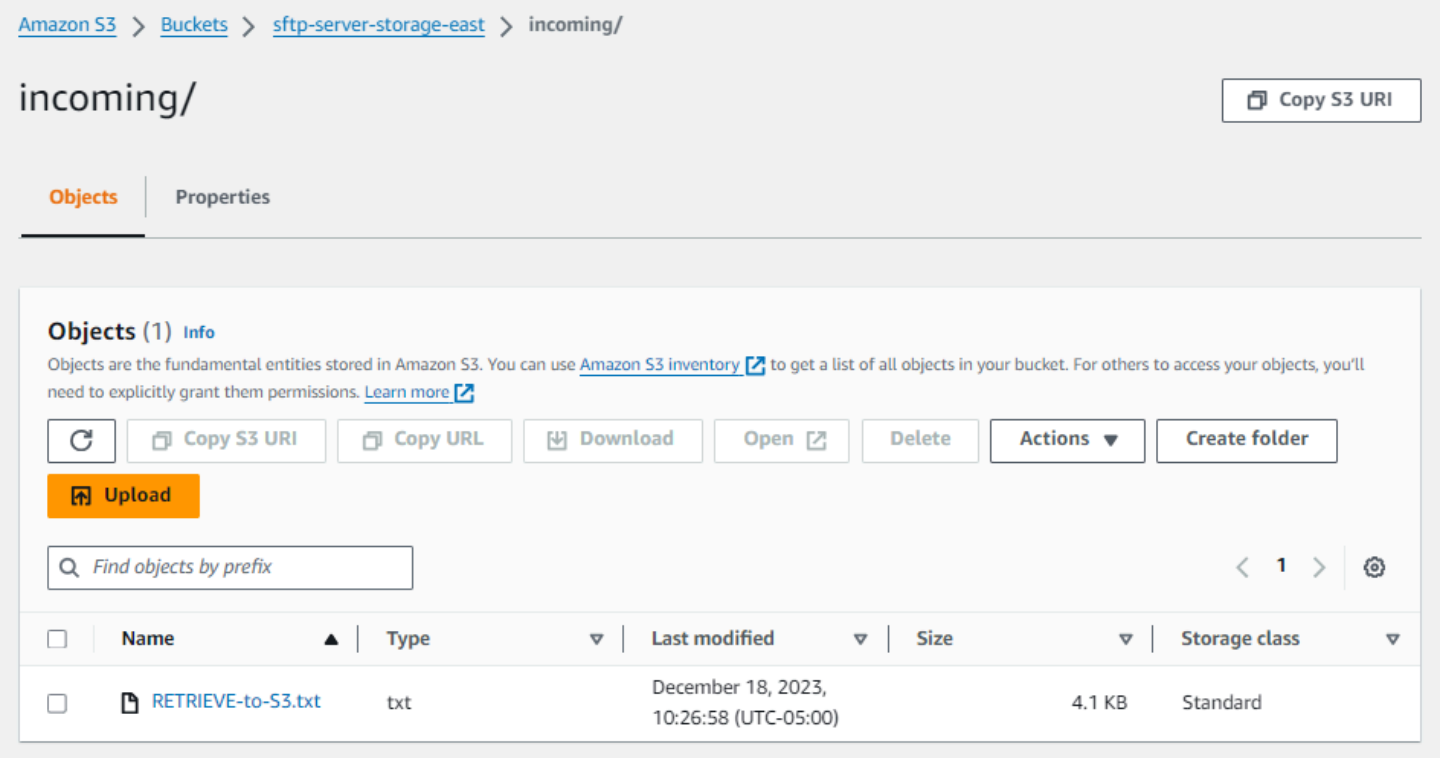
```
{
    "operation": "SEND",
    "timestamp": "2023-12-18T15:26:57.346283Z",
    "connector-id": "connector-id",
    "transfer-id": "transfer-id",
    "file-transfer-id": "transfer-id/file-transfer-id",
    "url": "sftp://server-id.server.transfer.us-east-1.amazonaws.com",
    "file-path": "/sftp-server-storage-east/SEND-to-SERVER.txt",
    "status-code": "COMPLETED",
    "start-time": "2023-12-18T15:26:56.915864Z",
    "end-time": "2023-12-18T15:26:57.298122Z",
    "account-id": "account-id",
    "connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/connector-id",
    "remote-directory-path": "/sftp-server-storage-east/incoming"
}
```

如果文件传输失败，则日志条目将包含一条指明问题的错误消息。常见的错误原因是 IAM 权限问题和文件路径不正确。

接下来，我们将文件从 SFTP 服务器检索到 Amazon S3 存储桶中。在命令提示符下，运行以下命令：

```
aws transfer start-file-transfer --connector-id c-connector-id --retrieve-file-paths
 "/sftp-server-storage-east/RETRIEVE-to-S3.txt" --local-directory-path "/sftp-server-
storage-east/incoming"
```

如果传输成功，则您的 Amazon S3 存储桶将包含传输的文件，如下所示。



如果成功，则日志条目如下所示：

```
{
    "operation": "RETRIEVE",
    "timestamp": "2023-12-18T15:36:40.017800Z",
    "connector-id": "c-connector-id",
    "transfer-id": "transfer-id",
    "file-transfer-id": "transfer-id/file-transfer-id",
    "url": "sftp://s-server-id.server.transfer.us-east-1.amazonaws.com",
    "file-path": "/sftp-server-storage-east/RETRIEVE-to-S3.txt",
    "status-code": "COMPLETED",
    "start-time": "2023-12-18T15:36:39.727626Z",
    "end-time": "2023-12-18T15:36:39.895726Z",
    "account-id": "account-id",
    "connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/c-connector-id",
    "local-directory-path": "/sftp-server-storage-east/incoming"
}
```

VPC 出口类型连接器故障排除

如果您在使用 VPC 出口类型连接器时遇到问题，请检查以下内容：

- 连接器状态为 “待处理”：VPC 连接器的 DNS 解析可能需要几分钟时间。等待状态变为 “活动” 后再尝试连接。
- 连接超时：验证安全组是否允许您的资源网关子网和目标 SFTP 服务器之间的端口 22 上的流量。
- 资源配置错误：确保您的资源配置指向正确的 IP 地址或 DNS 名称，并且资源网关与您的 SFTP 服务器（用于私有终端节点）位于同一个 VPC 中。有关更多信息，请参阅《Amazon VPC Lattice User Guide》中的 Resource configurations。
- 公共终端节点问题：对于公共终端节点，请确保在资源配置中使用的是 DNS 名称，而不是 IP 地址。确认您的 VPC 具有用于出站互联网访问的 NAT 网关。
- 可用区可用性：资源网关要求子网位于至少 2 个可用区。并非所有人都 AZs 支持 VPC Lattice — 请查看您所在 AZs 地区的支持情况。

VPC 出口类型的成本注意事项：

- 作为资源提供商，VPC Lattice 收取 0.006 美元/GB 的数据处理费用（由 VPC 莱迪思直接计费）
- Amazon Transfer Family 吸收了 0.01 美元/GB 的资源消耗成本（前 1 PB）
- 对于通过 VPC 的公共终端节点，可能会收取额外的 NAT 网关和数据传输费用
- 除了标准的 0.40 美元/GB 数据处理费外，Transfer Family 不收取额外费用

创建用作远程 SFTP 服务器的 Transfer Family 服务器的步骤

接下来，我们将概述创建用作本教程远程 SFTP 服务器的 Transfer Family 服务器的步骤。注意以下几点：

- 我们使用 Transfer Family 服务器来表示远程 SFTP 服务器。典型的 SFTP 连接器用户都有自己的远程 SFTP 服务器。请参阅创建 Transfer Family SFTP 服务器和一个用户。
- 因为我们使用的是 Transfer Family 服务器，所以我们也使用的是服务管理的 SFTP 用户。而且，为简单起见，我们将该用户访问 Transfer Family 服务器所需的权限与他们使用连接器所需的权限相结合。同样，大多数 SFTP 连接器用例都有单独的 SFTP 用户，该用户与 Transfer Family 服务器无关。请参阅创建 Transfer Family SFTP 服务器和一个用户。
- 在本教程中，由于我们在远程 SFTP 服务器上使用 Amazon S3 存储，因此我们需要创建第二个存储桶**`sftp-server-storage-east`**，以便我们可以将文件从一个存储桶传输到另一个存储桶。

创建 Transfer Family SFTP 服务器和一个用户

大多数用户不需要创建 Transfer Family SFTP 服务器和用户，因为您已经有一台包含用户的 SFTP 服务器，并且您可以使用此服务器来往传输文件。但是，在本教程中，为了简单起见，我们使用 Transfer Family 服务器来充当远程 SFTP 服务器。

按照中所述创建启用 SFTP 的服务器的步骤创建服务器和步骤 3：添加服务托管用户添加用户。以下是我们在本教程中使用的用户详细信息：

- 创建您的服务托管用户，`sftp-testuser`。
  - 将主目录设置为 `/sftp-server-storage-east/sftp-testuser`
  - 创建用户时，即存储公钥。稍后，当你在 Secrets Manager 中创建密钥时，你需要提供相应的私钥。
- 角色：`sftp-connector-role`。在本教程中，我们对 SFTP 用户和访问 SFTP 连接器使用相同的 IAM 角色。在为组织创建连接器时，您可能有不同的用户和访问角色。
- 服务器主机密钥：创建连接器时需要使用服务器主机密钥。您可以通过`ssh-keyscan`为服务器运行来检索此密钥。例如，如果您的服务器 ID 为`s-1111aaaa2222bbbb3`，且其端点位于中`us-east-1`，则以下命令将检索服务器主机密钥：

  ```
  ssh-keyscan s-1111aaaa2222bbbb3.server.transfer.us-east-1.amazonaws.com
  ```

  将此文本复制到某个地方，因为您需要将其粘贴到步骤 2：创建和测试 SFTP 连接器程序中。

用户和访问角色的组合

在本教程中，我们使用的是单一的组合角色。我们既对 SFTP 用户使用此角色，也用于访问连接器。以下示例包含此角色的详细信息，以备您要执行本教程中的任务时使用。

以下示例授予访问我们在 Amazon S3 中的两个存储桶以及存储在 Secrets Manager 中的名为`aws/transfer/sftp-connector1`的密钥所需的权限。在本教程中，这个角色被命名为`sftp-connector-role`。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowListingOfUserFolder",
            "Action": [
```

```
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::sftp-server-storage-east",
                "arn:aws:s3:::sftp-server-storage-east"
            ]
        },
        {
            "Sid": "HomeDirObjectAccess",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetObjectVersion",
                "s3:GetObjectACL",
                "s3:PutObjectACL"
            ],
            "Resource": [
                "arn:aws:s3:::sftp-server-storage-east/*",
                "arn:aws:s3:::sftp-server-storage-east/*"
            ]
        },
        {
            "Sid": "GetConnectorSecretValue",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": "arn:aws:secretsmanager:us-east-1:111122223333:secret:aws/
transfer/sftp-connector1-6RandomCharacters"
        }
    ]
}
```

有关为 Transfer Family 创建角色的完整详细信息，请按照中的创建用户角色步骤创建角色。

将 Amazon API Gateway 方法设置为自定义身份提供商

本教程演示如何设置 Amazon API Gateway 方法并将其用作自定义身份提供者将文件上传到 Amazon Transfer Family 服务器。本教程仅使用基本堆栈模板和其他基本功能作为示例。

主题

- 先决条件
- 步骤 1：创建 CloudFormation 堆栈
- 步骤 2：检查服务器的 API Gateway 方法配置。
- 步骤 3：查看 Transfer Family 服务器详细信息
- 步骤 4：测试您的用户是否可以连接到服务器
- 步骤 5：测试 SFTP 连接和文件传输
- 步骤 6：限制对存储桶的访问权限
- 如果使用 Amazon EFS，请更新 Lambda

先决条件

在中创建 Transfer Family 资源之前 Amazon CloudFormation，请创建您的存储空间和用户角色。

要指定存储并创建用户角色

1. 根据您使用的存储，请参阅以下文档：
   - 要创建 Amazon S3 存储桶，请参阅Amazon Simple Storage Service 用户指南中的如何创建 S3 存储桶？
   - 要创建 Amazon EFS 文件系统，请参阅配置 Amazon EFS 文件系统。
2. 要创建用户角色，请参阅 创建 IAM 角色和策略

在下一部分中创建 Amazon CloudFormation 堆栈时，您将输入存储和用户角色的详细信息。

步骤 1：创建 CloudFormation 堆栈

使用提供的模板创建 Amazon CloudFormation 堆栈

1. 在 https://console.aws.amazon.com/cloudformation 上打开 Amazon CloudFormation 控制台。
2. 选择创建堆栈，然后选择使用新资源（标准）。

3. 在“先决条件-准备模板”窗格中，选择选择现有模板。
4. 复制此链接，即基本堆栈模板，然后将其粘贴到 Amazon S3 URL 字段中。
5. 单击下一步。
6. 指定参数，包括堆栈的名称。务必执行以下操作：
   - 替换UserName和的默认值UserPassword。
   - 对于 UserHomeDirectory，请输入您之前创建的存储（Amazon S3 存储桶或 Amazon EFS 文件系统）的详细信息。
   - 将默认UserRoleArn角色替换为您之前创建的用户角色。 Amazon Identity and Access Management (IAM) 角色必须具有相应的权限。有关 IAM 角色和存储桶策略示例，请参阅 步骤 6：限制对存储桶的访问权限。
   - 如果要使用公钥而不是密码进行身份验证，请在 UserPublicKey1 字段中输入您的公钥。首次使用 SFTP 连接到服务器时，将提供私有密钥而不是密码。
7. 选择下一步，然后在配置堆栈选项页面上再次选择下一步。
8. 查看您正在创建的堆栈的详细信息，然后选择创建堆栈。

> **Note**
>
> 在页面底部的功能下，您必须确认 Amazon CloudFormation 可能会创建 IAM 资源。

步骤 2：检查服务器的 API Gateway 方法配置。

> **Note**
>
> 为了提高安全性，可以配置 Web 应用程序防火墙。 Amazon WAF 是一种 Web 应用程序防火墙，可让您监视转发到 Amazon API Gateway 的 HTTP 和 HTTPS 请求。有关更多信息，请参阅 添加 Web 应用程序防火墙。

> **不要启用 API Gateway 缓存**
>
> 将 API Gateway 方法用作 Transfer Family 的自定义身份提供者时，请勿为其启用缓存。缓存对身份验证请求不恰当且无效，因为：
>
> - 每个身份验证请求都是唯一的，需要实时响应，而不是缓存的响应

- 缓存没有任何好处，因为 Transfer Family 永远不会向 API Gateway 发送重复或重复的请求
- 启用缓存将导致 API Gateway 使用不匹配的数据进行响应，从而导致对身份验证请求的响应无效

检查服务器的 API Gateway 方法配置并部署它

1. 打开 API Gateway 控制台，网址为https://console.aws.amazon.com/apigateway/。
2. 选择模板生成的转移自定义身份提供商基本 Amazon CloudFormation 模板 API。
3. 在资源窗格中，选择获取，然后选择 方法请求。
4. 在操作，选择部署 API。对于部署阶段，选择 prod，然后选择部署。

   成功部署 API Gateway 方法后，在阶段编辑器部分查看其性能。

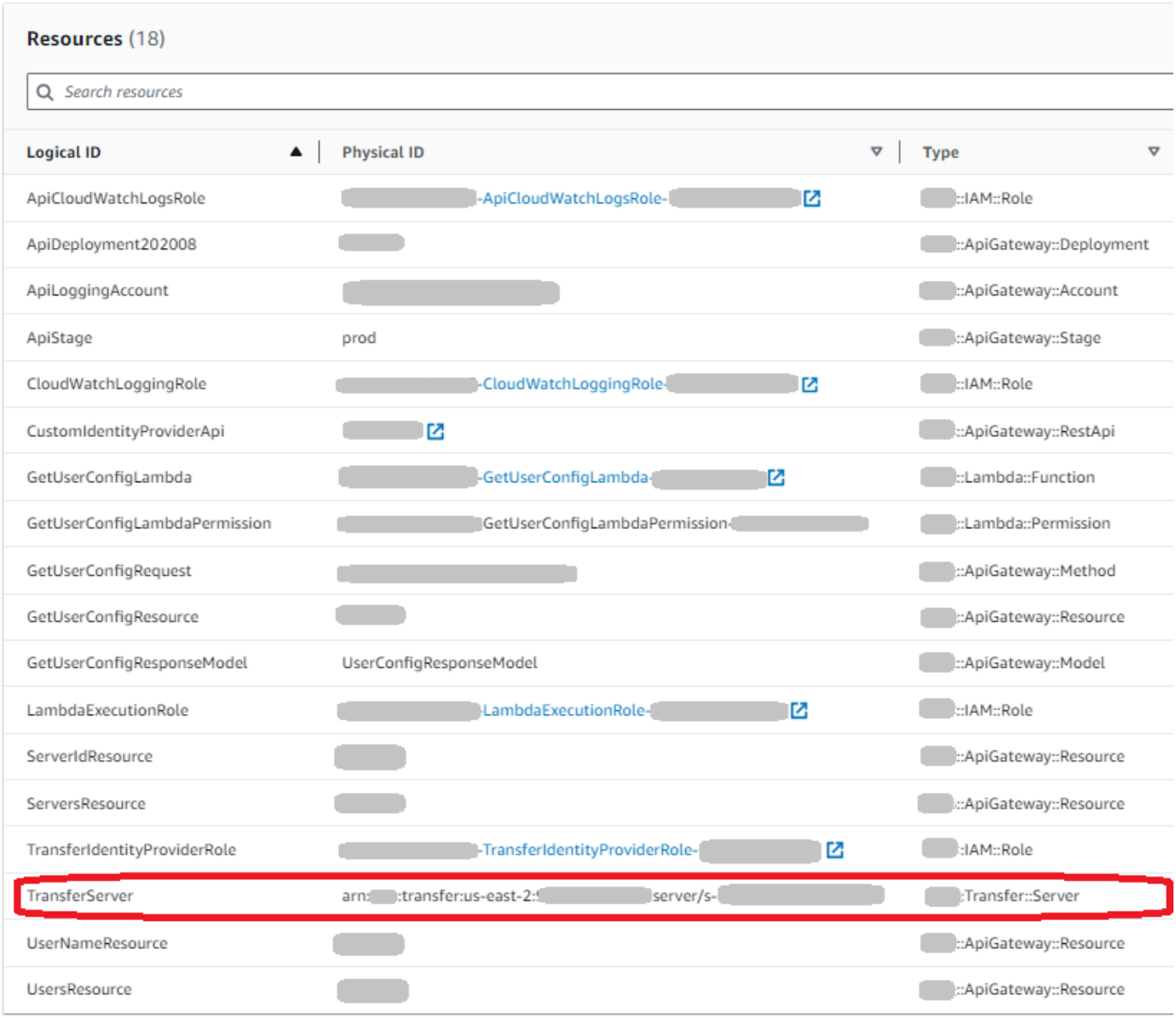
   > **Note**
   >
   > 复制显示在页面顶部的调用 URL 地址。在下一步骤中，您将需要该值。

步骤 3：查看 Transfer Family 服务器详细信息

当你使用模板创建 Amazon CloudFormation 堆栈时，会自动创建一个 Transfer Family 服务器。

要查看您的 Transfer Family 服务器详细信息

1. 在 https://console.aws.amazon.com/cloudformat ion 上打开 Amazon CloudFormation 控制台。
2. 选择您创建的堆栈。
3. 选择资源选项卡。



服务器 ARN 显示在该行的 “物理 ID” 列中。TransferServer服务器 ID 包含在 ARN 中，例如 s-11112222333344445。

4. 打开 Amazon Transfer Family 控制台 https://console.aws.amazon.com/transfer/，然后在 “服务器” 页面上，选择新服务器。

   服务器 ID 与中为TransferServer资源显示的 ID 相匹配 Amazon CloudFormation。

步骤 4：测试您的用户是否可以连接到服务器

要测试您的用户是否可以连接到服务器，请使用 Transfer Family 控制台

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在服务器页面上，选择您的新服务器，选择操作，然后选择测试。
3. 在用户名字段和密码字段中输入登录凭证的文本。这些是您在部署 Amazon CloudFormation 堆栈时设置的值。
4. 对于服务器协议，请选择 SFTP，对于源 IP，请输入**127.0.0.1**。
5. 选择测试。

   如果用户身份验证成功，则测试将返回一个 StatusCode: 200 HTML 响应和一个包含用户角色和权限详细信息的 JSON 对象。例如：

   ```
   {
       "Response": "{\"Role\": \"arn:aws:iam::123456789012:role/my-user-role\",
   \"HomeDirectory\": \"/${transfer:HomeBucket}/\"}",
       "StatusCode": 200,
       "Message": "",
       "Url": "https://1a2b3c4d5e.execute-api.us-east-2.amazonaws.com/prod/servers/
   s-1234abcd5678efgh0/users/myuser/config"
   }
   ```

   如果测试失败，请将其中一个 API Gateway Amazon 托管策略添加到您用于 API 的角色中。

步骤 5：测试 SFTP 连接和文件传输

测试 SFTP 连接

1. 在 Linux 或 macOS 设备上，打开命令终端。
2. 根据您是使用密码还是密钥对进行身份验证，输入以下命令之一。

   - 如果您使用的是密码，请输入如下命令：

     ```
     sftp -o PubkeyAuthentication=no myuser@server-
     ID.server.transfer.region-code.amazonaws.com
     ```

     出现提示时请输入密码。

- 如果您使用的是密钥对，请输入如下命令：

  ```
  sftp -i private-key-file myuser@server-ID.server.transfer.region-code.amazonaws.com
  ```

> **Note**
>
> 对于这些 `sftp` 命令，请插入 Transfer Family 服务器所在位置 Amazon Web Services 区域 的代码。例如，如果您的服务器位于美国东部（俄亥俄州），请输入 **us-east-2**。

3. `sftp>` 出现提示时，请确保您可以上传 (`put`)、下载 (`get`) 以及查看目录和文件（`pwd` 和 `ls`）。

步骤 6：限制对存储桶的访问权限

您可以限制谁能够访问特定 Amazon S3 存储桶。以下示例显示了要在 CloudFormation 堆栈和为用户选择的策略中使用的设置。

在此示例中，我们为 Amazon CloudFormation 堆栈设置了以下参数：

- CreateServer: `true`
- UserHomeDirectory: `/amzn-s3-demo-bucket1`
- UserName: `myuser`
- UserPassword: `MySuperSecretPassword`

> **Important**
>
> 这是密码示例。在配置 API Gateway 方法时，请务必输入一个强密码。

- UserPublicKey1: *your-public-key*
- UserRoleArn: `arn:aws:iam::`*role-id*`:role/myuser-api-gateway-role`

UserPublicKey1 是您作为密钥对（key pair）一部分生成的公 public/private 钥。

role-id 对于您创建的用户角色而言是唯一的。附加到 `myuser-api-gateway-role` 的策略如下：

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObjectAcl",
                "s3:GetObject",
                "s3:DeleteObjectVersion",
                "s3:DeleteObject",
                "s3:PutObjectAcl",
                "s3:GetObjectVersion"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*"
        }
    ]
}
```

要使用 SFTP 连接到服务器，请在提示符下输入以下命令之一。

- 如果您使用密码进行身份验证，请运行如下命令：

  ```
  sftp -o PubkeyAuthentication=no myuser@transfer-server-ID.server.transfer.region-id.amazonaws.com
  ```

  出现提示时请输入密码。

- 如果您使用密钥对进行身份验证，请运行如下命令：

  ```
  sftp -i private-key-file myuser@transfer-server-ID.server.transfer.region-id.amazonaws.com
  ```

> **Note**
>
> 对于这些sftp命令，请使用您的 Transf Amazon Web Services 区域 er Family 服务器所在位置的 ID。例如，如果您的服务器位于美国东部（俄亥俄州），请使用 us-east-2。

在 sftp 提示符下，您将被定向到主目录，您可以通过运行 pwd 命令来查看该目录。例如：

```
sftp> pwd
Remote working directory: /amzn-s3-demo-bucket1
```

用户无法查看主目录之上的任何目录。例如：

```
sftp> pwd
Remote working directory: /amzn-s3-demo-bucket1
sftp> cd ..
sftp> ls
Couldn't read directory: Permission denied
```

如果使用 Amazon EFS，请更新 Lambda

如果您选择 Amazon EFS 作为 Transfer Family 服务器的存储选项，则需要编辑堆栈的 lambda 函数。

向你的 Lambda 函数添加 Posix 配置文件

1. 打开 Lambda 控制台，网址为。https://console.aws.amazon.com/lambda/
2. 选择先前创建的 Lambda 函数。Lambda 函数的格式为 ***stack-name***-GetUserConfigLambda-***lambda-identifier***，其中*stack-name*是 CloudFormation 堆栈名称，*lambda-identifier*也是函数的标识符。
3. 在代码选项卡中，选择 index.js 以显示该函数的代码。
4. 在 response 中，在 Policy 和 HomeDirectory 之间添加以下行：

   ```
   PosixProfile: {"Uid": uid-value, "Gid": gid-value},
   ```

   其中，*uid-value*和*gid-value*是分别代表用户 ID 和群组 ID 的 0 或大于整数。

   例如，添加 Posix 配置文件后，响应字段可能如下所示：

   ```
   response = {
   ```

```
      Role: 'arn:aws:iam::123456789012:role/api-gateway-transfer-efs-role', // The
user will be authenticated if and only if the Role field is not blank
      Policy: '', // Optional JSON blob to further restrict this user's permissions
      PosixProfile: {"Gid": 65534, "Uid": 65534},
      HomeDirectory: '/fs-fab2c234' // Not required, defaults to '/'
    };
```

设置 AS2 配置

本教程介绍如何使用设置适用性声明 2 (AS2) 配置 Amazon Transfer Family。完成此处描述的步骤后，您将拥有一 AS2台支持该服务器的服务器，可以接受来自示例交易伙伴的 AS2 消息。您还将有一个连接器，可用于向示例贸易伙伴发送 AS2 消息。

> **Note**
>
> 示例设置的某些部分使用 Amazon Command Line Interface (Amazon CLI)。如果您尚未安装 Amazon CLI，请参阅Amazon Command Line Interface 用户指南 Amazon CLI中的安装或更新最新版本的。

1. 为自己和您的交易伙伴创建证书。如果您拥有可以使用的现有证书，则可跳过此部分。

   步骤 1：为创建证书 AS2 中介绍了此过程。
2. 导入已在第 1 步中创建的证书。

   第 2 步：将证书作为 Transfer Family 证书资源导入 中介绍了此过程。
3. 要设置您的交易伙伴，请创建本地配置文件和合作伙伴配置文件。

   第 3 步：为您和您的贸易伙伴创建档案 中介绍了此过程。
4. 创建使用该 AS2 协议的 Amazon Transfer Family 服务器。或者，您可以向服务器添加弹性 IP 地址，使其面向互联网。

   步骤 4：创建使用该 AS2协议的 Transfer Family 服务器 中介绍了此过程。

> **Note**
>
> 您必须仅为入站传输创建 Transfer Family 服务器。如果您只执行出站传输，则不需要 Transfer Family 服务器。

5. 在您和您的交易伙伴之间创建协议。

   第 5 步：创建您与合作伙伴之间的协议 中介绍了此过程。

> **Note**
>
> 您必须仅为入站传输创建协议。如果您只执行出站传输，则无需协议。

6. 在您和您的交易伙伴之间创建连接器。

   第 6 步：创建您与合作伙伴之间的连接器 中介绍了此过程。

> **Note**
>
> 您必须仅为出站传输创建连接器。如果您仅执行入站传输，则不需要连接器。

7. 测试 AS2 文件交换。

   第 7 步：使用 Transfer Famil AS2 y 测试文件交换情况 中介绍了此过程。

完成这些步骤后，您可以执行以下操作：

- 使用 Transfer AS2 Family `start-file-transfer` Amazon Command Line Interface (Amazon CLI) 命令将文件发送到启用远程功能的伙伴服务器。
- 通过您的虚拟私有云 (VPC) 终端节点在端口 5080 上从 AS2支持远程功能的合作伙伴服务器接收文件。

步骤 1：为创建证书 AS2

AS2 交易所的双方都需要 X.509 证书。您可以按喜欢的任何方式创建这些证书。本主题介绍如何通过命令行使用 OpenSSL 创建根证书，然后对从属证书进行签名。双方都必须生成自己的证书。

> **Note**
>
> AS2 证书的密钥长度必须至少为 2048 位，最多为 4096 位。

要与合作伙伴传输文件，请注意以下事项：

- 您可以将证书附加到配置文件。证书包含公钥或私钥。
- 您的交易伙伴将他们的公钥发送给您，而您则将您的公钥发送给他们。
- 您的交易伙伴使用您的公钥对消息进行加密，并使用其私钥对消息进行签名。相反，您可以使用合作伙伴的公钥对消息进行加密，然后使用您的私钥对消息进行签名。

> **Note**
>
> 如果您更喜欢使用 GUI 管理密钥，Portecle 则是您可以使用的一个选项。

生成示例证书

> **Important**
>
> 不要将您的私钥发送给您的合作伙伴。在此示例中，您为一方生成一组自签名的公钥和私钥。如果您打算同时充当两个交易伙伴进行测试，则可以重复这些说明以生成两组密钥：每个交易伙伴一组。在这种情况下，您无需生成两个根证书颁发机构 (CAs)。

1. 运行以下命令以生成带有 2048 位长度模数的 RSA 私有密钥。

```
/usr/bin/openssl genrsa -out root-ca-key.pem 2048
```

2. 运行以下命令以使用您的 `root-ca-key.pem` 文件创建自签名证书。

```
/usr/bin/openssl req \
-x509 -new -nodes -sha256 \
-days 1825 \
-subj "/C=US/ST=MA/L=Boston/O=TransferFamilyCustomer/OU=IT-dept/CN=ROOTCA" \
-key root-ca-key.pem \
-out root-ca.pem
```

-subj 参数由以下值组成。

	Name	说明
C	国家/地区代码	由两个字母组成的代码，代表您的组织所在的国家/地区。
ST	州、地区或省	组织所在的州、地区或省。（在本例中，区域不是指您的 Amazon Web Services 区域。）
L	所在地名称	组织所在的城市。
O	组织名称	您组织的法定全名，包括后缀，例如 LLC、Corp 等。
OU	组织部门名称	您组织中负责处理此证书的部门。
CN	公用名或完全限定域名 (FQDN)	在这种情况下，我们将创建一个根证书，因此值为 ROOTCA。在这些示例中，我们使用 CN 来描述证书的用途。

3. 为您的本地配置文件创建签名密钥和加密密钥。

```
/usr/bin/openssl genrsa -out signing-key.pem 2048
/usr/bin/openssl genrsa -out encryption-key.pem 2048
```

> **Note**
>
> 某些 AS2启用了 Open 的服务器（例如 Op AS2 en）要求您使用相同的证书进行签名和加密。在这种情况下，您可以为这两个目的导入相同的私钥和证书。为此，请运行以下命令而不是之前的两个命令：

```
/usr/bin/openssl genrsa -out signing-and-encryption-key.pem 2048
```

4. 运行以下命令创建证书签名请求 (CSRs)，供根密钥签名。

```
/usr/bin/openssl req -new -key signing-key.pem -subj \
"/C=US/ST=MA/L=Boston/O=TransferFamilyCustomer/OU=IT-dept/CN=Signer" -out signing-
key-csr.pem
```

```
/usr/bin/openssl req -new -key encryption-key.pem -subj \
"/C=US/ST=MA/L=Boston/O=TransferFamilyCustomer/OU=IT-dept/CN=Encrypter" -out
 encryption-key-csr.pem
```

5. 接下来，必须创建一个 `signing-cert.conf` 文件和一个 `encryption-cert.conf` 文件。

   - 使用文本编辑器创建包含以下内容的 `signing-cert.conf` 文件：

   ```
   authorityKeyIdentifier=keyid,issuer
   keyUsage = digitalSignature, nonRepudiation
   ```

   - 使用文本编辑器创建包含以下内容的 `encryption-cert.conf` 文件：

   ```
   authorityKeyIdentifier=keyid,issuer
   keyUsage = dataEncipherment
   ```

6. 最后，您可以通过运行以下命令来创建签名证书。

```
/usr/bin/openssl x509 -req -sha256 -CAcreateserial -days 1825 -in signing-key-
csr.pem -out signing-cert.pem -CA \
root-ca.pem -CAkey root-ca-key.pem -extfile signing-cert.conf
```

```
/usr/bin/openssl x509 -req -sha256 -CAcreateserial -days 1825 -in encryption-key-
csr.pem -out encryption-cert.pem \
-CA root-ca.pem -CAkey root-ca-key.pem -extfile encryption-cert.conf
```

第 2 步：将证书作为 Transfer Family 证书资源导入

此过程介绍如何使用 Amazon CLI导入证书。如果您想改用 Transfer Family 控制台，请参阅 the section called “导入 AS2 证书”。

要导入您在第 1 步中创建的签名和加密证书，请运行以下 import-certificate 命令。如果您使用相同的证书进行加密和签名，请两次导入相同的证书（一次是 SIGNING 用法，另一次是 ENCRYPTION 用法）。

> **Note**
>
> 如果您的文件同时包含证书及其链，则只需使用certificate参数即可将该文件提供给import-certificate命令。例如：
>
> ```
> aws transfer import-certificate --usage ENCRYPTION --certificate
>  file://combined-cert-and-chain-file.pem
> ```
>
> 如果您使用certificate参数上传证书及其链，请不要使用该certificate-chain参数。如果合并证书及其链，则密钥将使用传统的 PEM 标准进行格式化，其中包括每 64 个字符换行符 “\ n”。存储的证书在功能上与您上传的证书相同，唯一的区别是通过的DescribeCertificate响应 Amazon CLI 将包含这些换行符。

```
aws transfer import-certificate --usage SIGNING --certificate file://signing-cert.pem \
            --private-key file://signing-key.pem --certificate-chain file://root-ca.pem
```

此命令返回您的签名 CertificateId。在下一节中，此证书 ID 被称为 *my-signing-cert-id*。

```
aws transfer import-certificate --usage ENCRYPTION --certificate file://encryption-
cert.pem \
            --private-key file://encryption-key.pem --certificate-chain file://root-
ca.pem
```

此命令返回您的加密信息 CertificateId。在下一节中，此证书 ID 被称为 *my-encrypt-cert-id*。

接下来，通过运行以下命令导入合作伙伴的加密和签名证书。

```
aws transfer import-certificate --usage ENCRYPTION --certificate file://partner-
encryption-cert.pem \
--certificate-chain file://partner-root-ca.pem
```

此命令返回您的合作伙伴的加密信息 CertificateId。在下一节中，此证书 ID 被称为 *partner-encrypt-cert-id*。

```
aws transfer import-certificate --usage SIGNING --certificate file://partner-signing-cert.pem \
--certificate-chain file://partner-root-ca.pem
```

此命令返回您的合作伙伴的签名 CertificateId。在下一节中，此证书 ID 被称为 *partner-signing-cert-id*。

第 3 步：为您和您的贸易伙伴创建档案

此过程说明如何使用创建 AS2 配置文件 Amazon CLI。如果您想改用 Transfer Family 控制台，请参阅 the section called “创建 AS2 个人资料”。

通过运行以下命令创建您的本地 AS2 配置文件。此命令引用包含您的公钥和私钥的证书。

```
aws transfer create-profile --as2-id MYCORP --profile-type LOCAL --certificate-ids \
my-signing-cert-id my-encrypt-cert-id
```

此命令会返回您的配置文件 ID。在下一节中，此 ID 被称为 *my-profile-id*。

现在，通过运行以下命令来创建合作伙伴配置文件。此命令仅使用合作伙伴的公钥证书。要使用此命令，请将*user input placeholders*替换为您自己的信息；例如，您的合作伙伴的 AS2 姓名和证书 IDs。

```
aws transfer create-profile --as2-id PARTNER-COMPANY --profile-type PARTNER --
certificate-ids \
partner-signing-cert-id partner-encrypt-cert-id
```

此命令会返回您的合作伙伴的配置文件 ID。在下一节中，此 ID 被称为 *partner-profile-id*。

> **Note**
>
> 在前面的命令中，*MYCORP*替换为您的组织*PARTNER-COMPANY*名称和贸易伙伴的组织名称。

步骤 4：创建使用该 AS2协议的 Transfer Family 服务器

此过程说明了如何使用 Transfer Family 创建 AS2启用了 Transfer Famil Amazon CLI y 的服务器。

> **Note**
>
> 许多示例步骤都使用从文件加载参数的命令。有关使用文件加载参数的更多详细信息，请参阅如何从文件加载参数。

如果要改用控制台，请参阅 使用 Tran AS2 sfer Family 控制台创建服务器。

与创建 SFTP 或 FTPS Amazon Transfer Family 服务器的方式类似，您可以使用 AS2命令的`--protocols AS2`参数创建启用了的服务器。`create-server` Amazon CLI 目前，Transfer Family 仅支持 VPC 终端节点类型和带有该 AS2 协议的 Amazon S3 存储。

当您使用`create-server`命令为 AS2 Transfer Family 创建已启用的服务器时，系统会自动为您创建一个 VPC 终端节点。此端点公开 TCP 端口 5080，以便它可以接受 AS2 消息。

如果您想向互联网公开您的 VPC 端点，可以将弹性 IP 地址与您的 VPC 端点关联起来。

要使用这些说明，您需要以下内容：

- 您的 VPC 的 ID（例如 vpc-abcdef01）。
- 您的 IDs VPC 子网（例如 sub net-abcdef01、01、subnet-021345ab）。subnet-subnet-abcdef
- 允许贸易伙伴通过 TCP 端口 5080 传入流量的一个或多个 IDs 安全组（例如 sg-1234567890abcdef0 和 sg-abcdef0123 4567890）。
- （可选）您要与 VPC 端点关联的弹性 IP 地址。
- 如果您的交易伙伴未通过 VPN 连接到您的 VPC，则需要互联网网关。有关更多信息，请参阅 Amazon VPC 用户指南中的使用互联网网关连接到互联网。

创建 AS2启用了的服务器

1. 运行如下命令。将每个 *user input placeholder* 替换为您自己的信息。

```
aws transfer create-server --endpoint-type VPC \
--endpoint-details VpcId=vpc-abcdef01,SubnetIds=subnet-abcdef01,subnet-
abcdef01,subnet-
021345ab,SecurityGroupIds=sg-abcdef01234567890,sg-1234567890abcdef0 --protocols AS2
 \
--protocol-details As2Transports=HTTP
```

2. （可选）您可以将 VPC 端点设为公有。您只能通过 update-server 操作将弹性 IP 地址附加到 Transfer Family 服务器。以下命令停止服务器，使用弹性 IP 地址对其进行更新，然后重新启动服务器。

```
aws transfer stop-server --server-id your-server-id
```

```
aws transfer update-server --server-id your-server-id --endpoint-details \
AddressAllocationIds=eipalloc-abcdef01234567890,eipalloc-
1234567890abcdef0,eipalloc-abcd012345ccccccc
```

```
aws transfer start-server --server-id your-server-id
```

此 start-server 命令会自动为您创建 DNS 记录，其中包含您的服务器的公有 IP 地址。要让您的交易伙伴访问服务器，您需要向他们提供以下信息。在这种情况下，*your-region* 指的是您的 Amazon Web Services 区域。

s-*your-server-id*.server.transfer.*your-region*.amazonaws.com

您提供给交易伙伴的完整 URL 如下：

http://s-*your-server-id*.server.transfer.*your-region*.amazonaws.com:5080

3. 要测试 AS2启用了您的服务器是否可以访问，请使用以下命令。确保可以通过您的 VPC 端点的私有 DNS 地址或公有端点（如果您将弹性 IP 地址与端点相关联）访问您的服务器。

   如果您的服务器配置正确，则连接将成功。但是，您将收到 HTTP 状态码 400（错误请求）响应，因为您没有发送有效的 AS2 消息。

   - 对于公共端点（如果您在上一步中关联了弹性 IP 地址），请运行以下命令，替换您的服务器 ID 和区域。

     ```
     curl -vv -X POST http://s-your-server-id.transfer.your-region.amazonaws.com:5080
     ```

   - 如果您在 VPC 内进行连接，请运行以下命令查找 VPC 端点的私有 DNS 名称。

     ```
     aws transfer describe-server --server-id s-your-server-id
     ```

     此 describe-server 命令在 VpcEndpointId 参数中返回您的 VPC 端点 ID。使用此值运行以下命令。

```
aws ec2 describe-vpc-endpoints --vpc-endpoint-ids vpce-your-vpc-endpoint-id
```

此 describe-vpc-endpoints 命令返回一个包含多个 DnsName 参数的 DNSEntries 数组。在以下命令中使用区域 DNS 名称（不包括可用区的名称）。

```
curl -vv -X POST http://vpce-your-vpce.vpce-svc-your-vpce-svc.your-region.vpce.amazonaws.com:5080
```

例如，以下命令显示了上一个命令中占位符的示例值。

```
curl -vv -X POST http://vpce-0123456789abcdefg-fghij123.vpce-svc-11111aaaa2222bbbb.us-east-1.vpce.amazonaws.com:5080
```

4. （可选）配置日志记录角色。Transfer Family 以结构化 JSON 格式将发送和接收的消息的状态记录到亚马逊 CloudWatch 日志中。要让 Transfer Family 能够访问您账户中的 CloudWatch 日志，您必须在服务器上配置日志角色。

   创建信任transfer.amazonaws.com的 Amazon Identity and Access Management (IAM) 角色并附加AWSTransferLoggingAccess托管策略。有关更多信息，请参阅 创建 IAM 角色和策略。请注意您刚创建的 IAM 角色的 Amazon 资源名称 (ARN)，然后通过运行以下 update-server 命令将其与服务器关联：

   ```
   aws transfer update-server --server-id your-server-id --logging-role
    arn:aws:iam::your-account-id:role/logging-role-name
   ```

   > **Note**
   >
   > 尽管日志记录角色是可选的，但我们强烈建议您对其进行设置，以便您可以查看消息的状态并对配置问题进行故障排除。

第 5 步：创建您与合作伙伴之间的协议

此过程说明了如何使用创建 AS2 协议 Amazon CLI。如果您想改用 Transfer Family 控制台，请参阅 the section called “创建 AS2 协议”。

协议汇集了两个配置文件（本地和合作伙伴）、它们的证书以及允许双方之间入站 AS2 传输的服务器配置。您可以通过运行以下命令来列出您的项目。

```
aws transfer list-profiles --profile-type LOCAL
aws transfer list-profiles --profile-type PARTNER
aws transfer list-servers
```

此步骤需要一个 Amazon S3 存储桶和 IAM 角色，该角色 read/write 可以访问和访问该存储桶。创建此角色的说明与 Transfer Family SFTP、FTP 和 FTPS 协议的说明相同，可在 创建 IAM 角色和策略 中找到。

要创建协议，您需要以下项目：

- 用于存储 AS2文件的 Amazon S3 存储桶名称（以及对象前缀，如果已指定）。我们建议您为不同的文件类型指定单独的目录。
- 具有存储桶访问权限的 IAM 角色的 ARN
- 您的 Transfer Family 服务器 ID
- 您的配置文件 ID 和合作伙伴的配置文件 ID

将以下代码保存到文件中，例如agreementDetails.json。将每个 *user input placeholder* 替换为您自己的信息。

```
{
    "Description": "ExampleAgreementName",
    "ServerId": "your-server-id",
    "LocalProfileId": "your-profile-id",
    "PartnerProfileId": "your-partner-profile-id",
    "AccessRole": "arn:aws:iam::111111111111:role/TransferAS2AccessRole",
    "Status": "ACTIVE",
    "PreserveFilename": "ENABLED",
    "EnforceMessageSigning": "ENABLED",
    "CustomDirectories": {
        "FailedFilesDirectory": "/amzn-s3-demo-destination-bucket/AS2-failed",
        "MdnFilesDirectory": "/amzn-s3-demo-destination-bucket/AS2-mdn",
        "PayloadFilesDirectory": "/amzn-s3-demo-destination-bucket/AS2-payload",
        "StatusFilesDirectory": "/amzn-s3-demo-destination-bucket/AS2-status",
        "TemporaryFilesDirectory": "/amzn-s3-demo-destination-bucket/AS2-temp"
    }
}
```

> **Note**
>
> 要使用单个基本目录而不是单独的目录，请从之前的代码中删除该CustomDirectories行及其各个目录行，然后改用以下参数：
> "BaseDirectory": "/amzn-s3-demo-destination-bucket*/AS2-inbox*"
> 不要同时使用基本目录和单独的目录参数，否则命令将失败。

然后运行以下命令。

```
aws transfer create-agreement --cli-input-json file://agreementDetails.json
```

如果成功，此命令将返回协议的 ID。然后，您可以使用以下命令查看协议的详细信息。

```
aws transfer describe-agreement --agreement-id agreement-id --server-id your-server-id
```

第 6 步：创建您与合作伙伴之间的连接器

此过程说明了如何使用创建 AS2 连接器 Amazon CLI。如果您想改用 Transfer Family 控制台，请参阅the section called “配置 AS2 连接器”。

您可以使用 StartFileTransfer API 操作通过连接器将存储在 Amazon S3 中的文件发送到贸易伙伴的 AS2 终端节点。您可以通过运行以下命令找到之前创建的配置文件。

```
aws transfer list-profiles
```

创建连接器时，必须提供合作伙伴的 AS2 服务器 URL。将以下文本复制到名为 testAS2Config.json 的文件中。

```
{
"Compression": "ZLIB",
"EncryptionAlgorithm": "AES256_CBC",
"LocalProfileId": "your-profile-id",
"MdnResponse": "SYNC",
"MdnSigningAlgorithm": "DEFAULT",
"MessageSubject": "Your Message Subject",
"PartnerProfileId": "partner-profile-id",
"PreserveContentType": "FALSE",
"SigningAlgorithm": "SHA256"
```

```
}
```

> **Note**
>
> 对于EncryptionAlgorithm，除非必须支持需要该DES_EDE3_CBC算法的旧版客户端，否则不要指定算法，因为该算法是一种弱加密算法。

然后运行以下命令以创建连接器。

```
aws transfer create-connector --url "http://partner-as2-server-url" \
--access-role your-IAM-role-for-bucket-access \
--logging-role arn:aws:iam::your-account-id:role/service-role/AWSTransferLoggingAccess
 \
--as2-config file:///path/to/testAS2Config.json
```

第 7 步：使用 Transfer Famil AS2 y 测试文件交换情况

从您的交易伙伴那里接收文件

如果您将公有弹性 IP 地址与 VPC 端点相关联，Transfer Family 会自动创建包含您的公有 IP 地址的 DNS 名称。子域名是您的 Amazon Transfer Family 服务器 ID（格式为s-1234567890abcdef0）。采用以下格式向交易伙伴提供您的服务器 URL。

```
http://s-1234567890abcdef0.server.transfer.us-east-1.amazonaws.com:5080
```

如果您没有将公有弹性 IP 地址与 VPC 终端节点相关联，请查找 VPC 终端节点的主机名，该终端节点可以在端口 5080 上通过 HTTP POST 接受来自贸易伙伴的 AS2 消息。要检索 VPC 端点详细信息，请使用以下命令。

```
aws transfer describe-server --server-id s-1234567890abcdef0
```

例如，假设前面的命令返回 VPC 端点 ID vpce-1234abcd5678efghi。然后，您可以使用以下命令检索 DNS 名称。

```
aws ec2 describe-vpc-endpoints --vpc-endpoint-ids vpce-1234abcd5678efghi
```

此命令返回运行以下命令所需的 VPC 端点的所有详细信息。

DNS 名称列在 DnsEntries 数组中。您的交易伙伴必须在您的 VPC 内才能访问您的 VPC 端点（例如通过 Amazon PrivateLink 或 VPN）。采用以下格式向您的合作伙伴提供您的 VPC 端点 URL。

```
http://vpce-your-vpce-id.vpce-svc-your-vpce-svc-id.your-region.vpce.amazonaws.com:5080
```

例如，以下 URL 显示了前面命令中占位符的示例值。

```
http://vpce-0123456789abcdefg-fghij123.vpce-svc-11111aaaa2222bbbb.us-
east-1.vpce.amazonaws.com:5080
```

在此示例中，成功的传输存储在您在 第 5 步：创建您与合作伙伴之间的协议 中指定的 base-directory 参数中指定的位置。如果我们成功接收名为 myfile1.txt 和 myfile2.txt 的文件，则这些文件将存储为 */path-defined-in-the-agreement/processed/original_filename.messageId.original_extension*。在这里，文件存储为 /amzn-s3-demo-destination-bucket/AS2-inbox/processed/myfile1.*messageId*.txt 和 /amzn-s3-demo-destination-bucket/AS2-inbox/processed/myfile2.*messageId*.txt。

如果您在创建 Transfer Family 服务器时配置了日志角色，则还可以查看 CloudWatch 日志以了解 AS2 消息的状态。

向您的交易伙伴发送文件

您可以使用 Transfer Family 通过引用连接器 ID 和文件路径来发送 AS2 消息，如以下 start-file-transfer Amazon Command Line Interface (Amazon CLI) 命令所示：

```
aws transfer start-file-transfer --connector-id c-1234567890abcdef0 \
--send-file-paths "/amzn-s3-demo-source-bucket/myfile1.txt" "/amzn-s3-demo-source-
bucket/myfile2.txt"
```

要获取连接器详细信息，请运行以下命令：

```
aws transfer list-connectors
```

该list-connectors命令会返回连接器 IDs URLs、以及连接器的 Amazon 资源名称 (ARNs)。

要返回特定连接器的属性，请使用要使用的 ID 运行以下命令：

```
aws transfer describe-connector --connector-id your-connector-id
```

该describe-connector命令返回连接器的所有属性，包括其 URL、角色、配置文件、邮件处置通知 (MDNs)、标签和监控指标。

您可以通过查看 JSON 和 MDN 文件来确认合作伙伴已成功接收文件。这些文件是根据 文件名和位置 中描述的约定命名的。如果您在创建连接器时配置了日志记录角色，则还可以检查 CloudWatch 日志中的 AS2 消息状态。

教程：设置基本的 Transfer Family 网络应用程序

本教程介绍如何设置 Transfer Family 网络应用程序。Transfer Family 网络应用程序提供了一个简单的界面，用于通过网络浏览器与亚马逊 S3 传输数据和从亚马逊S3传输数据。有关此功能的详细文档，请参阅Transfer Family 网络应用程序。

Web 应用程序教程：先决条件

- 创建的账户实例或组织实例 Amazon IAM Identity Center。有关更多信息，请参阅 为 Transfer Family 网络应用程序配置您的身份提供商。

  如果您不使用 IAM Identity Center 作为身份提供商，请将 Okta 整合为你的 Web 应用程序身份提供商说明如何使用替代身份提供商（在本例中为 Okta）。
- 你需要一个 Amazon S3 存储桶来与你的 Transfer Family 网络应用程序进行交互。有关详细信息，请参阅 配置 Amazon S3 存储桶

> **Note**
>
> 本教程假设您使用的是身份提供商的 IAM Identity Center 目录，如果不是这样，请在继续本教程为 Transfer Family 网络应用程序配置您的身份提供商之前参阅。

完成本教程后，您的用户可以登录并与您创建的 Web 应用程序进行交互。

步骤 1：创建必要的支持资源

您需要将用户添加到 IAM 身份中心目录。您还需要两个角色：一个用作您的 Web 应用程序的身份持有者角色，另一个用于配置 Amazon S3 访问授权。在本教程中，我们允许 Amazon 服务为我们创建这些角色。

如何添加用户

1. 登录 Amazon Web Services 管理控制台 并打开 Amazon IAM Identity Center 控制台，网址为https://console.aws.amazon.com/singlesignon/。
2. 从左侧导航窗格中选择 “用户”。
3. 选择添加用户并指定用户详细信息。

   指定用户名、电子邮件地址和其他必填信息。您可以选择向用户发送一封包含密码设置说明的电子邮件，也可以选择生成一次性密码与他们共享。
4. 选择 “下一步”，然后选择将新用户分配到一个或多个群组。
5. 选择 “下一步” 并查看您的选择。

   如果一切正常，请选择 “添加用户” 以使用您指定的详细信息创建新用户。

   在本教程中，示例用户是 Bob Stiles、用户名 bob stiles 和电子邮件地址 bobstiles@example.com。

第 2 步：创建 Transfer Family 网络应用程序

创建 Transfer Family 网络应用程序

1. 登录 Amazon Web Services 管理控制台 并打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在左侧导航窗格中，选择 Web 应用程序。
3. 选择 “创建 Web 应用程序”。

   对于身份验证访问，请注意，该服务会自动找到您设置为先决条件的 Amazon IAM Identity Center 实例。
4. 在 “权限类型” 窗格中，选择 “创建并使用新的服务角色”。该服务为您创建身份持有者角色。身份持有者角色在其会话中包括经过身份验证的用户的身份。
5. 在 Web 应用程序单位窗格中，接受默认值 1，或者根据需要调整为更高的值。
6. 添加标签以帮助您整理 Web 应用程序。在本教程中，为密钥输入名称，为值输入教程 Web 应用程序。

> **Tip**
>
> 创建 Web 应用程序名称后，您可以直接从 Web 应用程序列表页面对其进行编辑。

7. 选择 “下一步” 打开 “设计 Web 应用程序” 页面。在此屏幕上，提供以下信息。

   您可以选择为 Web 应用程序提供标题。您也可以上传徽标和网站图标的图片文件。

   - 对于页面标题，请自定义用户在连接到 Web 应用程序时看到的浏览器选项卡的标题。如果您没有为页面标题输入任何内容，则默认为 Transfer Web App。
   - 要获取徽标，请上传图片文件。徽标图片的最大文件大小为 50 KB。
   - 对于网站图标，请上传图片文件。您的网站图标的最大文件大小为 20 KB。

8. 选择 “下一步”，然后选择 “创建 Web 应用程序”。

要提供品牌化体验，您可以为用户提供一个自定义网址，让他们访问您的 Transfer Family 网络应用程序。有关更多信息，请参阅 使用自定义 URL 更新您的访问终端节点。

步骤 3：为您的存储桶配置跨源资源共享 (CORS)

您必须为 Web 应用程序使用的所有存储分区设置跨源资源共享 (CORS)。CORS 配置是定义规则的文档，这些规则用于识别您将允许访问存储桶的来源。有关 CORS 的更多信息，请参阅配置跨域资源共享 (CORS)。

为您的 Amazon S3 存储桶设置跨源资源共享 (CORS)

1. 登录 Amazon Web Services 管理控制台 并打开 Amazon S3 控制台，网址为https://console.aws.amazon.com/s3/。
2. 从左侧导航面板中选择 Buckets，在搜索对话框中搜索您的存储桶，然后选择权限选项卡。
3. 在跨源资源共享 (CORS) 中，选择编辑并粘贴以下代码。*AccessEndpoint*替换为您的 Web 应用程序的实际访问端点。确保不要在尾部输入斜杠，因为这样做会导致用户尝试登录您的 Web 应用程序时出错。

   - 不正确的例子：`https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws/`
   - 正确的例子：`https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws`

如果您要将存储桶重复用于多个 Web 应用程序，请将其的 Web 应用程序访问终端节点附加到列表中AllowedOrigins。

```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "GET",
      "PUT",
      "POST",
      "DELETE",
      "HEAD"
    ],
    "AllowedOrigins": [
      "https://AccessEndpoint"
    ],
    "ExposeHeaders": [
      "last-modified",
       "content-length",
      "etag",
      "x-amz-version-id",
      "content-type",
      "x-amz-request-id",
      "x-amz-id-2",
      "date",
      "x-amz-cf-id",
      "x-amz-storage-class",
      "access-control-expose-headers"
     ],
    "MaxAgeSeconds": 3000
  }
]
```

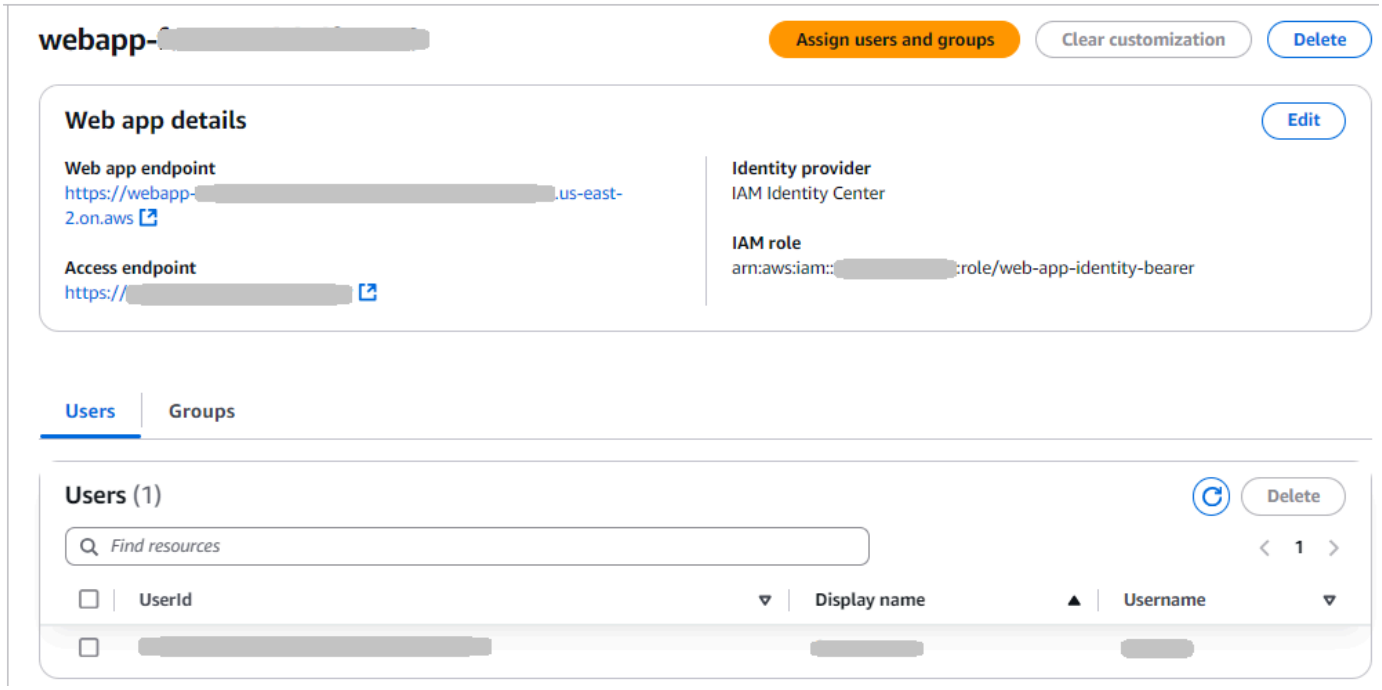
4. 选择 “保存更改” 以更新 CORS。

第 4 步：将用户添加到你的 Transfer Family 网络应用程序

添加您之前在 IAM 身份中心创建的用户。

将用户分配给 Transfer Family 网络应用程序

1. 导航到您之前创建的 Web 应用程序。
2. 选择分配用户和组。



3. 要分配您之前在 IAM Identity Center 中创建的用户，请选择分配现有用户和群组，然后选择下一步。

   a. 按显示名称搜索用户。请注意，在您开始输入搜索条件之前，不会显示任何用户。要添加**Bob Stiles**，请在搜索框中输入 bo b。如果您找不到您的用户，请导航到 IAM Identity Center 管理控制台，找到该用户，然后将其显示名称复制并粘贴到此处。

   b. 选择**Bob Stiles**用户，然后选择 “分配”。

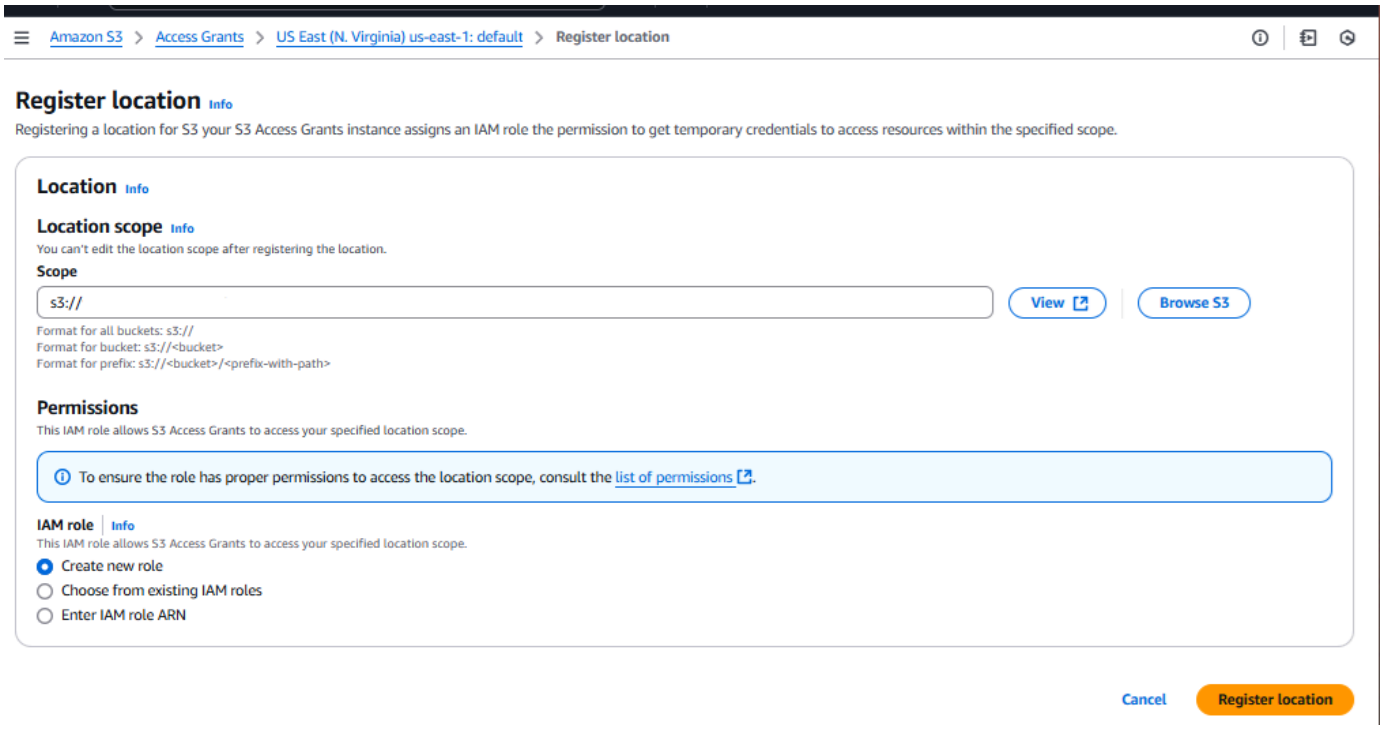
步骤 5：在 Amazon S3 中注册营业地点并创建访问授权

将用户分配给您的 Web 应用程序后，您需要注册存储分区并为该用户创建访问授权。

> **Note**
>
> 您必须拥有 S3 访问权限授予实例，然后才能继续。有关详细信息，请参阅 Amazon 简单存储服务用户指南中的创建 S3 访问授权实例。

注册营业地点并创建访问授权

1. 登录 Amazon Web Services 管理控制台 并打开 Amazon S3 控制台，网址为https://console.aws.amazon.com/s3/。
2. 从左侧导航窗格中选择 “访问授权”。
3. 选择查看详细信息以查看您的 S3 访问权限授予实例的详细信息。
4. 选择 “地点” 选项卡，然后选择 “注册地点”。
5. 提供以下信息：
   - 对于范围，请浏览存储桶或输入存储桶的名称以及可选的前缀。请注意，作用域以字符串开头**s3://**。
   - 对于 IAM 角色，选择创建新角色让 Amazon S3 创建一个角色。此角色允许 S3 访问权限授予访问您指定的位置范围。



选择注册地点以继续。

6. 选择 “授权” 选项卡，然后选择 “创建授权”，并提供以下详细信息。
   - 在 “位置” 中，选择 “浏览地点”，然后选择您在上一步中注册的位置。
   - 在 S ubprefix 中，输入*表示访问权限授予适用于整个存储桶。

- 在 “权限” 中，选择 “读取” 和 “写入”。
- 对于被授权者类型，请从 IAM 身份中心选择目录身份。
- 对于 “目录” 身份类型，选择 “用户”。
- 在 IAM Identity Center 用户/ ID 中，复制并粘贴的用户 ID。**`Bob Stiles`**此 ID 可在您的 Transfer Family 网络应用程序的 “用户” 面板中找到。

7. 选择 “创建授权”。

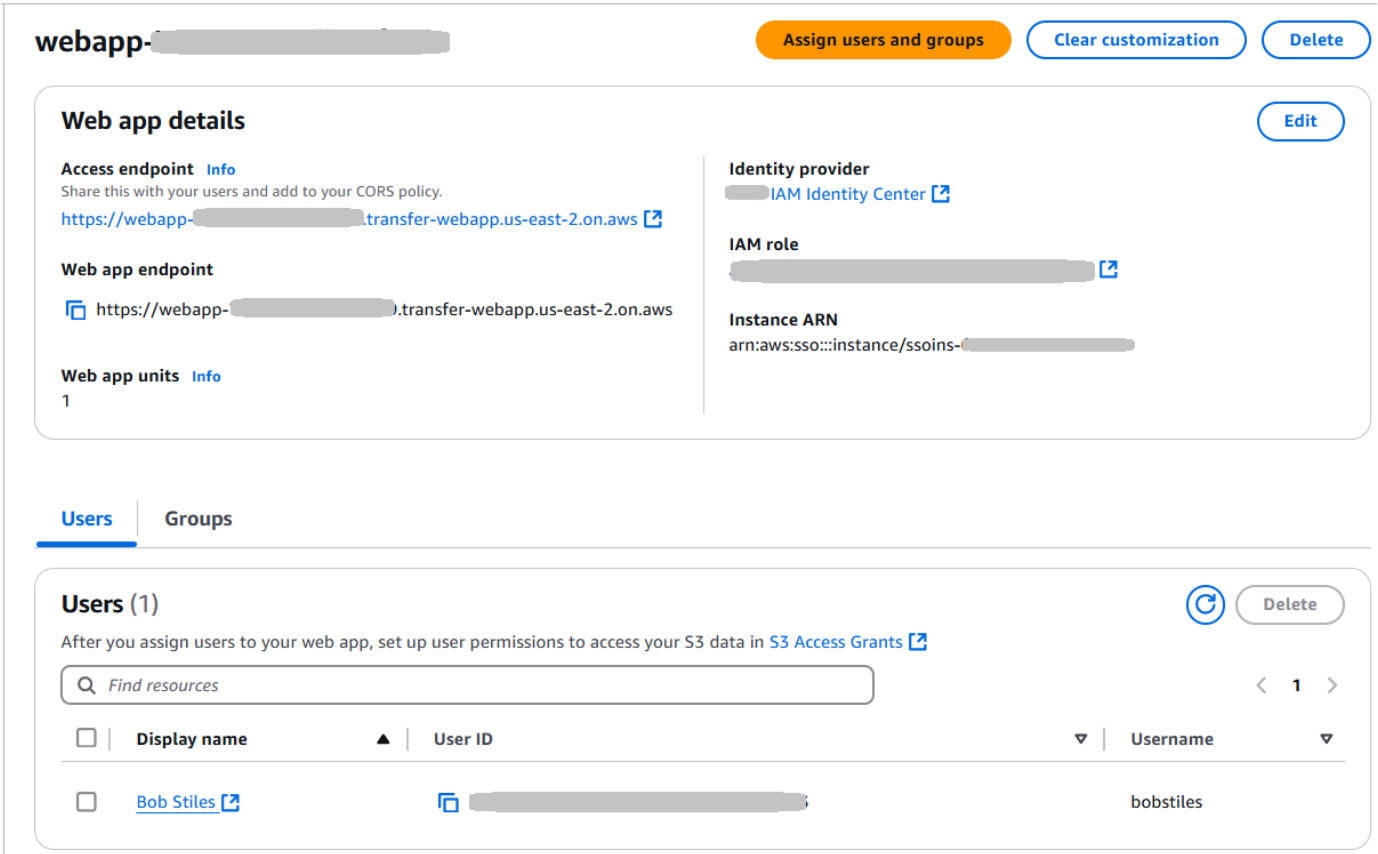
访问权限已创建。

第 6 步：以用户身份访问你的 Transfer Family 网络应用程序

现在，我们导航到 Web 应用程序的 URL，并以之前分配的用户身份登录。

登录 Transfer Family 网络应用程序

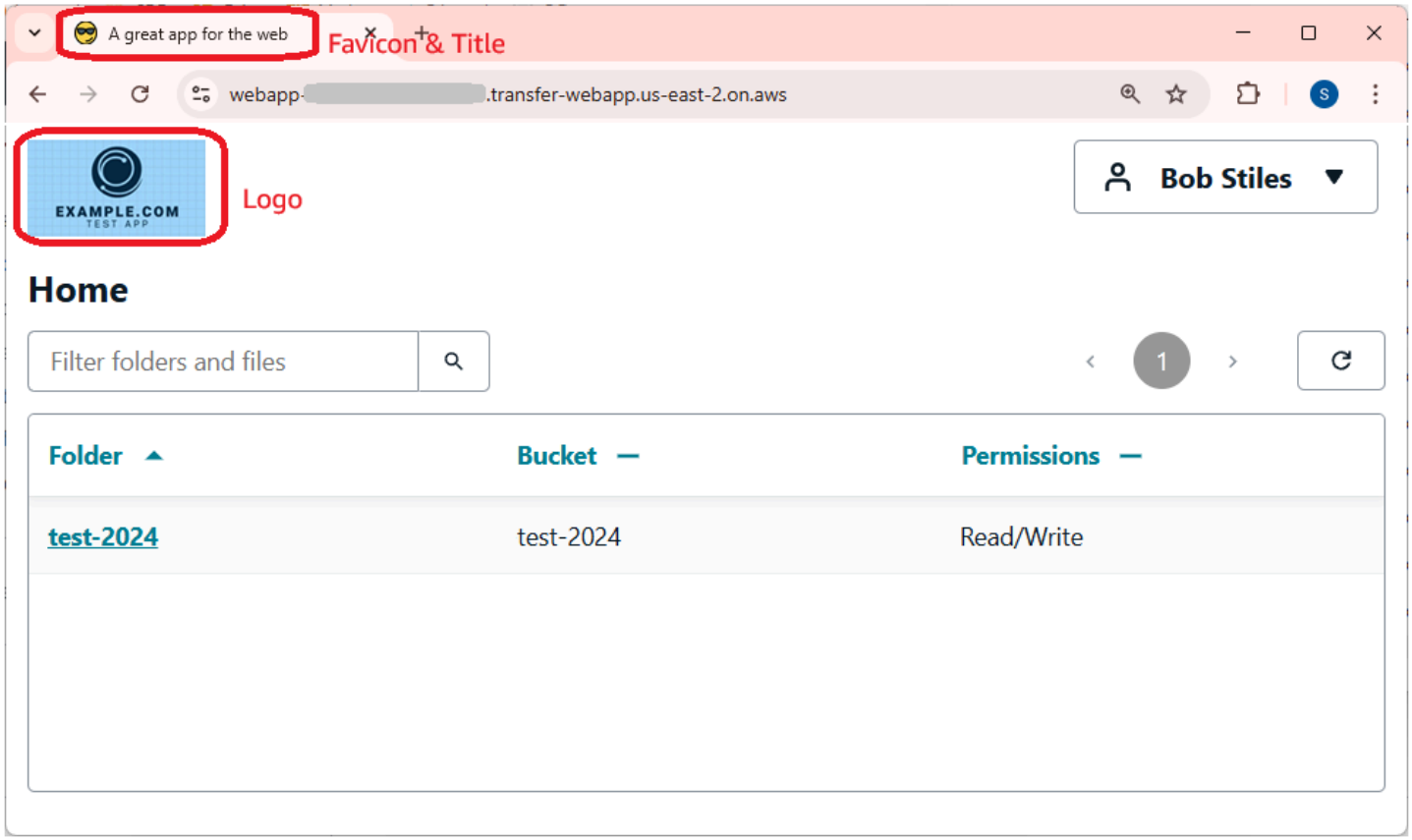
1. 导航到您的 Web 应用程序
2. 从 Web 应用程序详细信息窗格中选择访问端点。



3. 在登录屏幕上，输入您创建的用户**`bobstiles`**，然后选择下一步。

4. 输入系统在创建时分配给该用户的密码，然后选择下一步。
5. 如果您的组织需要多因素身份验证 (MFA)，则需要立即进行设置。如果没有，请直接跳到步骤 6。
   a. 您将看到一个用于注册 MFA 设备的屏幕。选择一个可用选项，然后选择 “下一步”。
   b. 执行必要步骤为该用户配置 MFA：这些步骤取决于您选择的 MFA 选项。
   c. 您可能需要为用户设置新密码：如果需要，请立即设置。系统可能还会要求您使用您配置的新 MFA 凭证重新登录。

您的用户应该会看到类似于以下内容的屏幕。请注意，此屏幕截图包括网站图标和徽标的自定义。



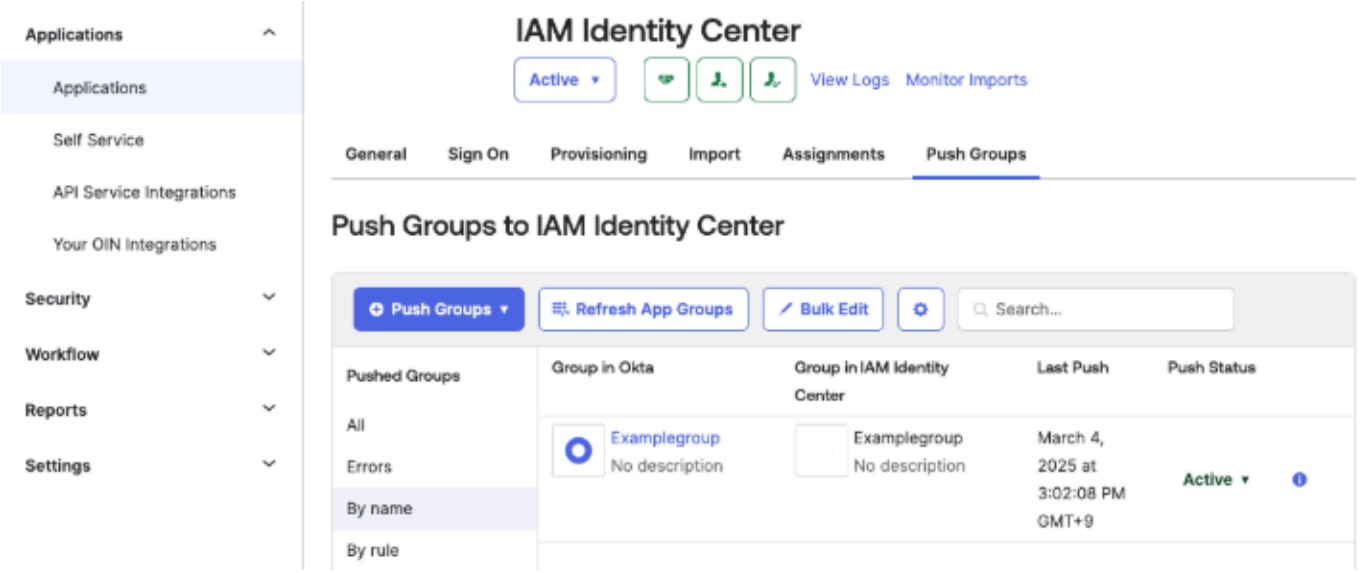
后续步骤

您已成功设置具有标准 S3 存储桶访问权限的基本 Transfer Family 网络应用程序。如果您需要对存储桶权限进行更精细的控制，例如允许用户从一个存储桶下载并上传到另一个存储桶，请参阅教程：设置具有选择性多存储桶访问权限的 Amazon Transfer Family Web 应用程序。

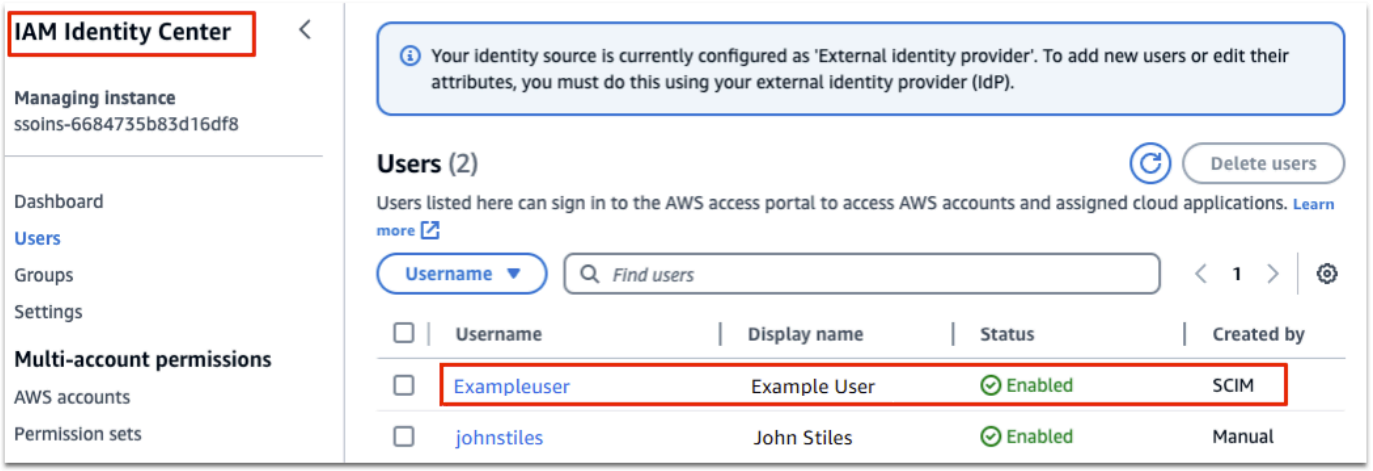
将 Okta 整合为你的 Web 应用程序身份提供商

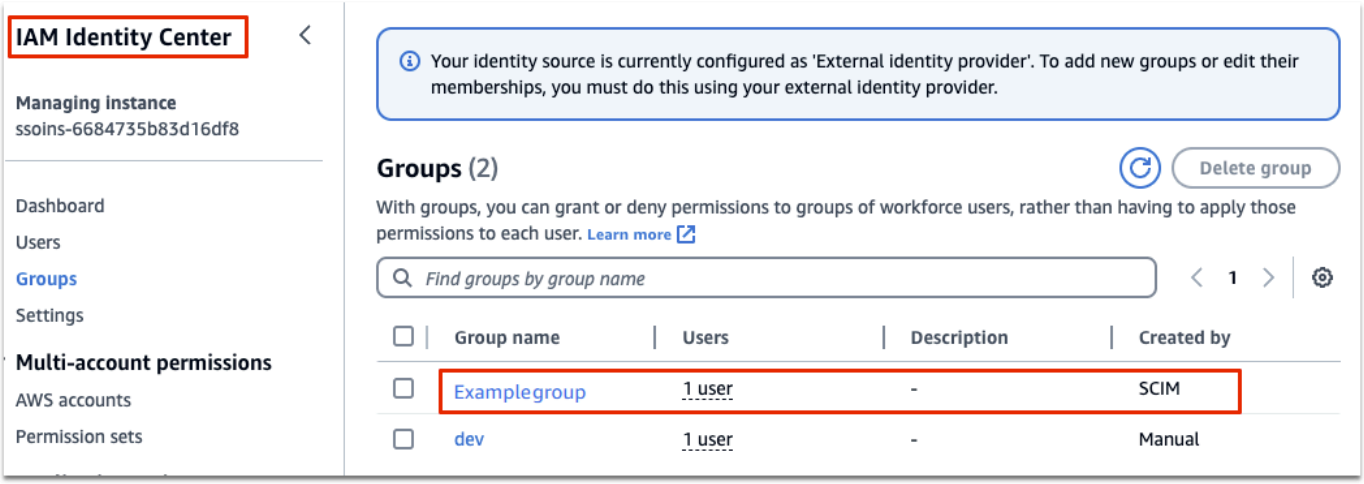
您可以将外部身份提供商与 Transfer Family 网络应用程序集成。本节介绍如何将 Okta 设置为身份提供商。

1. 在 Okta 中，创建用户、组和应用程序。有关如何执行此操作的详细信息，请参阅使用 Okta 和 IAM 身份中心配置 SAML 和 SCIM。

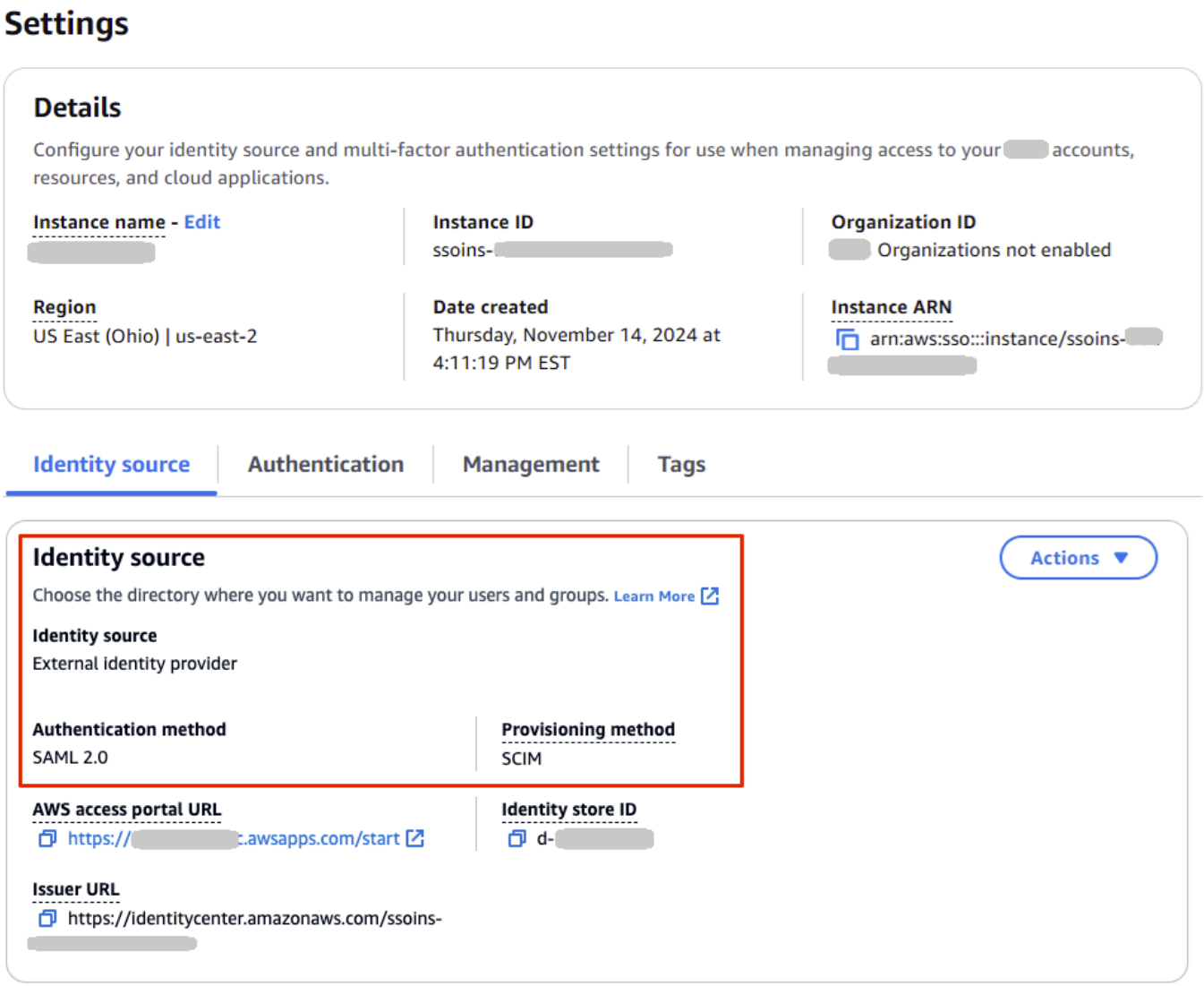


2. 连接 Okta 并将用户和群组从 Okta 导入到。 Amazon IAM Identity Center按照使用 Okta 和 IAM 身份中心配置 SAML 和 SCIM 中的步骤 1—4 进行操作。





3. 确认 IAM 身份中心中的身份源是 SAML 2.0。



4. 分配您的用户和群组，如中所述[第 4 步：将用户添加到你的 Transfer Family 网络应用程序](#)。

5. 为避免让您的用户在登录您的网络应用程序时需要使用 MFA，请在 Okta 中执行以下步骤。

   a. 从 Okta 管理员控制台访问 [应用程序]-[应用程序]，然后选择 Amazon IAM Identity Center 应用程序。

   b. 在 “登录” 选项卡上，选择 [用户身份验证]-编辑。

   c. 选择 “仅限密码”。

完成本教程的所有其他步骤后，您的用户应该能够通过在网络浏览器中导航到该网络应用程序的访问端点来访问您的 Transfer Family 网络应用程序。

教程：设置具有选择性多存储桶访问权限的 Amazon Transfer Family Web 应用程序

本教程将指导您为单个用户配置具有特定的 Amazon S3 存储桶权限的 Transfer Family 网络应用程序。您将学习如何设置一个解决方案，允许用户从一个存储桶下载并上传到另一个存储桶，同时保持安全性。这是一个基于基础教程中介绍的概念的高级教程。如果你不熟悉 Amazon Transfer Family Web 应用程序，可以考虑从开始教程：设置基本的 Transfer Family 网络应用程序。

先决条件

开始本教程之前，您需要：

- IAM 身份中心配置在与您的 Amazon Transfer Family Web 应用程序相同的区域。请注意，所有区域的每个 Amazon 账户只 Amazon 允许一个 IAM 身份中心实例。
- 在 IAM 身份中心中配置了至少一个用户。
- 两个 S3 存储桶：一个用于下载，一个用于上传。

> **Note**
>
> 本教程与基本 Web 应用程序教程有许多共同的前提条件。有关设置 IAM 身份中心和创建用户的更多信息，请参阅教程：设置基本的 Transfer Family 网络应用程序。

第 1 步：创建 Transfer Family 网络应用程序

创建 Transfer Family 网络应用程序

1. 登录 Amazon Web Services 管理控制台 并打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在左侧导航窗格中，选择 Web 应用程序。
3. 选择创建 Web 应用程序。

   对于身份验证访问，请注意，该服务会自动找到您设置为先决条件的 Amazon IAM Identity Center 实例。
4. 在 “权限类型” 窗格中，选择 “创建并使用新的服务角色”。该服务为您创建身份持有者角色。身份持有者角色在其会话中包括经过身份验证的用户的身份。
5. 在 Web 应用程序单位窗格中，接受默认值 1，或者根据需要调整为更高的值。
6. 添加标签以帮助您整理 Web 应用程序。在本教程中，为密钥输入名称，为值输入教程 Web 应用程序。

   > **Tip**
   >
   > 创建 Web 应用程序名称后，您可以直接从 Web 应用程序列表页面对其进行编辑。
7. 选择 “下一步” 打开 “设计 Web 应用程序” 页面。在此屏幕上，提供以下信息。

   您可以选择为 Web 应用程序提供标题。您也可以上传徽标和网站图标的图片文件。

   - 对于页面标题，请自定义用户在连接到 Web 应用程序时看到的浏览器选项卡的标题。如果您没有为页面标题输入任何内容，则默认为 Transfer Web App。
   - 要获取徽标，请上传图片文件。徽标图片的最大文件大小为 50 KB。
   - 对于网站图标，请上传图片文件。您的网站图标的最大文件大小为 20 KB。
8. 选择 “下一步”，然后选择 “创建 Web 应用程序”。

步骤 2：为 S3 访问权限配置 IAM 角色

您需要创建两个 IAM 角色：一个对第一个存储桶具有仅下载访问权限，另一个对第二个存储桶具有仅限上传访问权限。

两个角色的信任政策

对两个 IAM 角色使用以下信任策略：

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AccessGrantsTrustPolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "access-grants.s3.amazonaws.com"
            },
            "Action": [
                "sts:AssumeRole",
                "sts:SetSourceIdentity",
                "sts:SetContext"
            ]
        }
    ]
}
```

下载存储桶的 IAM 政策

使用以下策略创建 IAM 角色，以获取对您的下载存储桶的只读访问权限：

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ObjectLevelReadPermissions",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion",
                "s3:GetObjectAcl",
                "s3:GetObjectVersionAcl",
                "s3:ListMultipartUploadParts",
                "s3:ListBucket"
            ],
```

```
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket1/*",
                "arn:aws:s3:::amzn-s3-demo-bucket1"
            ]
        }
    ]
}
```

> **Important**
>
> 将 amzn-s3-demo-bucket1 替换为下载存储桶的实际名称。

上传存储桶的 IAM 政策

使用以下策略创建另一个 IAM 角色以获取对上传存储桶的写入权限：

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ObjectLevelWritePermissions",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectVersionAcl",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:AbortMultipartUpload",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket2/*",
                "arn:aws:s3:::amzn-s3-demo-bucket2"
            ]
        }
    ]
}
```

> **Important**
>
> 将 amzn-s3-demo-bucket2 替换为上传存储桶的实际名称。

步骤 3：设置 S3 访问授权

1. 打开 S3 控制台，网址为https://console.amazonaws.cn/s3/。
2. 在导航窗格中，选择访问授权。
3. 单击 “创建 S3 访问权限授予实例”。
4. 选择添加 IAM 身份中心实例选项并输入身份中心实例 ARN。
5. 单击 “下一步”，然后单击 “取消” 以完成 S3 访问权限授予实例的创建，无需继续执行其他步骤。

此步骤创建 S3 访问权限授予实例。现在，您将注册营业地点并创建访问授权。

步骤 4：注册 S3 存储桶位置

使用 S3 访问权限将两个 S3 存储桶注册为位置：

1. 在 S3 访问权限授予控制台中，导航到 “位置”，然后单击 “注册位置”。
2. 在 “位置范围” 下，选择用于下载的特定的 S3 存储桶（amzn-s3-demo-bucket1）。
3. 当系统提示您选择 IAM 角色时，请选择您之前创建的下载 IAM 角色。
4. 完成注册流程。
5. 重复该过程注册上传存储桶 (amzn-s3-demo-bucket2)，并在出现提示时选择上传 IAM 角色。

步骤 5：创建访问授权

创建两个赠款，每个注册地点一个：

1. 在 S3 访问权限授权控制台中，导航到 “授权”，然后单击 “创建授权”。
2. 在 “位置” 中，单击 “浏览位置”，然后选择下载存储桶位置 (amzn-s3-demo-bucket1)。
3. 在 Subprefix（可选）中，输入*以允许访问整个存储桶，或者指定路径，例如限制`folder1/folder2/*`对特定前缀的访问。

使用*会将授权范围设置为s3://bucket-name/*，允许访问整个存储桶。要仅允许访问特定的前缀，请输入类似的路径folder1/folder2/*，该路径会将授权范围设置为s3://bucket-name/folder1/folder2/*。

4. 在 “权限和访问权限” 下，为下载存储桶选择读取。
5. 在被授权者类型中，从 IAM 身份中心选择目录身份。
6. 对于 IAM 委托人类型，选择用户并输入您的 IAM 身份中心用户的用户 ID。
7. 完成赠款创建流程。
8. 重复该过程为上传存储桶 (amzn-s3-demo-bucket2) 创建授权，但为权限选择读写。

步骤 6：为 S3 存储桶配置 CORS 策略

为两个 S3 存储桶配置 CORS 策略，以允许通过以下方式进行访问： Amazon Transfer Family WebApp

1. 打开 S3 控制台并导航到您的下载存储桶 (amzn-s3-demo-bucket1)。
2. 选择权限选项卡。
3. 向下滚动到跨源资源共享 (CORS) 部分，然后点击编辑。
4. 添加以下 CORS 配置，替换为实际*WebAppEndpoint*的 WebApp 终端节点 URL：

   你可以在 Amazon Transfer Family 控制台的下方找到你的 Web 应用程序终端节点 URL WebApps。它看起来会像 https://webapp-**********.transfer-webapp.us-west-2.on.aws。

```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "GET",
      "PUT",
      "POST",
      "DELETE",
      "HEAD"
    ],
    "AllowedOrigins": [
      "https://WebAppEndpoint"
    ],
```

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

5. 单击保存更改。
6. 对您的上传存储桶 (amzn-s3-demo-bucket2) 重复该过程。

步骤 7：测试配置

1. 打开您的 Amazon Transfer Family 网络应用程序网址。您可以在 Amazon Transfer Family 控制台的 “访问端点” 字段 WebApps 下找到此 URL。
2. 使用您配置了访问权限的 IAM Identity Center 用户证书登录。
3. 登录后，您应该会在主页上看到两个 S3 位置。
4. 导航到下载存储桶 (amzn-s3-demo-bucket1)，确认您可以下载文件但不能上传。
5. 导航到上传存储桶 (amzn-s3-demo-bucket2)，然后验证您是否可以上传文件。

结论

您已成功为单个用户配置 Amazon Transfer Family WebApp 了选择性 S3 存储桶访问权限。此设置允许用户从一个存储桶下载并上传到另一个存储桶，同时通过 IAM 角色和 S3 访问权限授权维护安全。

通过在 S3 访问权限中为每个用户创建额外的授权，可以将此方法扩展到多个用户，从而对存储桶访问权限进行精细控制。有关基本 Web 应用程序设置的信息，请参阅教程：设置基本的 Transfer Family 网络应用程序。

配置 SFTP、FTPS 或 FTP 服务器端点

本主题提供有关创建和使用一个或多个 SFTP、FTPS 和 FTP 协议的 Amazon Transfer Family 服务器端点的详细信息。

主题

- 身份提供商选项
- Amazon Transfer Family 端点类型矩阵
- 配置 SFTP、FTPS 或 FTP 服务器端点
- FTP 和 FTPS 网络负载均衡器注意事项
- 使用客户端通过服务器端点传输文件
- 管理服务器端点的用户
- 使用逻辑目录简化您的 Transfer Family 目录结构

身份提供商选项

Amazon Transfer Family 提供了几种对用户进行身份验证和管理的方法。下表比较了您可以与 Transfer Family 一起使用的可用身份提供商。

Action	Amazon Transfer Family 服务托管	Amazon Managed Microsoft AD	Amazon API Gateway	Amazon Lambda
受支持的协议	SFTP	SFTP、FTPS、FTP	SFTP、FTPS、FTP	SFTP、FTPS、FTP
基于密钥的身份验证	是	否	是	是
密码验证	否	是	是	是
Amazon Identity and Access Management (IAM) 和 POSIX	支持	是	是	是

Action	Amazon Transfer Family 服务托管	Amazon Managed Microsoft AD	Amazon API Gateway	Amazon Lambda
逻辑主目录	支持	是	是	是
参数化访问权限（基于用户名）	支持	是	是	是
临时访问结构	是	否	是	是
Amazon WAF	否	否	是	否

备注：

- IAM 用于控制 Amazon S3 后备存储的访问权限，Amazon EFS 使用 POSIX。
- Ad hoc 是指在运行时发送用户配置文件的能力。例如，您可以通过将用户名作为变量传递来将用户置于他们的主目录中。
- 有关的详细信息 Amazon WAF，请参阅添加 Web 应用程序防火墙。
- 有一篇博客文章描述了使用与微软 Entra ID（前身为 Azure AD）集成的 Lambda 函数作为 Transfer Family 身份提供商。有关详细信息，请参阅使用 Azure 活动目录 Amazon Transfer Family 进行身份验证和。 Amazon Lambda
- 我们提供了多个 Amazon CloudFormation 模板来帮助您快速部署使用自定义身份提供程序的 Transfer Family 服务器。有关更多信息，请参阅 Lambda 函数模板。

在以下步骤中，您可以创建启用 SFTP 的服务器、启用 FTPS 的服务器、启用 FTP 的服务器或启用 FTP 的服务器。 AS2

下一步

- 创建启用 SFTP 的服务器
- 创建启用 FTPS 的服务器
- 创建启用 FTP 的服务器
- 正在配置 AS2

Amazon Transfer Family 端点类型矩阵

创建 Transfer Family 服务器时，您需要选择要使用的端点类型。下表介绍了每种端点类型的特性。

端点类型矩阵

特征	Public	VPC - 互联网	VPC - 内部	VPC_Endpoint（已弃用）
受支持的协议	SFTP	SFTP、FTPS、AS2	SFTP、FTP、FTPS、 AS2	SFTP
访问	来自互联网。此端点类型不需要在您的 VPC 中进行任何特殊配置。	通过互联网以及在 VPC 和 VPC 连接的环境中，例如本地数据中心或 VPN。Amazon Direct Connect	在 VPC 和与 VPC 连接的环境中，例如本地数据中心或 VPN。Amazon Direct Connect	在 VPC 和与 VPC 连接的环境中，例如本地数据中心或 VPN。Amazon Direct Connect
静态 IP 地址	您无法附加静态 IP 地址。Amazon 提供随时可能更改的 IP 地址。	您可以将弹性 IP 地址附加到端点。这些地址可以是 Amazon自有的 IP 地址或您自己的 IP 地址（自带 IP 地址）。附加到端点的弹性 IP 地址不会更改。 附加到服务器的私有 IP 地址也不会更改。	附加到端点的私有 IP 地址不会更改。	附加到端点的私有 IP 地址不会更改。
源 IP 允许列表	此端点类型不支持按源 IP 地址列出的允许列表。	要允许通过源 IP 地址进行访问，您可以使用连接到服务器端	要允许通过源 IP 地址进行访问，您可以使用连接到服务器端	要允许通过源 IP 地址进行访问，您可以使用连接到服务器端

特征	Public	VPC - 互联网	VPC - 内部	VPC_Endpoint（已弃用）
	端点可公开访问并侦听端口 22 上的流量。 **Note** 对于 VPC 托管的端点，SFTP Transfer Family 服务器可以通过端口 22（默认）、2222、2223 或 22000 运行。	点的安全组以及 ACLs 连接到终端节点所在子网的网络。	点的安全组以及连接到端点所在子网的网络访问控制列表（网络 ACLs）。	点的安全组以及 ACLs 连接到终端节点所在子网的网络。
客户端防火墙允许列表	您必须允许服务器的 DNS 名称。 由于 IP 地址可能会发生更改，因此请避免将 IP 地址用于您的客户端防火墙允许列表。	您可以允许服务器的 DNS 名称或附加到服务器的弹性 IP 地址。	您可以允许端点的私有 IP 地址或 DNS 名称。	您可以允许端点的私有 IP 地址或 DNS 名称。

特征	Public	VPC - 互联网	VPC - 内部	VPC_Endpoint（已弃用）
IP 地址类型	IPv4 （默认）或双堆栈（IPv4 和 IPv6）	IPv4 仅限（不支持双堆栈）	IPv4 （默认）或双堆栈（IPv4 和 IPv6）	IPv4 仅限（不支持双堆栈）

> **Note**
>
> VPC_ENDPOINT 端点类型现已弃用，无法用于创建新的服务器。不使用EndpointType=VPC_ENDPOINT，而是使用 VPC 终端节点类型 (EndpointType=VPC)，您可以将其用作内部终端节点或面向 Internet，如上表所述。
>
> - 有关弃用的详细信息，请参阅停止使用 VPC_ENDPOINT。
> - 有关管理 VPC 终端节点权限的信息，请参阅限制 Transfer Family 服务器的 VPC 终端节点访问权限。

考虑以下选项来提高 Amazon Transfer Family 服务器的安全状况：

- 使用具有内部访问权限的 VPC 终端节点，这样只有您的 VPC 或 VPC 连接的环境（例如本地数据中心或 VPN）中的客户端才能访问服务器。 Amazon Direct Connect
- 要允许客户端通过互联网访问端点并保护您的服务器，请使用具有面向互联网访问权限的 VPC 端点。然后，修改 VPC 的安全组，使其仅允许来自托管用户客户端的某些 IP 地址的流量。
- 如果您需要基于密码的身份验证，并且在服务器上使用自定义身份提供商，则最佳做法是，您的密码策略可以防止用户创建弱密码并限制失败的登录尝试次数。
- Amazon Transfer Family 是一项托管服务，因此它不提供 shell 访问权限。您无法直接访问底层 SFTP 服务器以在 Transfer Family 服务器上运行 OS 本机命令。
- 在具有内部访问权限的 VPC 端点前使用网络负载均衡器。将负载均衡器上的侦听器端口从端口 22 更改为其他端口。这可以降低但不能消除端口扫描器和机器人探测服务器的风险，因为端口 22 最常用于扫描。有关详细信息，请参阅博客文章网络负载均衡器现在支持安全组。

> **Note**
>
> 如果您使用 Network Load Balancer，则 Amazon Transfer Family CloudWatch 日志会显示 NLB 的 IP 地址，而不是实际的客户端 IP 地址。

配置 SFTP、FTPS 或 FTP 服务器端点

您可以使用该 Amazon Transfer Family 服务创建文件传输服务器。以下文件传输协议可用：

- Secure Shell (SSH) 文件传输协议 (SFTP) — 通过 SSH 的文件传输 有关更多信息，请参阅 the section called “创建启用 SFTP 的服务器”。

> **Note**
>
> 我们提供了创建 SFTP Transfer Family 服务器的 Amazon CDK 示例。该示例使用 TypeScript，可 GitHub 在此处找到。

- 文件传输协议安全 (FTPS) _— 使用 TLS 加密的文件传输功能 有关更多信息，请参阅 the section called “创建启用 FTPS 的服务器”。
- 文件传输协议 (FTP) — 未加密的文件传输功能 有关更多信息，请参阅 the section called “创建启用 FTP 的服务器”。
- 适用性声明 2 (AS2) — 用于传输结构化 business-to-business数据的文件传输。有关更多信息，请参阅 the section called “配置 AS2”。对于 AS2，您可以快速创建 Amazon CloudFormation 堆栈以进行演示。有关此过程的说明，请参阅 使用模板创建演示 Transfer Family AS2 堆栈。

您可以创建具有多个协议的服务器。

> **Note**
>
> 如果您为同一个服务器端点启用了多个协议，并且想要通过多个协议使用相同的用户名提供访问权限，则只要在身份提供商中设置了该协议的特定凭据，就可以这样做。对于 FTP，建议保留与 SFTP 和 FTPS 不同的凭证。这是因为，与 SFTP 和 FTPS 不同，FTP 以明文形式传输凭证。通过将 FTP 凭证与 SFTP 或 FTPS 隔离开来，如果共享或公开 FTP 凭证，则使用 SFTP 或 FTPS 的工作负载会保持安全。

创建服务器时，您可以选择特定的服务器 Amazon Web Services 区域 来执行分配给该服务器的用户的文件操作请求。除了为服务器分配一个或多个协议外，您还可以分配以下身份提供商类型之一：

- 使用 SSH 密钥托管的服务。有关更多信息，请参阅 与服务托管用户合作。
- Amazon Directory Service for Microsoft Active Directory (Amazon Managed Microsoft AD)。 此方法允许你整合 Microsoft Active Directory 群组以提供对 Transfer Family 服务器的访问权限。有关更多信息，请参阅 使用微软 Active Directory 的 Amazon 目录服务。
- 自定义身份提供商。Transfer Family 提供了多种使用自定义身份提供者的选项，如使用自定义身份提供程序主题中所述。

您还可以使用默认服务器端点为服务器分配端点类型（可公开访问或 VPC 托管）和主机名，或者使用 Amazon Route 53 服务或使用您选择的域名系统 (DNS) 服务为服务器分配自定义主机名。服务器主机名在创建时 Amazon Web Services 区域 必须是唯一的。

此外，您可以分配 Amazon CloudWatch CloudWatch 日志角色将事件推送到您的日志，选择包含可供服务器使用的加密算法的安全策略，并以键值对的标签形式向服务器添加元数据。

> **Important**
>
> 实例化的服务器和数据传输会产生费用。有关定价以及用于估算使用 Amazon 定价计算器 Transfer Family 的成本的信息，请参阅Amazon Transfer Family 定价。

创建启用 SFTP 的服务器

Secure Shell (SSH) 文件传输协议 (SFTP) 是一种用于通过互联网安全传输数据的网络协议。该协议支持 SSH 的完整安全和身份验证功能。它被广泛应用于金融服务、医疗保健、零售和广告等各行各业的业务合作伙伴之间交换数据，包括敏感信息。

请注意以下几点

- Transfer Family 的 SFTP 服务器通过端口 22 运行。对于 VPC 托管的端点，SFTP Transfer Family 服务器也可以通过端口 2222、2223 或 22000 运行。有关更多信息，请参阅 在虚拟私有云中创建服务器。
- 公共端点无法通过安全组限制流量。要将安全组与 Transfer Family 服务器配合使用，您必须将服务器的终端节点托管在虚拟私有云 (VPC) 内，如中所述在虚拟私有云中创建服务器。

另请参阅

- 我们提供了创建 SFTP Transfer Family 服务器的 Amazon CDK 示例。该示例使用 TypeScript，可 GitHub 在此处找到。
- 有关如何在 VPC 内部署 Transfer Family 服务器的演练，请参阅使用 IP 允许列表保护您的 Amazon Transfer Family 服务器。

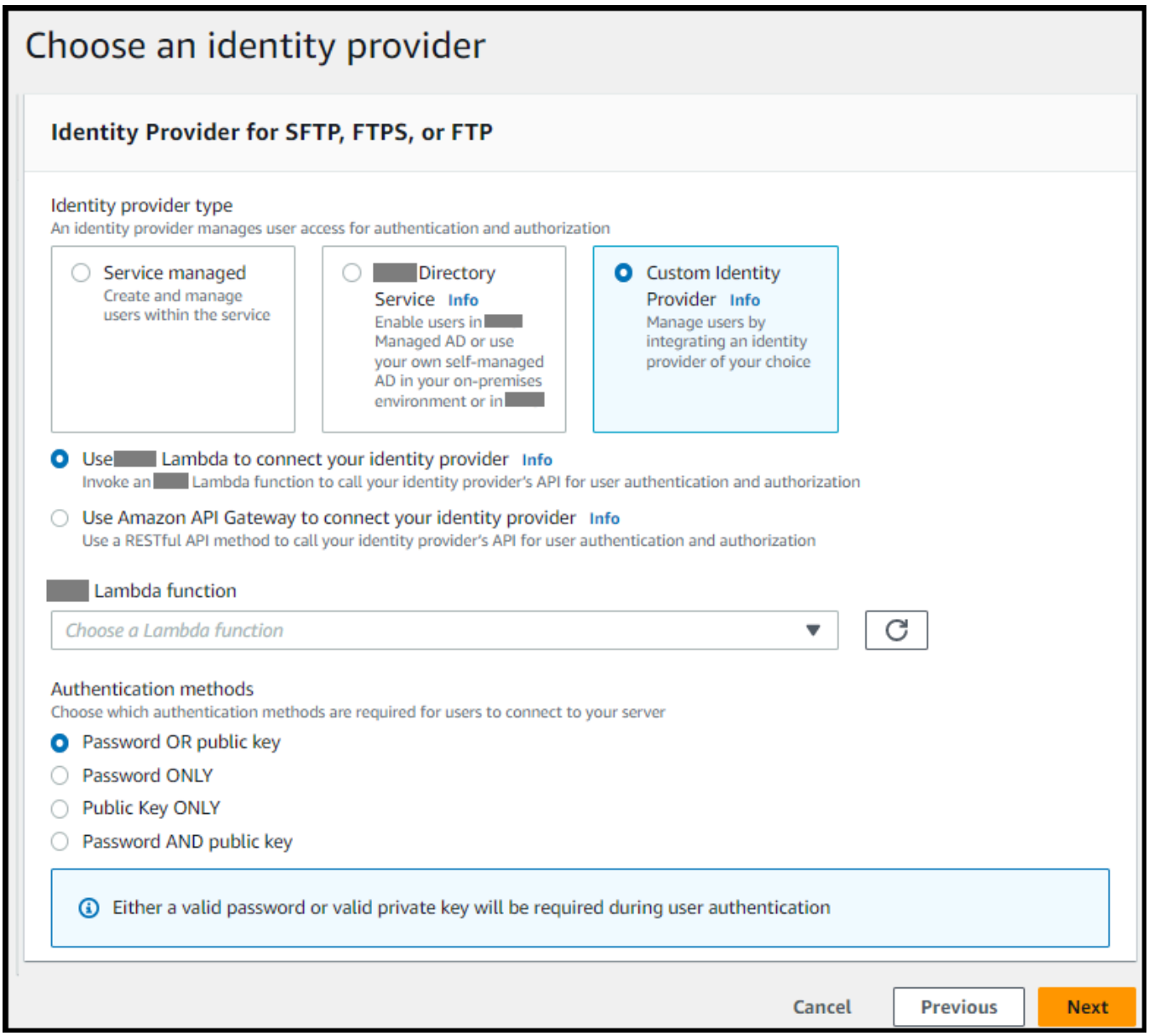
创建启用 SFTP 的服务器

1. 打开 Amazon Transfer Family 控制台，从导航窗格中选择 “服务器”，然后选择 “创建服务器”。https://console.aws.amazon.com/transfer/
2. 在选择协议中，选择 SFTP，然后选择下一步。
3. 在选择身份提供商中，选择要用于管理用户访问权限的身份提供商。您有以下选项：

   - 服务托管-您将用户身份和密钥存储在中 Amazon Transfer Family。
   - Amazon Directory Service for Microsoft Active Directory— 您提供用于访问端点的 Amazon Directory Service 目录。这样，您就可以使用存储在 Activity Directory 中的凭证对用户进行身份验证。要了解有关与 Amazon Managed Microsoft AD 身份提供商合作的更多信息，请参阅使用微软 Active Directory 的 Amazon 目录服务。

     > **Note**
     > - 不支持跨账户目录和共享目录。 Amazon Managed Microsoft AD
     > - 要设置以 Directory Service 作为身份提供者的服务器，您需要添加一些 Amazon Directory Service 权限。有关更多信息，请参阅 在你开始使用之前 Amazon Directory Service for Microsoft Active Directory。

   - 自定义身份提供商 — 请选择以下任一选项：
     - Amazon Lambda 用于连接您的身份提供商-您可以使用由 Lambda 函数支持的现有身份提供商。您提供 Lambda 函数名称。有关更多信息，请参阅 Amazon Lambda 用于整合您的身份提供商。
     - 使用 Amazon API Gateway 连接您的身份提供商 — 您可以创建由 Lambda 函数支持的 API 网关方法以用作身份提供商。您提供一个 Amazon API Gateway URL 和一个调用角色。有关更多信息，请参阅 使用 Amazon API Gateway 整合您的身份提供程序。



4. 选择下一步。
5. 在选择端点中，执行以下操作：
   a. 对于端点类型，选择可公开访问的端点类型。有关 VPC 托管的端点，请参阅 在虚拟私有云中创建服务器。
   b. 对于 IP 地址类型，选择 IPv4（默认）以实现向后兼容，或者选择 Dual-Stack 以同时启用两者 IPv4 以及与终 IPv6端节点的连接。

> **Note**
>
> 双栈模式允许你的 Transfer Family 端点 IPv4 与两个 IPv6 已启用的客户端通信。这使您无需同时切换所有系统即可逐步从 IPv4 IPv6 基于系统的过渡。

c. （可选）对于自定义主机名，选择无。

您将获得由提供的服务器主机名 Amazon Transfer Family。服务器主机名使用格式 *serverId*.server.transfer.*regionId*.amazonaws.com。

对于自定义主机名，您可以为服务器端点指定自定义别名。要了解有关使用自定义主机名的更多信息，请参阅使用自定义主机名。

d. （可选）对于启用 FIPS，请选中启用 FIPS 端点复选框以确保端点符合联邦信息处理标准 (FIPS)。

> **Note**
>
> 启用 FIPS 的端点仅在北美 Amazon 地区可用。有关可用区域，请参阅 Amazon Web Services 一般参考 中的 Amazon Transfer Family 端点和限额。有关 FIPS 的更多信息，请参阅联邦信息处理标准 (FIPS) 140-2。

e. 选择下一步。

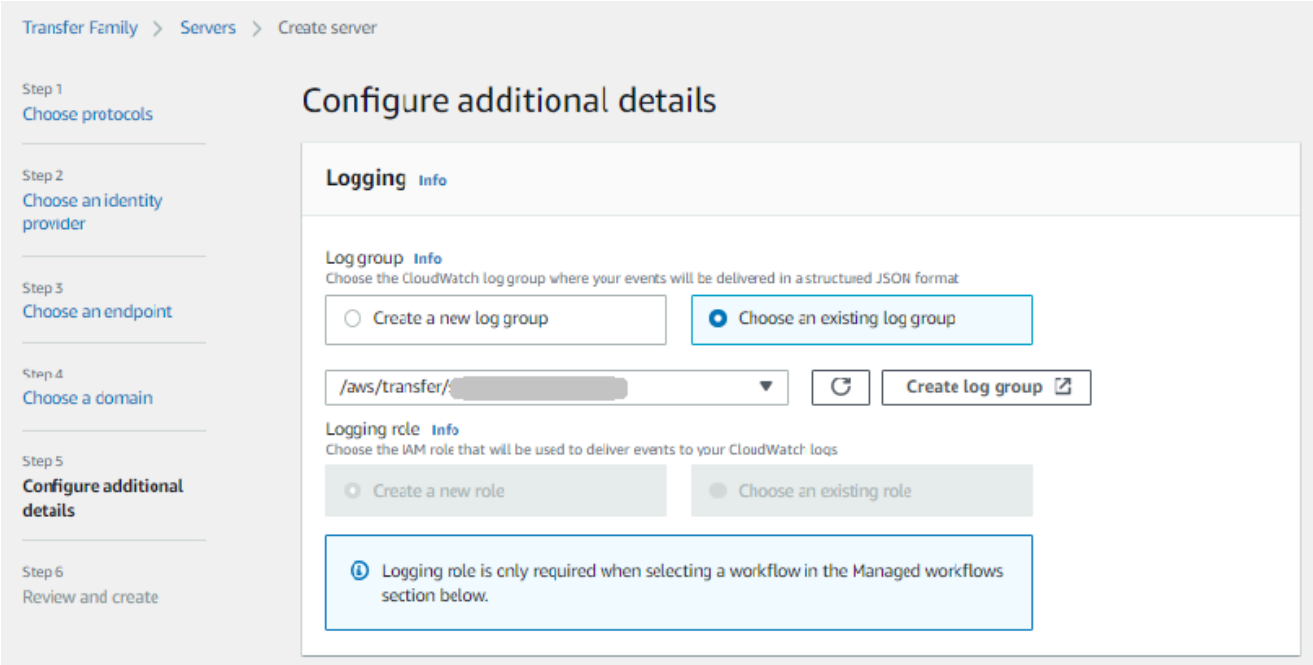
6. 在“选择域”页面上，选择要用于通过所选协议 Amazon 存储和访问数据的存储服务：

- 选择 Amazon S3，通过所选协议将您的文件作为对象存储和访问。
- 选择 Amazon EFS，通过所选协议在 Amazon EFS 文件系统中存储和访问您的文件。

选择下一步。

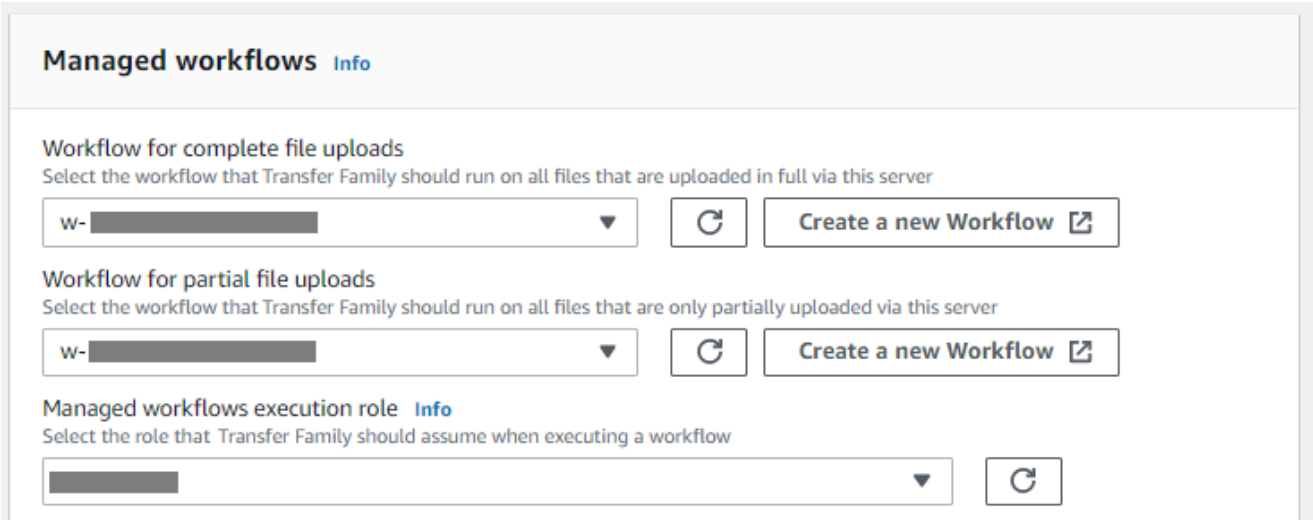
7. 在配置其他详细信息中，执行以下操作：

a. 对于日志记录，指定现有日志组或创建新日志组（默认选项）。如果您选择现有日志组，则必须选择与您的日志组关联的日志组 Amazon Web Services 账户。



如果选择 “创建日志组”，则 CloudWatch 控制台 (https://console.aws.amazon.com/cloudwatch/) 将打开 “创建日志组” 页面。有关详细信息，请参阅在 Log CloudWatch s 中创建日志组。

b. （可选）对于托管工作流程，选择 Tr IDs ansfer Family 在执行工作流程时应担任的工作流程（和相应的角色）。您可以选择一个工作流程在完成上传后执行，选择另一个工作流程在部分上传时执行。要了解有关使用托管工作流程处理文件的更多信息，请参阅 Amazon Transfer Family 托管工作流程。



c. 对于加密算法选项，请选择包含允许服务器使用的加密算法的安全策略。我们的最新安全策略是默认策略：有关详细信息，请参阅Amazon Transfer Family 服务器的安全策略。

d. （可选）在服务器主机密钥中，输入一个 RSA ED25519、或 ECDSA 私钥，当客户端通过 SFTP 连接到服务器时，该私钥将用于识别您的服务器。您还可以添加描述以区分多个主机密钥。

创建服务器后，您可以添加其他主机密钥。如果您想轮换密钥或想要使用不同类型的密钥（例如 RSA 密钥和 ECDSA 密钥），则拥有多个主机密钥非常有用。

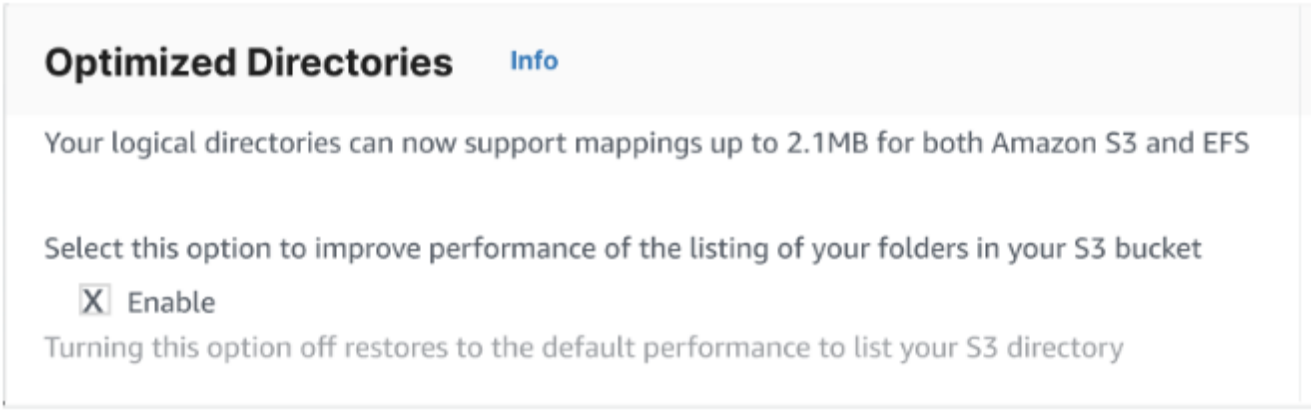
> **Note**
>
> 服务器主机密钥部分仅用于从启用 SFTP 的现有服务器迁移用户。

e. （可选）对于标签，在密钥和值中，输入一个或多个标签作为键值对，然后选择添加标签。

f. 选择下一步。

g. 您可以优化 Amazon S3 目录的性能。例如，假设您进入主目录，并且有 10,000 个子目录。换句话说，您的亚马逊 S3 存储桶有 10,000 个文件夹。在这种情况下，如果您运行 `ls` (list) 命令，则列表操作需要六到八分钟。但是，如果您优化目录，则此操作只需要几秒钟。

使用控制台创建服务器时，默认情况下会启用优化的目录。如果您使用 API 创建服务器，则默认情况下不启用此行为。

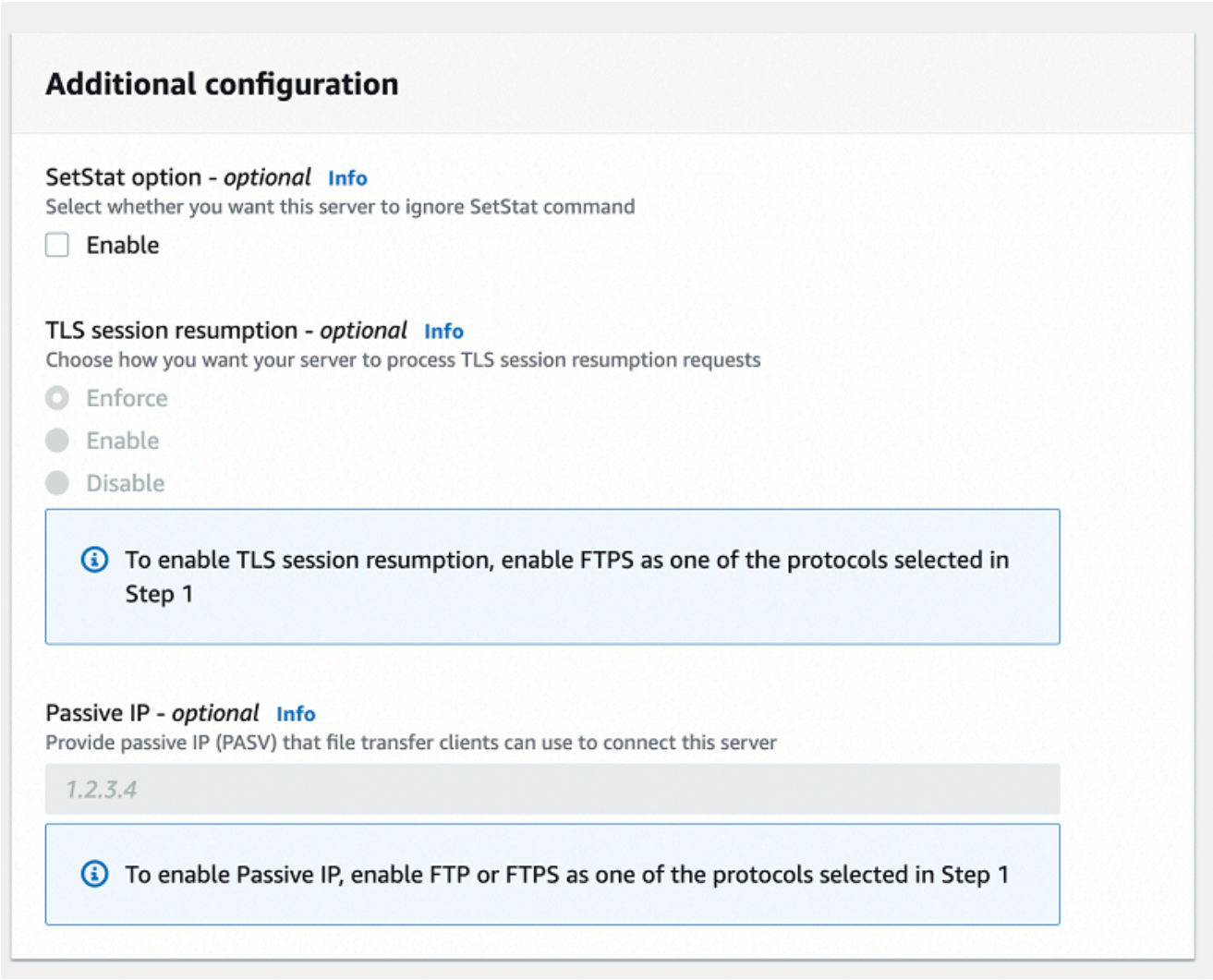


h. （可选）配置 Amazon Transfer Family 服务器以向最终用户显示自定义消息，例如组织政策或条款和条件。对于显示横幅，在预身份验证显示横幅文本框中，输入要在用户进行身份验证之前向其显示的短信。

i. （可选）您可以配置以下其他选项。

- SetStat 选项：启用此选项可忽略客户端尝试对您上传到 Amazon S3 存储桶的文件使用SETSTAT时生成的错误。有关更多详细信息，请参阅中的`SetStatOption`文档ProtocolDetails。
- TLS 会话恢复：仅当您启用 FTPS 作为该服务器的协议之一时，此选项才可用。

- 被动 IP：仅当您启用 FTPS 或 FTP 作为该服务器的协议之一时，此选项才可用。



8. 在审核和创建页面上，审核您的选择。

   - 如果要编辑其中任何一个，请选择该步骤旁边的编辑。

     > **Note**
     >
     > 在选择编辑的步骤之后，您必须审核每个步骤。

   - 如果没有任何更改，请选择创建服务器来创建您的服务器。您将转至如下所示的服务器页面，其中列出了您的新服务器。

您的新服务器状态更改为在线可能需要几分钟时间。此时，您的服务器可以执行文件操作，但您需要先创建一个用户。有关创建用户的详细信息，请参阅管理服务器端点的用户。

创建启用 FTPS 的服务器

安全文件传输协议 (FTPS) 是 FTP 的扩展。它使用传输层安全性协议 (TLS)/安全套接字层 (SSL) 加密协议对流量进行加密。FTPS 允许同时或独立地对控制和数据通道连接进行加密。

> **Note**
>
> 有关网络负载均衡器的重要注意事项，请参阅避免将服务器放在 NLBs Amazon Transfer Family 服务器前面 NATs 。

创建启用 FTPS 的服务器

1. 打开 Amazon Transfer Family 控制台，从导航窗格中选择 “服务器”，然后选择 “创建服务器”。https://console.aws.amazon.com/transfer/
2. 在选择协议中，选择 FTPS。

   对于服务器证书，请选择存储在 Amazon Certificate Manager (ACM) 中的证书，当客户端通过 FTPS 连接到服务器时，该证书将用于识别您的服务器，然后选择下一步。

   要请求新的公有证书，请参阅 Amazon Certificate Manager 用户指南中的请求公有证书。

   要将现有证书导入到 ACM 中，请参阅 Amazon Certificate Manager 用户指南中的将证书导入到 ACM。

   要请求私有证书以通过私有 IP 地址使用 FTPS，请参阅 Amazon Certificate Manager 用户指南中的请求私有证书。

   支持具有以下加密算法和密钥大小的证书：

   - 2048 位 RSA (RSA_2048)
   - 4096 位 RSA (RSA_4096)
   - Elliptic Prime Curve 256 位 (EC_prime256v1)
   - Elliptic Prime Curve 384 位 (EC_secp384r1)
   - Elliptic Prime Curve 521 位 (EC_secp521r1)

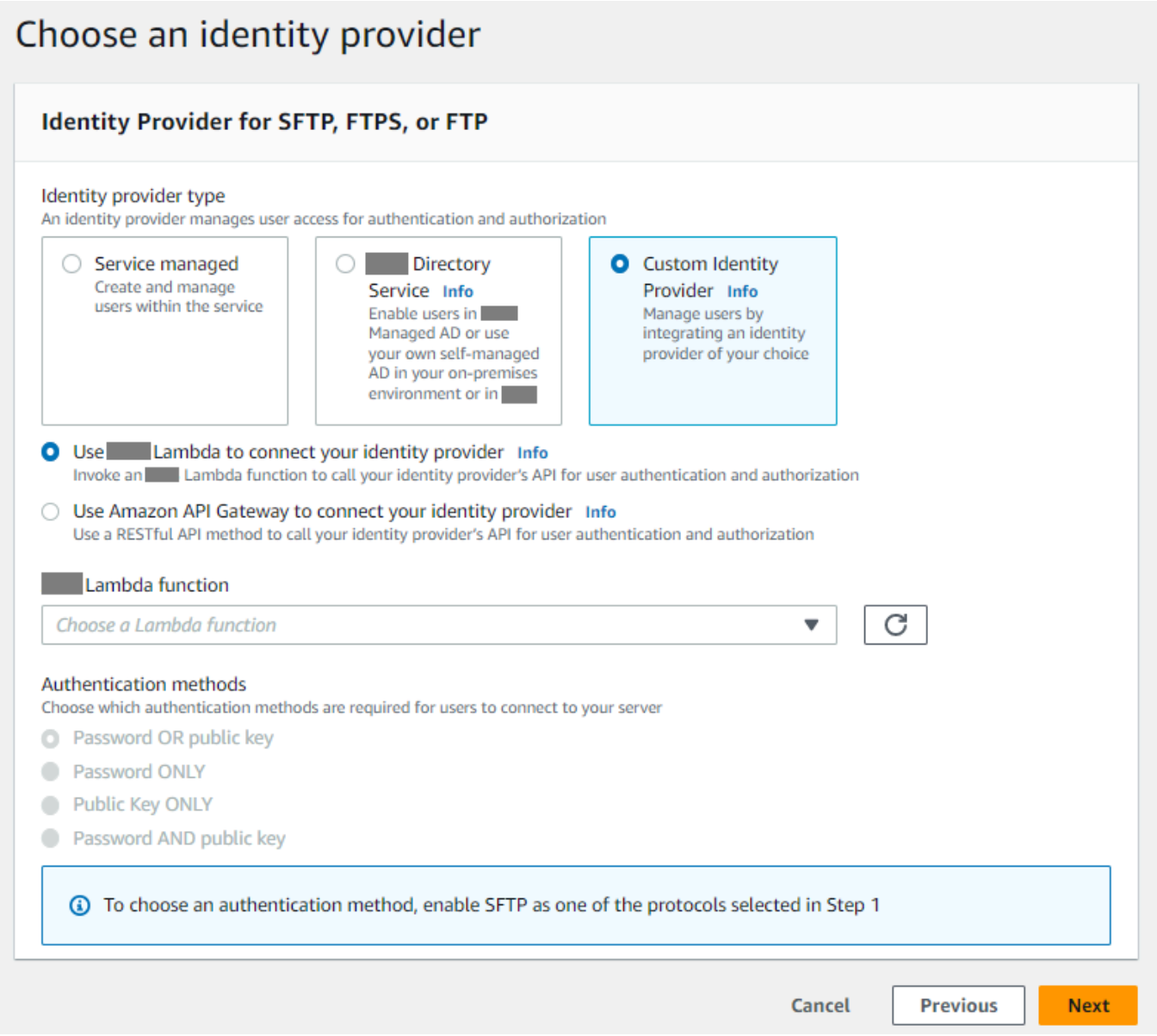
> **Note**
>
> 该证书必须是指定了 FQDN 或 IP 地址的有效 SSL/TLS X.509 版本 3 证书，并包含有关颁发者的信息。

3. 在选择身份提供商中，选择要用于管理用户访问权限的身份提供商。您有以下选项：

- Amazon Directory Service for Microsoft Active Directory— 您提供用于访问终端节点的 Amazon Directory Service 目录。这样，您就可以使用存储在 Activity Directory 中的凭证对用户进行身份验证。要了解有关与 Amazon Managed Microsoft AD 身份提供商合作的更多信息，请参阅使用微软 Active Directory 的 Amazon 目录服务。

  > **Note**
  >
  > - 不支持跨账户目录和共享目录。 Amazon Managed Microsoft AD
  > - 要设置以 Directory Service 作为身份提供者的服务器，您需要添加一些 Amazon Directory Service 权限。有关更多信息，请参阅 在你开始使用之前 Amazon Directory Service for Microsoft Active Directory。

- 自定义身份提供商 — 请选择以下任一选项：
  - Amazon Lambda 用于连接您的身份提供商-您可以使用由 Lambda 函数支持的现有身份提供商。您提供 Lambda 函数名称。有关更多信息，请参阅 Amazon Lambda 用于整合您的身份提供商。
  - 使用 Amazon API Gateway 连接您的身份提供商 — 您可以创建由 Lambda 函数支持的 API 网关方法以用作身份提供商。您提供一个 Amazon API Gateway URL 和一个调用角色。有关更多信息，请参阅 使用 Amazon API Gateway 整合您的身份提供程序。



4. 选择下一步。
5. 在选择端点中，执行以下操作：

> **Note**
>
> Transfer Family 的 FTPS 服务器通过端口 21（控制通道）和端口范围 8192–8200（数据通道）运行。

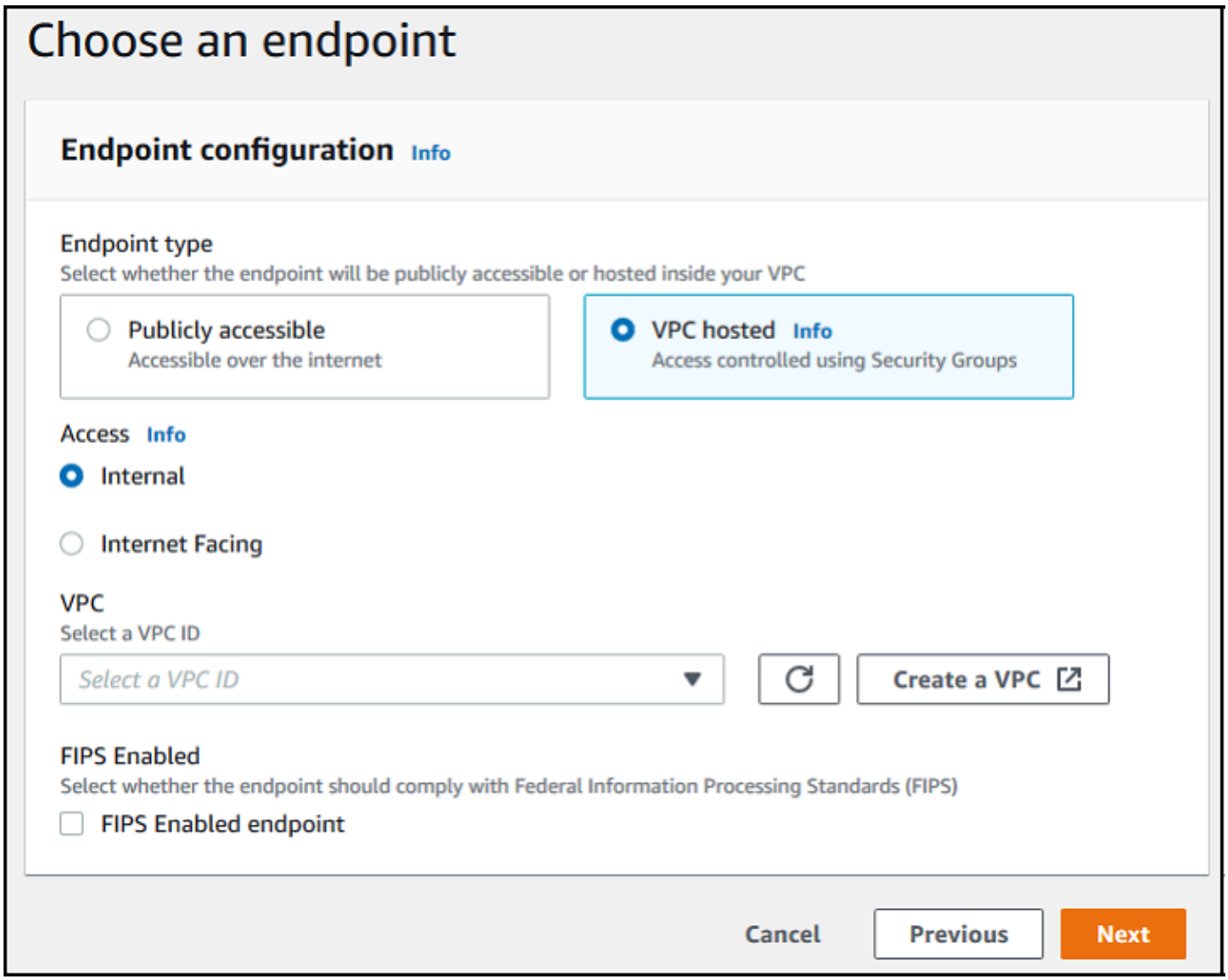
a. 对于端点类型，选择托管服务器端点的 VPC 托管端点类型。有关设置 VPC 主机端点的信息，请参阅 在虚拟私有云中创建服务器。

> **Note**
>
> 不支持可公共访问的端点。

b. （可选）对于启用 FIPS，请选中启用 FIPS 端点复选框以确保端点符合联邦信息处理标准 (FIPS)。

> **Note**
>
> 启用 FIPS 的端点仅在北美 Amazon 地区可用。有关可用区域，请参阅 Amazon Web Services 一般参考 中的 Amazon Transfer Family 端点和限额。有关 FIPS 的更多信息，请参阅联邦信息处理标准 (FIPS) 140-2。

c. 选择下一步。



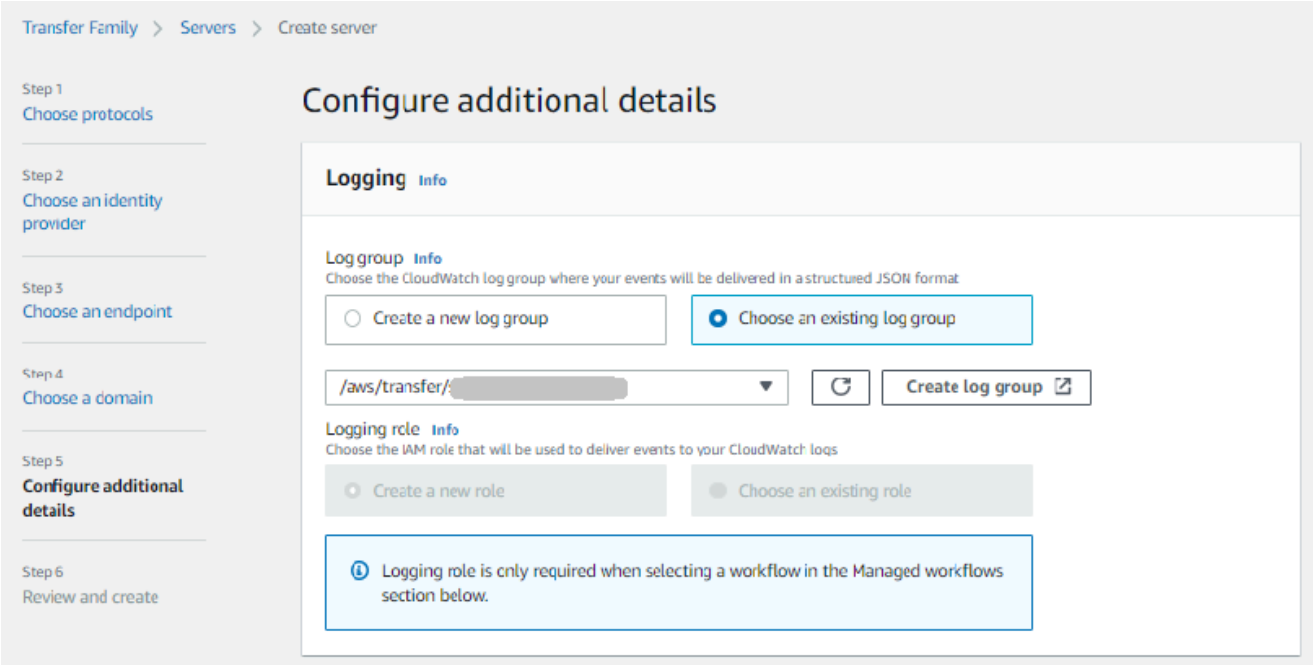
6. 在“选择域”页面上，选择要用于通过所选协议 Amazon 存储和访问数据的存储服务：

   - 选择 Amazon S3，通过所选协议将您的文件作为对象存储和访问。
   - 选择 Amazon EFS，通过所选协议在 Amazon EFS 文件系统中存储和访问您的文件。

   选择下一步。

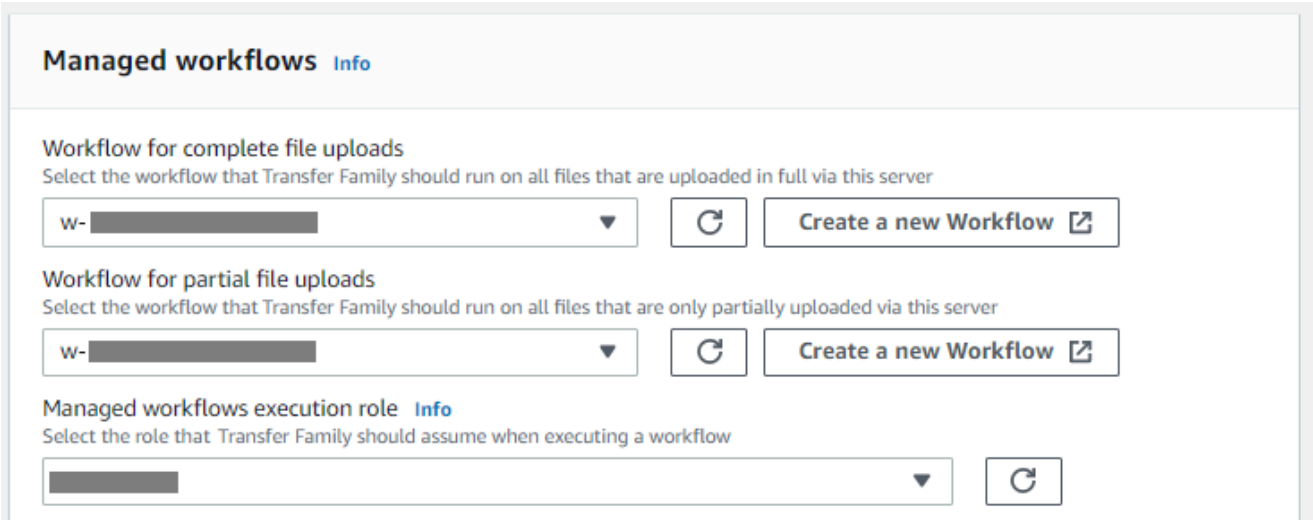
7. 在配置其他详细信息中，执行以下操作：

   a. 对于日志记录，指定现有日志组或创建新日志组（默认选项）。



如果选择 “创建日志组”，则 CloudWatch 控制台 (https://console.aws.amazon.com/cloudwatch/) 将打开 “创建日志组” 页面。有关详细信息，请参阅在 Log CloudWatch s 中创建日志组。

b. （可选）对于托管工作流程，选择 Tr IDs ansfer Family 在执行工作流程时应担任的工作流程（和相应的角色）。您可以选择一个工作流程在完成上传后执行，选择另一个工作流程在部分上传时执行。要了解有关使用托管工作流程处理文件的更多信息，请参阅 Amazon Transfer Family 托管工作流程。



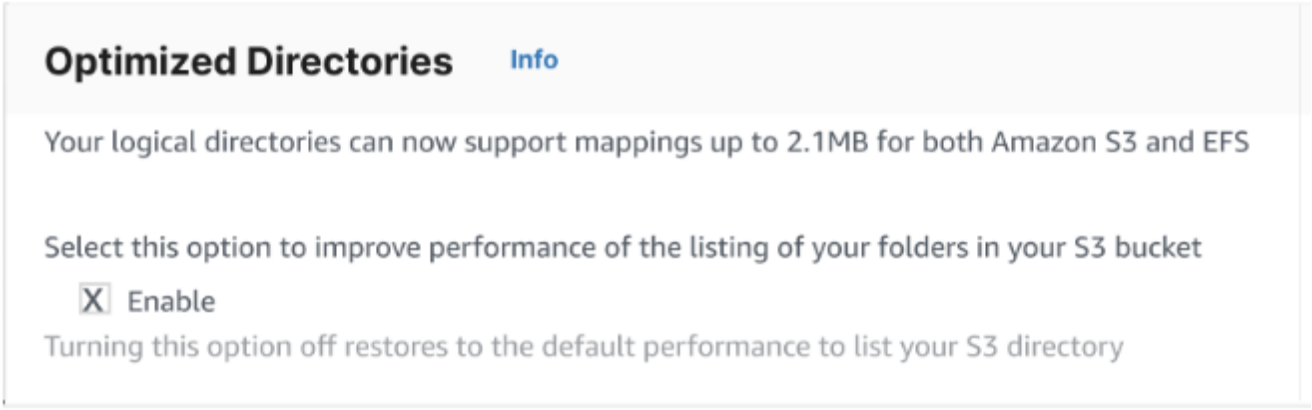
c. 对于加密算法选项，请选择包含允许服务器使用的加密算法的安全策略。我们的最新安全策略是默认策略：有关详细信息，请参阅Amazon Transfer Family 服务器的安全策略。

d. 对于服务器主机密钥，请将其留空。

e. （可选）对于标签，在密钥和值中，输入一个或多个标签作为键值对，然后选择添加标签。

f. 您可以优化 Amazon S3 目录的性能。例如，假设您进入主目录，并且有 10,000 个子目录。换句话说，您的亚马逊 S3 存储桶有 10,000 个文件夹。在这种情况下，如果您运行 `ls` (list) 命令，则列表操作需要六到八分钟。但是，如果您优化目录，则此操作只需要几秒钟。

使用控制台创建服务器时，默认情况下会启用优化的目录。如果您使用 API 创建服务器，则默认情况下不启用此行为。



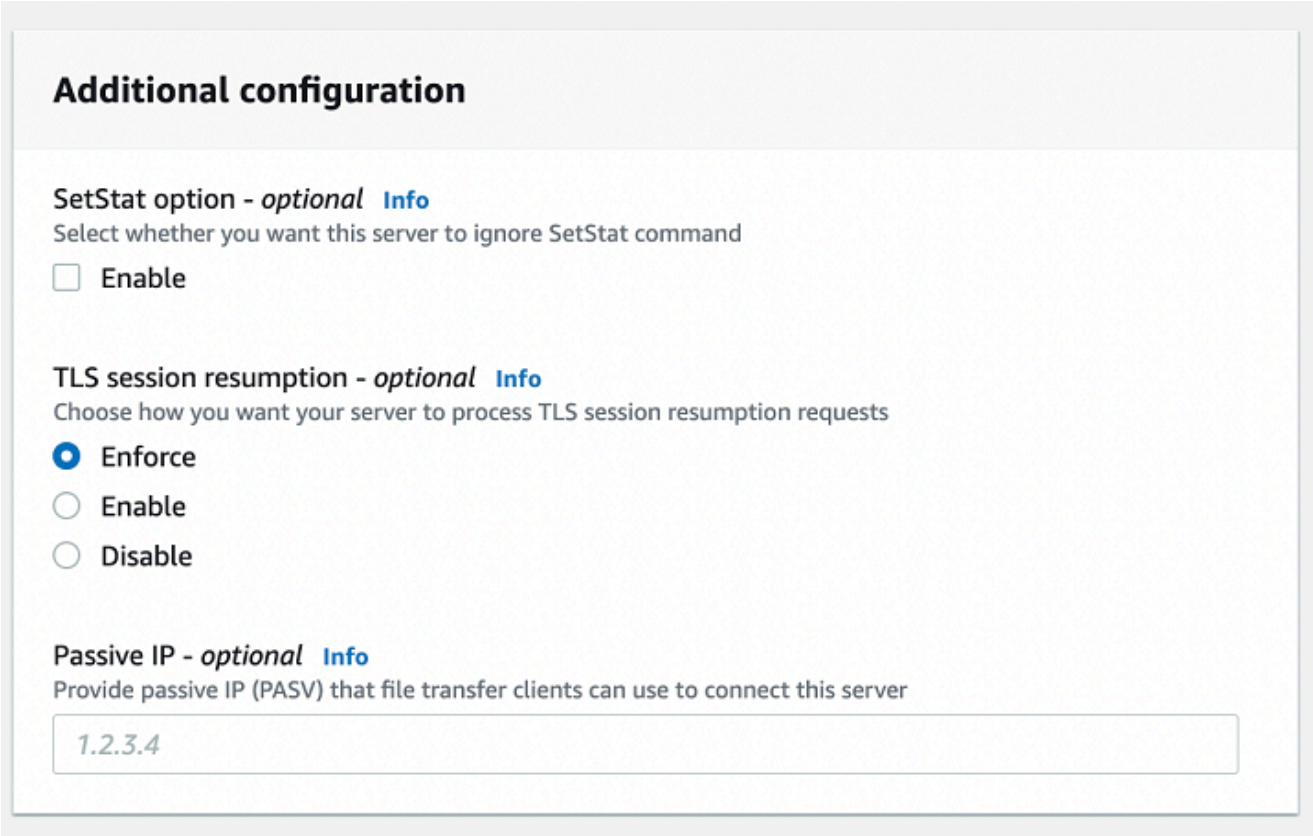
g. 选择下一步。

h. （可选）您可以将 Amazon Transfer Family 服务器配置为向最终用户显示自定义消息，例如组织政策或条款和条件。您还可以向成功通过身份验证的用户显示自定义的每日消息 (MOTD)。

对于显示横幅，在预身份验证显示横幅文本框中，输入要在用户进行身份验证之前向他们显示的短信，然后在后身份验证显示横幅文本框中，输入要在用户成功进行身份验证后向他们显示的文本。

i. （可选）您可以配置以下其他选项。

- SetStat 选项：启用此选项可忽略客户端尝试对您上传到 Amazon S3 存储桶的文件使用`SETSTAT`时生成的错误。有关其他详细信息，请参阅ProtocolDetails主题中的`SetStatOption`文档。
- TLS 会话恢复：提供一种机制来恢复或共享 FTPS 会话的控制和数据连接之间协商的私有密钥。有关其他详细信息，请参阅ProtocolDetails主题中的`TlsSessionResumptionMode`文档。
- 被动 IP：表示 FTP 和 FTPS 协议的被动模式。输入单个 IPv4 地址，例如防火墙、路由器或负载均衡器的公有 IP 地址。有关其他详细信息，请参阅ProtocolDetails主题中的`PassiveIp`文档。



8. 在审核和创建页面上，审核您的选择。

   - 如果要编辑其中任何一个，请选择该步骤旁边的编辑。

     > **Note**
     >
     > 在选择编辑的步骤之后，您必须审核每个步骤。

   - 如果没有任何更改，请选择创建服务器来创建您的服务器。您将转至如下所示的服务器页面，其中列出了您的新服务器。

您的新服务器状态更改为在线可能需要几分钟时间。到时候，您的服务器可以执行用户的文件操作。

后续步骤：对于下一步，请继续前往 使用自定义身份提供程序 设置用户。

创建启用 FTP 的服务器

文件传输协议 (FTP) 是一种用于数据传输的网络协议。FTP 使用单独的通道进行控制和数据传输。控制通道保持打开状态，直至终止或不活动超时状态。数据通道在传输期间处于活动状态。FTP 使用明文且不支持流量加密。

> **Note**
>
> 启用 FTP 时，必须为托管 VPC 的终端节点选择内部访问选项。如果您需要服务器让数据通过公共网络，则必须使用安全协议，例如 SFTP 或 FTPS。

> **Note**
>
> 有关网络负载均衡器的重要注意事项，请参阅避免将服务器放在 NLBs Amazon Transfer Family 服务器前面 NATs 。

创建启用 FTP 的服务器

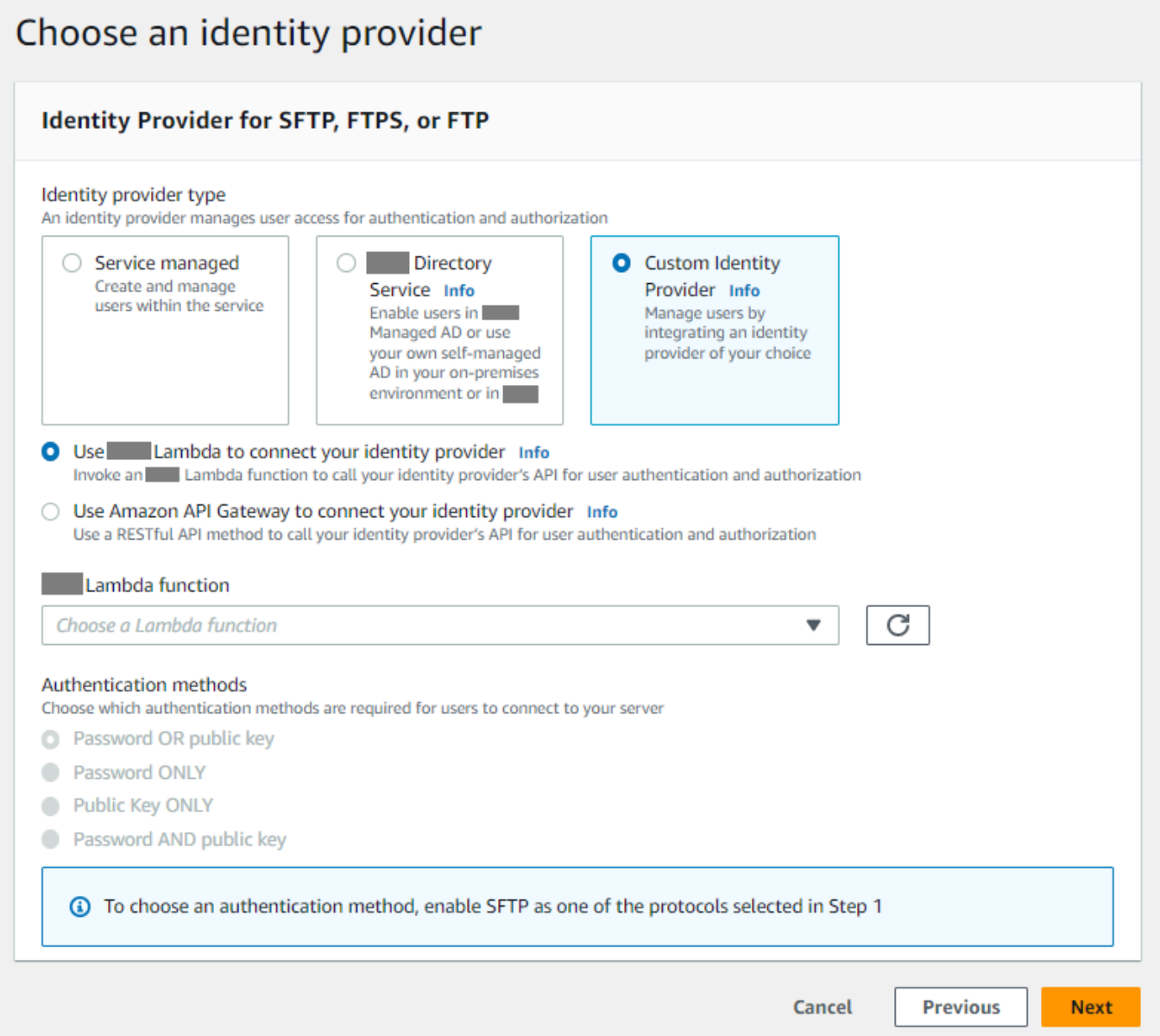
1. 打开 Amazon Transfer Family 控制台，从导航窗格中选择 “服务器”，然后选择 “创建服务器”。https://console.aws.amazon.com/transfer/
2. 在选择协议中，选择 FTP，然后选择下一步。
3. 在选择身份提供商中，选择要用于管理用户访问权限的身份提供商。您有以下选项：

   - Amazon Directory Service for Microsoft Active Directory— 您提供用于访问终端节点的 Amazon Directory Service 目录。这样，您就可以使用存储在 Activity Directory 中的凭证对用户进行身份验证。要了解有关与 Amazon Managed Microsoft AD 身份提供商合作的更多信息，请参阅使用微软 Active Directory 的 Amazon 目录服务。

     > **Note**
     >
     > - 不支持跨账户目录和共享目录。 Amazon Managed Microsoft AD
     > - 要设置以 Directory Service 作为身份提供者的服务器，您需要添加一些 Amazon Directory Service 权限。有关更多信息，请参阅 在你开始使用之前 Amazon Directory Service for Microsoft Active Directory。

   - 自定义身份提供商 — 请选择以下任一选项：

- Amazon Lambda 用于连接您的身份提供商-您可以使用由 Lambda 函数支持的现有身份提供商。您提供 Lambda 函数名称。有关更多信息，请参阅 Amazon Lambda 用于整合您的身份提供商。
- 使用 Amazon API Gateway 连接您的身份提供商 — 您可以创建由 Lambda 函数支持的 API 网关方法以用作身份提供商。您提供一个 Amazon API Gateway URL 和一个调用角色。有关更多信息，请参阅 使用 Amazon API Gateway 整合您的身份提供程序。



4. 选择下一步。
5. 在选择端点中，执行以下操作：

> **Note**
>
> Transfer Family 的 FTP 服务器通过端口 21（控制通道）和端口范围 8192–8200（数据通道）运行。

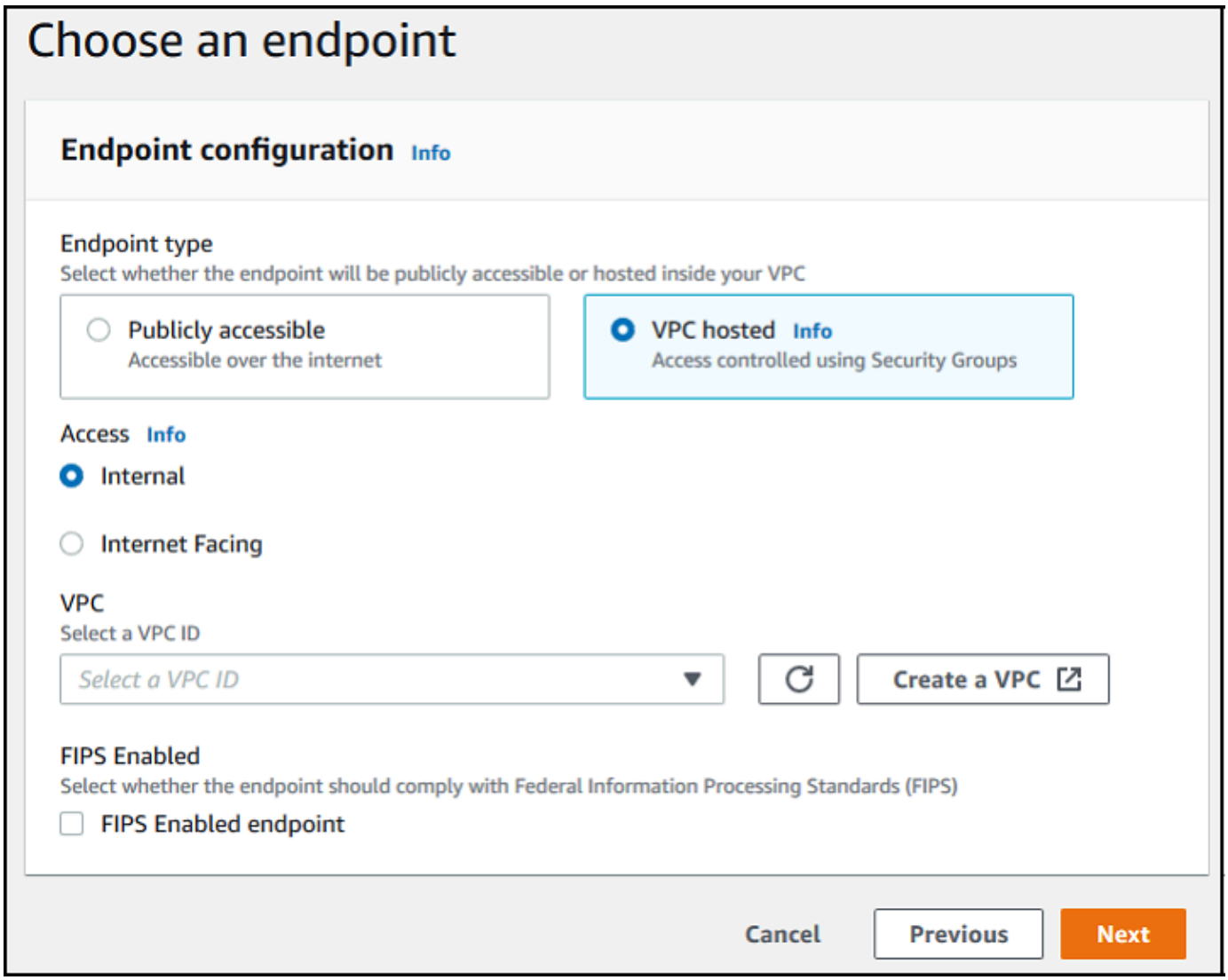
a. 对于端点类型，选择托管服务器端点的 VPC 托管。有关设置 VPC 主机端点的信息，请参阅在虚拟私有云中创建服务器。

> **Note**
>
> 不支持可公共访问的端点。

b. 对于启用 FIPS，请清除启用 FIPS 端点复选框。

> **Note**
>
> FTP 服务器不支持启用 FIPS 的端点。

c. 选择下一步。



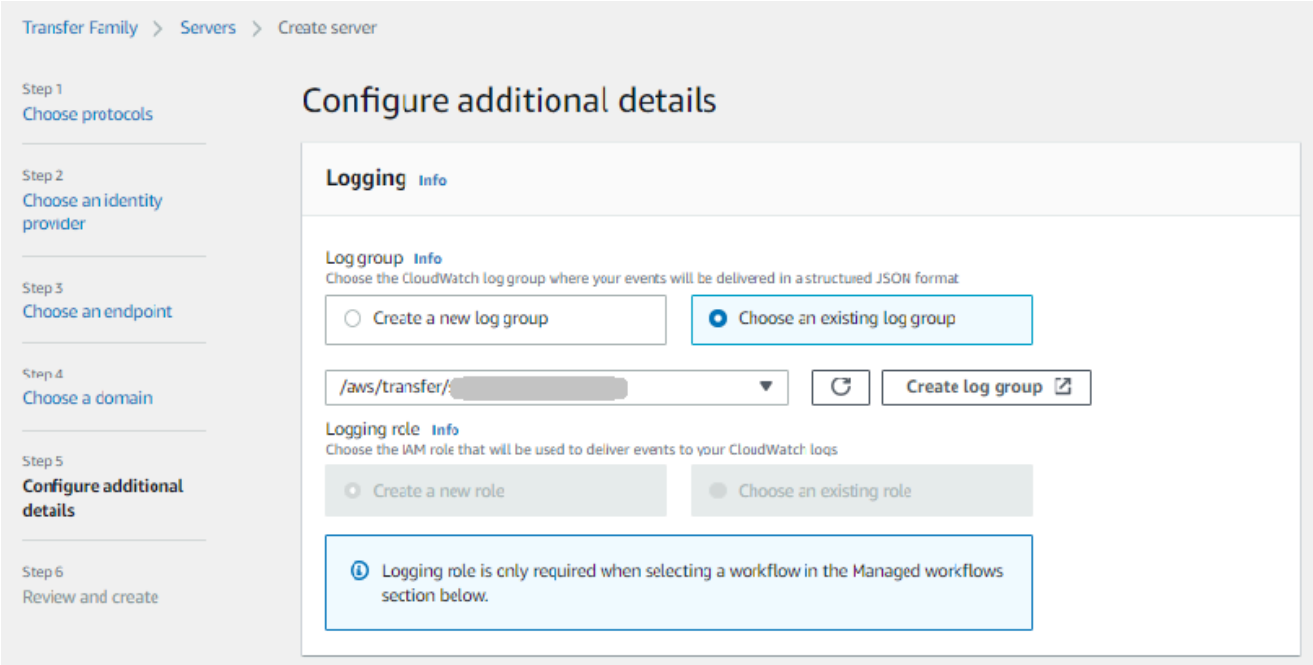
6. 在“选择域”页面上，选择要用于通过所选协议 Amazon 存储和访问数据的存储服务。

   - 选择 Amazon S3，通过所选协议将您的文件作为对象存储和访问。
   - 选择 Amazon EFS，通过所选协议在 Amazon EFS 文件系统中存储和访问您的文件。

   选择下一步。

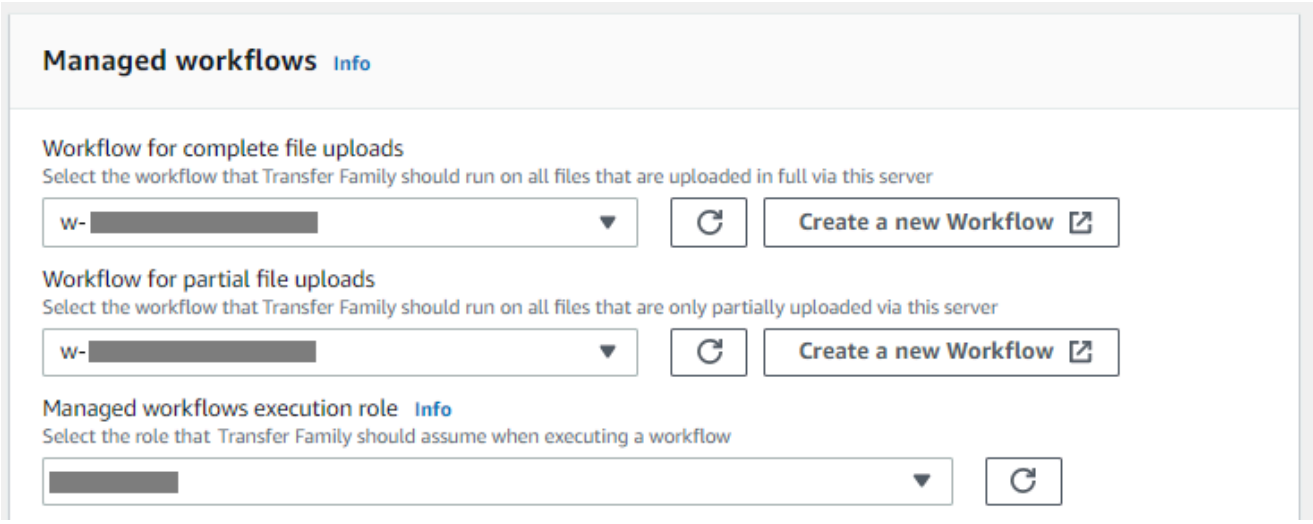
7. 在配置其他详细信息中，执行以下操作：

   a. 对于日志记录，指定现有日志组或创建新日志组（默认选项）。



如果选择 “创建日志组”，则 CloudWatch 控制台 (https://console.aws.amazon.com/cloudwatch/) 将打开 “创建日志组” 页面。有关详细信息，请参阅在 Log CloudWatch s 中创建日志组。

b. （可选）对于托管工作流程，选择 Tr IDs ansfer Family 在执行工作流程时应担任的工作流程（和相应的角色）。您可以选择一个工作流程在完成上传后执行，选择另一个工作流程在部分上传时执行。要了解有关使用托管工作流程处理文件的更多信息，请参阅 Amazon Transfer Family 托管工作流程。



c. 对于加密算法选项，请选择包含允许服务器使用的加密算法的安全策略。

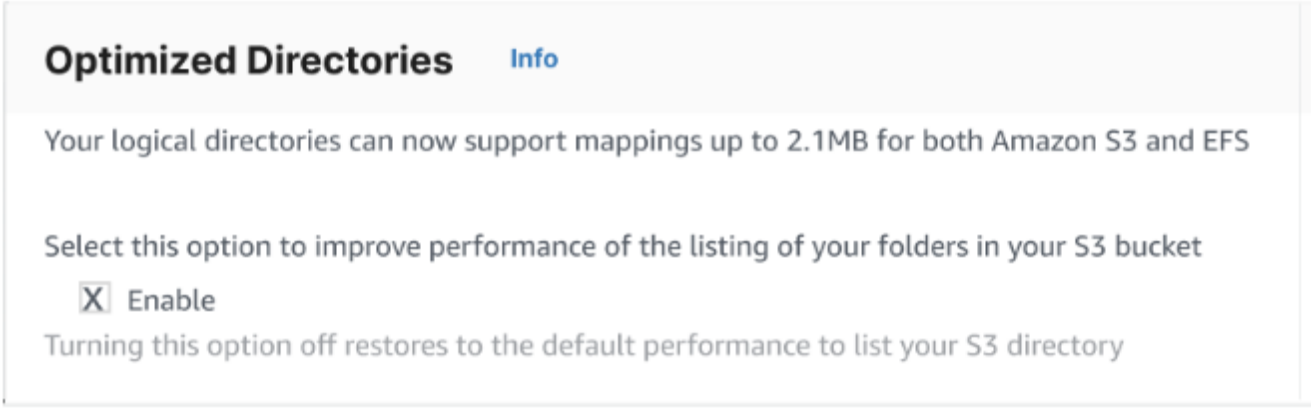
> **Note**
>
> Transfer Family 会将最新的安全策略分配给你的 FTP 服务器。但是，由于 FTP 协议不使用任何加密，因此 FTP 服务器不使用任何安全策略算法。除非您的服务器也使用 FTPS 或 SFTP 协议，否则安全策略将保持未使用状态。

d. 对于服务器主机密钥，请将其留空。

e. （可选）对于标签，在密钥和值中，输入一个或多个标签作为键值对，然后选择添加标签。

f. 您可以优化 Amazon S3 目录的性能。例如，假设您进入主目录，并且有 10,000 个子目录。换句话说，您的亚马逊 S3 存储桶有 10,000 个文件夹。在这种情况下，如果您运行 `ls` (list) 命令，则列表操作需要六到八分钟。但是，如果您优化目录，则此操作只需要几秒钟。

使用控制台创建服务器时，默认情况下会启用优化的目录。如果您使用 API 创建服务器，则默认情况下不启用此行为。



g. 选择下一步。

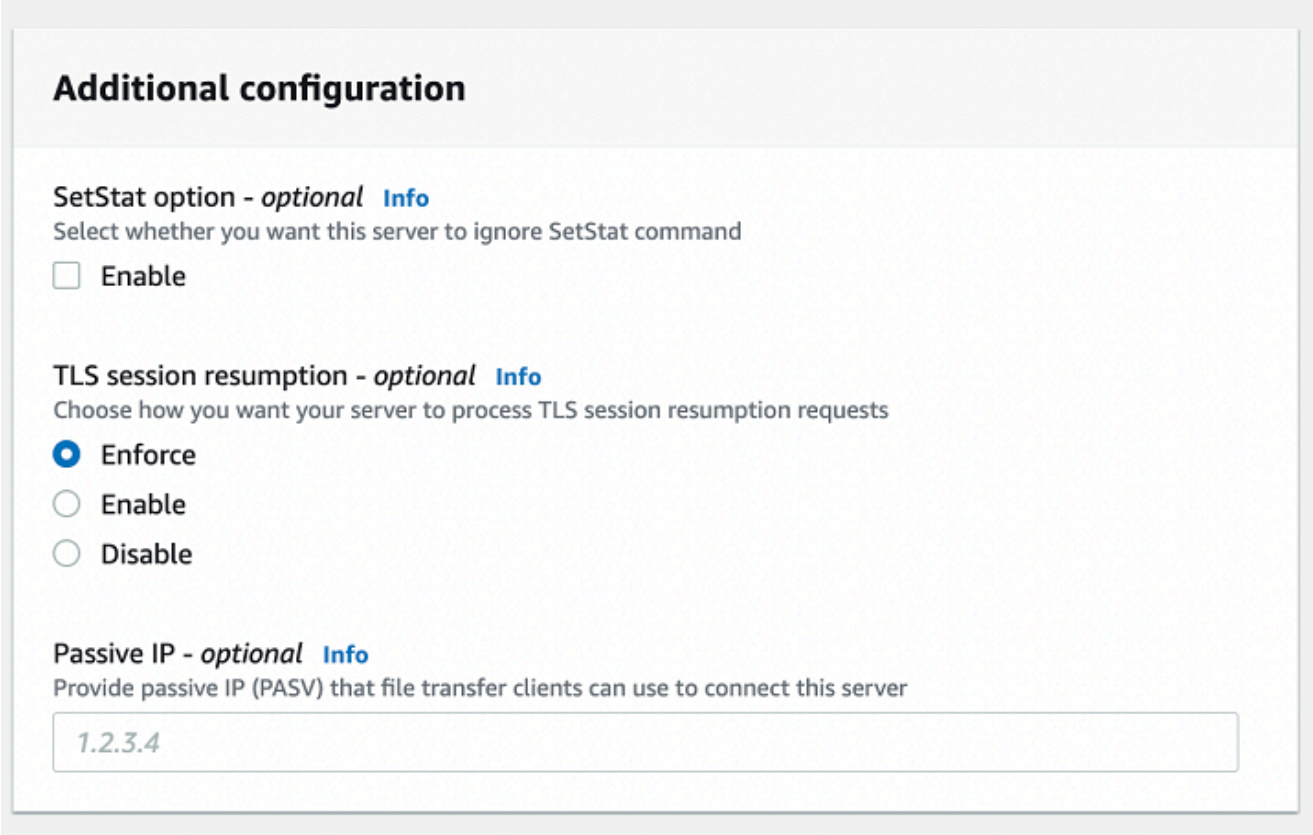
h. （可选）您可以将 Amazon Transfer Family 服务器配置为向最终用户显示自定义消息，例如组织政策或条款和条件。您还可以向成功通过身份验证的用户显示自定义的每日消息 (MOTD)。

对于显示横幅，在预身份验证显示横幅文本框中，输入要在用户进行身份验证之前向他们显示的短信，然后在后身份验证显示横幅文本框中，输入要在用户成功进行身份验证后向他们显示的文本。

i. （可选）您可以配置以下其他选项。

- SetStat 选项：启用此选项可忽略客户端尝试对您上传到 Amazon S3 存储桶的文件使用`SETSTAT`时生成的错误。有关其他详细信息，请参阅ProtocolDetails主题中的`SetStatOption`文档。

- TLS 会话恢复：提供一种机制来恢复或共享 FTPS 会话的控制和数据连接之间协商的私有密钥。有关其他详细信息，请参阅ProtocolDetails主题中的`TlsSessionResumptionMode`文档。
- 被动 IP：表示 FTP 和 FTPS 协议的被动模式。输入单个 IPv4 地址，例如防火墙、路由器或负载均衡器的公有 IP 地址。有关其他详细信息，请参阅ProtocolDetails主题中的`PassiveIp`文档。



8. 在审核和创建页面上，审核您的选择。
   - 如果要编辑其中任何一个，请选择该步骤旁边的编辑。

     > **Note**
     >
     > 在选择编辑的步骤之后，您必须审核每个步骤。

   - 如果没有任何更改，请选择创建服务器来创建您的服务器。您将转至如下所示的服务器页面，其中列出了您的新服务器。

您的新服务器状态更改为在线可能需要几分钟时间。到时候，您的服务器可以执行用户的文件操作。

后续步骤 — 对于下一步，请继续前往 使用自定义身份提供程序 设置用户。

在虚拟私有云中创建服务器

您可以将服务器的端点托管在虚拟私有云 (VPC) 中，用于在不通过公共互联网的情况下向 Amazon S3 存储桶或 Amazon EFS 文件系统传输数据和从 Amazon S3 存储桶或 Amazon EFS 文件系统中传输数据。

> **Note**
>
> 2021 年 5 月 19 日之后，如果您的 Amazon 账户`EndpointType=VPC_ENDPOINT`在 2021 年 5 月 19 日之前尚未使用您的账户创建服务器，则您将无法创建服务器。如果您在 2021 年 2 月 21 日当天或之前已经在 Amazon 账户`EndpointType=VPC_ENDPOINT`中创建了服务器，则不会受到影响。在此日期之后，使用 `EndpointType` = **`VPC`**。有关更多信息，请参阅 the section called “停止使用 VPC_ENDPOINT”。

如果您使用亚马逊虚拟私有云（Amazon VPC）托管 Amazon 资源，则可以在您的 VPC 和服务器之间建立私有连接。然后，您可以使用此服务器通过客户端将数据传输到您的 Amazon S3 存储桶或从您的 Amazon S3 存储桶中传输数据，而无需使用公有 IP 地址或需要互联网网关。

使用 Amazon VPC，您可以在自定义虚拟网络中启动 Amazon 资源。可以使用 VPC 控制您的网络设置，例如 IP 地址范围、子网、路由表和网络网关。有关更多信息 VPCs，请参阅什么是 Amazon VPC？ 在《亚马逊 VPC 用户指南》中。

在下一部分中，查找如何创建 VPC 并将其连接到服务器的说明。作为概述，您可以按如下方式执行此操作：

1. 使用 VPC 端点设置服务器。
2. 使用 VPC 内的客户端通过 VPC 端点连接到您的服务器。这样，您就可以使用 Amazon Transfer Family通过客户端传输存储在 Amazon S3 存储桶中的数据。即使网络已与公共互联网断开连接，您也可以执行此传输。
3. 此外，如果您选择将服务器的端点设为面向互联网，则可以将弹性 IP 地址与您的端点相关联。这样做可以让 VPC 之外的客户端连接到您的服务器。您可以使用 VPC 安全组以控制请求仅来自允许地址的经过身份验证的用户的访问权限。

> **Note**
>
> Amazon Transfer Family 支持双栈端点，允许您的服务器通过 IPv4 和 IPv6进行通信。要启用双堆栈支持，请在创建 VPC 终端节点时选择启用 DNS 双堆栈终端节点选项。请注意，您的 VPC 和子网都必须配置为支持， IPv6 然后才能使用此功能。当您的客户端需要使用任一协议进行连接时，双栈支持特别有用。
> 有关双栈（ IPv4 和 IPv6 ）服务器端点的信息，请参见IPv6 支持 Transfer Family 服务器。

主题

- 创建仅在您的 VPC 内访问的服务器端点
- 为服务器创建面向互联网的端点
- 更改 SFTP 服务器的端点类型
- 停止使用 VPC_ENDPOINT
- 限制 Transfer Family 服务器的 VPC 终端节点访问权限
- 其他联网功能
- 将 Amazon Transfer Family 服务器终端节点类型从 VPC_ENDPOINT 更新到 VPC

创建仅在您的 VPC 内访问的服务器端点

在以下步骤中，您将创建仅由您的 VPC 内的资源访问的服务器端点。

在 VPC 内创建服务器端点

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 从导航窗格中，选择服务器，然后选择创建服务器。
3. 在选择协议中，选择一个或多个协议，然后选择下一步。有关协议的更多信息，请参阅 步骤 2：创建启用 SFTP 的服务器。
4. 在选择身份提供商中，选择管理服务以存储用户身份和密钥 Amazon Transfer Family，然后选择下一步。

   此过程使用服务托管选项。如果您选择自定义，则提供 Amazon API Gateway 端点和 Amazon Identity and Access Management IAM 角色来访问端点。执行此操作后，您可以集成目录服务，用于对用户进行身份验证和授权。要了解有关使用自定义身份提供商的更多信息，请参阅 使用自定义身份提供程序。

5. 在选择端点中，执行以下操作：

   a. 对于端点类型，选择托管服务器端点的 VPC 托管端点类型。

   b. 对于访问，请选择内部，使您的端点仅可由使用端点的私有 IP 地址的客户端访问。

      有关面向互联网选项的详细信息，请参阅 为服务器创建面向互联网的端点。在 VPC 中创建的仅用于内部访问的服务器不支持自定义主机名。

   c. 对于 VPC，选择现有 VPC ID 或选择创建 VPC 以创建新的 VPC。

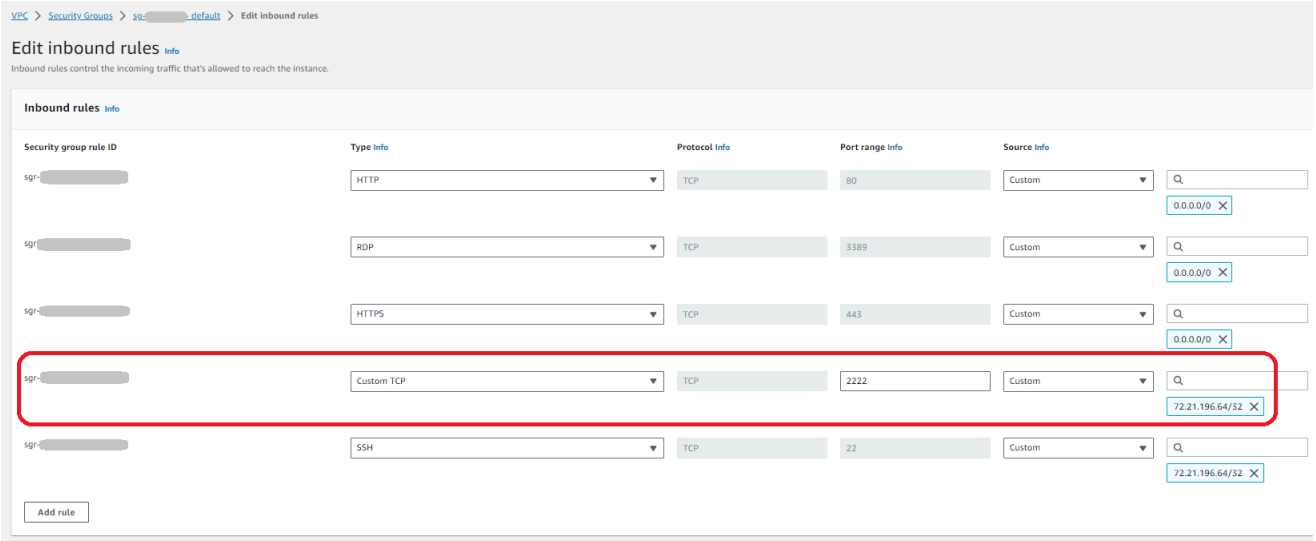
   d. 在可用区部分，最多选择三个可用区和关联的子网。

   e. 在 “安全组” 部分，选择现有安全组 ID IDs 或选择 “创建安全组” 来创建新的安全组。有关安全组的更多信息，请参阅 Amazon Virtual Private Cloud 用户指南中的 VPC 的安全组。要创建安全组，请参阅 Amazon Virtual Private Cloud 用户指南中的创建安全组。

      > **Note**
      >
      > 您的 VPC 会自动带有默认的安全组。如果您在启动服务器时没有指定其他安全组或组，我们会将默认安全组与您的服务器相关联。

      - 对于安全组的入站规则，您可以将 SSH 流量配置为使用端口 22、2222、22000 或任意组合。默认情况下，端口 22 已配置。要使用端口 2222 或端口 22000，您需要向安全组添加入站规则。对于类型，选择 “自定义 TCP”，然后在 “端口范围” 中输入**2222**或**22000**，对于源，输入与 SSH 端口 22 规则相同的 CIDR 范围。
      - 对于安全组的入站规则，请将 FTP 和 FTPS 流量配置**21**为使用控制通道和数据通道**8192-8200**的端口范围。

      > **Note**
      >
      > 对于需要 TCP “搭载” 的客户端，也可以使用端口 2223 ACKs，或者让 TCP 三向握手的最终确认也包含数据。
      > 某些客户端软件可能与端口 2223 不兼容：例如，客户端要求服务器在客户端发送 SFTP 标识字符串之前发送 SFTP 标识字符串。



f. （可选）对于启用 FIPS，请选中启用 FIPS 的端点复选框以确保端点符合联邦信息处理标准 (FIPS)。

> **Note**
>
> 启用 FIPS 的端点仅在北美 Amazon 地区可用。有关可用区域，请参阅 Amazon Web Services 一般参考 中的 Amazon Transfer Family 端点和限额。有关 FIPS 的更多信息，请参阅联邦信息处理标准 (FIPS) 140-2。

g. 选择下一步。

6. 在配置其他详细信息中，执行以下操作：

a. 要进行CloudWatch 日志记录，请选择以下选项之一以启用 Amazon CloudWatch 记录您的用户活动：

- 创建一个新角色，允许 Transfer Family 自动创建 IAM 角色，前提是您拥有创建新角色的相应权限。创建的 IAM 角色被称为`AWSTransferLoggingAccess`。
- 选择现有角色以从您的帐户中选择现有 IAM 角色。在日志记录角色下，选择该角色。此 IAM 角色应包括将服务设置为 `transfer.amazonaws.com` 的信任策略。

  有关 CloudWatch 日志记录的更多信息，请参阅配置 CloudWatch 日志记录角色。

> **Note**
>
> - 如果您未指定日志记录角色， CloudWatch 则无法在中查看最终用户活动。
> - 如果您不想设置 CloudWatch 日志记录角色，请选择选择现有角色，但不要选择日志记录角色。

b. 对于加密算法选项，请选择包含允许服务器使用的加密算法的安全策略。

> **Note**
>
> 默认情况下，除非选择不同的服务器，否则 `TransferSecurityPolicy-2024-01` 安全策略将连接到服务器。

有关安全策略的更多信息，请参阅 Amazon Transfer Family 服务器的安全策略。

c. （可选：此部分仅适用于从启用 SFTP 的现有服务器迁移用户。）在服务器主机密钥中，输入一个 RSA ED25519、或 ECDSA 私钥，当客户端通过 SFTP 连接到服务器时，该私钥将用于识别您的服务器。

d. （可选）对于标签，在密钥和值中，输入一个或多个标签作为键值对，然后选择添加标签。

e. 选择下一步。

7. 在审核和创建页面上，审核您的选择。如果您：

- 要编辑其中任何一个，请选择该步骤旁边的编辑。

> **Note**
>
> 在选择编辑的步骤之后，您将需要查看每个步骤。

- 如果没有更改，请选择创建服务器来创建您的服务器。您将转至如下所示的服务器页面，其中列出了您的新服务器。

您的新服务器状态更改为在线可能需要几分钟时间。此时，您的服务器可以执行文件操作，但您需要先创建一个用户。有关创建用户的详细信息，请参阅管理服务器端点的用户。

为服务器创建面向互联网的端点

在以下过程中，创建服务器端点。只有在您的 VPC 默认安全组中允许其源 IP 地址的客户端才能通过互联网访问此端点。此外，通过使用弹性 IP 地址使您的端点面向互联网，您的客户可以使用弹性 IP 地址来允许在其防火墙中访问您的端点。

> **Note**
>
> 在面向互联网的 VPC 托管端点上，只能使用 SFTP 和 FTPS。

创建面向互联网的端点

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 从导航窗格中，选择服务器，然后选择创建服务器。
3. 在选择协议中，选择一个或多个协议，然后选择下一步。有关协议的更多信息，请参阅 步骤 2：创建启用 SFTP 的服务器。
4. 在选择身份提供商中，选择管理服务以存储用户身份和密钥 Amazon Transfer Family，然后选择下一步。

   此过程使用服务托管选项。如果您选择自定义，则提供 Amazon API Gateway 端点和 Amazon Identity and Access Management IAM 角色来访问端点。执行此操作后，您可以集成目录服务，用于对用户进行身份验证和授权。要了解有关使用自定义身份提供商的更多信息，请参阅 使用自定义身份提供程序。
5. 在选择端点中，执行以下操作：

   a. 对于端点类型，选择托管服务器端点的 VPC 托管端点类型。

   b. 对于访问，请选择面向互联网，使客户端可以通过互联网访问您的端点。

   > **Note**
   >
   > 选择面向互联网时，可以在每个子网或多个子网中选择一个现有的弹性 IP 地址。或者，您可以前往 VPC 控制台 (https://console.aws.amazon.com/vpc/) 分配一个或多个新的弹性 IP 地址。这些地址可以归您所有，也可以归您所有。 Amazon 您无法将已在使用的弹性 IP 地址与您的端点相关联。

   c. （可选）对于自定义主机名，请选择以下选项之一：

> **Note**
>
> Amazon GovCloud (US) 需要直接通过弹性 IP 地址进行连接的客户，或者在商用 Route 53 中创建指向其 EIP 的主机名记录。有关将 Route 53 用于 GovCloud 终端节点的更多信息，请参阅Amazon GovCloud (US) 用户指南中的使用您的 Amazon GovCloud (US) 资源设置 Amazon Route 53。

- Amazon Route 53 DNS 别名— 如果要使用的主机名已注册到 Route 53。然后，您可以输入主机名。
- 其他 DNS— 如果要使用的主机名已注册到另一个 DNS 提供商。然后，您可以输入主机名。
- 无 — 使用服务器的端点，而不是使用自定义主机名。服务器主机名使用格式 *server-id*`.server.transfer.`*region*`.amazonaws.com`。

> **Note**
>
> 对于中的客户 Amazon GovCloud (US)，选择 “无” 不会以这种格式创建主机名。

要了解有关使用自定义主机名的更多信息，请参阅 使用自定义主机名。

d. 对于 VPC，选择现有 VPC ID 或选择创建 VPC 以创建新的 VPC。

e. 在可用区部分，最多选择三个可用区和关联的子网。对于IPv4地址，为每个子网选择一个弹性 IP 地址。这是您的客户端可用来允许在其防火墙中访问您的端点的 IP 地址。

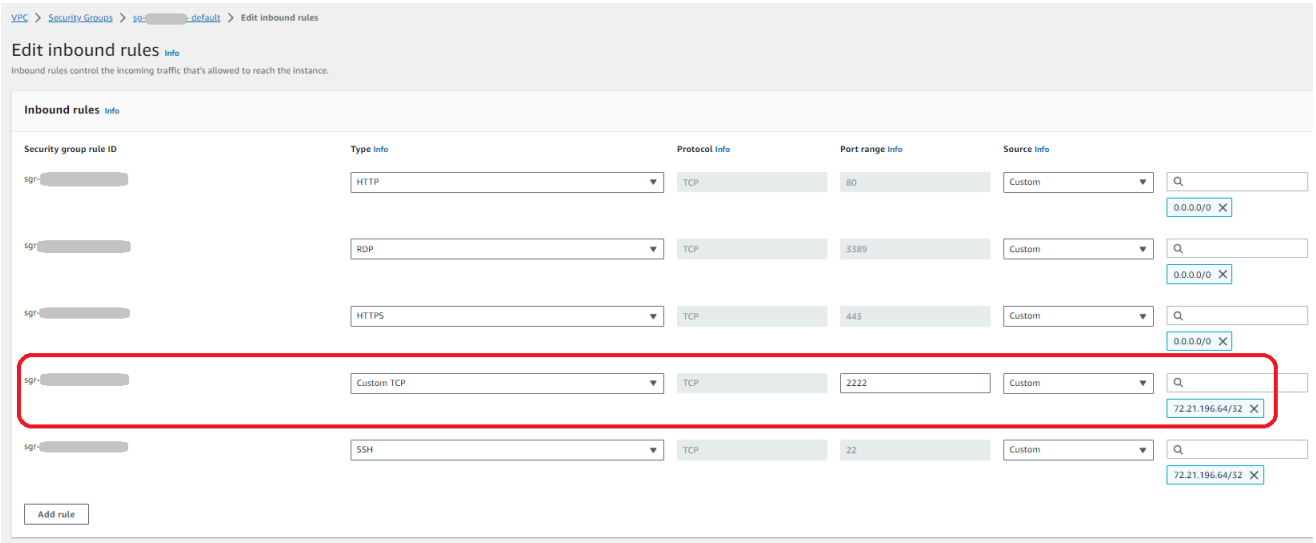
   提示：您必须为可用区使用公有子网，或者如果要使用私有子网，请先设置互联网网关。

f. 在 “安全组” 部分，选择现有安全组 ID IDs 或选择 “创建安全组” 来创建新的安全组。有关安全组的更多信息，请参阅 Amazon Virtual Private Cloud 用户指南中的 VPC 的安全组。要创建安全组，请参阅 Amazon Virtual Private Cloud 用户指南中的创建安全组。

> **Note**
>
> 您的 VPC 会自动带有默认的安全组。如果您在启动服务器时没有指定其他安全组或组，我们会将默认安全组与您的服务器相关联。

- 对于安全组的入站规则，您可以将 SSH 流量配置为使用端口 22、2222、22000 或任意组合。默认情况下，端口 22 已配置。要使用端口 2222 或端口 22000，您需要向安全组添加入站规则。对于类型，选择 “自定义 TCP”，然后在 “端口范围” 中输入**2222**或**22000**，对于源，输入与 SSH 端口 22 规则相同的 CIDR 范围。
- 对于安全组的入站规则，请将 FTPS 流量配置**21**为使用控制信道和数据通道**8192-8200**的端口范围。

> **Note**
>
> 对于需要 TCP “搭载” 的客户端，也可以使用端口 2223 ACKs，或者让 TCP 三向握手的最终确认也包含数据。
> 某些客户端软件可能与端口 2223 不兼容：例如，客户端要求服务器在客户端发送 SFTP 标识字符串之前发送 SFTP 标识字符串。



g. （可选）对于启用 FIPS，请选中启用 FIPS 的端点复选框以确保端点符合联邦信息处理标准 (FIPS)。

> **Note**
>
> 启用 FIPS 的端点仅在北美 Amazon 地区可用。有关可用区域，请参阅 Amazon Web Services 一般参考 中的 Amazon Transfer Family 端点和限额。有关 FIPS 的更多信息，请参阅联邦信息处理标准 (FIPS) 140-2。

h. 选择下一步。

6. 在配置其他详细信息中，执行以下操作：

a. 要进行CloudWatch 日志记录，请选择以下选项之一以启用 Amazon CloudWatch 记录您的用户活动：

- 创建一个新角色，允许 Transfer Family 自动创建 IAM 角色，前提是您拥有创建新角色的相应权限。创建的 IAM 角色被称为`AWSTransferLoggingAccess`。
- 选择现有角色以从您的帐户中选择现有 IAM 角色。在日志记录角色下，选择该角色。此 IAM 角色应包括将服务设置为 `transfer.amazonaws.com` 的信任策略。

  有关 CloudWatch 日志记录的更多信息，请参阅配置 CloudWatch 日志记录角色。

> **Note**
>
> - 如果您未指定日志记录角色， CloudWatch 则无法在中查看最终用户活动。
> - 如果您不想设置 CloudWatch 日志记录角色，请选择选择现有角色，但不要选择日志记录角色。

b. 对于加密算法选项，请选择包含允许服务器使用的加密算法的安全策略。

> **Note**
>
> 默认情况下，除非选择不同的服务器，否则 `TransferSecurityPolicy-2024-01` 安全策略将连接到服务器。

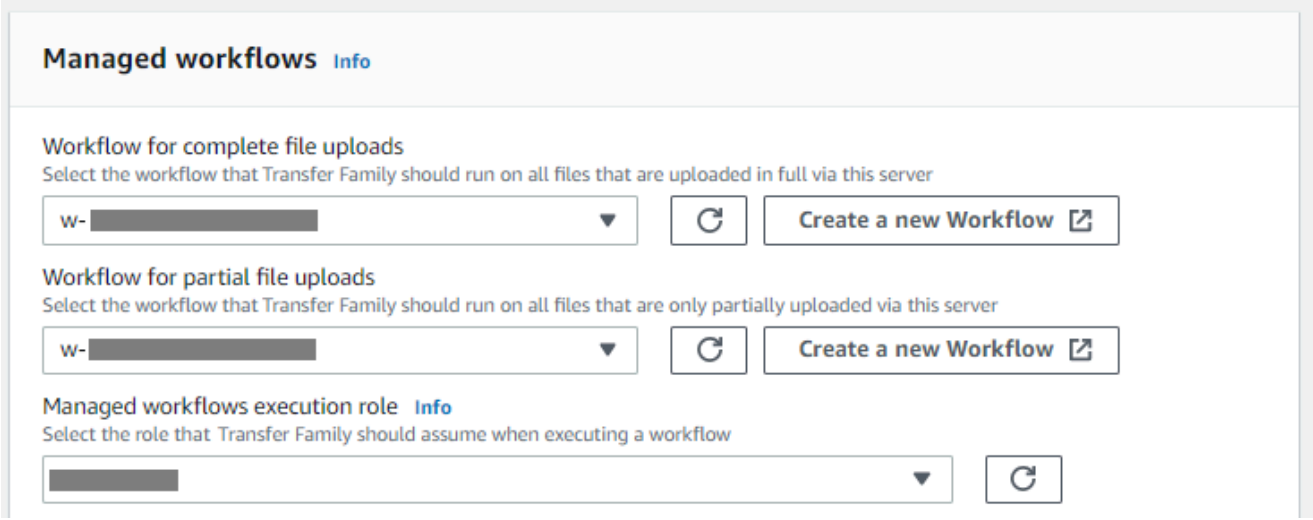
有关安全策略的更多信息，请参阅 Amazon Transfer Family 服务器的安全策略。

c. （可选：此部分仅适用于从启用 SFTP 的现有服务器迁移用户。）在服务器主机密钥中，输入一个 RSA ED25519、或 ECDSA 私钥，当客户端通过 SFTP 连接到服务器时，该私钥将用于识别您的服务器。

d. （可选）对于标签，在密钥和值中，输入一个或多个标签作为键值对，然后选择添加标签。

e. 选择下一步。

f. （可选）对于托管工作流程，选择 Tr IDs ansfer Family 在执行工作流程时应担任的工作流程（和相应的角色）。您可以选择一个工作流程在完成上传后执行，选择另一个工作流程在部分上传时执行。要了解有关使用托管工作流程处理文件的更多信息，请参阅 Amazon Transfer Family 托管工作流程。



7. 在审核和创建页面上，审核您的选择。如果您：

- 要编辑其中任何一个，请选择该步骤旁边的编辑。

> **Note**
>
> 在选择编辑的步骤之后，您将需要查看每个步骤。

- 如果没有更改，请选择创建服务器来创建您的服务器。您将转至如下所示的服务器页面，其中列出了您的新服务器。

您可以选择服务器 ID，以查看您已创建的服务器的详细设置。填充 “公共 IPv4 地址” 列后，您提供的弹性 IP 地址将成功关联到服务器的终端节点。

> **Note**
>
> 当 VPC 中的服务器处于联机状态时，只能通过 UpdateServerAPI 修改子网。必须停止服务器才能添加或更改服务器端点的弹性 IP 地址。

更改 SFTP 服务器的端点类型

如果您现有的服务器可通过互联网访问（即，具有公有端点类型），您可以将其端点更改为 VPC 端点。

> **Note**
>
> 如果您在 VPC 中有一台显示为 VPC_ENDPOINT 的现有服务器，建议您将其修改为新的 VPC 端点类型。有了这种新的端点类型，您就不再需要使用网络负载均衡器 (NLB) 将弹性 IP 地址与服务器的端点关联起来。此外，您还可以使用 VPC 安全组来限制对服务器端点的访问。不过，您可以按需继续使用 VPC_ENDPOINT 端点类型。

以下过程假设您具有使用当前公有端点类型或较旧 VPC_ENDPOINT 类型的服务器。

更改服务器的端点类型

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在导航窗格中，选择服务器。
3. 选中要更改其端点类型的服务器的复选框。

   > **Important**
   >
   > 您必须先停止服务器，然后才能更改其终端节点。

4. 对于操作，选择停止。
5. 在出现的确认对话框中，通过选择停止来确认您要停止服务器。

   > **Note**
   >
   > 在继续下一步之前，在端点详细信息中，等待服务器的状态更改为离线；这可能需要几分钟时间。您可能必须在服务器页面上选择刷新才能查看状态更改。

服务器离线之前，您无法进行任何编辑。

6. 在端点详细信息中，选择编辑。
7. 在编辑端点配置中，执行以下操作：

   a. 对于端点类型，选择 VPC 托管。

   b. 对于访问权限，请选择下列选项之一：

   - 内部，使您的端点只能由使用端点的私有 IP 地址的客户端访问。
   - 面向互联网，使客户端可以通过公共互联网访问您的端点。

   > **Note**
   >
   > 选择面向互联网时，可以在每个子网或多个子网中选择一个现有的弹性 IP 地址。或者，您可以前往 VPC 控制台 (https://console.aws.amazon.com/vpc/) 分配一个或多个新的弹性 IP 地址。这些地址可以归您所有，也可以归您所有。 Amazon 您无法将已在使用的弹性 IP 地址与您的端点相关联。

   c. （仅适用于面向互联网的访问权限是可选的）对于自定义主机名，请选择以下选项之一：

   - Amazon Route 53 DNS 别名— 如果要使用的主机名已注册到 Route 53。然后，您可以输入主机名。
   - 其他 DNS— 如果要使用的主机名已注册到另一个 DNS 提供商。然后，您可以输入主机名。
   - 无 — 使用服务器的端点，而不是使用自定义主机名。服务器主机名使用格式 *serverId*.server.transfer.*regionId*.amazonaws.com。

     要了解有关使用自定义主机名的更多信息，请参阅 使用自定义主机名。

   d. 对于 VPC，选择现有 VPC ID 或选择创建 VPC 以创建新的 VPC。

   e. 在可用区部分，最多选择三个可用区和关联的子网。如果选择面向互联网，则还要为每个子网选择一个弹性 IP 地址。

   > **Note**
   >
   > 如果您想要最多三个可用区，但可用区域不足，请在 VPC 控制台中创建它们（https://console.aws.amazon.com/vpc/）。

如果您修改子网或弹性 IP 地址，则服务器需要几分钟才能更新。在服务器更新完成之前，您无法保存更改。

f. 选择保存。

8. 在操作中，选择启动，然后等待服务器状态更改为在线；这可能需要几分钟。

> **Note**
>
> 如果您将公有端点类型更改为 VPC 端点类型，请注意您的服务器的端点类型已更改为 VPC。

默认安全组已附加到端点。要更改或添加其他安全组，请参阅创建安全组。

停止使用 VPC_ENDPOINT

Amazon Transfer Family 已停止使用新 Amazon 帐户创建服务器`EndpointType=VPC_ENDPOINT`的功能。自 2021 年 5 月 19 日起，不拥有终端节点类型为的 Amazon Transfer Family 服务器的 Amazon 账户`VPC_ENDPOINT`将无法使用创建新服务器`EndpointType=VPC_ENDPOINT`。如果您已经拥有使用该 `VPC_ENDPOINT` 端点类型的服务器，建议您 `EndpointType=VPC` 尽快开始使用。有关详细信息，请参阅将您的 Amazon Transfer Family 服务器终端节点类型从 VPC_ENDPOINT 更新为 VPC。

我们在 2020 年初推出了新的 VPC 端点类型。有关更多信息，请参阅 Amazon Transfer Family for SFTP 支持 VPC 安全组和弹性 IP 地址。这个新的端点功能更丰富，更具成本效益，而且不 PrivateLink 收费。有关更多信息，请参阅Amazon PrivateLink 定价。

此端点类型在功能上等同于以前的端点类型 (`VPC_ENDPOINT`)。您可以将弹性 IP 地址直接附加到端点，使其面向互联网，并使用安全组进行源 IP 筛选。有关更多信息，请参阅 “使用 IP 允许列表来保护您 Amazon Transfer Family 的 SFTP 服务器安全” 博客文章。

您也可以在共享 VPC 环境中托管此端点。有关更多信息，请参阅Amazon Transfer Family 现在支持共享服务 VPC 环境。

除了 SFTP 之外，您还可以使用 VPC `EndpointType` 来启用 FTPS 和 FTP。我们不打算将这些功能和 FTPS/FTP 支持添加到`EndpointType=VPC_ENDPOINT`。我们还从 Amazon Transfer Family 控制台中删除了此端点类型作为选项。

您可以使用 Transfer Family 控制台、 Amazon CLI SDKs、API 或更改服务器的终端节点类型 Amazon CloudFormation。要更改服务器的端点类型，请参阅 将 Amazon Transfer Family 服务器终端节点类型从 VPC_ENDPOINT 更新到 VPC。

如果您有任何疑问，请联系 Amazon Web Services 支持 或您的 Amazon 客户团队。

> **Note**
>
> 我们不打算在 EndpointType =VPC_ENDPOINT 中添加这些功能以及 FTPS 或 FTP 支持。我们不再在 Amazon Transfer Family 控制台上将其作为选项提供。

如果您还有其他问题，可以通过 Amazon Web Services 支持 或您的客户团队联系我们。

限制 Transfer Family 服务器的 VPC 终端节点访问权限

创建具有 VPC 终端节点类型的 Amazon Transfer Family 服务器时，您的 IAM 用户和委托人需要权限才能创建和删除 VPC 终端节点。但是，贵组织的安全策略可能会限制这些权限。您可以使用 IAM 策略允许专门为 Transfer Family 创建和删除 VPC 终端节点，同时保持对其他服务的限制。

> **Important**
>
> 以下 IAM 策略仅允许用户为 Transfer Family 服务器创建和删除 VPC 终端节点，同时拒绝对其他服务执行这些操作：

```
{
    "Effect": "Deny",
    "Action": [
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteVpcEndpoints"
    ],
    "Resource": ["*"],
    "Condition": {
        "ForAnyValue:StringNotLike": {
            "ec2:VpceServiceName": [
                "com.amazonaws.INPUT-YOUR-REGION.transfer.server.*"
            ]
        },
        "StringNotLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::*:role/INPUT-YOUR-ROLE"
            ]
        }
    }
```

```
}
```

*INPUT-YOUR-REGION*替换为您的 Amazon 区域（例如**us-east-1**）和*INPUT-YOUR-ROLE*您要向其授予这些权限的 IAM 角色。

其他联网功能

Amazon Transfer Family 提供了多项高级联网功能，可在使用 VPC 配置时增强安全性和灵活性：

- 共享 VPC 环境支持 ——您可以在共享 VPC 环境中托管 Transfer Family 服务器终端节点。有关更多信息，请参阅 VPCs 与共享中的使用 VPC 托管的终端节点 Amazon Transfer Family。
- 身份验证和安全-您可以使用 Amazon Web 应用程序防火墙来保护您的 Amazon API Gateway 终端节点。有关更多信息，请参阅Amazon Transfer Family 使用 Amazon Web 应用程序防火墙和 Amazon API Gateway 进行保护。

将 Amazon Transfer Family 服务器终端节点类型从 VPC_ENDPOINT 更新到 VPC

你可以使用 Amazon Web Services 管理控制台 Amazon CloudFormation、或 Transfer Family API 将服务器`EndpointType`从更新`VPC_ENDPOINT`为`VPC`。以下各部分提供了使用每种方法更新服务器端点类型的详细过程和示例。如果您在多个 Amazon 区域和多个 Amazon 账户中拥有服务器，则可以使用下一节中提供的示例脚本进行修改，使用需要更新的`VPC_ENDPOINT`类型来识别服务器。

主题

- 使用 VPC_ENDPOINT 端点类型识别服务器
- 使用更新服务器端点类型 Amazon Web Services 管理控制台
- 使用更新服务器端点类型 Amazon CloudFormation
- EndpointType 使用 API 更新服务器

使用 **VPC_ENDPOINT** 端点类型识别服务器

您可以使用 `VPC_ENDPOINT` 来识别哪些服务器正在使用 Amazon Web Services 管理控制台。

识别通过控制台使用 **VPC_ENDPOINT** 端点类型的服务器

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在导航窗格中选择服务器，显示该区域中您账户中的服务器列表。
3. 按端点类型对服务器列表进行排序，以查看所有使用 `VPC_ENDPOINT` 的服务器。

识别跨多个 **VPC_ENDPOINT** 区域和账户使用 Amazon 的服务器

如果您在多个 Amazon 区域和多个 Amazon 账户中拥有服务器，则可以使用以下示例脚本（经过修改）来识别使用VPC_ENDPOINT终端节点类型的服务器。示例脚本使用亚马逊 EC2 DescribeRegions和 Transfer Family ListServersAPI 操作。如果您有许多 Amazon 账户，如果您使用身份提供商的会话配置文件进行身份验证，则可以使用具有只读审计员访问权限的 IAM 角色遍历您的账户。

1. 以下是一个简单示例。

```
import boto3

profile = input("Enter the name of the Amazon account you'll be working in: ")
session = boto3.Session(profile_name=profile)

ec2 = session.client("ec2")

regions = ec2.describe_regions()

for region in regions['Regions']:
    region_name = region['RegionName']
    if region_name=='ap-northeast-3': #https://github.com/boto/boto3/issues/1943
        continue
    transfer = session.client("transfer", region_name=region_name)
    servers = transfer.list_servers()
    for server in servers['Servers']:
       if server['EndpointType']=='VPC_ENDPOINT':
           print(server['ServerId'], region_name)
```

2. 获得要更新的服务器列表后，您可以使用以下各部分中描述的方法之一将 EndpointType 更新为 VPC。

使用更新服务器端点类型 Amazon Web Services 管理控制台

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在导航窗格中，选择服务器。
3. 选中要更改其端点类型的服务器的复选框。

> **Important**
>
> 您必须先停止服务器，然后才能更改其终端节点。

4. 对于操作，选择停止。
5. 在出现的确认对话框中，通过选择停止来确认您要停止服务器。

> **Note**
>
> 在继续下一步之前，请等待服务器的状态变为离线；这可能需要几分钟。您可能必须在服务器页面上选择刷新才能查看状态更改。

6. 状态更改为离线后，选择服务器以显示服务器详细信息页面。
7. 在端点详细信息部分中，选择编辑。
8. 为端点类型选择 VPC 托管。
9. 选择保存
10. 在操作中，选择启动，然后等待服务器状态更改为在线；这可能需要几分钟。

使用更新服务器端点类型 Amazon CloudFormation

本节介绍 Amazon CloudFormation 如何使用将服务器更新`EndpointType`为`VPC`。对于使用部署的 Transfer Family 服务器，请使用此过程 Amazon CloudFormation。在此示例中，用于部署 Transfer Family 服务器的原始 Amazon CloudFormation 模板如下所示：

```
Amazon TemplateFormatVersion: '2010-09-09'
Description: 'Create Amazon Transfer Server with VPC_ENDPOINT endpoint type'
Parameters:
  SecurityGroupId:
    Type: Amazon::EC2::SecurityGroup::Id
  SubnetIds:
    Type: List<Amazon::EC2::Subnet::Id>
  VpcId:
    Type: Amazon::EC2::VPC::Id
Resources:
  TransferServer:
    Type: Amazon::Transfer::Server
    Properties:
      Domain: S3
```

```
      EndpointDetails:
        VpcEndpointId: !Ref VPCEndpoint
      EndpointType: VPC_ENDPOINT
      IdentityProviderType: SERVICE_MANAGED
      Protocols:
        - SFTP
  VPCEndpoint:
    Type: Amazon::EC2::VPCEndpoint
    Properties:
      ServiceName: com.amazonaws.us-east-1.transfer.server
      SecurityGroupIds:
        - !Ref SecurityGroupId
      SubnetIds:
        - !Select [0, !Ref SubnetIds]
        - !Select [1, !Ref SubnetIds]
        - !Select [2, !Ref SubnetIds]
      VpcEndpointType: Interface
      VpcId: !Ref VpcId
```

模板已更新，其中包含以下更改：

- EndpointType 已更改为 VPC。
- AWS::EC2::VPCEndpoint 资源已删除。
- SecurityGroupId、SubnetIds、和 VpcId 已移至EndpointDetails资源AWS::Transfer::Server部分，
- VpcEndpointId 的 EndpointDetails 属性已删除。

更新后的模板如下所示：

```
Amazon TemplateFormatVersion: '2010-09-09'
Description: 'Create Amazon Transfer Server with VPC endpoint type'
Parameters:
  SecurityGroupId:
    Type: Amazon::EC2::SecurityGroup::Id
  SubnetIds:
    Type: List<Amazon::EC2::Subnet::Id>
  VpcId:
    Type: Amazon::EC2::VPC::Id
Resources:
  TransferServer:
    Type: Amazon::Transfer::Server
```

```
    Properties:
      Domain: S3
      EndpointDetails:
        SecurityGroupIds:
          - !Ref SecurityGroupId
        SubnetIds:
          - !Select [0, !Ref SubnetIds]
          - !Select [1, !Ref SubnetIds]
          - !Select [2, !Ref SubnetIds]
        VpcId: !Ref VpcId
      EndpointType: VPC
      IdentityProviderType: SERVICE_MANAGED
      Protocols:
        - SFTP
```

更新使用部署的 Transfer Family 服务器的端点类型 Amazon CloudFormation

1. 使用以下步骤停止要更新的服务器。

   a. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。

   b. 在导航窗格中，选择服务器。

   c. 选中要更改其端点类型的服务器的复选框。

   > **Important**
   >
   > 您必须先停止服务器，然后才能更改其终端节点。

   d. 对于操作，选择停止。

   e. 在出现的确认对话框中，通过选择停止来确认您要停止服务器。

   > **Note**
   >
   > 在继续下一步之前，请等待服务器的状态变为离线；这可能需要几分钟。您可能必须在服务器页面上选择刷新才能查看状态更改。

2. 更新堆 CloudFormation 栈

   a. 在 https://console.aws.amazon.com/cloudformat ion 上打开 Amazon CloudFormation 控制台。

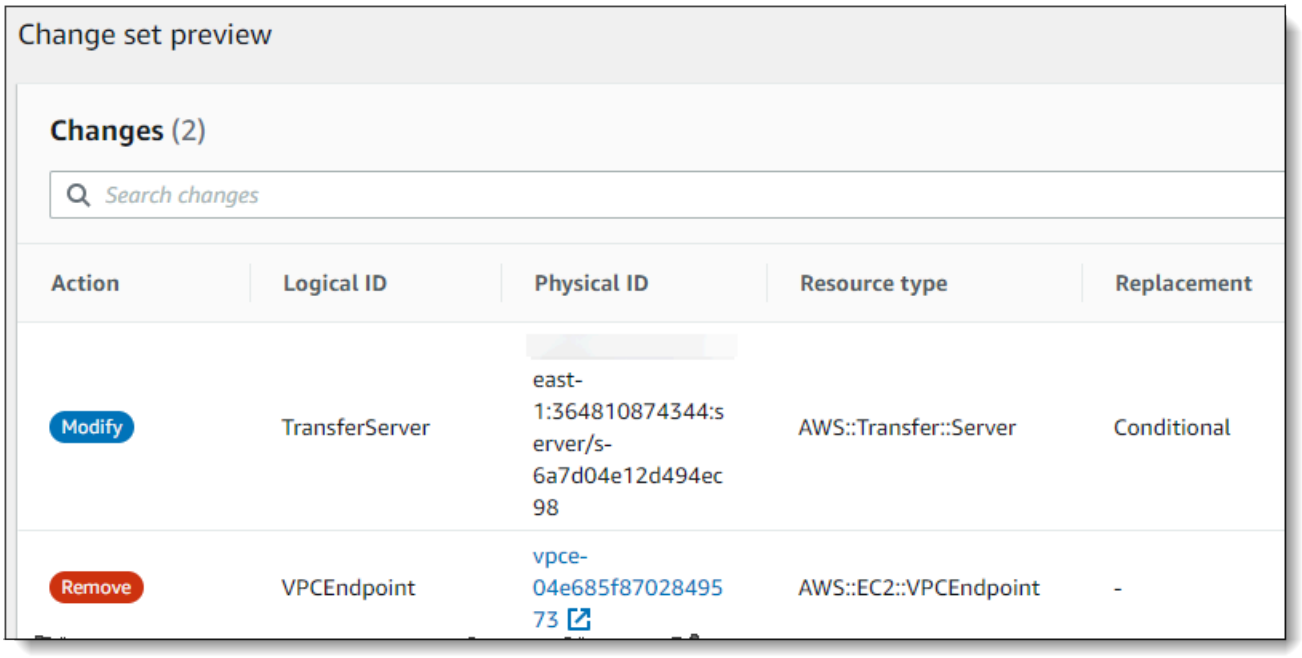
   b. 选择用于创建 Transfer Family 服务器的堆栈。

c. 选择更新。

d. 选择替换当前模板

e. 上传新模板。 CloudFormation 更改集可帮助您在实施模板更改之前了解模板更改将如何影响正在运行的资源。在此示例中，将修改传输服务器资源，并删除该 VPCEndpoint 资源。VPC 端点类型服务器代表您创建 VPC 端点，替换原始 `VPCEndpoint` 资源。

上传新模板后，更改集将与以下所示类似：



f. 更新堆栈。

3. 堆栈更新完成后，导航至 Transfer Family 管理控制台，网址为https://console.aws.amazon.com/transfer/。

4. 重新启动服务器。选择您更新的服务器 Amazon CloudFormation，然后从 “操作” 菜单中选择 “启动”。

EndpointType 使用 API 更新服务器

您可以使用 describe-server Amazon CLI 命令或 UpdateServer API 命令。以下示例脚本停止 Transfer Family 服务器、更新 EndpointType、移除 VPC_ENDPOINT 并启动服务器。

```
import boto3
import time

profile = input("Enter the name of the Amazon account you'll be working in: ")
```

```
region_name = input("Enter the Amazon Region you're working in: ")
server_id = input("Enter the Amazon Transfer Server Id: ")

session = boto3.Session(profile_name=profile)

ec2 = session.client("ec2", region_name=region_name)
transfer = session.client("transfer", region_name=region_name)

group_ids=[]

transfer_description = transfer.describe_server(ServerId=server_id)
if transfer_description['Server']['EndpointType']=='VPC_ENDPOINT':
    transfer_vpc_endpoint = transfer_description['Server']['EndpointDetails']
['VpcEndpointId']
    transfer_vpc_endpoint_descriptions =
 ec2.describe_vpc_endpoints(VpcEndpointIds=[transfer_vpc_endpoint])
    for transfer_vpc_endpoint_description in
 transfer_vpc_endpoint_descriptions['VpcEndpoints']:
        subnet_ids=transfer_vpc_endpoint_description['SubnetIds']
        group_id_list=transfer_vpc_endpoint_description['Groups']
        vpc_id=transfer_vpc_endpoint_description['VpcId']
        for group_id in group_id_list:
             group_ids.append(group_id['GroupId'])
   if transfer_description['Server']['State']=='ONLINE':
        transfer_stop = transfer.stop_server(ServerId=server_id)
        print(transfer_stop)
        time.sleep(300) #safe
        transfer_update =
 transfer.update_server(ServerId=server_id,EndpointType='VPC',EndpointDetails={'SecurityGroupId
        print(transfer_update)
        time.sleep(10)
        transfer_start = transfer.start_server(ServerId=server_id)
        print(transfer_start)
        delete_vpc_endpoint =
 ec2.delete_vpc_endpoints(VpcEndpointIds=[transfer_vpc_endpoint])
```

使用自定义主机名

服务器主机名是用户连接到服务器时在客户端中输入的主机名。使用时，您可以使用已注册的自定义域作为服务器主机名 Amazon Transfer Family。例如，您可以使用类似于 `mysftpserver.mysubdomain.domain.com` 的自定义主机名。

要将流量从注册的自定义域重定向到您的服务器端点，您可以使用 Amazon Route 53 或任何域名系统 (DNS) 提供商。Route 53 是 Amazon Transfer Family 原生支持的 DNS 服务。

主题

- 使用 Amazon Route 53 作为 DNS 提供商
- 使用其他 DNS 提供商
- 非控制台创建的服务器的自定义主机名

在控制台上，您可以选择下列选项之一来设置自定义主机名：

- Amazon Route 53 DNS 别名— 如果要使用的主机名已注册到 Route 53。然后，您可以输入主机名。
- 其他 DNS— 如果要使用的主机名已注册到另一个 DNS 提供商。然后，您可以输入主机名。
- 无 — 使用服务器的端点，而不是使用自定义主机名。

在创建新的服务器或编辑现有服务器的配置时设置此选项。有关创建新的服务器的更多信息，请参阅步骤 2：创建启用 SFTP 的服务器。有关编辑现有服务器配置的更多信息，请参阅 编辑服务器详细信息。

有关使用自己的域作为服务器主机名以及如何 Amazon Transfer Family 使用 Route 53 的更多详细信息，请参阅以下各节。

使用 Amazon Route 53 作为 DNS 提供商

当您创建服务器时，您可以使用 Amazon Route 53 作为您的 DNS 提供程序。在将一个域用于 Route 53 之前，请先注册该域。有关更多信息，请参阅 Amazon Route 53 开发人员指南中的域注册工作原理。

当您使用 Route 53 为服务器提供 DNS 路由时，会 Amazon Transfer Family 使用您输入的自定义主机名来提取其托管区域。 Amazon Transfer Family 提取托管区域时，可能会发生三种情况：

1. 如果您是 Route 53 的新手并且没有托管区域，请 Amazon Transfer Family 添加新的托管区域和CNAME记录。此 CNAME 记录的值为服务器的端点主机名。CNAME 为备用域名。
2. 如果您在 Route 53 中有一个不带任何 CNAME 记录的托管区域，则 Amazon Transfer Family 会向该托管区域添加一条 CNAME 记录。
3. 如果服务检测到该托管区域中已有一条 CNAME 记录，则会显示一个错误，指示 CNAME 记录已存在。在此情况下，请将 CNAME 记录的值更改为服务器的主机名。

有关 Route 53 中托管区域的更多信息，请参阅 Amazon Route 53 开发人员指南中的托管区域。

使用其他 DNS 提供商

在创建服务器时，您还可以使用 Amazon Route 53 之外的 DNS 提供商。如果您使用替代 DNS 提供商，请确保域中的流量被定向到服务器端点。

为此，请将域设置为服务器的端点主机名。

- 对于 IPv4 端点，控制台中的主机名如下所示：

  serverid.server.transfer.*region*.amazonaws.com

- 对于双栈端点，主机名在控制台中如下所示：

  serverid.transfer-server.*region*.on.aws

> **Note**
>
> 如果您的服务器有 VPC 终端节点，则主机名的格式与上述格式不同。要查找您的 VPC 端点，请在服务器的详细信息页面上选择 VPC，然后在 VPC 控制面板上选择 VPC 端点 ID。端点是列出的第一个 DNS 名称。

非控制台创建的服务器的自定义主机名

使用 Amazon Cloud Development Kit (Amazon CDK) Amazon CloudFormation、或 CLI 创建服务器时，如果您希望该服务器具有自定义主机名，则必须添加标记。当您使用控制台创建 Transfer Family 服务器时，会自动完成标记。

> **Note**
>
> 您还需要创建 DNS 记录，以将流量从您的域名重定向到服务器端点。有关详细信息，请参阅《Amazon Route 53 开发者指南》中的处理记录。

使用以下密钥作为您的自定义主机名：

- 添加 `transfer:customHostname` 以在控制台中显示自定义主机名。

- 如果您使用 Route 53 作为 DNS 提供商，请添加 `transfer:route53HostedZoneId`。此标签将自定义主机名链接到您的 Route 53 托管区 ID。

要添加自定义主机名，请发出以下 CLI 命令。

```
aws transfer tag-resource --arn arn:aws:transfer:region:Amazon Web Services #
#:server/server-ID --tags Key=transfer:customHostname,Value="custom-host-name"
```

例如：

```
aws transfer tag-resource --arn arn:aws:transfer:us-east-1:111122223333:server/
s-1234567890abcdef0 --tags Key=transfer:customHostname,Value="abc.example.com"
```

如果您使用的是 Route 53，请发出以下命令将您的自定义主机名链接到您的 Route 53 托管区 ID。

```
aws transfer tag-resource --arn server-ARN:server/server-ID --tags
 Key=transfer:route53HostedZoneId,Value=HOSTED-ZONE-ID
```

例如：

```
aws transfer tag-resource --arn arn:aws:transfer:us-east-1:111122223333:server/
s-1234567890abcdef0 --tags Key=transfer:route53HostedZoneId,Value=ABCDE1111222233334444
```

假设上一个命令中的示例值，运行以下命令来查看标签：

```
aws transfer list-tags-for-resource --arn arn:aws:transfer:us-
east-1:111122223333:server/s-1234567890abcdef0
```

```
"Tags": [
   {
      "Key": "transfer:route53HostedZoneId",
      "Value": "/hostedzone/ABCDE1111222233334444"
   },
   {
      "Key": "transfer:customHostname",
      "Value": "abc.example.com"
   }
 ]
```

> **Note**
>
> 您的公共、托管区域及其 IDs 在 Amazon Route 53 上可用。
> 登录 Amazon Web Services 管理控制台 并打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。

FTP 和 FTPS 网络负载均衡器注意事项

尽管我们建议避免在 Amazon Transfer Family 服务器前面使用网络负载均衡器，但如果您的 FTP 或 FTPS 实施需要在客户端的通信路由中使用 NLB 或 NAT，请遵循以下建议：

- 对于 NLB，请使用端口 21 而不是端口 8192-8200 进行运行状况检查。
- 对于 Amazon Transfer Family 服务器，通过设置启用 TLS 会话恢复`TlsSessionResumptionMode = ENFORCED`。

  > **Note**
  >
  > 这是推荐的模式，因为它提供了增强的安全性：
  >
  > - 要求客户端在后续连接中使用 TLS 会话恢复。
  > - 通过确保一致的加密参数来提供更强的安全保障。
  > - 有助于防止潜在的降级攻击。
  > - 在优化性能的同时保持对安全标准的合规性。

- 如果可能，请停止使用 NLB，以充分利用 Amazon Transfer Family 性能和连接限制。

有关 NLB 替代方案的更多指导，请通过 Amazon Support 联系 Amazon Transfer Family 产品管理团队。有关改善安全状况的更多信息，请参阅博客文章《提高 Amazon Transfer Family 服务器安全性的六个技巧》。

中提供了安全指南避免将服务器放在 NLBs Amazon Transfer Family 服务器前面 NATs 。 NLBs

使用客户端通过服务器端点传输文件

通过在客户端中指定传输操作，您可以通过 Amazon Transfer Family 服务传输文件。 Amazon Transfer Family 支持以下客户端：

- 我们支持 SFTP 协议的第 3 版。
- OpenSSH (macOS 和 Linux)

> **Note**
>
> 此客户端仅适用于启用了 Secure Shell (SSH) 文件传输协议 (SFTP) 的服务器。

- WinSCP（仅 Microsoft Windows）
- Cyberduck（Windows、macOS 和 Linux）
- FileZilla （Windows、macOS 和 Linux）

以下限制适用于每个客户端：

- 不支持 SCP 协议，因为它被认为是不安全的。您可以按中所述使用 OpenSSH `scp` 命令。使用 scp 命令
- 每个连接的并发、多路复用、SFTP 会话的最大数量为 10。
- 对于空闲连接，所有协议 () 的超时值均为 1800 秒（30 分钟SFTP/FTP/FTPS）。如果在此期间之后没有任何活动，则客户端可能会断开连接。对于无响应的连接：
  - 当客户端完全无响应时，SFTP 会有 300 秒（5 分钟）的超时时间。
  - FTPS 和 FTP 有大约 10 分钟的无响应超时，由底层库处理。
- 亚马逊 S3 和 Amazon EFS（由于 NFSv4 协议）要求文件名采用 UTF-8 编码。使用不同的编码可能会导致意想不到的结果。对于 Amazon S3，请参阅对象密钥命名指南。
- 对于 安全文件传输协议 (FTPS)，仅支持显式模式。不支持隐式模式。
- 对于文件传输协议 (FTP) 和 FTPS，仅支持被动模式。
- 对于 FTP 和 FTPS，仅支持流模式。
- 对于 FTP 和 FTPS，仅支持 Image/Binary 模式。
- 对于 FTP 和 FTPS，数据连接的 TLS-PROT C（未受保护）TLS 是默认值，但是 Amazon Transfer Family FTPS 协议不支持端口 C。因此，对于 FTPS，您需要发出 PROT P，您的数据操作才能被接受。
- 如果您使用 Amazon S3 作为服务器存储，并且您的客户端包含使用多个连接进行单次传输的选项，请务必禁用该选项。否则，上传大文件可能会突然失败。请注意，如果您使用 Amazon EFS 作为存储后端，EFS 确实支持多个连接进行单次传输。

以下是 FTP 和 FTPS 的可用命令列表：

可用命令					
ABOR	FEAT	MLST	PASS	RETR	STOR
AUTH	LANG	MKD	PASV	RMD	STOU
CDUP	LIST	MODE	PBSZ	RNFR	STRU
CWD	MDTM	NLST	PROT	RNTO	SYST
DELE	MFMT	NOOP	PWD	SIZE	TYPE
EPSV	MLSD	OPTS	QUIT	STAT	USER

> **Note**
>
> 不支持 APPE。

对于 SFTP，目前不支持在使用 Amazon Elastic File System (Amazon EFS) 的服务器上使用逻辑主目录的用户执行以下操作。

SFTP 命令不受支持			
SSH_FXP_READLINK	SSH_FXP_SYMLINK	SSH_FXP_STAT（当请求的文件是符号链接时）	SSH_FXP_REALPATH（当请求的路径包含任何符号链接组件时）

生成公有-私有密钥对

在传输文件之前，必须有可用的公有-私有密钥对。如果您之前没有生成过密钥对，请参阅 为服务托管用户生成 SSH 密钥。

主题

- 可用SFTP/FTPS/FTP命令
- 查找您的 Amazon VPC 端点

- 避免 setstat 错误
- 使用 OpenSSH
- 使用 WinSCP
- 使用 Cyberduck
- 使用 FileZilla
- 使用 Perl 客户端
- 使用 LFTP
- 上传后处理
- SFTP 消息

可用SFTP/FTPS/FTP命令

下表描述了 SFTP Amazon Transfer Family、FTPS 和 FTP 协议的可用命令。

> **Note**
>
> 该表提到了仅支持存储桶和对象的 Amazon S3 的文件和目录：无层次结构。但是，您可以在对象键名称中使用前缀来暗示层次结构，并以类似于文件夹的方式组织数据。Amazon Simple Storage Service 用户指南中的使用对象元数据中描述了该行为。

SFTP/FTPS/FTP 命令

命令	Amazon S3	Amazon EFS
`cd`	支持	支持
`chgrp`	不支持	支持（仅 `root` 或 `owner`）
`chmod`	不支持	支持（仅 `root`）
`chmtime`	不支持	支持
`chown`	不支持	支持（仅 `root`）
`get`	支持	支持（包括解析符号链接）

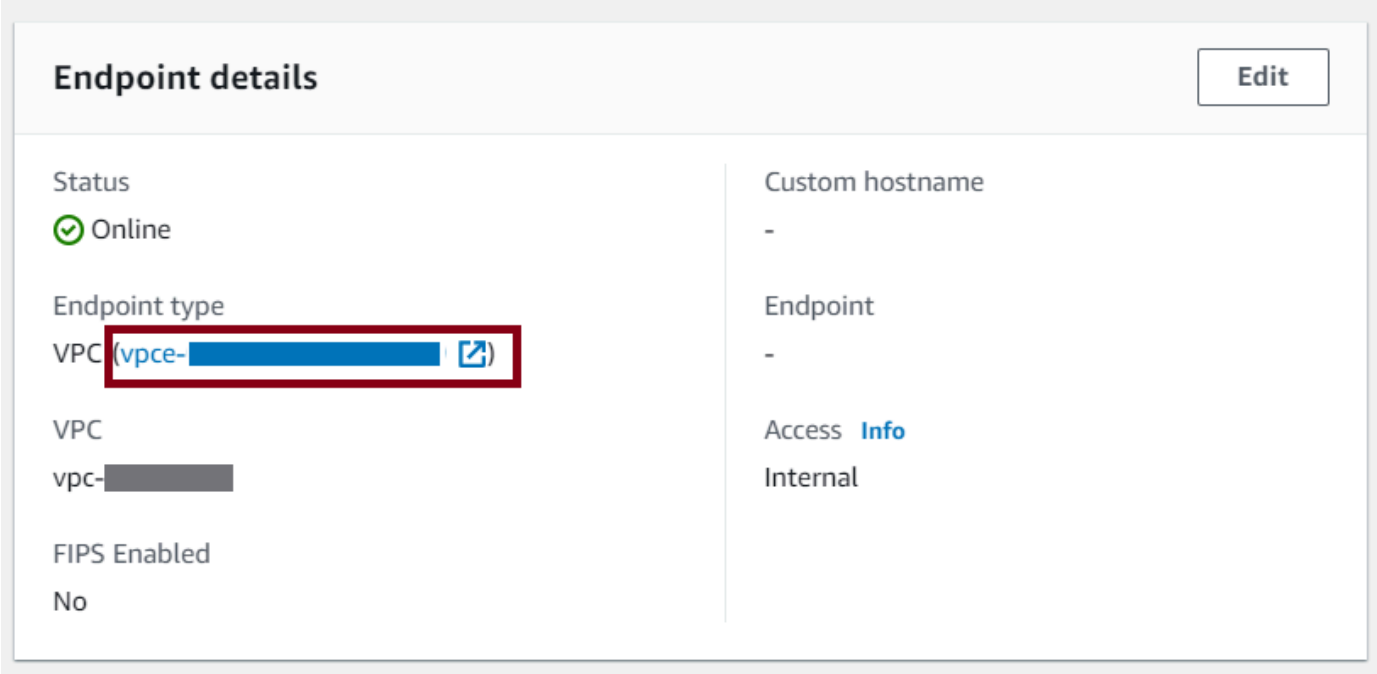
命令	Amazon S3	Amazon EFS
`ln -s`	不支持	支持
`ls/dir`	支持	支持
`mkdir`	支持	支持
`put`	支持	支持
`pwd`	支持	支持
`rename`	仅支持文件 **Note** 不支持会覆盖现有文件的重命名。	支持 **Note** 不支持会覆盖现有文件或目录的重命名。
`rm`	支持	支持
`rmdir`	支持（仅限空目录）	支持
`version`	支持	支持

查找您的 Amazon VPC 端点

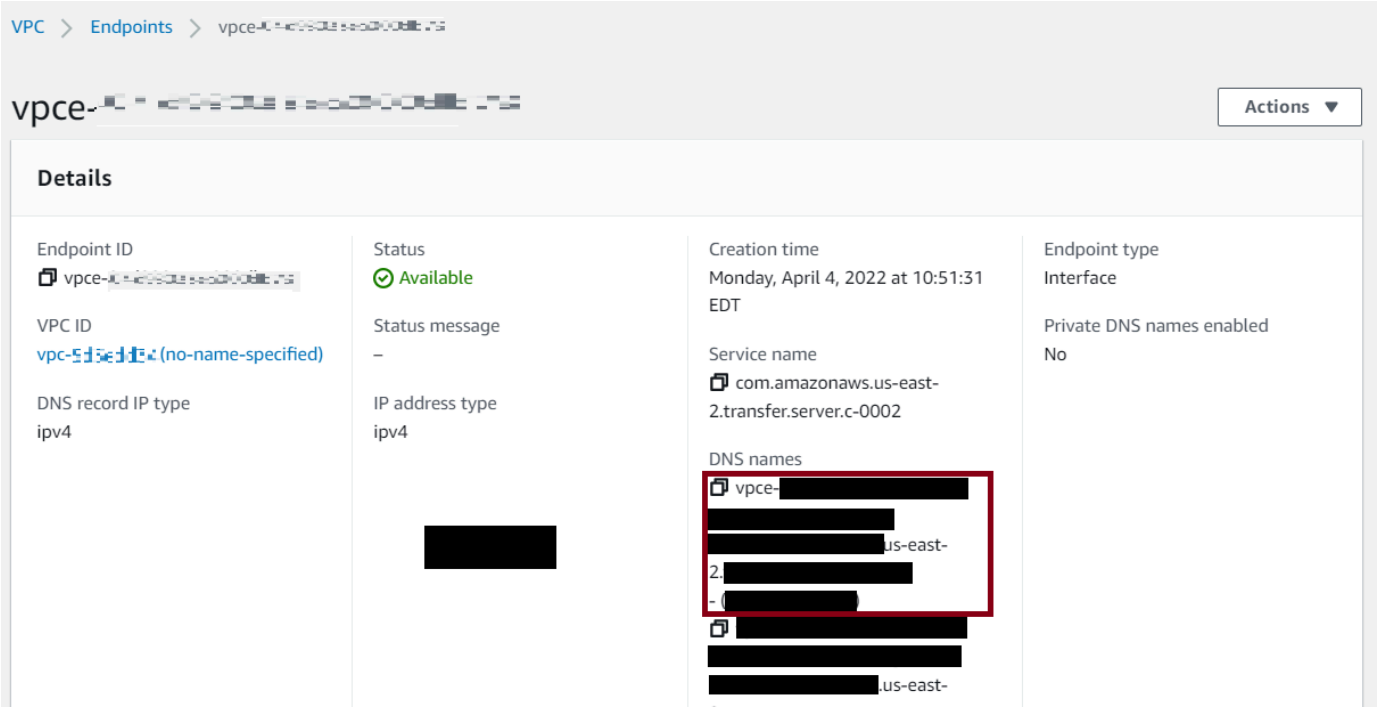
如果您的 Transfer Family 服务器的端点类型是 VPC，则识别用于传输文件的端点并不简单。在这种情况下，使用以下过程查找您的 Amazon VPC 端点。

查找您的亚马逊 VPC 终端节点

1. 导航到您的服务器详细信息页面。
2. 在端点详细信息窗格中，选择 VPC。



3. 在 Amazon VPC 控制面板中，选择 VPC 端点 ID。
4. 在 DNS 名称列表中，您的服务器端点是第一个列出的端点。



避免 setstat 错误

一些 SFTP 文件传输客户端可以在上传文件时尝试使用命令（例如 SETSTAT）更改远程文件的属性，包括时间戳和权限。但是，这些命令与 Amazon S3 等对象存储系统不兼容。由于这种不兼容性，即使文件以其他方式成功上传，从这些客户端上传文件也可能导致错误。

- 当您调用 `CreateServer` 或 `UpdateServer` API 时，使用 `ProtocolDetails` 选项 `SetStatOption` 可以忽略当客户端尝试对要上传到 S3 存储桶的文件使用 SETSTAT 时生成的错误。
- 将该值设置为 `ENABLE_NO_OP` 以使 Transfer Family 服务器忽略 SETSTAT 命令，并上传文件而无需对您的 SFTP 客户端进行任何更改。
- 请注意，虽然该`SetStatOption``ENABLE_NO_OP`设置忽略了错误，但它确实会在日志中 CloudWatch 生成一个日志条目，因此您可以确定客户端何时进行 SETSTAT 调用。

有关此选项的 API 详细信息，请参阅ProtocolDetails。

使用 OpenSSH

本节包含使用 OpenSSH 从命令行传输文件的说明。

> **Note**
>
> 此客户端仅适用于启用 SFTP 的服务器。

主题

- 使用 OpenSSH
- 使用 scp 命令

使用 OpenSSH

Amazon Transfer Family 使用 OpenSSH 命令行实用程序传输文件

1. 在 Linux、macOS 或 Windows 上，打开命令终端。
2. 在提示符中，输入以下命令：

```
sftp -i transfer-key sftp_user@service_endpoint
```

在前面的命令中，*sftp_user* 是用户名，*transfer-key* 是 SSH 私有密钥。此处*service_endpoint*是服务器的终端节点，如所选服务器的 Amazon Transfer Family 控制台中所示。

> **Note**
>
> 此命令使用默认ssh_config文件中的设置。除非您之前编辑过此文件，否则 SFTP 使用端口 22。您可以通过在命令中添加**-P**标志来指定其他端口（例如 2222），如下所示。
>
> ```
> sftp -P 2222 -i transfer-key sftp_user@service_endpoint
> ```
>
> 或者，如果您一直想使用端口 2222 或端口 22000，则可以更新文件中的ssh_config默认端口。

此时应显示 sftp 提示符。

3. （可选）要查看用户的主目录，请在 sftp 提示符下输入以下命令：

   ```
   pwd
   ```

4. 要将文件从您的文件系统上传到 Transfer Family 服务器，请使用 put 命令。例如，要上传 hello.txt（假设该文件位于文件系统的当前目录中），请在 sftp 提示符下运行以下命令：

   ```
   put hello.txt
   ```

   此时将显示类似于下文的消息，指示文件传输正在进行或者已完成。

   ```
   Uploading hello.txt to /amzn-s3-demo-bucket/home/sftp_user/hello.txt

   hello.txt 100% 127 0.1KB/s 00:00
   ```

> **Note**
>
> 在您的服务器创建之后，环境中的 DNS 服务可能需要几分钟时间才能解析服务器端点主机名。

使用 scp 命令

Transfer Family 不支持 SCP 协议。但是，如果您需要此功能，则可以使用 OpenSSH `scp` 命令。

通过 SFTP 使用 SCP 的建议是使用 OpenSSH 版本 9.0 或更高版本。在 OpenSSH 版本 9 及更高版本中，该`scp`命令默认使用 SFTP 协议进行文件传输，而不是传统的 SCP 协议。

> **Important**
>
> 确保您的 Transfer Family 服务器已配置为使用 S3 优化的目录访问权限。

使用 WinSCP

按照下文中的说明，使用 WinSCP 从命令行传输文件。

> **Note**
>
> 如果您使用的是 WinSCP 5.19，则可以使用您的证书和文件直接连接到 Amazon S3。Amazon upload/download 有关更多详细信息，请参阅连接到 Amazon S3 服务。

Amazon Transfer Family 使用 WinSCP 传输文件

1. 打开 WinSCP 客户端。
2. 在登录对话框中，为文件协议选择一个协议：SFTP 或 FTP。

   如果您选择了加密，请选择下列选项之一：

   - FTP 没有加密
   - 适用于 FTPS 的 TLS/SSL 显式加密
3. 对于主机名，输入您的服务器端点。服务器端点位于服务器详细信息页面。有关更多信息，请参阅查看 SFTP、FTPS 和 FTP 服务器的详细信息。

   如果您的服务器使用 VPC 端点，请参阅 查找您的 Amazon VPC 端点。
4. 在端口号中，输入以下内容：

   - 适用于 SFTP 的 **22**
   - 适用于 FTP/FTPS 的 **21**

5. 在用户名中，输入您为特定身份提供商创建的用户名称。

   提示：用户名应是您为身份提供商创建或配置的用户之一。 Amazon Transfer Family 提供以下身份提供商：

   - 与服务托管用户合作
   - 使用微软 Active Directory 的 Amazon 目录服务
   - 使用自定义身份提供程序
6. 选择高级打开高级站点设置对话框。在 SSH 部分中，选择身份验证。
7. 对于私有密钥文件，从文件系统中浏览并选择 SSH 私有密钥文件。

   如果 WinSCP 提供将 SSH 私有密钥转换为 PPK 格式，请选择确定。
8. 选择确定以返回到登录对话框，然后选择保存。
9. 在将会话保存为站点对话框中，选择确定以完成您的连接设置。
10. 在登录对话框中，选择工具，然后选择首选项。
11. 在首选项对话框中的传输中，选择耐力。

    对于 “允许传输 resume/transfer 到临时文件名” 选项，选择 “禁用”。

    > **Important**
    >
    > 如果您启用此选项，则会增加上传成本，从而显著降低上传性能。它还可能导致大文件上传失败。
12. 对于传输，选择背景，然后清除使用多个连接进行单次传输复选框。

    提示：如果选择此选项，则上传大文件可能会以不可预知的方式失败。例如，可以创建会产生 Amazon S3 费用的孤立分段上传。还可能发生静默数据损坏。
13. 执行文件传输。

    您可以使用 drag-and-drop方法在目标窗口和源窗口之间复制文件。在 WinSCP 中，您可以使用工具栏图标来上传、下载、删除、编辑或修改文件的属性。

> **Note**
>
> 如果您使用 Amazon EFS 进行存储，则本说明不适用。

尝试更改远程文件属性（包括时间戳）的命令与 Amazon S3 等对象存储系统不兼容。因此，如果您使用 Amazon S3 进行存储，请务必在执行文件传输之前禁用 WinSCP 时间戳设置（或按 SetStatOption 中所述使用 避免 setstat 错误）。为此，请在 WinSCP 传输设置对话框中，禁用设置权限上传选项和保留时间戳常用选项。

使用 Cyberduck

按照下文中的说明，使用 Cyberduck 从命令行传输文件。

Amazon Transfer Family 使用 Cyberduck 传输文件

1. 打开 Cyberduck 客户端。
2. 选择打开连接。
3. 在打开连接对话框中，选择协议：SFTP（SSH 文件传输协议）、FTP-SSL（显式身份验证 TLS）或 FTP（文件传输协议）。
4. 对于服务器，输入您的服务器端点。服务器端点位于服务器详细信息页面。有关更多信息，请参阅查看 SFTP、FTPS 和 FTP 服务器的详细信息。

   如果您的服务器使用 VPC 端点，请参阅 查找您的 Amazon VPC 端点。
5. 在端口号中，输入以下内容：

   - 适用于 SFTP 的 **22**
   - 适用于 FTP/FTPS 的 **21**
6. 对于用户名，输入您在管理服务器端点的用户中创建的用户的名称。
7. 如果选择了 SFTP，则在 SSH 私有密钥中，选择或输入 SSH 私有密钥。
8. 选择连接。
9. 执行文件传输。

   根据您的文件所在的位置，执行以下操作之一：

   - 在您的本地目录（源）中，选择您要传输的文件，然后将这些文件拖放到 Amazon S3 目录（目标）中。
   - 在 Amazon S3 目录（源）中，选择您要传输的文件，然后将这些文件拖放到您的本地目录（目标）中。

使用 FileZilla

按照以下说明使用传输文件 FileZilla。

设置 FileZilla 文件传输

1. 打开 FileZilla 客户端。
2. 选择文件，然后选择站点管理器。
3. 在站点管理器对话框中，选择新建站点。
4. 在常规选项卡的协议中选择一个协议：SFTP 或 FTP。

   如果您选择了加密，请选择下列选项之一：

   - 仅使用纯 FTP（不安全）— 用于 FTP
   - 使用 TLS 上的显式 FTP（如果可用）— 用于 FTPS
5. 在主机名中，输入您正在使用的协议，然后输入您的服务器端点。服务器端点位于服务器详细信息页面。有关更多信息，请参阅 查看 SFTP、FTPS 和 FTP 服务器的详细信息。

   - 如果您使用的是 SFTP，请输入：`sftp://`*`hostname`*
   - 如果您使用的是 FTPS，请输入：`ftps://`*`hostname`*

   请务必*`hostname`*替换为实际的服务器端点。

   如果您的服务器使用 VPC 端点，请参阅 查找您的 Amazon VPC 端点。
6. 在端口号中，输入以下内容：

   - 适用于 SFTP 的 **22**
   - 适用于 FTP/FTPS 的 **21**
7. 如果选择了 SFTP，则选择密钥文件作为登录类型。

   对于密钥文件，选择或输入 SSH 私有密钥。
8. 对于用户名，输入您在 管理服务器端点的用户 中创建的用户的名称。
9. 选择连接。
10. 执行文件传输。

> **Note**
>
> 如果您中断正在进行的文件传输， Amazon Transfer Family 可能会在您的 Amazon S3 存储桶中写入部分对象。如果您中断上传，在继续之前，请检查 Amazon S3 存储桶中文件大小是否与源对象的文件大小相符。

使用 Perl 客户端

如果您使用 NET::SFTP::Foreign perl 客户端，则必须将设置queue_size为。1例如：

```
my $sftp = Net::SFTP::Foreign->new('user@s-12345.server.transfer.us-east-2.amazonaws.com', queue_size => 1);
```

> **Note**
>
> 1.92.02 之前的 Net::SFTP::Foreign 修订版本需要使用此解决方法。

使用 LFTP

LFTP 是一个免费的 FTP 客户端，它允许用户通过命令行界面从大多数 Linux 计算机上执行文件传输。

对于大文件下载，LFTP 存在已知的乱序数据包问题，导致文件传输失败。

上传后处理

您可以查看上传后的处理信息，包括 Amazon S3 对象元数据和事件通知。

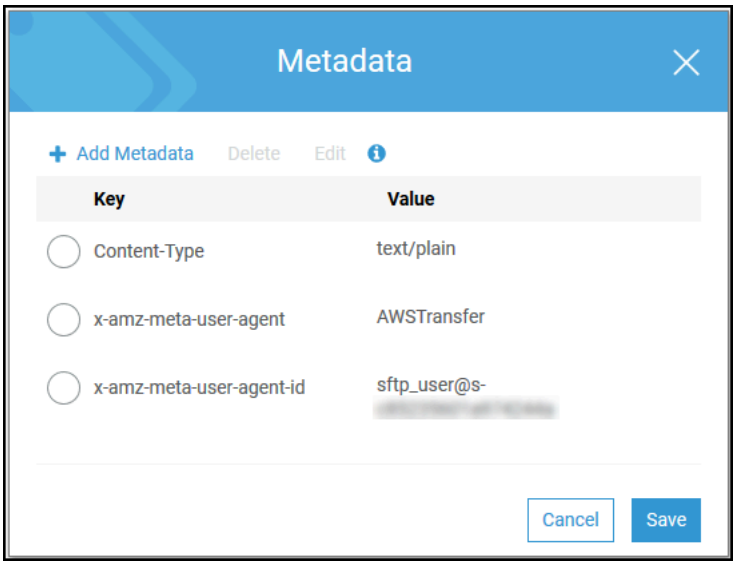
主题

- Amazon S3 对象元数据
- Amazon S3 事件通知

Amazon S3 对象元数据

作为对象元数据的一部分，您会看到一个名为 x-amz-meta-user-agent 的密钥，其值为 AWSTransfer，x-amz-meta-user-agent-id 的值为 username@server-id。username 是上

传文件的 Transfer Family 用户，`server-id` 也是用于上传的服务器。可以使用对 Lambda 函数中的 S3 对象进行HeadObject操作来访问这些信息。



Amazon S3 事件通知

当使用 Transfer Family 将对象上传到您的 S3 存储桶时，`RoleSessionName` 作为 `[AWS:Role Unique Identifier]/username.sessionid@server-id` 包含在 S3 事件通知结构的请求者字段中。例如，以下是来自 S3 访问权限日志的、用于复制到 S3 存储桶中的请求者字段示例内容。

```
arn:aws:sts::AWS-Account-ID:assumed-role/IamRoleName/
username.sessionid@server-id
```

在上述中请求者字段中，它显示了名为 `IamRoleName` 的 IAM 角色。有关配置 S3 事件通知的更多信息，请参阅 Amazon Simple Storage Service 开发人员指南中的配置 Amazon S3 事件通知。有关 Amazon Identity and Access Management (IAM) 角色唯一标识符的更多信息，请参阅Amazon Identity and Access Management 用户指南中的唯一标识符。

SFTP 消息

本节介绍使用 Transfer Family 服务器时，您在传输 SFTP 文件期间或之后可能收到的客户端消息。有关任何 SFTP 事件的更多信息，请查看您的 SFTP 客户端日志。您可以使用该信息对任何错误进行故障排除，也可以将该信息转发给您的网络团队，以帮助他们识别问题。

SFTP 客户端消息

Activity	描述
身份验证失败	用户身份验证失败。这可能是来自自定义身份提供商或服务托管用户的任何类型的故障。事件中的详细信息有助于阐明失败的根本原因。
CLOSE	表示已成功关闭打开的文件或目录。
已连接/已断开	表示正常连接成功和断开连接。
创建符号链接	符号链接已创建（成功或失败）。
DELETE	文件已删除（成功或失败）。
ERROR	一个一般的、意想不到的错误。相关的描述包含可以帮助您或您的网络管理员识别具体问题的信息。
退出原因	当意外错误导致您的 SFTP 会话终止时发出。与事件关联的消息描述了原因。
MKDIR	目录已创建（成功或失败）。
OPEN	已打开文件进行读取或写入（成功或失败）
部分关闭	当文件仍处于打开状态但未收到 CLOSE 消息时，客户端与服务器断开了连接。Transfer Family 存储文件中收到的部分（实际上可能是完整的文件），并发出 PARTIAL_CLOSE 事件以提醒客户注意问题。工作流集成还会收到一个`onPartialClose` 事件，以适当地处理文件。
RENAME	文件已重命名（成功或失败）
RMDIR	目录已删除（成功或失败）
SETSTAT	文件的属性已更改（成功或失败）。

Activity	描述
	Note 如果你使用亚马逊 S3 进行存储，Transfer Family 不支持 SETSTAT。本避免 setstat 错误节详细介绍了如何通过关闭设置来避免SetStat错误。这样可以避免你收到fail unsupported error：相反，你会收到success but do nothing消息。
TLS_恢复失败	服务器配置为强制执行 TLS 会话恢复，但客户端不支持。

管理服务器端点的用户

在以下各节中，您可以找到有关如何使用 Amazon Transfer Family Amazon Directory Service for Microsoft Active Directory 或自定义身份提供商添加用户的信息。

作为各个用户属性的一部分，您还可以存储该用户的安全外壳 (SSH) 公有密钥。基于密钥的身份验证需要这样做。私有密钥存储在您用户的计算机本地。当用户使用客户端发送身份验证请求到服务器时，您的服务器首先确认用户具有关联 SSH 私有密钥的访问权限。然后，服务器成功验证用户身份。

Note

有关自动部署和管理拥有多个 SSH 密钥的用户，请参阅Transfer Family terraform 模块。

此外，您指定用户的主目录或登录目录，并将 Amazon Identity and Access Management IAM 角色分配给用户。或者，您可以提供一个会话策略来限制用户仅访问 AmazonS3 存储桶的主目录。

Important

Amazon Transfer Family 阻止长度为 1 或 2 个字符的用户名向 SFTP 服务器进行身份验证。此外，我们还屏蔽了 root 用户名。
其背后的原因是密码扫描器进行了大量的恶意登录尝试。

Amazon EFS 与 Amazon S3

每种存储选项的特点：

- 限制访问权限：Amazon S3 支持会话策略；Amazon EFS 支持 POSIX 用户、群组和辅助群组 IDs
- 两者都支持 public/private 按键
- 两者都支持主目录
- 两者都支持逻辑目录

> **Note**
>
> 对于 Amazon S3，对逻辑目录的大部分支持是通过 API/CLI 实现的。您可以使用控制台中的受限复选框将用户锁定至其主目录，但不能指定虚拟目录结构。

逻辑目录

如果要为用户指定逻辑目录值，则使用的参数取决于用户的类型。

- 对于服务托管的用户，请在 `HomeDirectoryMappings` 中提供逻辑目录值。
- 对于自定义身份提供商用户，请在中提供逻辑目录值`HomeDirectoryDetails`。

Amazon Transfer Family 支持在使用 LO HomeDirectory GICAL 时指定值 HomeDirectoryType。这适用于响应中提供的服务托管用户、Active Directory 访问权限和自定义身份提供 HomeDirectoryDetails 者实现。

> **Important**
>
> HomeDirectory 使用 LOGICAL 指定 a 时 HomeDirectoryType，该值必须映射到您的一个逻辑目录映射。该服务在用户创建和更新过程中都会对此进行验证，以防止配置失效。

默认 行为

默认情况下，如果未指定， HomeDirectory 则逻辑模式将设置为 “/”。此行为保持不变，并且与现有用户定义保持兼容。

- 确保将您的映射 HomeDirectory 到条目而不是目标。有关更多详细信息，请参阅使用逻辑目录的规则。
- 有关虚拟目录结构的详细信息，请参阅虚拟目录结构。

自定义身份提供商注意事项

使用自定义身份提供程序时，您现在可以在使用 LOGICA HomeDirectory L 的同时在响应中指定 HomeDirectoryType。当自定义 IDP 在逻辑模式下指定时， TestIdentityProvider API 调用将生成正确的结果。 HomeDirectory

带有 HomeDirectory 和逻辑 HomeDirectoryType的自定义 IDP 响应示例：

```
{
  "Role": "arn:aws:iam::123456789012:role/transfer-user-role",
  "HomeDirectoryType": "LOGICAL",
  "HomeDirectory": "/marketing",
  "HomeDirectoryDetails": "[{\"Entry\":\"/\",\"Target\":\"/bucket/home\"},{\"Entry\":
\"/marketing\",\"Target\":\"/marketing-bucket/campaigns\"}]"
}
```

活动目录组配额

Amazon Transfer Family 默认限制为每台服务器 100 个 Active Directory 组。如果您的用例需要超过 100 个群组，请考虑使用自定义身份提供商解决方案，如使用自定义身份提供商简化 Active Directory 身份验证中所述 Amazon Transfer Family。

此限制适用于使用以下身份提供商的服务器：

- Amazon 微软 Active Directory 的目录服务
- Amazon 适用于 Entra ID 域服务的目录服务

如果您需要申请提高服务限制，请参阅中的Amazon Web Services 服务 配额Amazon Web Services 一般参考。如果您的用例需要超过 100 个群组，请考虑使用自定义身份提供商解决方案，如使用自定义身份提供商简化 Active Directory 身份验证中所述 Amazon Transfer Family。

有关 Active Directory 组限制的疑难解答信息，请参阅已超出活动目录组限制。

主题

- 与服务托管用户合作
- 使用自定义身份提供程序
- 使用微软 Active Directory 的 Amazon 目录服务
- 将 Amazon Directory Service 用于 Entra ID 域服务

与服务托管用户合作

您可以将 Amazon S3 或 Amazon EFS 服务托管用户添加到您的服务器，具体取决于服务器的域设置。有关更多信息，请参阅 配置 SFTP、FTPS 或 FTP 服务器端点。

如果您使用服务托管身份类型，则将用户添加到您启用文件传输协议的服务器。在执行此操作时，服务器上的各个用户名必须唯一。

要以编程方式添加服务管理用户，请参阅 AP I 示例。CreateUser

> **Note**
>
> 对于服务管理的用户，逻辑目录条目的限制为 2,000 个。有关使用逻辑目录的信息，请参见使用逻辑目录简化您的 Transfer Family 目录结构。

主题

- 添加 Amazon S3 服务托管用户
- 添加 Amazon EFS 服务托管用户
- 管理服务托管用户

添加 Amazon S3 服务托管用户

> **Note**
>
> 如果要配置跨账户 Amazon S3 存储桶，请按照知识中心文章中提到的步骤进行操作：如何将 Amazon Transfer Family 服务器配置为使用其他 Amazon 账户中的 Amazon 简单存储服务存储桶？ 。

将 Amazon S3 服务托管用户添加至您的服务器

1. 打开 Amazon Transfer Family 控制台 https://console.aws.amazon.com/transfer/，然后从导航窗格中选择 “服务器”。
2. 在服务器页面上，选中您要将用户添加到的服务器复选框。
3. 选择添加用户。
4. 在用户配置部分的用户名中，输入用户名。此用户名长度最少为 3 个字符，最多为 100 个字符。你可以在用户名中使用以下字符：a—z、A-Z、0—9、下划线 '_'、连字符 '-'、句点 '.' 和 at 符号 '@'。用户名不能以连字符 “-”、“句点” 或 “@” 开头。
5. 对于访问权限，选择您之前创建的提供对 Amazon S3 存储桶访问权限的 IAM 角色。

   您可使用创建 IAM 角色和策略中的过程创建此 IAM 角色。该 IAM 角色包括一个提供对您 Amazon S3 存储桶访问权限的 IAM policy。它还包括与 Amazon Transfer Family 服务的信任关系，该关系在另一个 IAM 策略中定义。如果您需要对用户进行精细的访问控制，请参阅使用Amazon Transfer Family 和 Amazon S3 增强数据访问控制博客文章。
6. （可选）对于策略，选择下列选项之一：

   - 无
   - 现有策略
   - 从 IAM 中选择策略：允许您选择现有的会话策略。选择查看以查看包含策略详细信息的 JSON 对象。
   - 基于主文件夹自动生成策略：为您生成会话策略。选择查看以查看包含策略详细信息的 JSON 对象。

   > **Note**
   >
   > 如果选择基于主文件夹自动生成策略，请不要为此用户选择受限。

   要了解有关会话策略的更多信息，请参阅创建 IAM 角色和策略为 Amazon S3 存储桶创建会话策略、或动态权限管理方法。
7. 对于主目录，选择用于存储要传输的数据的 Amazon S3 存储桶 Amazon Transfer Family。输入用户在使用其客户端登录时转到的 home 目录的路径。

   如果您将此参数留空，则使用 Amazon S3 存储桶的 `root` 目录。在这种情况下，请确保您的 IAM 角色提供对此 `root` 目录的访问权限。

> **Note**
>
> 我们建议您选择包含用户的用户名的目录路径，这使得您可以更高效地使用会话策略。会话策略将用户在 Amazon S3 存储桶中的访问权限限制为该用户的 home 目录。

8. （可选）对于受限，选中该复选框，这样您的用户就无法访问该文件夹之外的任何内容，也看不到 Amazon S3 存储桶或文件夹名称。

> **Note**
>
> 为用户分配主目录并限制用户访问该主目录应该足以锁定用户对指定文件夹的访问权限。如果您需要应用进一步的控制措施，请使用会话策略。
> 如果您为此用户选择受限，则无法选择基于主文件夹自动生成策略，因为主文件夹不是为受限用户定义的值。

9. 对于 SSH 公有密钥，输入 SSH 密钥对的 SSH 公有密钥部分。

   您的密钥先由服务进行验证，然后才能添加新用户。

> **Note**
>
> 有关如何生成 SSH 密钥对的说明，请参阅 为服务托管用户生成 SSH 密钥。

10. （可选）对于键和值，输入一个或多个标记作为键-值对，然后选择添加标记。
11. 选择 Add (添加) 可将您的新用户添加到所选服务器。

    新用户将出现在服务器详细信息页面的用户部分。

后续步骤 — 对于下一步，请继续前往 使用客户端通过服务器端点传输文件。

添加 Amazon EFS 服务托管用户

Amazon EFS 使用便携式操作系统接口 (POSIX) 文件权限模型来表示文件所有权。

- 有关 Amazon EFS 文件所有权的更多详细信息，请参阅 Amazon EFS 文件所有权。
- 有关为 EFS 用户设置目录的更多详细信息，请参阅 为 Transfer Family 设置 Amazon EFS 用户。

将 Amazon EFS 服务托管用户添加至您的服务器

1. 打开 Amazon Transfer Family 控制台 https://console.aws.amazon.com/transfer/，然后从导航窗格中选择 “服务器”。
2. 在服务器页面上，选择要向其添加用户的 Amazon EFS 服务器。
3. 选择添加用户以显示添加用户页面。
4. 在用户配置部分中，使用以下设置。

   a. 此用户名长度最少为 3 个字符，最多为 100 个字符。您可以在用户名中使用以下字符：a–z、A-Z、0–9、下划线“_”、连字符“-”、句点“.”和“@”符号。用户名不能以连字符“-”、句点“.”或“@”符号开头。

   b. 对于用户 ID 和组 ID，请注意以下几点：

      - 对于您创建的第一个用户，我们建议您为组 ID 和用户 ID 输入一个值 **0**。这将授予用户使用 Amazon EFS 的管理员权限。
      - 对于其他用户，请输入用户的 POSIX 用户 ID 和组 ID。 IDs 它们用于用户执行的所有 Amazon Elastic File System 操作。
      - 对于用户 ID 和组 ID，请勿使用任何前导零。例如，可以接受 **12345**，但不能接受 **012345**。

   c. （可选）对于辅助组 IDs，为每个用户输入一个或多个其他 POSIX 组 IDs ，用逗号分隔。

   d. 对于访问权限，请选择符合以下条件的 IAM 角色：

      - 仅允许用户访问您希望他们访问的 Amazon EFS 资源（文件系统）。
      - 定义用户可以执行哪些文件系统操作和不能执行哪些文件系统操作。

      我们建议您使用具有挂载访问 read/write 权限和权限的 Amazon EFS 文件系统选择的 IAM 角色。例如，以下两个 Amazon 托管策略的组合虽然相当宽松，但可以为您的用户授予必要的权限：

      - AmazonElasticFileSystemClientFullAccess
      - AWSTransferConsoleFullAccess

      有关更多信息，请参阅 Amazon Transfer Family 对 Amazon Elastic File System 的支持博客文章。

   e. 对于主目录，请执行以下操作：

- 选择您希望用于存储使用 Amazon Transfer Family传输的数据的 Amazon EFS 文件系统。
- 决定是否将主目录设置为受限。将主目录设置为受限会产生以下影响：
  - Amazon EFS 用户无法访问该文件夹之外的任何文件或目录。
  - Amazon EFS 用户看不到 Amazon EFS 文件系统名称 (fs-xxxxxxx)。

  > **Note**
  >
  > 当您选择受限选项时，符号链接无法为 Amazon EFS 用户解析。

- （可选）输入您希望用户在使用客户端登录时进入的主目录路径。

  如果您未指定主目录，则使用您的 Amazon EFS 文件系统的根目录。在这种情况下，请确保您的 IAM 角色提供对此根目录的访问权限。

5. 对于 SSH 公有密钥，输入 SSH 密钥对的 SSH 公有密钥部分。

   您的密钥先由服务进行验证，然后才能添加新用户。

   > **Note**
   >
   > 有关如何生成 SSH 密钥对的说明，请参阅 为服务托管用户生成 SSH 密钥。

6. （可选）为用户输入任何标签。对于键和值，输入一个或多个标记作为键-值对，然后选择添加标记。
7. 选择 Add (添加) 可将您的新用户添加到所选服务器。

   新用户将出现在服务器详细信息页面的用户部分。

首次通过 SFTP 连接到 Transfer Family 服务器时可能会遇到的问题：

- 如果您运行 `sftp` 命令但提示符未出现，则可能会遇到以下消息：

  ```
  Couldn't canonicalize: Permission denied

  Need cwd
  ```

  在这种情况下，您必须增加用户角色的策略权限。您可以添加 Amazon 托管策略，例如`AmazonElasticFileSystemClientFullAccess`。

- 如果您在sftp提示pwd时输入查看用户的主目录，则可能会看到以下消息，其中*USER-HOME-DIRECTORY*是 SFTP 用户的主目录：

  ```
  remote readdir("/USER-HOME-DIRECTORY"): No such file or directory
  ```

  在这种情况下，您应该能够导航到父目录 (`cd ..`)，并创建用户的主目录 (`mkdir username`)。

后续步骤 — 对于下一步，请继续前往 使用客户端通过服务器端点传输文件。

管理服务托管用户

在本部分中，您可以找到有关如何查看用户列表、如何编辑用户详细信息以及如何添加 SSH 公有密钥的信息。

- 查看用户列表
- 查看或编辑用户详细信息
- 删除用户
- 添加 SSH 公钥
- 删除 SSH 公钥

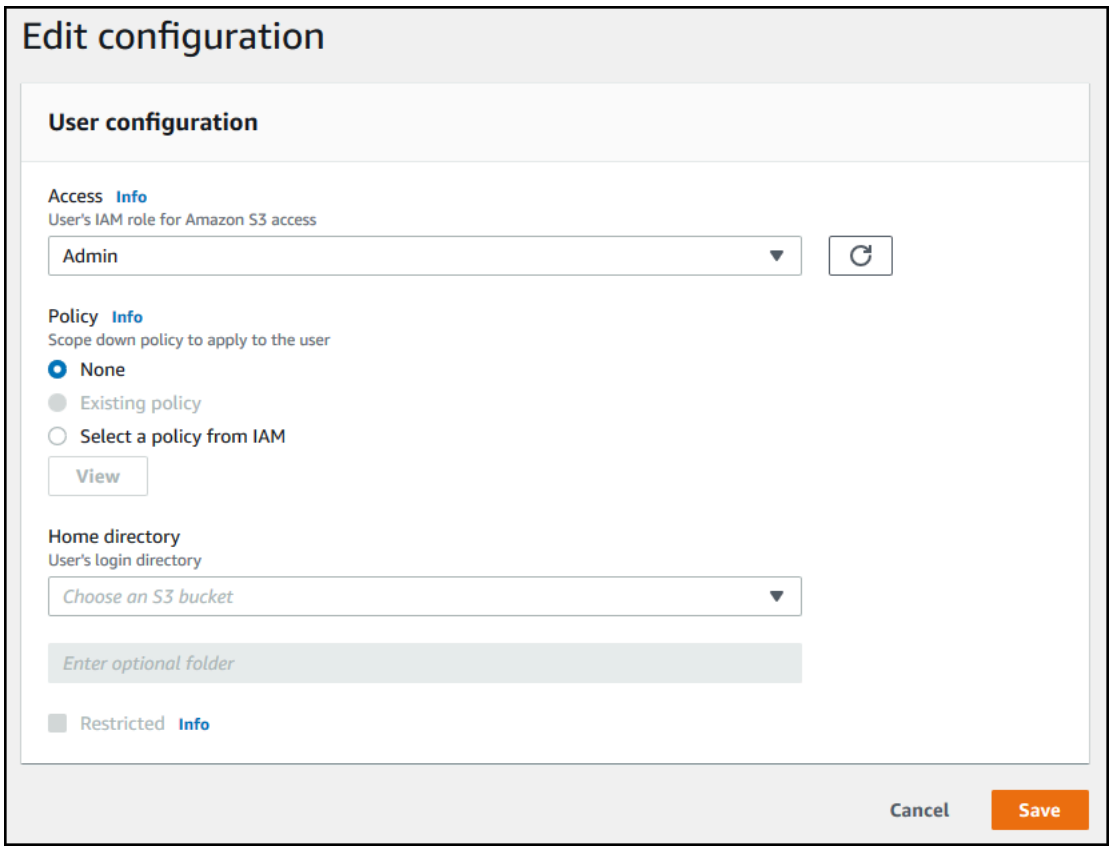
查找您的用户列表

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 从导航窗格中选择服务器以显示服务器页面。
3. 选择服务器 ID 列中的标识符以查看服务器详细信息页面。
4. 在用户下，查看用户列表。

要查看或编辑用户详细信息

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 从导航窗格中选择服务器以显示服务器页面。
3. 选择服务器 ID 列中的标识符以查看服务器详细信息页面。
4. 在用户下，选择一个用户名以查看用户详细信息页面。

   您可以通过选择编辑来更改该页面上的用户属性。
5. 在用户详细信息页面上，选择用户配置旁边的编辑。



6. 在编辑配置页面上的访问权限，选择您之前创建的 IAM 角色，该角色提供对您的 Amazon S3 存储桶的访问权限。

   您可使用创建 IAM 角色和策略中的过程创建此 IAM 角色。该 IAM 角色包括一个提供对您 Amazon S3 存储桶访问权限的 IAM policy。它还包括与 Amazon Transfer Family 服务的信任关系，该关系在另一个 IAM 策略中定义。

7. （可选）对于策略，请选择以下选项之一：

   - 无
   - 现有策略
   - 从 IAM 中选择策略以选择现有策略。选择查看以查看包含策略详细信息的 JSON 对象。

   要了解有关会话策略的更多信息，请参阅 创建 IAM 角色和策略。要了解有关创建会话策略的更多信息，请参阅 为 Amazon S3 存储桶创建会话策略。

8. 对于主目录，选择用于存储要传输的数据的 Amazon S3 存储桶 Amazon Transfer Family。输入用户在使用其客户端登录时转到的 home 目录的路径。

如果您将此参数留空，则使用 Amazon S3 存储桶的 `root` 目录。在这种情况下，请确保您的 IAM 角色提供对此 `root` 目录的访问权限。

> **Note**
>
> 我们建议您选择包含用户的用户名的目录路径，这使得您可以更高效地使用会话策略。会话策略将用户在 Amazon S3 存储桶中的访问权限限制为该用户的 home 目录。

9. （可选）对于受限，选中该复选框，这样您的用户就无法访问该文件夹之外的任何内容，也看不到 Amazon S3 存储桶或文件夹名称。

> **Note**
>
> 当为用户分配主目录并限制用户访问该主目录时，这应该足以锁定用户对指定文件夹的访问权限。当您需要应用进一步的控制措施，请使用会话策略。

10. 选择 保存 以保存您的更改。

删除用户

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 从导航窗格中选择服务器以显示服务器页面。
3. 选择服务器 ID 列中的标识符以查看服务器详细信息页面。
4. 在用户下，选择一个用户名以查看用户详细信息页面。
5. 在用户详细信息页面上，选择用户名右侧的删除。
6. 在显示的确认对话框中，输入单词 **`delete`**，然后选择删除以确认您要删除该用户。

将从用户列表中删除该用户。

为用户添加 SSH 公钥

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在导航窗格中，选择服务器。
3. 选择服务器 ID 列中的标识符以查看服务器详细信息页面。
4. 在用户下，选择一个用户名以查看用户详细信息页面。

5. 选择 Add SSH public key (添加 SSH 公有密钥) 以向用户添加新的 SSH 公有密钥。

> **Note**
>
> SSH 密钥仅由启用 Secure Shell (SSH) 文件传输协议 (SFTP) 的服务器使用。有关如何生成 SSH 密钥对的信息，请参阅 为服务托管用户生成 SSH 密钥。

6. 对于 SSH public key (SSH 公有密钥)，输入 SSH 密钥对的 SSH 公有密钥部分。

   您的密钥先由服务进行验证，然后才能添加新用户。SSH 密钥的格式为 `ssh-rsa string`。要生成 SSH 密钥对，请参阅 为服务托管用户生成 SSH 密钥。

7. 选择添加密钥。

删除用户的 SSH 公钥

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在导航窗格中，选择服务器。
3. 选择服务器 ID 列中的标识符以查看服务器详细信息页面。
4. 在用户下，选择一个用户名以查看用户详细信息页面。
5. 要删除公钥，请选中其 SSH 密钥复选框并选择删除。

使用自定义身份提供程序

Amazon Transfer Family 为自定义身份提供商提供了多种选项，用于对用户进行身份验证和授权，以实现安全的文件传输。以下是主要方法：

- 自定义身份提供商解决方案— 本主题使用中托管的工具包介绍 Transfer Family 自定义身份提供商解决方案。 GitHub

> **Note**
>
> 对于大多数用例，这是推荐的选项。具体而言，如果您需要支持 100 个以上的 Active Directory 群组，则自定义身份提供商解决方案可提供不受群组限制的可扩展替代方案。此解决方案在博客文章《使用自定义身份提供商简化 Active Directory 身份验证》中进行了介绍 Amazon Transfer Family。

- 使用 Amazon API Gateway 整合您的身份提供程序— 本主题介绍如何使用 Amazon Lambda 函数支持 Amazon API Gateway 方法。

  您可以使用单个 Amazon API Gateway 方法提供 RESTful 接口。Transfer Family 调用此方法连接到您的身份提供程序，该提供程序会对您的用户进行身份验证和授权，使其能够访问 Amazon S3 或 Amazon EFS。如果您需要一个 RESTful API 来集成您的身份提供商，或者想要利用其功能来处理地理封锁或速率限制请求，请使用 Amazon WAF 此选项。有关更多信息，请参阅 使用 Amazon API Gateway 整合您的身份提供程序。
- 动态权限管理方法— 本主题介绍使用会话策略动态管理用户权限的方法。

  要对您的用户进行身份验证，可以将现有的身份提供程序与 Amazon Transfer Family一同使用。您可以使用 Amazon Lambda 函数集成您的身份提供程序，该函数会对您的用户进行身份验证和授权，使其能够访问 Amazon S3 或 Amazon Elastic File System (Amazon EFS)。有关更多信息，请参阅 Amazon Lambda 用于整合您的身份提供商。您还可以访问 Amazon Transfer Family 管理控制台中传输的文件数和字节数等指标的 CloudWatch 图表，从而通过单一控制面板使用集中式仪表板监控文件传输。
- Transfer Family 提供了一篇博客文章和一个研讨会，引导你完成文件传输解决方案的构建。该解决方案利用托管 SFTP/FTPS 终端节点 Amazon Transfer Family ，利用 Amazon Cognito 和 DynamoDB 进行用户管理。

  该博客文章可在使用 Amazon Cognito 作为身份提供商 Amazon Transfer Family 和 Amazon S3 上找到。您可以在此处查看研讨会的详细信息。

> **Note**
>
> 对于自定义身份提供商，用户名必须至少为 3 个字符，最多 100 个字符。你可以在用户名中使用以下字符：a—z、A-Z、0—9、下划线 '_'、连字符 '-'、句点 '.' 和 at 符号 '@'。用户名不能以连字符 “-”、“句点” 或 “@” 开头。

在实现自定义身份提供商时，请考虑以下最佳实践：

- 将解决方案部署在与 Trans Amazon Web Services 账户 fer Family 服务器相同的区域。
- 在配置 IAM 角色和策略时实施最低权限原则。
- 使用 IP 允许名单和标准化日志记录等功能来增强安全性。
- 部署之前，请在非生产环境中彻底测试您的自定义身份提供商。

主题

- 自定义身份提供商解决方案
- Amazon Lambda 用于整合您的身份提供商
- 使用 Amazon API Gateway 整合您的身份提供程序
- 使用多种身份验证方法
- IPv6 支持自定义身份提供商

自定义身份提供商解决方案

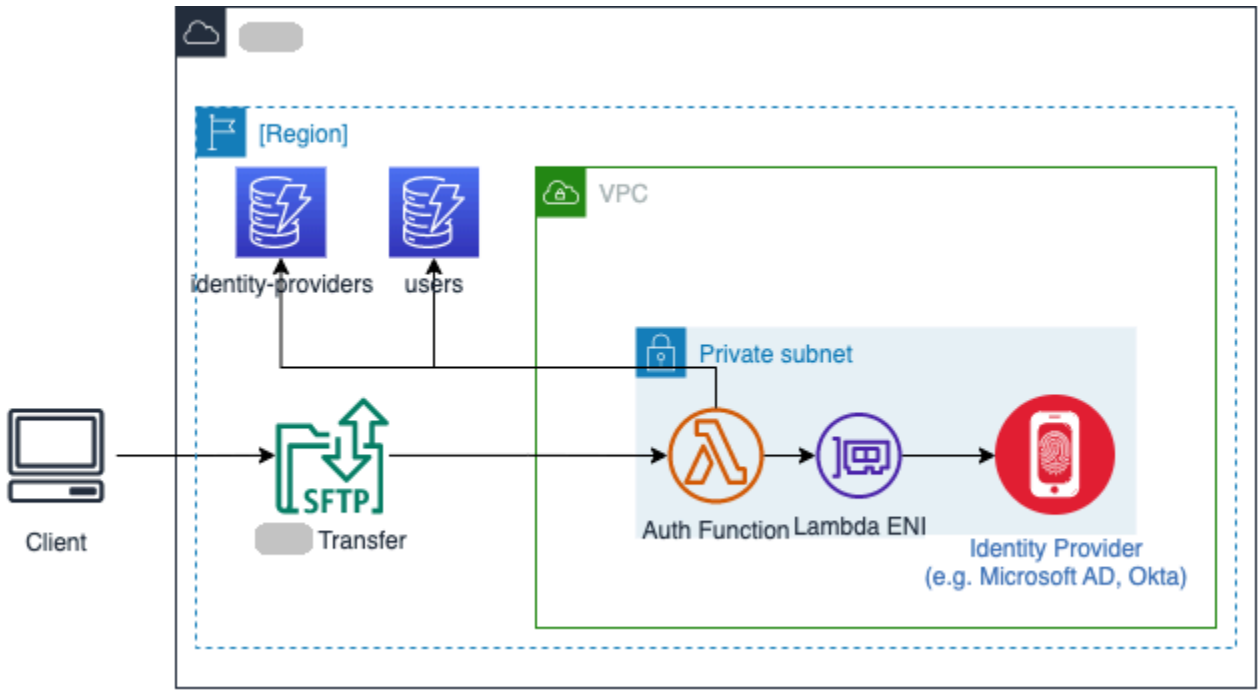
Amazon Transfer Family 自定义身份提供商解决方案是一种模块化的自定义身份提供商解决方案，可解决企业在实施服务时遇到的许多常见身份验证和授权用例。该解决方案为通过精细的每用户会话配置实现自定义身份提供商提供了可重复使用的基础，并将身份验证和授权逻辑分开，为各种用例提供了灵活的 easy-to-maintain基础。

借助 Amazon Transfer Family 自定义身份提供商解决方案，您可以解决常见的企业身份验证和授权用例。该模块化解决方案提供：

- 实现自定义身份提供商的可重复使用的基础
- 精细的每用户会话配置
- 独立的身份验证和授权逻辑

自定义身份工具包的实现细节

该解决方案为各种用例提供了灵活且可维护的基础。要开始使用，请查看 https://github.com/aws-samples/toolkit-for-aws-transfer-family 中的工具包，然后按照入门部分中的部署说明进行操作。



> **Note**
>
> 如果您之前使用过自定义身份提供商模板和示例，请考虑改用此解决方案。展望未来，特定于提供商的模块将以此解决方案为基础进行标准化。将对该解决方案进行持续维护和功能增强。

此解决方案包含用于实现自定义提供程序的标准模式，该提供程序会考虑详细信息，包括日志记录以及在何处存储所需的其他会话元数据 Amazon Transfer Family，例如`HomeDirectoryDetails`参数。该解决方案为通过精细的每用户会话配置实现自定义身份提供者提供了可重复使用的基础，并将身份提供者身份验证逻辑与可重用逻辑分离，后者构建的配置返回给 Transfer Family 以完成身份验证并建立会话设置。

该解决方案的代码和支持资源可在 https://github.com/aws-samples/toolkit-for-aws-transfer-famil y中找到。

该工具包包含以下功能：

- 预置所需资源的Amazon Serverless Application Model模板。（可选）部署和配置要合并的 Amazon API Gateway Amazon WAF，如博客文章《Amazon Transfer Family 使用 Amazon Web 应用程序防火墙和 Amazon API Gateway 确保安全》中所述。
- A mazon Dy namoDB 架构，用于存储有关身份提供商的配置元数据，包括用户会话设置，`HomeDirectoryDetails`例如`Role`、和。`Policy`

- 一种模块化方法，使您能够在将来将新的身份提供者作为模块添加到解决方案中。
- 属性检索：（可选）从支持的身份提供商（包括 AD、LDAP 和 Okta）检索 IAM 角色和 POSIX 配置文件（UID 和 GID）属性。
- 支持使用相同的解决方案部署连接到单个 Transfer Family 服务器和多个 Transfer Family 服务器的多个身份提供商。
- 内置 IP 允许列表检查，例如 IP 允许列表，可以选择根据每个用户或每个身份提供商进行配置。
- 详细的日志记录以及可配置的日志级别和跟踪支持，以帮助进行故障排除。

在开始部署自定义身份提供商解决方案之前，您需要具备以下 Amazon 资源。

- 带有私有子网的亚马逊虚拟私有云 (VPC)，可通过 NAT 网关或 DynamoDB 网关终端节点进行互联网连接。
- 执行以下任务的相应的 IAM 权限：
  - 部署`custom-idp.yaml` Amazon CloudFormation 模板，
  - 创建 Amazon CodePipeline 项目
  - 创建 Amazon CodeBuild 项目
  - 创建 IAM 角色和策略

> **Important**
>
> 您必须将解决方案部署到包含目标 Trans Amazon Web Services 账户 f Amazon Web Services 区域 er Family 服务器的相同服务器上。

支持的身份提供商

以下列表包含自定义身份提供商解决方案支持的身份提供商的详细信息。

Provider	密码流	公钥流	多因子	属性检索	Details
活动目录和 LDAP	支持	是	否	是	用户验证可以作为公钥身份验证流程的一部分来执行。

Provider	密码流	公钥流	多因子	属性检索	Details
Argon2（本地哈希）	是	否	否	否	Argon2 哈希存储在基于“本地”密码的身份验证用例的用户记录中。
Amazon Cognito	是	否	是*	否	仅限基于时间的一次性密码 (TOTP) 的多因素身份验证。 *不支持基于短信的 MFA。
入口 ID（以前是 Azure AD）	是	否	否	否	
Okta	支持	是	是*	是	仅限基于 TOTP 的 MFA。
公有密钥	否	是	否	否	公钥存储在 DynamoDB 的用户记录中。
Secrets Manager	支持	是	否	否	

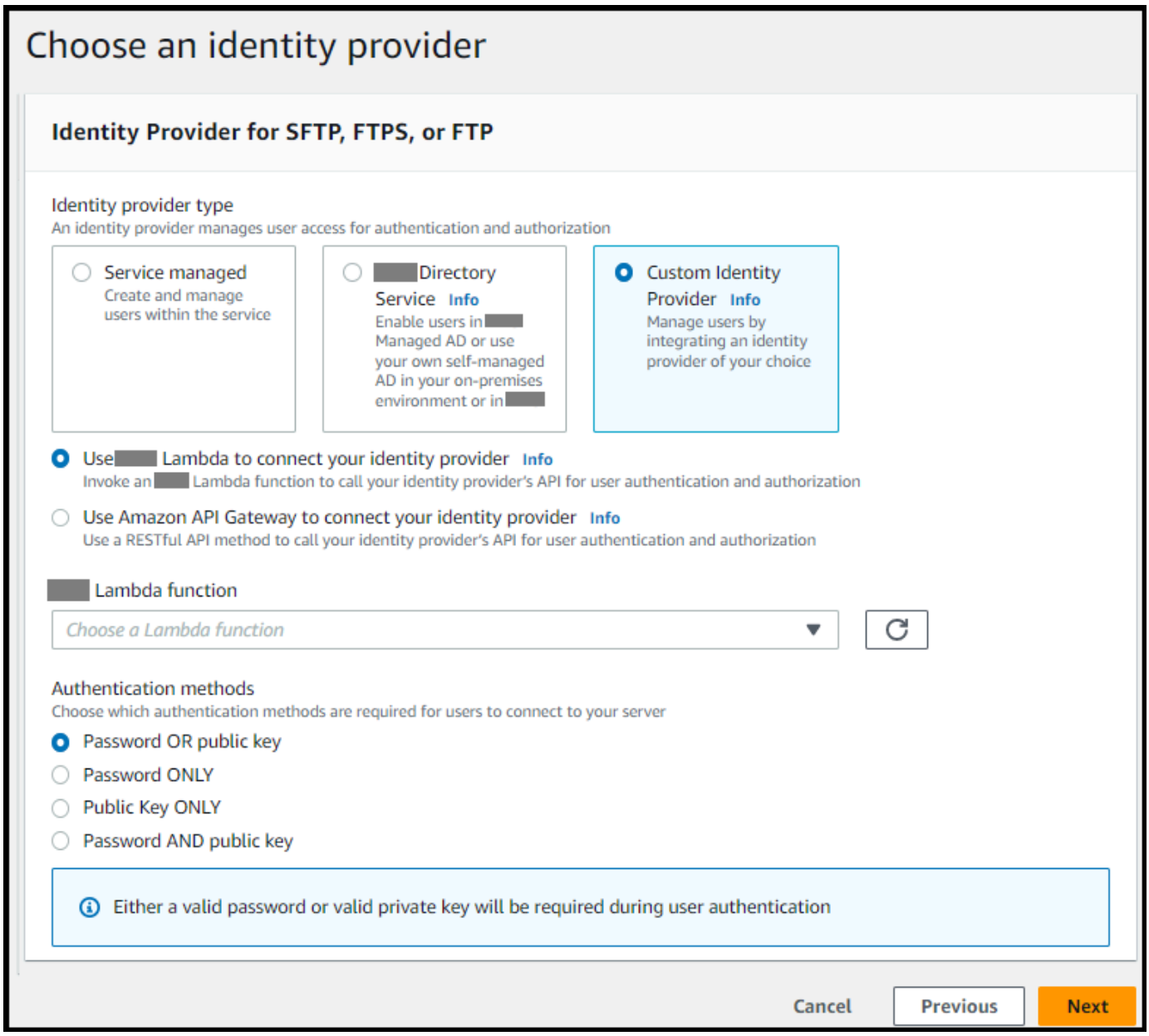
Amazon Lambda 用于整合您的身份提供商

本主题介绍如何创建连接到您的自定义身份提供商的 Amazon Lambda 函数。您可以使用任何自定义身份提供商，例如 Okta、Secrets Manager 或包含授权和身份验证逻辑的自定义数据存储。 OneLogin

对于大多数用例，配置自定义身份提供商的推荐方法是使用自定义身份提供商解决方案。

> **Note**
>
> 在创建使用 Lambda 作为身份提供程序的 Transfer Family 服务器之前，必须创建该函数。有关示例 Lambda 函数，请参阅 Lambda 函数示例。或者，您可以部署使用其中一个的 CloudFormation 堆栈Lambda 函数模板。此外，请确保您的 Lambda 函数使用信任 Transfer Family 的基于资源的策略。有关策略示例，请参阅 Lambda 资源策略。

1. 打开 Amazon Transfer Family 控制台。
2. 选择“创建服务器”以打开“创建服务器”页面。在“选择身份提供程序”中，选择“自定义身份提供程序”，如以下屏幕截图所示。



> **Note**
>
> 只有启用 SFTP 作为 Transfer Family 服务器的协议之一时，才能选择身份验证方法。

3. 确保选择了默认值 “ Amazon Lambda 用于连接您的身份提供商”。
4. 对于 Amazon Lambda 函数，选择 Lambda 函数名称。
5. 填写其余的方框，然后选择“创建服务器”。有关创建服务器的其余步骤的详细信息，请参阅 配置 SFTP、FTPS 或 FTP 服务器端点。

Lambda 资源策略

您必须有一个引用 Transfer Family 服务器和 Lambda ARNs 的策略。例如，您可以将以下策略与连接到您的身份提供程序的 Lambda 函数一起使用。策略会以 JSON 格式转义为字符串。

```
"Policy":
"{\"Version\":\"2012-10-17\",
\"Id\":\"default\",
\"Statement\":[
  {\"Sid\":\"AllowTransferInvocation\",
  \"Effect\":\"Allow\",
  \"Principal\":{\"Service\":\"transfer.amazonaws.com\"},
  \"Action\":\"lambda:InvokeFunction\",
  \"Resource\":\"arn:aws:lambda:region:account-id:function:my-lambda-auth-function\",
  \"Condition\":{\"ArnLike\":{\"AWS:SourceArn\":\"arn:aws:transfer:region:account-id:server/server-id\"}}}
]}"
```

> **Note**
>
> 在上面的示例政策中，用您自己的信息替换每项*user input placeholder*政策。

事件消息结构

来自自定义 IDP 的 SFTP 服务器发送给授权程序 Lambda 函数的事件消息结构如下所示。

```
{
    "username": "value",
    "password": "value",
    "protocol": "SFTP",
    "serverId": "s-abcd123456",
    "sourceIp": "192.168.0.100"
}
```

其中 `username` 和 `password` 是发送到服务器的登录凭证的值。

例如，您可输入以下连接命令。

```
sftp bobusa@server_hostname
```

系统会提示您输入密码：

```
Enter password:
    mysecretpassword
```

您可以在 Lambda 函数中进行检查，方法是在 Lambda 函数中打印传递的事件。此部分与以下文本块类似。

```
{
    "username": "bobusa",
    "password": "mysecretpassword",
    "protocol": "SFTP",
    "serverId": "s-abcd123456",
    "sourceIp": "192.168.0.100"
}
```

FTP 和 FTPS 的事件结构类似：唯一的区别是 `protocol` 参数会使用这些值，而不是 SFTP。

用于身份验证的 Lambda 函数

要实现不同的身份验证策略，请编辑 Lambda 函数。为了帮助您满足应用程序的需求，您可以部署堆 CloudFormation 栈。有关更多信息，请参见 Amazon Lambda 开发人员指南 或 通过 Node.js 构建 Lambda 函数。

主题

- 有效的 Lambda 值
- Lambda 函数示例
- 测试您的配置
- Lambda 函数模板

有效的 Lambda 值

下表详细介绍了 Transfer Family 接受的用于自定义身份提供程序的 Lambda 函数的值。

值	说明	必填
`Role`	指定控制用户对 Amazon S3 存储桶或 Amazon EFS 文件系统访问权限的 IAM 角色的 Amazon Resource Name (ARN) 。附加到此角色的策略确定在将文件传入和传出 Amazon S3 存储桶或 Amazon EFS 文件系统时要为用户提供的访问权限级别。IAM 角色还应包含一个信任关系，从而允许服务器在为用户的传输请求提供服务时访问您的资源。 有关建立信任关系的详细信息，请参阅 建立信任关系。	必需
`PosixProfile`	控制用户访问您的 Amazon EFS 文件系统的完整 POSIX 身份，包括用户 ID IDs (`UidGidSecondaryGids`)、群组 ID () 和任何辅助群组 ()。POSIX 权限针对文件系统中的文件和目录设置，用于确定用户在将文件传入和传出 Amazon EFS 文件系统时获得的访问权限级别。	Amazon EFS 后备存储为必填项
`PublicKeys`	对此用户有效的 SSH 公钥值列表。空列表表示这不是有效的登录名。密码认证期间不得返回。	可选
`Policy`	适用于您的用户的会话策略，可让您跨多个用户使用相同的 IAM 角色。此策略将用户的访	可选

值	说明	必填
	问范围缩小至 Amazon S3 存储桶的一部分。有关使用自定义身份提供商的会话策略的更多信息，请参阅本主题中的会话策略示例。	
HomeDirectoryType	您希望用户在登录服务器时，用户主目录的登录目录（文件夹）的类型。 • 如果您将其设置为 PATH，则用户将在其文件传输协议客户端中原样看到 Amazon S3 存储桶或 Amazon EFS 路径。 • 如果您将其设置为 LOGICAL，则必须在HomeDirectoryDetails 参数中提供映射，以使 Amazon S3 或 Amazon EFS 路径对用户可见。	可选
HomeDirectoryDetails	逻辑目录映射指定哪些 Amazon S3 或 Amazon EFS 路径和密钥应对您的用户可见，以及使其对用户可见的方式。您需要指定 Entry 和 Target 对，其中 Entry 显示如何使路径可见，Target 是实际的 Amazon S3 或 Amazon EFS 路径。	如果 HomeDirectoryType 值为 LOGICAL，则为必填项

值	说明	必填
HomeDirectory	用户使用客户端登录服务器时的登录目录。格式取决于您的存储后端： • 对于亚马逊 S3：/bucket-name/user-home-directory 示例：/amzn-s3-demo-bucket/users/john • 对于亚马逊 EFS：/fs-12345/user-home-directory 示例：/fs-faa1a123/users/john **Important** 路径中必须包含存储桶名称或 Amazon EFS 文件系统 ID。省略此信息将导致文件传输过程中出现 “找不到文件” 错误。	可选

Note

HomeDirectoryDetails 是 JSON 映射的字符串表示形式。这与 PosixProfile 形成鲜明对比，后者是一个实际的 JSON 映射对象，PublicKeys 是一个字符串的 JSON 数组。有关特定语言的详细信息，请参阅代码示例。

HomeDirectory 格式要求

使用HomeDirectory参数时，请确保包含完整的路径格式：

- 对于 Amazon S3 存储：请务必使用以下格式包含存储桶名称 /bucket-name/path
- 对于 Amazon EFS 存储：请务必使用以下格式包含文件系统 ID /fs-12345/path

“找不到文件” 错误的一个常见原因是HomeDirectory路径中省略了存储桶名称或 EFS 文件系统 ID。如果设置HomeDirectory为/不带存储标识符，则会导致身份验证成功，但文件操作失败。

Lambda 函数示例

本节介绍了一些 NodeJS 和 Python 中的 Lambda 函数示例。

Note

在这些示例中，用户、角色、POSIX 配置文件、密码和主目录详细信息均为示例，必须将其替换为实际值。

Logical home directory, NodeJS

以下 NodeJS 示例函数为拥有逻辑主目录的用户提供了详细信息。

```
// GetUserConfig Lambda

exports.handler = (event, context, callback) => {
  console.log("Username:", event.username, "ServerId: ", event.serverId);

  var response;
  // Check if the username presented for authentication is correct. This doesn't
 check the value of the server ID, only that it is provided.
  if (event.serverId !== "" && event.username == 'example-user') {
    var homeDirectoryDetails = [
      {
        Entry: "/",
        Target: "/fs-faa1a123"
      }
```

```
    ];
    response = {
      Role: 'arn:aws:iam::123456789012:role/transfer-access-role', // The user is
 authenticated if and only if the Role field is not blank
      PosixProfile: {"Gid": 65534, "Uid": 65534}, // Required for EFS access, but
 not needed for S3
      HomeDirectoryDetails: JSON.stringify(homeDirectoryDetails),
      HomeDirectoryType: "LOGICAL",
    };

    // Check if password is provided
    if (!event.password) {
      // If no password provided, return the user's SSH public key
      response['PublicKeys'] = [ "ssh-
rsa abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789" ];
    // Check if password is correct
    } else if (event.password !== 'Password1234') {
      // Return HTTP status 200 but with no role in the response to indicate
 authentication failure
      response = {};
    }
  } else {
    // Return HTTP status 200 but with no role in the response to indicate
 authentication failure
    response = {};
  }
  callback(null, response);
};
```

Path-based home directory, NodeJS

以下 NodeJS 示例函数为拥有基于路径的主目录的用户提供了详细信息。

```
// GetUserConfig Lambda

exports.handler = (event, context, callback) => {
  console.log("Username:", event.username, "ServerId: ", event.serverId);

  var response;
  // Check if the username presented for authentication is correct. This doesn't
 check the value of the server ID, only that it is provided.
  // There is also event.protocol (one of "FTP", "FTPS", "SFTP") and event.sourceIp
 (e.g., "127.0.0.1") to further restrict logins.
  if (event.serverId !== "" && event.username == 'example-user') {
```

```
    response = {
      Role: 'arn:aws:iam::123456789012:role/transfer-access-role', // The user is
 authenticated if and only if the Role field is not blank
      Policy: '', // Optional, JSON stringified blob to further restrict this user's
 permissions
      // HomeDirectory format depends on your storage backend:
      // For S3: '/bucket-name/user-home-directory' (e.g., '/my-transfer-bucket/
users/john')
      // For EFS: '/fs-12345/user-home-directory' (e.g., '/fs-faa1a123/users/john')
      HomeDirectory: '/my-transfer-bucket/users/example-user' // S3 example -
 replace with your bucket name
      // HomeDirectory: '/fs-faa1a123/users/example-user' // EFS example - uncomment
 for EFS
    };

    // Check if password is provided
    if (!event.password) {
      // If no password provided, return the user's SSH public key
     response['PublicKeys'] = [ "ssh-
rsa abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789" ];
    // Check if password is correct
    } else if (event.password !== 'Password1234') {
      // Return HTTP status 200 but with no role in the response to indicate
 authentication failure
      response = {};
    }
  } else {
    // Return HTTP status 200 but with no role in the response to indicate
 authentication failure
    response = {};
  }
  callback(null, response);
};
```

Logical home directory, Python

以下 Python 示例函数为拥有逻辑主目录的用户提供了详细信息。

```
# GetUserConfig Python Lambda with LOGICAL HomeDirectoryDetails
import json

def lambda_handler(event, context):
  print("Username: {}, ServerId: {}".format(event['username'], event['serverId']))
```

```
  response = {}

  # Check if the username presented for authentication is correct. This doesn't
 check the value of the server ID, only that it is provided.
  if event['serverId'] != '' and event['username'] == 'example-user':
    homeDirectoryDetails = [
      {
        'Entry': '/',
        'Target': '/fs-faa1a123'
      }
    ]
    response = {
      'Role': 'arn:aws:iam::123456789012:role/transfer-access-role', # The user will
 be authenticated if and only if the Role field is not blank
      'PosixProfile': {"Gid": 65534, "Uid": 65534}, # Required for EFS access, but
 not needed for S3
      'HomeDirectoryDetails': json.dumps(homeDirectoryDetails),
      'HomeDirectoryType': "LOGICAL"
    }

    # Check if password is provided
    if event.get('password', '') == '':
      # If no password provided, return the user's SSH public key
     response['PublicKeys'] = [ "ssh-
rsa abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789" ]
    # Check if password is correct
    elif event['password'] != 'Password1234':
      # Return HTTP status 200 but with no role in the response to indicate
 authentication failure
      response = {}
  else:
    # Return HTTP status 200 but with no role in the response to indicate
 authentication failure
    response = {}

  return response
```

Path-based home directory, Python

以下 Python 示例函数为拥有基于路径的主目录的用户提供了详细信息。

```
# GetUserConfig Python Lambda with PATH HomeDirectory

def lambda_handler(event, context):
```

```
  print("Username: {}, ServerId: {}".format(event['username'], event['serverId']))

  response = {}

  # Check if the username presented for authentication is correct. This doesn't
 check the value of the server ID, only that it is provided.
  # There is also event.protocol (one of "FTP", "FTPS", "SFTP") and event.sourceIp
 (e.g., "127.0.0.1") to further restrict logins.
  if event['serverId'] != '' and event['username'] == 'example-user':
    response = {
      'Role': 'arn:aws:iam::123456789012:role/transfer-access-role', # The user will
 be authenticated if and only if the Role field is not blank
      'Policy': '', #  Optional, JSON stringified blob to further restrict this
 user's permissions
      # HomeDirectory format depends on your storage backend:
      # For S3: '/bucket-name/user-home-directory' (e.g., '/my-transfer-bucket/
users/john')
      # For EFS: '/fs-12345/user-home-directory' (e.g., '/fs-faa1a123/users/john')
      'HomeDirectory': '/my-transfer-bucket/users/example-user', # S3 example -
 replace with your bucket name
      # 'HomeDirectory': '/fs-faa1a123/users/example-user', # EFS example -
 uncomment for EFS
      'HomeDirectoryType': "PATH" # Not strictly required, defaults to PATH
    }

    # Check if password is provided
    if event.get('password', '') == '':
      # If no password provided, return the user's SSH public key
     response['PublicKeys'] = [ "ssh-
rsa abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789" ]
    # Check if password is correct
    elif event['password'] != 'Password1234':
      # Return HTTP status 200 but with no role in the response to indicate
 authentication failure
      response = {}
  else:
    # Return HTTP status 200 but with no role in the response to indicate
 authentication failure
    response = {}

  return response
```

测试您的配置

创建自定义身份提供程序后，应测试您的配置。

Console

使用 Amazon Transfer Family 控制台测试您的配置

1. 打开 Amazon Transfer Family 控制台。
2. 在“服务器”页面上，选择您的新服务器，选择“操作”，然后选择“测试”。
3. 输入您在部署 Amazon CloudFormation 堆栈时设置的用户名和密码文本。如果您保留默认选项，则用户名为 `myuser`，密码为 `MySuperSecretPassword`。
4. 如果在部署 Amazon CloudFormation 堆栈时设置了源 IP 地址，请选择服务器协议并输入源 IP 地址。

CLI

使用 Amazon CLI 测试您的配置

1. 运行 test-identity-provider 命令。如后续步骤所述，将 *user input placeholder* 用您自己的信息进行替换。

```
aws transfer test-identity-provider --server-id s-1234abcd5678efgh --user-name myuser --user-password MySuperSecretPassword --server-protocol FTP --source-ip 127.0.0.1
```

2. 输入服务器 ID。
3. 输入您在部署 Amazon CloudFormation 堆栈时设置的用户名和密码。如果您保留默认选项，则用户名为 `myuser`，密码为 `MySuperSecretPassword`。
4. 如果在部署 Amazon CloudFormation 堆栈时设置了服务器协议和源 IP 地址，请输入它们。

如果用户身份验证成功，则测试将返回 `StatusCode: 200` HTTP 响应、一个空字符串 `Message: ""`（否则将包含失败原因）和一个 `Response` 字段。

> **Note**
>
> 在下面的响应示例中，`Response` 字段是一个已经“字符串化”的 JSON 对象（转换为可在程序中使用的扁平 JSON 字符串），其中包含用户角色和权限的详细信息。

```
{
    "Response":"{\"Policy\":\"{\\\"Version\\\":\\\"2012-10-17\\\",\\\"Statement\\\":
[{\\\"Sid\\\":\\\"ReadAndListAllBuckets\\\",\\\"Effect\\\":\\\"Allow\\\",\\\"Action\\
\":[\\\"s3:ListAllMybuckets\\\",\\\"s3:GetBucketLocation\\\",\\\"s3:ListBucket\\\",\\
\"s3:GetObjectVersion\\\",\\\"s3:GetObjectVersion\\\"],\\\"Resource\\\":\\\"*\\\"}]}\",
\"Role\":\"arn:aws:iam::000000000000:role/MyUserS3AccessRole\",\"HomeDirectory\":\"/
\"}",
    "StatusCode": 200,
    "Message": ""
}
```


Lambda 函数模板

您可以部署使用 Lambda 函数进行身份验证的 Amazon CloudFormation 堆栈。我们提供了多个模板，可使用登录凭证对您的用户进行身份验证和授权。您可以修改这些模板或 Amazon Lambda 代码以进一步自定义用户访问权限。

> **Note**
>
> 您可以通过在模板中指定启用 FIPS 的安全策略 Amazon CloudFormation 来创建启用 FIPS 的 Amazon Transfer Family 服务器。有关可用安全策略的描述，请参见 Amazon Transfer Family 服务器的安全策略

创建用于身份验证的 Amazon CloudFormation 堆栈

1. 在 https://console.aws.amazon.com/cloudformat ion 上打开 Amazon CloudFormation 控制台。
2. 按照Amazon CloudFormation 用户指南中的选择 Amazon CloudFormation 堆栈模板中的现有模板部署堆栈的说明进行操作。
3. 使用以下模板之一来创建在 Transfer Family 中进行身份验证的 Lambda 函数。

   - 经典 (Amazon Cognito) 堆栈模板

     用于在中创建用作 Amazon Lambda 自定义身份提供者的基本模板 Amazon Transfer Family。它会针对 Amazon Cognito 进行身份验证以进行基于密码的身份验证，如果使用基于公钥的身份验证，则会从 Amazon S3 存储桶返回公钥。部署后，您可以修改 Lambda 函数代码以执行不同的操作。

   - Amazon Secrets Manager 堆栈模板

与 Amazon Transfer Family 服务器 Amazon Lambda 一起使用的基本模板，用于将 Secrets Manager 作为身份提供者进行集成。它根据格式`aws/transfer/`*`server-id`*`/`*`username`*的条目 Amazon Secrets Manager 进行身份验证。此外，该密钥必须包含返回给 Transfer Family 的所有用户属性的键值对。部署后，您可以修改 Lambda 函数代码以执行不同的操作。

- Okta 堆栈模板：一种基本模板，与 Amazon Transfer Family 服务器 Amazon Lambda 一起使用，将 Okta 集成为自定义身份提供商。
- Okta-MFA 堆栈模板：一种基本模板，可与 Amazon Transfer Family 服务器 Amazon Lambda 一起使用，将 Okta 与多因素身份验证集成，作为自定义身份提供商。
- Azure Active Directory 模板：博客文章使用 Azure 活动目录进行 Amazon Transfer Family 身份验证中描述了此堆栈的详细信息。 Amazon Lambda

部署堆栈后，您可以在 CloudFormation 控制台的 Outputs 选项卡上查看有关堆栈的详细信息。

部署其中一个堆栈是将自定义身份提供程序集成到 Transfer Family 工作流程的最简单方法。

使用 Amazon API Gateway 整合您的身份提供程序

本主题介绍如何使用 Amazon Lambda 函数支持 API Gateway 方法。如果您需要一个 RESTful API 来集成您的身份提供商，或者想要利用其功能来处理地理封锁或速率限制请求，请使用 Amazon WAF 此选项。

对于大多数用例，配置自定义身份提供商的推荐方法是使用自定义身份提供商解决方案。

使用 API Gateway 集成身份提供程序时的限制

- 此配置不支持自定义域。
- 此配置不支持私有 API Gateway 网址。

如果您需要其中任何一个，则可以使用 Lambda 作为身份提供程序，而无需使用 API Gateway。有关更多信息，请参阅 Amazon Lambda 用于整合您的身份提供商。

使用 API Gateway 方法进行身份验证

您可以创建一个 API Gateway 方法，用作 Transfer Family 的身份提供程序。这种方法为您提供了一种高度安全的创建和提供方式 APIs。借助 API Gateway，您可以创建 HTTPS 终端节点，以便以更高的安全性传输所有传入的 API 操作。有关 API Gateway 服务的更多详细信息，请参阅 API Gateway 开发者指南。

API Gateway 提供了一种名为的授权方法AWS_IAM，该方法为您提供与内部 Amazon 使用的相同基于 Amazon Identity and Access Management (IAM) 的身份验证。如果您通过 AWS_IAM 启用身份验证，则只有具有调用 API 的明确权限的调用程序才能访问该 API 的 API Gateway 方法。

要将您的 API Gateway 方法用作 Transfer Family 的自定义身份提供程序，请为您的 API Gateway 方法启用 IAM。在此过程中，您需要为一个 IAM 角色提供 Transfer Family 使用您的网关的权限。

> **Note**
>
> 为了提高安全性，可以配置 Web 应用程序防火墙。 Amazon WAF 是一种 Web 应用程序防火墙，可让您监视转发到 Amazon API Gateway 的 HTTP 和 HTTPS 请求。有关更多信息，请参阅 添加 Web 应用程序防火墙。

> **不要启用 API Gateway 缓存**
>
> 将 API Gateway 方法用作 Transfer Family 的自定义身份提供者时，请勿为其启用缓存。缓存对身份验证请求不恰当且无效，因为：
>
> - 每个身份验证请求都是唯一的，需要实时响应，而不是缓存的响应
> - 缓存没有任何好处，因为 Transfer Family 永远不会向 API Gateway 发送重复或重复的请求
> - 启用缓存将导致 API Gateway 使用不匹配的数据进行响应，从而导致对身份验证请求的响应无效

使用您的 API Gateway 方法对 Transfer Family 进行自定义身份验证

1. 创建 Amazon CloudFormation 堆栈。要实现此目的，应按照以下步骤进行：

   > **Note**
   >
   > 堆栈模板已更新为使用 BASE64-编码的密码：有关详细信息，请参阅。对 Amazon CloudFormation 模板的改进

   a. 在 https://console.aws.amazon.com/cloudformat ion 上打开 Amazon CloudFormation 控制台。

b. 按照Amazon CloudFormation 用户指南中的选择 Amazon CloudFormation 堆栈模板中的现有模板部署堆栈的说明进行操作。

c. 使用以下基本模板之一创建由 Amazon Lambda支持的 API Gateway 方法，以便在 Transfer Family 中用作自定义身份提供程序。

- 基本堆栈模板

  默认情况下，您的 API Gateway 方法用作自定义身份提供者，使用硬编码的 SSH（安全外壳）密钥或密码对单个服务器中的单个用户进行身份验证。部署后，您可以修改 Lambda 函数代码以执行不同的操作。

- Amazon Secrets Manager 堆栈模板

  默认情况下，您的 API Gateway 方法会根据格式 `aws/transfer/server-id/username` 的 Secrets Manager 中的条目进行身份验证。此外，该密钥必须包含返回给 Transfer Family 的所有用户属性的键值对。部署后，您可以修改 Lambda 函数代码以执行不同的操作。有关更多信息，请参阅博客文章启用密码身份验证以供 Amazon Transfer Family 使用 Amazon Secrets Manager。

- Okta 堆栈模板

  您的 API Gateway 方法与 Okta 集成，以作为 Transfer Family 中的自定义身份提供程序。有关更多信息，请参阅博客文章：使用 Amazon Transfer Family将 Okta 用作身份提供程序。

部署其中一个堆栈是将自定义身份提供程序集成到 Transfer Family 工作流程的最简单方法。每个堆栈都使用 Lambda 函数来支持基于 API Gateway 的 API 方法。然后，您可以在 Transfer Family 中使用您的 API 方法作为自定义身份提供程序。默认情况下，Lambda 函数对使用 `MySuperSecretPassword` 密码 `myuser` 调用的单个用户进行身份验证。部署后，您可以编辑这些凭证或更新 Lambda 函数代码以执行不同的操作。

> **Important**
>
> 我们建议您编辑默认的用户和密码凭证。

部署堆栈后，您可以在 CloudFormation 控制台的 Outputs 选项卡上查看有关堆栈的详细信息。这些详细信息包括堆栈的 Amazon 资源名称 (ARN)、堆栈创建的 IAM 角色的 ARN 以及您的新网关的 URL。

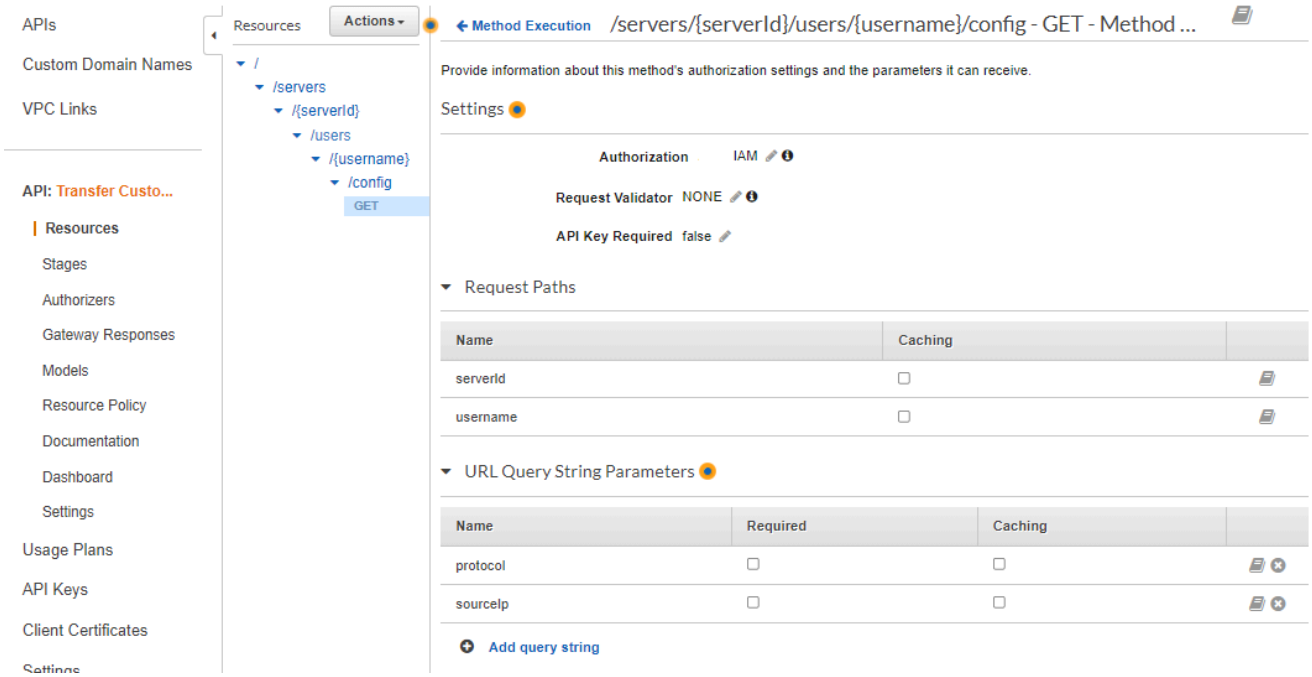
> **Note**
>
> 如果您使用自定义身份提供商选项为用户启用基于密码的身份验证，并且启用了 API Gateway 提供的请求和响应日志，API Gateway 会将用户的密码记录到您的 Amazon 日志中。 CloudWatch 我们建议不要在生产环境中使用此日志。有关更多信息，请参阅《CloudWatch API Gateway 开发者指南》中的 “在 API Gateway 中设置 API 日志”。

2. 检查您的服务器的 API Gateway 方法配置。要实现此目的，应按照以下步骤进行：

   a. 打开 API Gateway 控制台，网址为https://console.aws.amazon.com/apigateway/。

   b. 选择模板生成的转移自定义身份提供商基本 Amazon CloudFormation 模板 API。您可能需要选择您的区域才能看到您的网关。

   c. 在 “资源” 窗格中，选择 GET。以下屏幕截图显示了正确的方法配置。

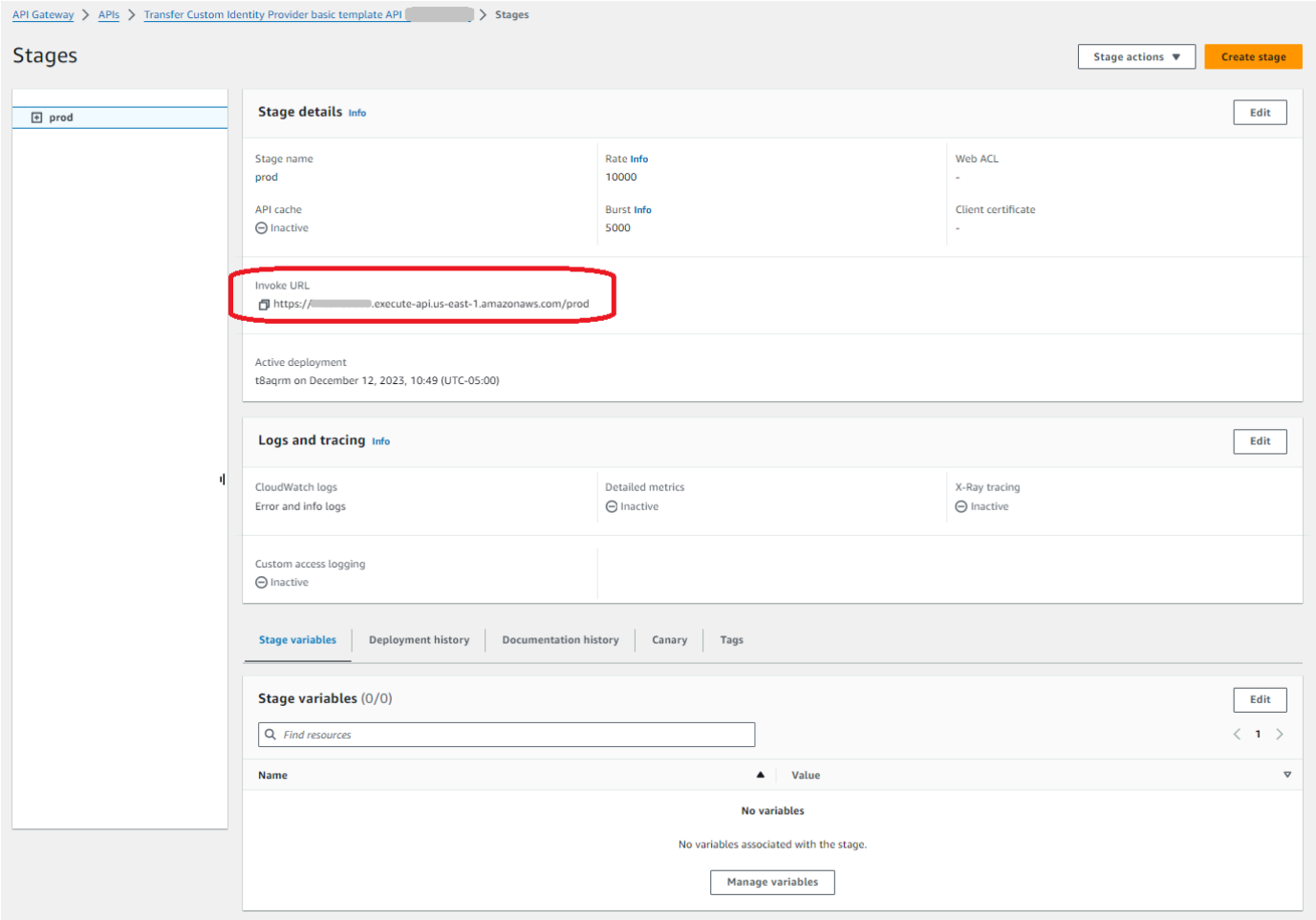


   此时，您的 API Gateway 已准备好部署。

3. 在操作，选择部署 API。对于部署阶段，选择 prod，然后选择部署。

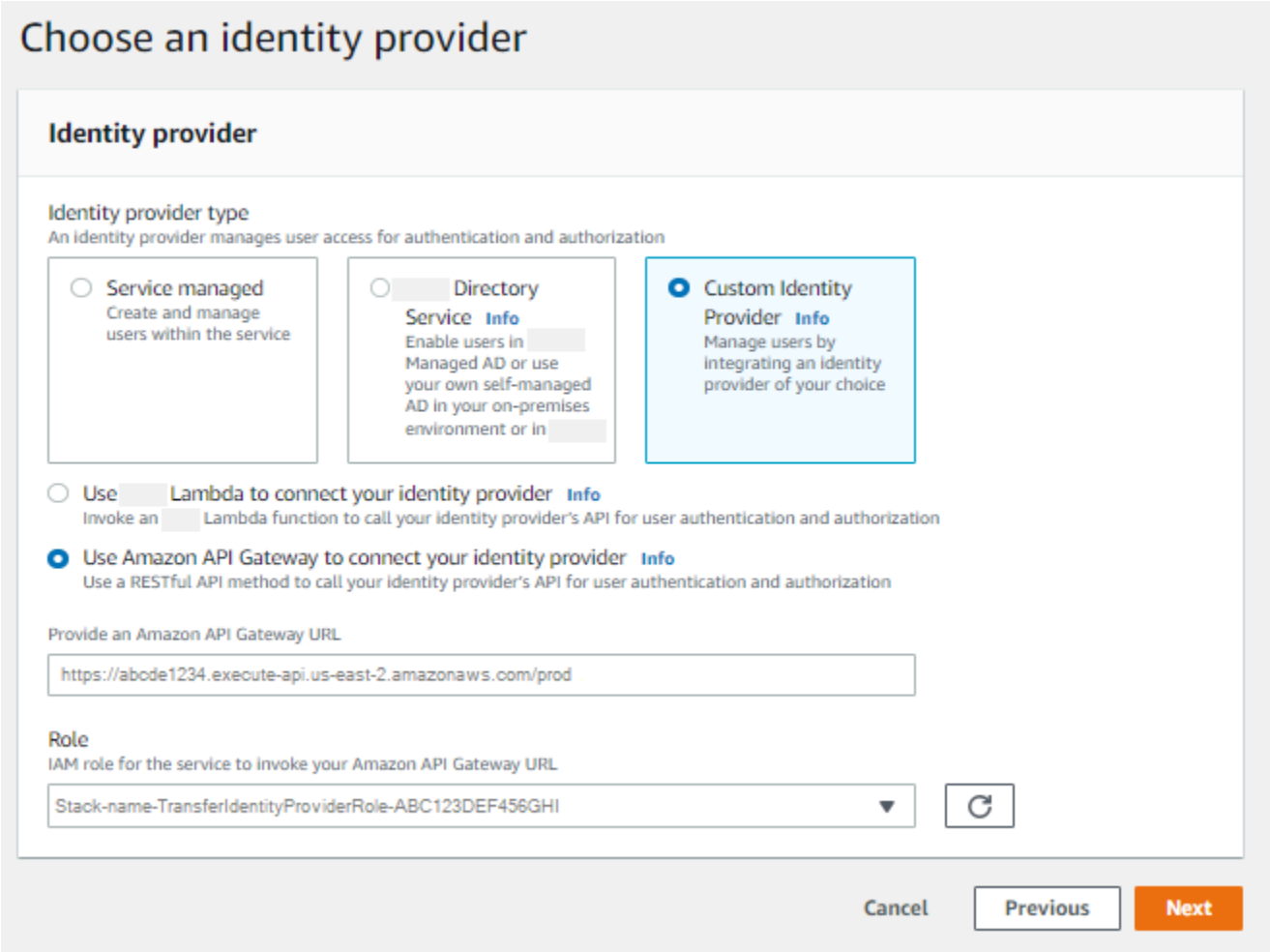
   成功部署 API Gateway 方法后，在 “阶段” > “阶段详情” 中查看其性能，如以下屏幕截图所示。

> **Note**
>
> 复制显示在屏幕顶部的调用 URL 地址。下一步可能需要它。



4. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
5. 在你创建堆栈时，应该已经为你创建了 Transfer Family。如果不是，请使用以下步骤配置您的服务器。

   a. 选择“创建服务器”以打开“创建服务器”页面。在“选择身份提供程序”中，选择“自定义”，然后选择“使用 Amazon API Gateway 连接到您的身份提供程序”，如以下屏幕截图所示。



b. 在提供 Amazon API Gateway 网址文本框中，粘贴您在本过程的步骤 3 中创建的 API Gateway 端点的调用 URL 地址。

c. 对于角色，选择由 Amazon CloudFormation 模板创建的 IAM 角色。此角色允许 Transfer Family 调用您的 API Gateway 方法。

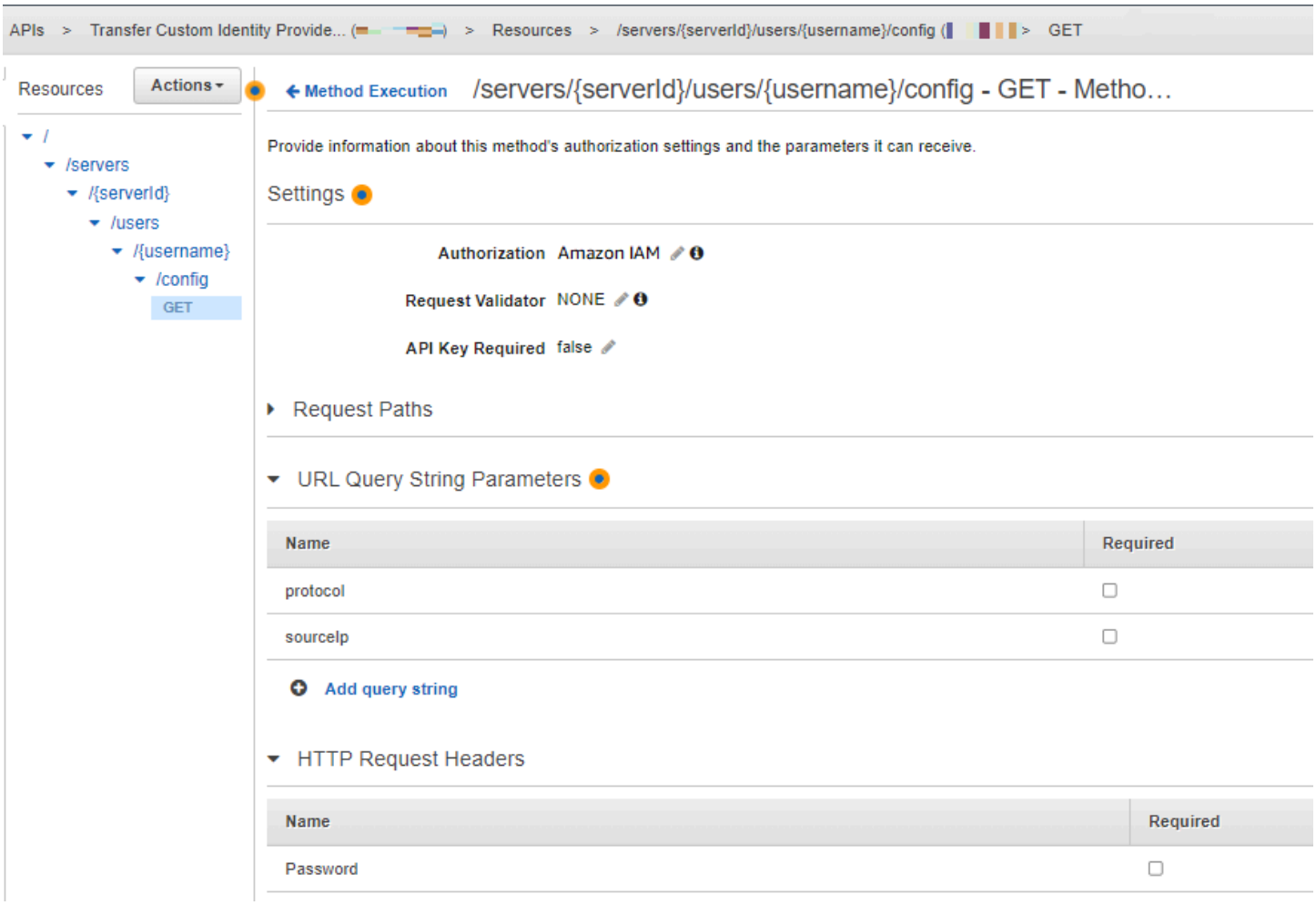
   调用角色包含您在步骤 1 中为创建的堆栈选择的堆栈名称。 Amazon CloudFormation 格式如下：*CloudFormation-stack-name*-TransferIdentityProviderRole-*ABC123DEF456GHI*。

d. 填写其余的方框，然后选择“创建服务器”。有关创建服务器的其余步骤的详细信息，请参阅 配置 SFTP、FTPS 或 FTP 服务器端点。

实施您的 API Gateway 方法

要为 Transfer Family 创建自定义身份提供程序，您的 API Gateway 方法必须实现资源路径为 /servers/*serverId*/users/*username*/config 的单个方法。*serverId*和*username*值来自

RESTful 资源路径。此外，在方法请求中添加 `sourceIp` 和 `protocol` 作为 URL 查询字符串参数，如下图所示。



> **Note**
>
> 此用户名长度最少为 3 个字符，最多为 100 个字符。你可以在用户名中使用以下字符：a—z、A-Z、0—9、下划线 '_'、连字符 '-'、句点 '.' 和 at 符号 '@'。用户名不能以连字符 “-”、“句点” 或 “@” 开头。

如果 Transfer Family 代表您的用户尝试进行密码身份验证，则该服务会提供 `Password:` 标头字段。在没有 `Password:` 标头的情况下，Transfer Family 会尝试通过公钥身份验证来验证您的用户。

当您使用身份提供商对最终用户进行身份验证和授权时，除了验证他们的凭据外，您还可以根据最终用户使用的客户端 IP 地址来允许或拒绝访问请求。您可以使用此功能来确保存储在 S3 存储桶或

Amazon EFS 文件系统中的数据只能通过支持的协议从您指定为可信的 IP 地址进行访问。要启用此功能，必须在查询字符串中包含 `sourceIp`。

如果您为服务器启用了多个协议，并且想要通过多个协议使用相同的用户名提供访问权限，则只要在身份提供程序中设置了每个协议的特定凭据，就可以这样做。要启用此功能，您必须在 RESTful 资源路径中包含该*protocol*值。

您的 API Gateway 方法应始终返回 HTTP 状态码 `200`。任何其他 HTTP 状态代码则表示访问 API 时出错。

Amazon S3 示例响应

示例响应正文是适用于 Amazon S3 的以下格式的 JSON 文档。

```
{
 "Role": "IAM role with configured S3 permissions",
 "PublicKeys": [
     "ssh-rsa public-key1",
     "ssh-rsa public-key2"
  ],
 "Policy": "STS Assume role session policy",
 "HomeDirectory": "/amzn-s3-demo-bucket/path/to/home/directory"
}
```

> **Note**
>
> 策略会以 JSON 格式转义为字符串。例如：
>
> ```
> "Policy":
> "{
>   \"Version\": \"2012-10-17\",
>   \"Statement\":
>      [
>      {\"Condition\":
>         {\"StringLike\":
>             {\"s3:prefix\":
>                [\"user/*\", \"user/\"]}},
>      \"Resource\": \"arn:aws:s3:::amzn-s3-demo-bucket\",
>      \"Action\": \"s3:ListBucket\",
>      \"Effect\": \"Allow\",
>      \"Sid\": \"ListHomeDir\"},
>      {\"Resource\": \"arn:aws:s3:::*\",
> ```

```
        \"Action\": [\"s3:PutObject\",
        \"s3:GetObject\",
        \"s3:DeleteObjectVersion\",
        \"s3:DeleteObject\",
        \"s3:GetObjectVersion\",
        \"s3:GetObjectACL\",
        \"s3:PutObjectACL\"],
    \"Effect\": \"Allow\",
    \"Sid\": \"HomeDirObjectAccess\"}]
}"
```

以下示例响应会显示用户具有逻辑主目录类型。

```
{
   "Role": "arn:aws:iam::123456789012:role/transfer-access-role-s3",
   "HomeDirectoryType":"LOGICAL",
   "HomeDirectoryDetails":"[{\"Entry\":\"/\",\"Target\":\"/amzn-s3-demo-bucket1\"}]",
   "PublicKeys":[""]
}
```

Amazon EFS 示例响应

示例响应正文是 Amazon EFS 的以下格式的 JSON 文档。

```
{
 "Role": "IAM role with configured EFS permissions",
 "PublicKeys": [
     "ssh-rsa public-key1",
     "ssh-rsa public-key2"
  ],
 "PosixProfile": {
   "Uid": "POSIX user ID",
   "Gid": "POSIX group ID",
   "SecondaryGids": [Optional list of secondary Group IDs],
 },
 "HomeDirectory": "/fs-id/path/to/home/directory"
}
```

Role 字段表示身份验证成功。在进行密码身份验证时（当您提供 Password: 标头时），您无需提供 SSH 公钥。如果无法对用户进行身份验证，例如，如果密码不正确，则您的方法应返回未设置 Role 的响应。此类响应的一个例子是空的 JSON 对象。

以下示例响应显示了具有逻辑主目录类型的用户。

```
{
    "Role": "arn:aws:iam::123456789012:role/transfer-access-role-efs",
    "HomeDirectoryType": "LOGICAL",
    "HomeDirectoryDetails":"[{\"Entry\":\"/\",\"Target\":\"/faa1a123\"}]",
    "PublicKeys":[""],
    "PosixProfile":{"Uid":65534,"Gid":65534}
}
```

您可以在 JSON 格式的 Lambda 函数中包含用户策略。有关在 Transfer Family 中配置用户策略的更多信息，请参阅 管理访问控制。

默认 Lambda 函数

要实施不同的身份验证策略，请编辑您的网关使用的 Lambda 函数。为了帮助您满足应用程序的需求，您可以在 Node.js 中使用以下示例 Lambda 函数。有关更多信息，请参见 Amazon Lambda 开发人员指南 或 通过 Node.js 构建 Lambda 函数。

以下示例 Lambda 函数使用您的用户名、密码（如果您正在执行密码身份验证）、服务器 ID、协议和客户端 IP 地址。您可以使用这些输入的组合来查找您的身份提供程序并确定是否应接受登录。

> **Note**
>
> 如果您为服务器启用了多个协议，并且想要通过多个协议使用相同的用户名提供访问权限，则只要在身份提供程序中设置了相关协议的特定凭据，就可以这样做。
> 对于文件传输协议 (FTP)，我们建议为 Secure Shell (SSH) 文件传输协议 (SFTP) 和 SSL (FTPS) 文件传输协议设置不同的凭证。我们建议为 FTP 保留单独的凭据，因为与 SFTP 和 FTPS 不同，FTP 以明文形式传输凭据。通过将 FTP 凭证与 SFTP 或 FTPS 隔离开来，如果共享或公开 FTP 凭证，则使用 SFTP 或 FTPS 的工作负载会保持安全。

此示例函数会返回角色和逻辑主目录详细信息以及公钥（如果它执行公钥身份验证）。

创建服务托管用户时，可以设置他们的主目录，无论是逻辑目录还是物理目录均是如此。同样，我们需要 Lambda 函数的结果来传达所需的用户物理或逻辑目录结构。您设置的参数取决于该 HomeDirectoryType 字段的值。

- `HomeDirectoryType` 设置为 `PATH` — 然后，`HomeDirectory` 字段必须是您的用户可见的 Amazon S3 存储桶绝对前缀或 Amazon EFS 绝对路径。

- HomeDirectoryType 设置为 LOGICAL — 请不要设置 HomeDirectory 字段。相反，我们设置了一个提供所需 Entry/Target 映射的HomeDirectoryDetails字段，类似于服务管理用户的HomeDirectoryDetails参数中描述的值。

Lambda 函数示例 中列出了示例函数。

用于的 Lambda 函数 Amazon Secrets Manager

要 Amazon Secrets Manager 用作您的身份提供商，您可以使用示例 Amazon CloudFormation 模板中的 Lambda 函数。Lambda 函数使用您的凭证查询 Secrets Manager 服务，如果成功，则会返回指定的密钥。有关 Secrets Manager 的更多信息，请参阅《Amazon Secrets Manager 用户指南》https://docs.amazonaws.cn/secretsmanager/latest/userguide/intro.html。

要下载使用此 Lambda 函数的示例 Amazon CloudFormation 模板，请访问提供的 Amazon S3 存储桶。 Amazon Transfer Family

对 Amazon CloudFormation 模板的改进

已发布的 CloudFormation模板已对 API Gateway 界面进行了改进。现在，这些模板在 API BASE64 Gateway 中使用经过编码的密码。如果没有此增强功能，您的现有部署可以继续运行，但不允许使用基本 US-ASCII 字符集之外的字符的密码。

启用此功能的模板更改如下：

- GetUserConfigRequest AWS::ApiGateway::Method资源必须有这个RequestTemplates代码（斜体行是更新的行）

```
RequestTemplates:
   application/json: |
   {
      "username": "$util.urlDecode($input.params('username'))",
      "password":
 "$util.escapeJavaScript($util.base64Decode($input.params('PasswordBase64'))).replaceAll("\
\'","'")",
      "protocol": "$input.params('protocol')",
      "serverId": "$input.params('serverId')",
      "sourceIp": "$input.params('sourceIp')"
}
```

- GetUserConfig资源必须更改RequestParameters为使用PasswordBase64标题（斜体行是更新的行）：

```
RequestParameters:
   method.request.header.PasswordBase64: false
   method.request.querystring.protocol: false
   method.request.querystring.sourceIp: false
```

检查堆栈的模板是否是最新的

1. 在 https://console.aws.amazon.com/cloudformation 上打开 Amazon CloudFormation 控制台。
2. 从堆栈列表中选择您的堆栈。
3. 在详细信息面板中，选择模板选项卡。
4. 寻找以下内容：

   - 搜索RequestTemplates并确保你有以下行：

     ```
     "password":
      "$util.escapeJavaScript($util.base64Decode($input.params('PasswordBase64'))).replaceAll(
     \'","''")",
     ```

   - 搜索RequestParameters并确保你有以下行：

     ```
     method.request.header.PasswordBase64: false
     ```

如果您没有看到更新的行，请编辑您的堆栈。有关如何更新 Amazon CloudFormation 堆栈的详细信息，请参阅《用户指南》中的Amazon CloudFormation修改堆栈模板。

使用多种身份验证方法

当您使用多种身份验证方法时，Transfer Family 服务器会控制 AND 逻辑。Transfer Family 将其视为向您的自定义身份提供者发出的两个单独请求：但是，它们的效果是结合在一起的。

两个请求都必须成功返回并返回正确的响应，才能完成身份验证。Transfer Family 要求这两个响应必须完整，这意味着它们包含所有必需的元素（角色、主目录、策略和 POSIX 配置文件（如果您使用 Amazon EFS 进行存储））。Transfer Family 还要求密码响应中不得包含公钥。

公钥请求必须有来自身份提供者的单独响应。使用 “密码或密钥” 或 “密码和密钥” 时，这种行为不会改变。

该 SSH/SFTP 协议首先向软件客户端发送公钥身份验证，然后请求密码身份验证。此操作要求在允许用户完成身份验证之前，两者都必须成功。

对于自定义身份提供商选项，您可以为如何进行身份验证指定以下任一选项。

- 密码或密钥-用户可以使用其密码或密钥进行身份验证。这是默认值。
- 仅限密码-用户必须提供密码才能连接。
- 仅限密钥 — 用户必须提供私钥才能连接。
- 密码和密钥 — 用户必须同时提供私钥和密码才能连接。服务器首先检查密钥，如果密钥有效，系统会提示输入密码。如果提供的私有密钥与存储的公有密钥不匹配，则身份验证失败。

IPv6 支持自定义身份提供商

Amazon Transfer Family 自定义身份提供商完全支持 IPv6 连接。在实现自定义身份提供商时，您的 Lambda 函数无需任何额外配置即可接收和处理来自双方 IPv4 和 IPv6 客户端的身份验证请求。Lambda 函数在请求`sourceIp`字段中接收客户端的 IP 地址，该地址可以是 IPv4 地址（例如`203.0.113.42`），也可以是 IPv6地址（例如）。`2001:db8:85a3:8d3:1319:8a2e:370:7348`您的自定义身份提供商实现应适当地处理这两种地址格式。

> **Important**
>
> 如果您的自定义身份提供商执行基于 IP 的验证或记录，请确保您的实现正确处理 IPv6 地址格式。 IPv6 地址比 IPv4 地址长，并且使用不同的符号格式。

> **Note**
>
> 在自定义身份提供商中处理 IPv6 地址时，请确保使用正确 IPv6 的地址解析函数，而不是简单的字符串比较。 IPv6地址可以用各种规范格式表示（例如`fd00:b600::ec2`或`fd00:b600:0:0:0:0:0:ec2`）。使用您的实现语言中的相应 IPv6 地址库或函数来正确验证和比较 IPv6 地址。

Example在自定义身份提供商中同时处理 IPv4 和 IPv6 地址

```
def lambda_handler(event, context):
```

```
    # Extract the source IP address from the request
    source_ip = event.get('sourceIp', '')

    # Log the client IP address (works for both IPv4 and IPv6)
    print(f"Authentication request from: {source_ip}")

    # Example of IP-based validation that works with both IPv4 and IPv6
    if is_ip_allowed(source_ip):
        # Continue with authentication
        # ...
    else:
        # Reject the authentication request
        return {
            "Role": "",
            "HomeDirectory": "",
            "Status": "DENIED"
        }
```

有关实现自定义身份提供商的更多信息，请参阅Amazon Lambda 用于整合您的身份提供商。

使用微软 Active Directory 的 Amazon 目录服务

您可以使用 Amazon Transfer Family 对文件传输的最终用户进行身份验证 Amazon Directory Service for Microsoft Active Directory。它可以无缝迁移依赖于活动目录身份验证的文件传输工作流程，而无需更改最终用户的凭证或需要自定义授权者。

使用 Amazon Managed Microsoft AD，您可以通过 SFTP、FTPS 和 FTP 安全地为 Amazon Directory Service 用户和群组提供对存储在亚马逊简单存储服务 (Amazon S3) 或亚马逊弹性文件系统 (Amazon EFS) 中的数据的访问权限。如果您使用活动目录来存储用户的凭证，则现在可以更轻松地为这些用户启用文件传输功能。

您可以使用 Active Directory 连接器在本地环境 Amazon Managed Microsoft AD 中或 Amazon 云端提供对 Active Directory 组的访问权限。你可以为已经在你的 Microsoft Windows 环境（无论是在 Amazon 云端还是在其本地网络中）中配置的用户提供访问 Amazon Managed Microsoft AD 用于身份的 Amazon Transfer Family 服务器的权限。 Amazon 存储博客包含一篇文章，详细介绍了将 Active Directory 与 Transfer Family 配合使用的解决方案：使用自定义身份提供程序简化 Active Directory 身份验证 Amazon Transfer Family。

> **Note**
>
> - Amazon Transfer Family 不支持 Simple AD。

- Transfer Family 不支持跨区域活动目录配置：我们仅支持与 Transfer Family 服务器位于同一区域的活动目录集成。
- Transfer Family 不支持使用 AD Connecto Amazon Managed Microsoft AD r 为现有的基于 RADIUS 的 MFA 基础设施启用多因素身份验证 (MFA)。
- Amazon Transfer Family 不支持托管活动目录的复制区域。

要使用 Amazon Managed Microsoft AD，必须执行以下步骤：

1. 使用 Amazon Directory Service 控制台创建一个或多个 Amazon Managed Microsoft AD 目录。
2. 使用 Transfer Family 控制台创建 Amazon Managed Microsoft AD 用作其身份提供者的服务器。
3. 使用 Amazon Active Directory 连接器设置目录。
4. 添加来自一个或多个 Amazon Directory Service 群组的访问权限。
5. 尽管不是必需的，但我们建议您测试和验证用户访问权限。

主题

- 在你开始使用之前 Amazon Directory Service for Microsoft Active Directory
- 使用活动目录领域
- 选择 Amazon Managed Microsoft AD 作为您的身份提供商
- 正在连接到本地微软 Active Directory
- 授予对组的访问权限
- 测试用户
- 删除群组的服务器访问权限
- 使用 SSH（安全外壳）连接到服务器
- 使用林和 Amazon Transfer Family 信任连接到自我管理的 Active Directory

在你开始使用之前 Amazon Directory Service for Microsoft Active Directory

> **Note**
>
> Amazon Transfer Family 默认限制为每台服务器 100 个 Active Directory 组。如果您的用例需要超过 100 个群组，请考虑使用自定义身份提供商解决方案，如使用自定义身份提供商简化 Active Directory 身份验证中所述 Amazon Transfer Family。

为您的 AD 组提供唯一标识符

在使用之前 Amazon Managed Microsoft AD，必须为 Microsoft AD 目录中的每个群组提供唯一标识符。您可以使用每个组的安全标识符 (SID) 来执行此操作。您关联的群组中的用户可以使用 Amazon Transfer Family 通过启用的协议访问您的 Amazon S3 或 Amazon EFS 资源。

使用以下 Windows PowerShell 命令检索组的 SID，*YourGroupName*替换为该组的名称。

```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties * | Select
 SamAccountName,ObjectSid
```

> **Note**
>
> 如果您使用 Amazon Directory Service 作为身份提供商，并且如果`userPrincipalName`和`SamAccountName`具有不同的值，则 Amazon Transfer Family 接受中的值`SamAccountName`。Transfer Family 不接受 `userPrincipalName` 中指定的值。

为您的角色添加 Amazon Directory Service 权限

您还需要 Amazon Directory Service API 权限才能 Amazon Directory Service 用作您的身份提供商。需要建议使用以下权限：

- `ds:DescribeDirectories` 是 Transfer Family 查找目录所必需的
- `ds:AuthorizeApplication` 是为 Transfer Family 添加授权所必需的
- `ds:UnauthorizeApplication` 是移除所有临时创建的资源，以防服务器创建过程中出现问题所建议的

将这些权限添加到您用于创建 Transfer Family 服务器的角色中。有关这些权限的更多详细信息，请参阅 Amazon Directory Service API 权限：操作、资源和条件参考。

使用活动目录领域

在考虑如何让活动目录用户访问 Amazon Transfer Family 服务器时，请记住用户的领域及其组的领域。理想情况下，用户的领域和他们所在群组的领域应该匹配。也就是说，用户和组都在默认领域中，或者两者都位于可信领域。如果不是这样，Transfer Family 将无法对用户进行身份验证。

您可以测试用户以确保配置正确。有关更多信息，请参阅 测试用户。如果 user/group 领域出现问题，您会收到错误消息，“找不到用户组的关联访问权限。

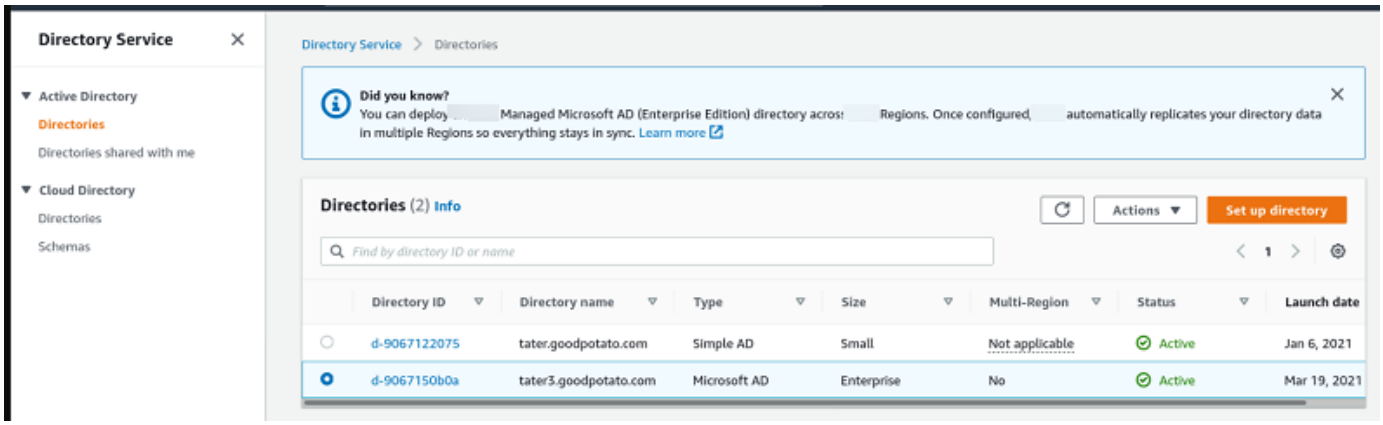
选择 Amazon Managed Microsoft AD 作为您的身份提供商

本节介绍如何与服务器 Amazon Directory Service for Microsoft Active Directory 配合使用。

要与 Transfer Family Amazon Managed Microsoft AD 一起使用

1. 登录 Amazon Web Services 管理控制台 并打开 Amazon Directory Service 控制台，网址为https://console.aws.amazon.com/directoryservicev2/。

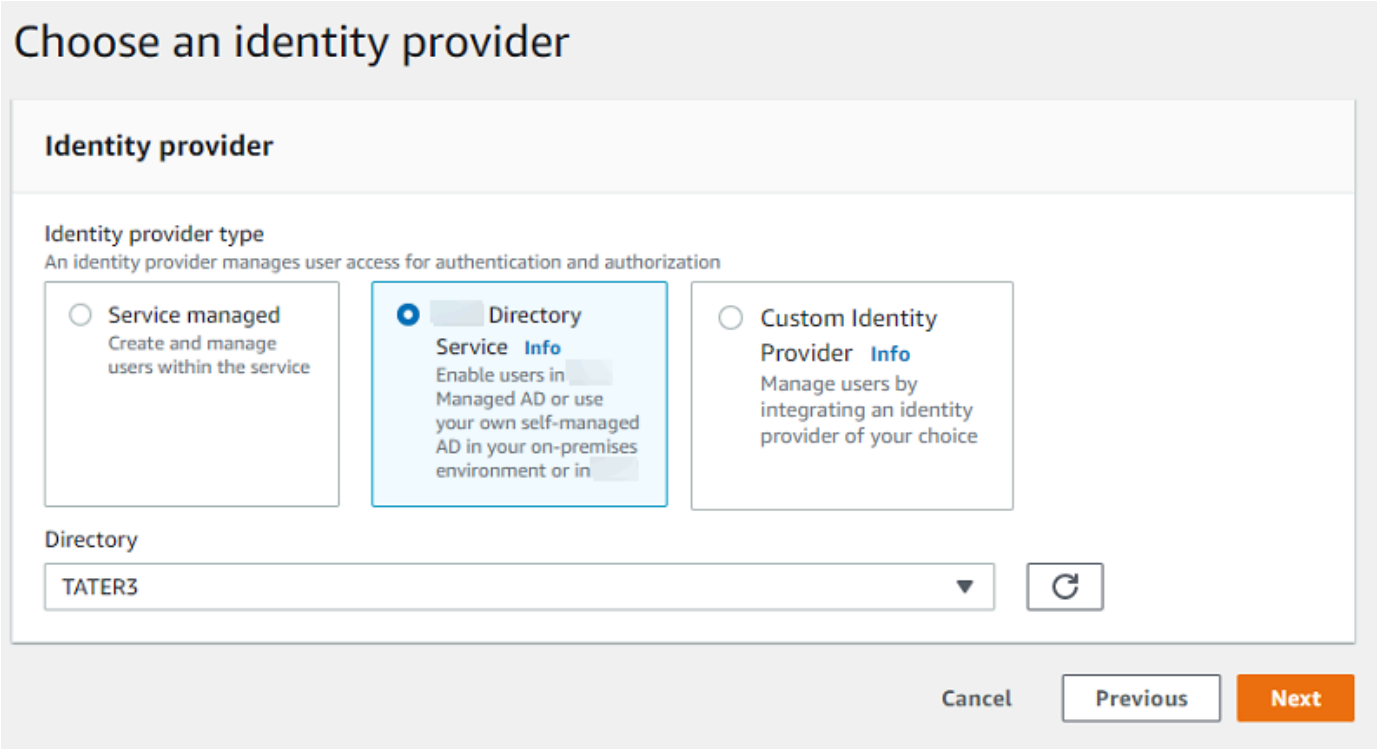
   使用 Amazon Directory Service 控制台配置一个或多个托管目录。有关更多信息，请参阅《 Amazon Directory Service 管理员指南》中的 Amazon Managed Microsoft AD。



2. 在打开 Amazon Transfer Family 控制台 https://console.aws.amazon.com/transfer/ ，然后选择创建服务器。
3. 在选择协议页面上，从列表中选择一个或多个协议。

   > **Note**
   >
   > 如果选择 FTPS，则必须提供 Amazon Certificate Manager 证书。

4. 在选择身份提供程序中，选择 Amazon 目录服务。



5. 目录列表包含您配置的所有托管目录。从列表中选择目录，然后选择下一步。

> **Note**
>
> - 不支持跨账户目录和共享目录。 Amazon Managed Microsoft AD
> - 要设置以 Directory Service 作为身份提供者的服务器，您需要添加一些 Amazon Directory Service 权限。有关更多信息，请参阅 在你开始使用之前 Amazon Directory Service for Microsoft Active Directory。

6. 要完成服务器的创建，请使用下列过程之一：

- 创建启用 SFTP 的服务器
- 创建启用 FTPS 的服务器
- 创建启用 FTP 的服务器

在这些步骤中，继续执行选择身份提供程序之后的步骤。

> **Important**
>
> Amazon Directory Service 如果你在 Transfer Family 服务器中使用了 Microsoft AD 目录，则无法将其删除。必须先删除服务器，然后才能删除目录。

正在连接到本地微软 Active Directory

本节介绍如何使用 AD Conn Amazon ector 设置目录

使用 AD Connector 设置您的 Amazon 目录

1. 打开 Directory Service 控制台并选择目录。
2. 选择设置目录。
3. 对于目录类型，请选择 AD Connector。
4. 选择目录大小，选择下一步，然后选择您的 VPC 和子网。
5. 选择 下一步，然后如下所示填写各字段：
   - 目录 DNS 名称：输入你用于 Microsoft Active Directory 的域名。
   - DNS IP 地址：输入你的微软 Active Directory IP 地址。
   - 服务器帐户用户名和密码：输入要使用的服务帐户的详细信息。
6. 完成屏幕内容以创建目录服务。

下一步是使用 SFTP 协议创建一个 Transfer Family 服务器，身份提供者类型为 Amazon Directory Service。从目录下拉列表中，选择您在上一个过程中添加的目录。

授予对组的访问权限

创建服务器后，必须使用已启用的协议选择目录中哪些组有权通过已启用的协议上传和下载文件 Amazon Transfer Family。您可以通过创建访问权限来实现此目的。

> **Note**
>
> Amazon Transfer Family 默认限制为每台服务器 100 个 Active Directory 组。如果您的用例需要超过 100 个群组，请考虑使用自定义身份提供商解决方案，如使用自定义身份提供商简化 Active Directory 身份验证中所述 Amazon Transfer Family。

> **Note**
>
> 用户必须直接属于您授予访问权限的群组。例如，假设 Bob 是用户并属于 GroupA，而 groupA 本身包含在 groupB 中。
>
> - 如果您向 GroupA 授予访问权限，Bob 就会被授予访问权限。
> - 如果您授予对 GroupB（而不是 GroupA）的访问权限，则 Bob 没有访问权限。

向组授予访问权限

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 导航到您的服务器详细信息页面。
3. 在访问权限部分中，选择添加访问权限。
4. 输入您想要访问此服务器的 Amazon Managed Microsoft AD 目录的 SID。

   > **Note**
   >
   > 有关如何查找组的 SID 的信息，请参阅 the section called “在你开始使用之前 Amazon Directory Service for Microsoft Active Directory”。

5. 对于访问权限，请为群组选择一个 Amazon Identity and Access Management (IAM) 角色。
6. 在策略部分，选择一个策略。默认设置为无。
7. 对于主目录，选择与该组的主目录对应的 Amazon S3 存储桶。

   > **Note**
   >
   > 您可以通过创建会话策略来限制用户在存储桶中看到的部分。例如，要将用户限制在 `/filetest` 目录下他们自己的文件夹中，请在框中输入以下文本。
   >
   > ```
   > /filetest/${transfer:UserName}
   > ```
   >
   > 要了解有关创建会话策略的更多信息，请参阅 为 Amazon S3 存储桶创建会话策略。

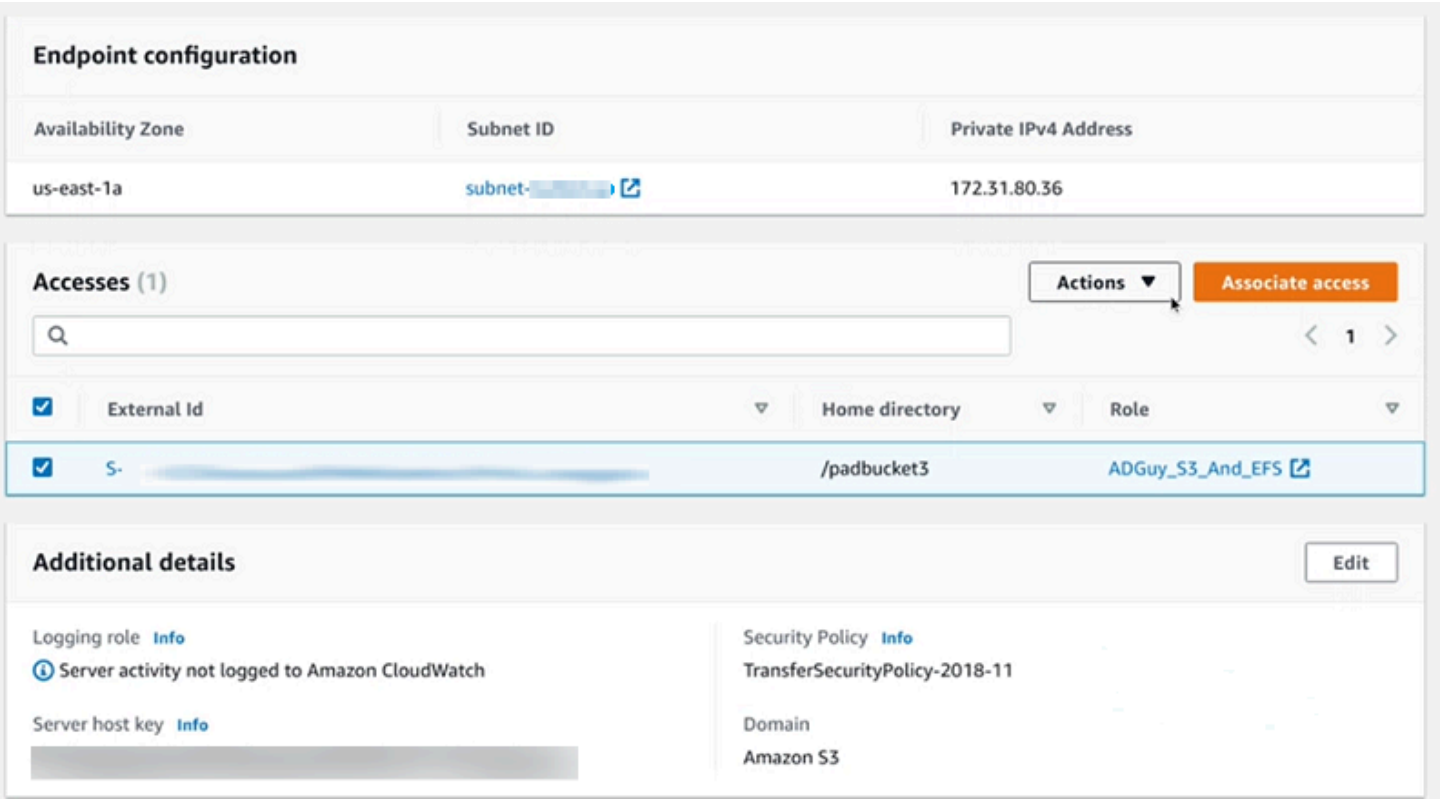
8. 选择添加以创建关联。
9. 请选择您的服务器。
10. 选择添加访问权限。

- 输入该组的 SID。

> **Note**
>
> 有关如何查找 SID 的信息，请参阅 the section called “在你开始使用之前 Amazon Directory Service for Microsoft Active Directory”。

11. 选择添加访问权限。

在访问权限部分中，列出了服务器的访问权限。



测试用户

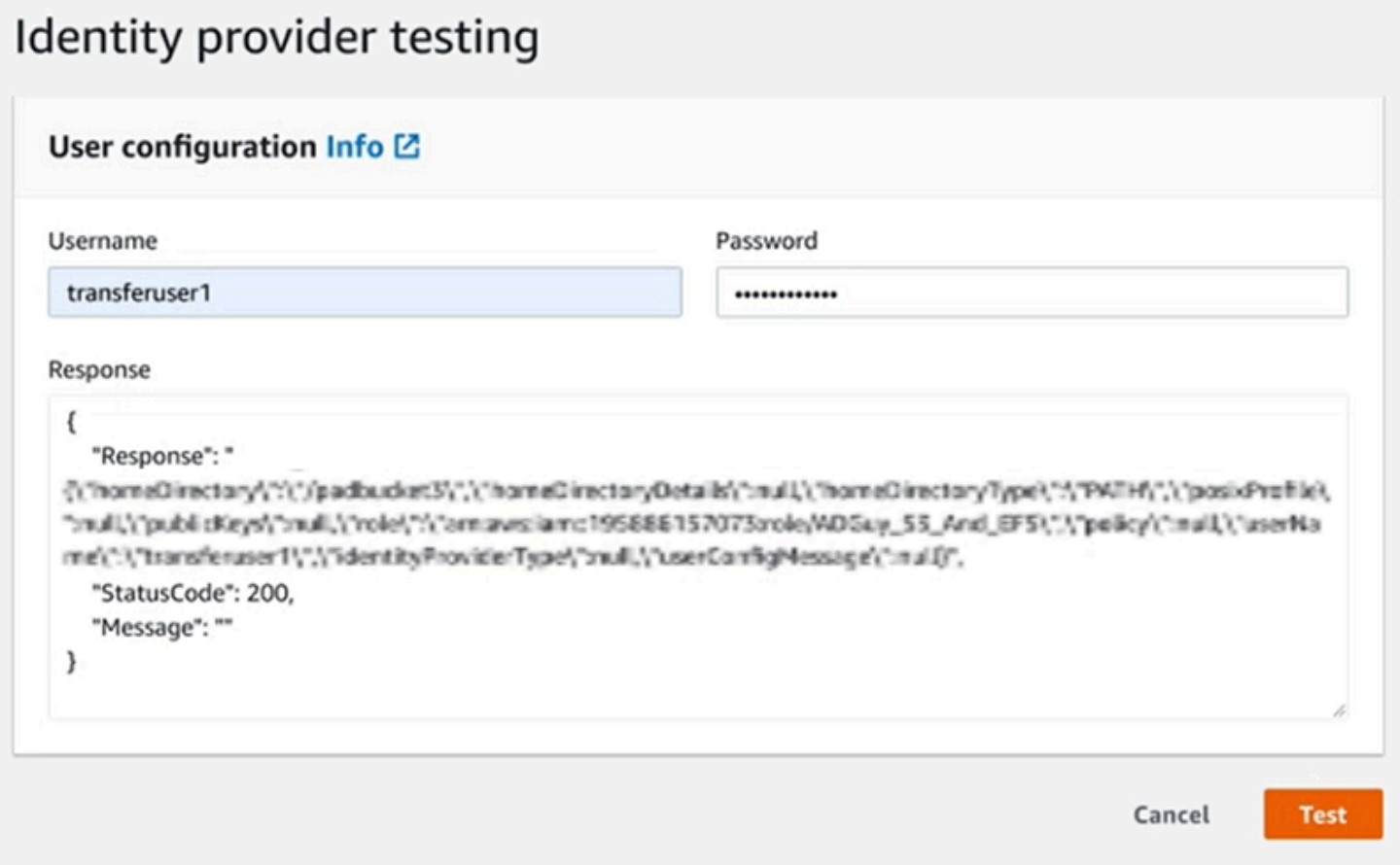
您可以测试用户是否有权访问您的服务器的 Amazon Managed Microsoft AD 目录。

> **Note**
>
> 用户必须正好属于端点配置页面的访问权限部分中列出的一个组（外部 ID）。如果用户不属于任何群组，或者属于多个群组，则不会向该用户授予访问权限。

测试特定用户是否具有访问权限

1. 在服务器详细信息页面上，选择操作，然后选择测试。
2. 要进行身份提供程序测试，请输入其中一个具有访问权限的群组中的用户的登录凭证。
3. 选择测试。

您会看到身份提供程序测试成功，显示所选用户已被授予服务器访问权限。



如果用户属于多个具有访问权限的群组，则您会收到以下响应。

```
"Response":"",
"StatusCode":200,
"Message":"More than one associated access found for user's groups."
```

删除群组的服务器访问权限

删除群组的服务器访问权限

1. 在服务器详细信息页面上，选择操作，然后选择删除访问权限。

2. 在对话框中，确认您要移除该组的访问权限。

返回到服务器详细信息页面时，您会看到不再列出该组的访问权限。

使用 SSH（安全外壳）连接到服务器

配置服务器和用户后，您可以使用 SSH 连接到服务器，并使用具有访问权限的用户的完全限定用户名。

```
sftp user@active-directory-domain@vpc-endpoint
```

例如：`transferuserexample@mycompany.com@vpce-0123456abcdef-789xyz.vpc-svc-987654zyxabc.us-east-1.vpce.amazonaws.com`。

此格式以联合身份验证搜索为目标，限制了对可能很大的活动目录的搜索。

> **Note**
>
> 您可以指定简单的用户名。但是，在这种情况下，活动目录代码必须搜索联合身份验证中的所有目录。这可能会限制搜索，即使用户本应具有访问权限，身份验证也可能失败。

身份验证后，用户位于在配置用户时指定的主目录中。

使用林和 Amazon Transfer Family 信任连接到自我管理的 Active Directory

Amazon Directory Service 有以下选项可用于连接到自我管理的 Active Directory：

- 单向林信任（来自本地 Active Directory 的传出 Amazon Managed Microsoft AD 和传入）仅适用于根域。
- 对于子域，您可以使用以下方法之一：
  - 在 Amazon Managed Microsoft AD 和本地活动目录之间使用双向信任
  - 对每个子域使用单向外部信任。

例如，当使用可信域连接到服务器时，用户需要指定可信域，例如 `transferuserexample@mycompany.com`。

将 Amazon Directory Service 用于 Entra ID 域服务

对于只需要 SFTP 传输且不想管理域的客户，可以使用 Simple Active Directory。或者，想要在完全托管的服务中享受 活动目录的好处和高可用性的客户可以使用 Amazon 托管 Microsoft AD。最后，对于想要利用现有活动目录林进行 SFTP 传输的客户，可以使用 Active Directory Connector。

请注意以下几点：

- 要利用现有的活动目录林来满足 SFTP 传输需求，可以使用 Active Directory Connector。
- 如果您想在完全托管的服务中获得活动目录的好处和高可用性，则可以使用 Amazon Directory Service for Microsoft Active Directory。有关更多信息，请参阅 使用微软 Active Directory 的 Amazon 目录服务。

本主题介绍如何使用 Active Directory 连接器和 E ntra ID（以前称为 Azure AD）域服务对具有 Entra ID 的 SFTP Transfer 用户进行身份验证。

主题

- 在开始使用 Entra ID 域服务的 Di Amazon rectory Service 之前
- 步骤 1：添加 Entra ID 域服务
- 步骤 2：创建服务账号
- 步骤 3：使用 AD Connector 设置 Amazon 目录
- 步骤 4：设置 Amazon Transfer Family 服务器
- 步骤 5：授予对组的访问权限
- 步骤 6：测试用户

在开始使用 Entra ID 域服务的 Di Amazon rectory Service 之前

> **Note**
>
> Amazon Transfer Family 默认限制为每台服务器 100 个 Active Directory 组。如果您的用例需要超过 100 个群组，请考虑使用自定义身份提供商解决方案，如使用自定义身份提供商简化 Active Directory 身份验证中所述 Amazon Transfer Family。

对于 Amazon，你需要以下内容：

- 位于您使用 Transfer Family 服务器的 Amazon 区域中的虚拟私有云 (VPC)
- 您的 VPC 中至少有两个私有子网
- VPC 必须具备互联网连接
- 用于与 Microsoft Entra 的 site-to-site VPN 连接的客户网关和虚拟专用网关

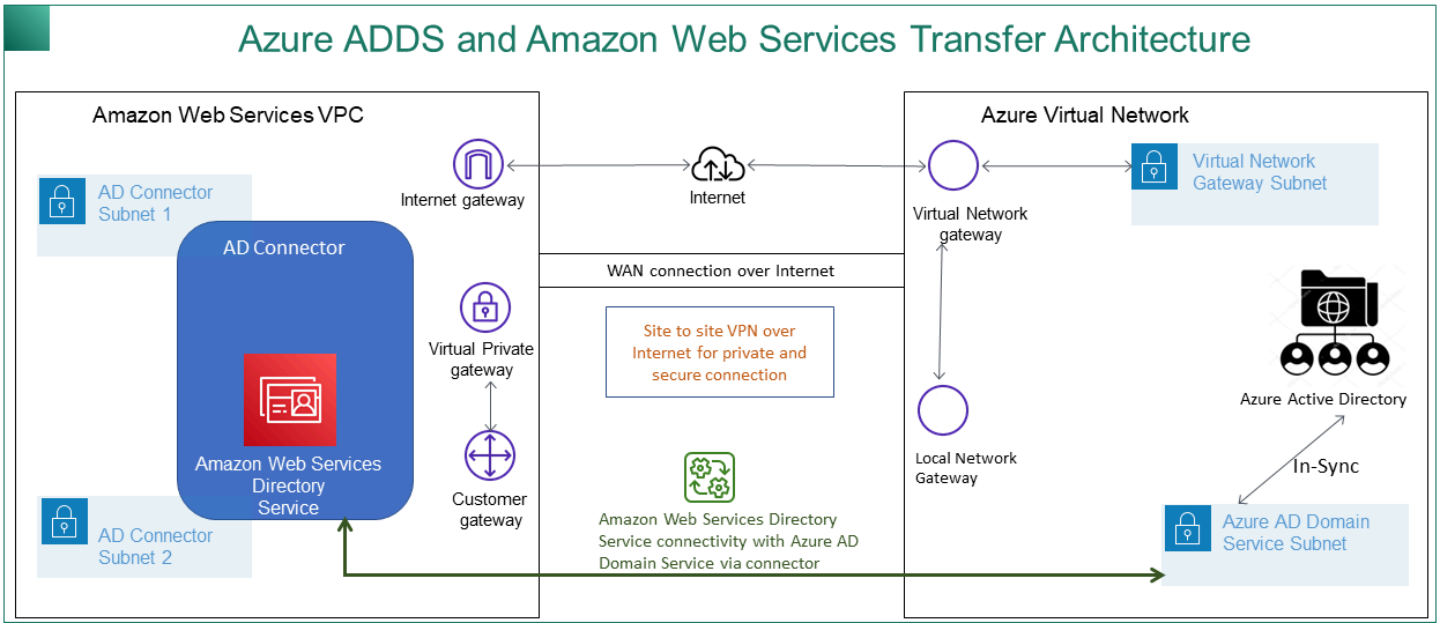
对于 Microsoft Entra，你需要以下内容：

- Entra ID 和活动目录域服务
- Entra 资源组
- Entra 虚拟网络
- 您的 Amazon VPC 和 Entra 资源组之间的 VPN 连接

> **Note**
>
> 这可以通过本地 IPSEC 隧道或使用 VPN 设备实现。在本主题中，我们使用 Entra 虚拟网络网关和本地网络网关之间的 IPSEC 隧道。必须将隧道配置为允许 Entra Domain Service 终端节点和容纳 VPC Amazon 的子网之间的流量。

- 用于与 Microsoft Entra 的 site-to-site VPN 连接的客户网关和虚拟专用网关

下图显示了在开始之前所需的配置。

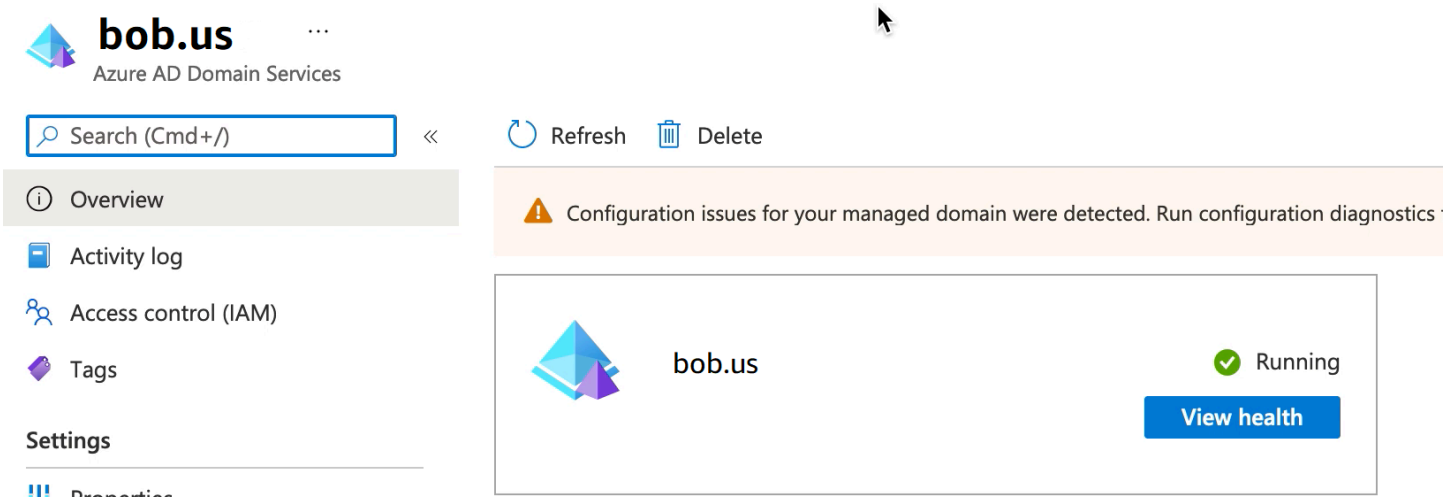


步骤 1：添加 Entra ID 域服务

默认情况下，Entra ID 不支持域加入实例。要执行诸如加入域之类的操作以及使用组策略等工具，管理员必须启用 Entra ID 域服务。如果您尚未添加 Entra DS，或者您的现有实现与您希望 SFTP 传输服务器使用的域名没有关联，则必须添加一个新实例。

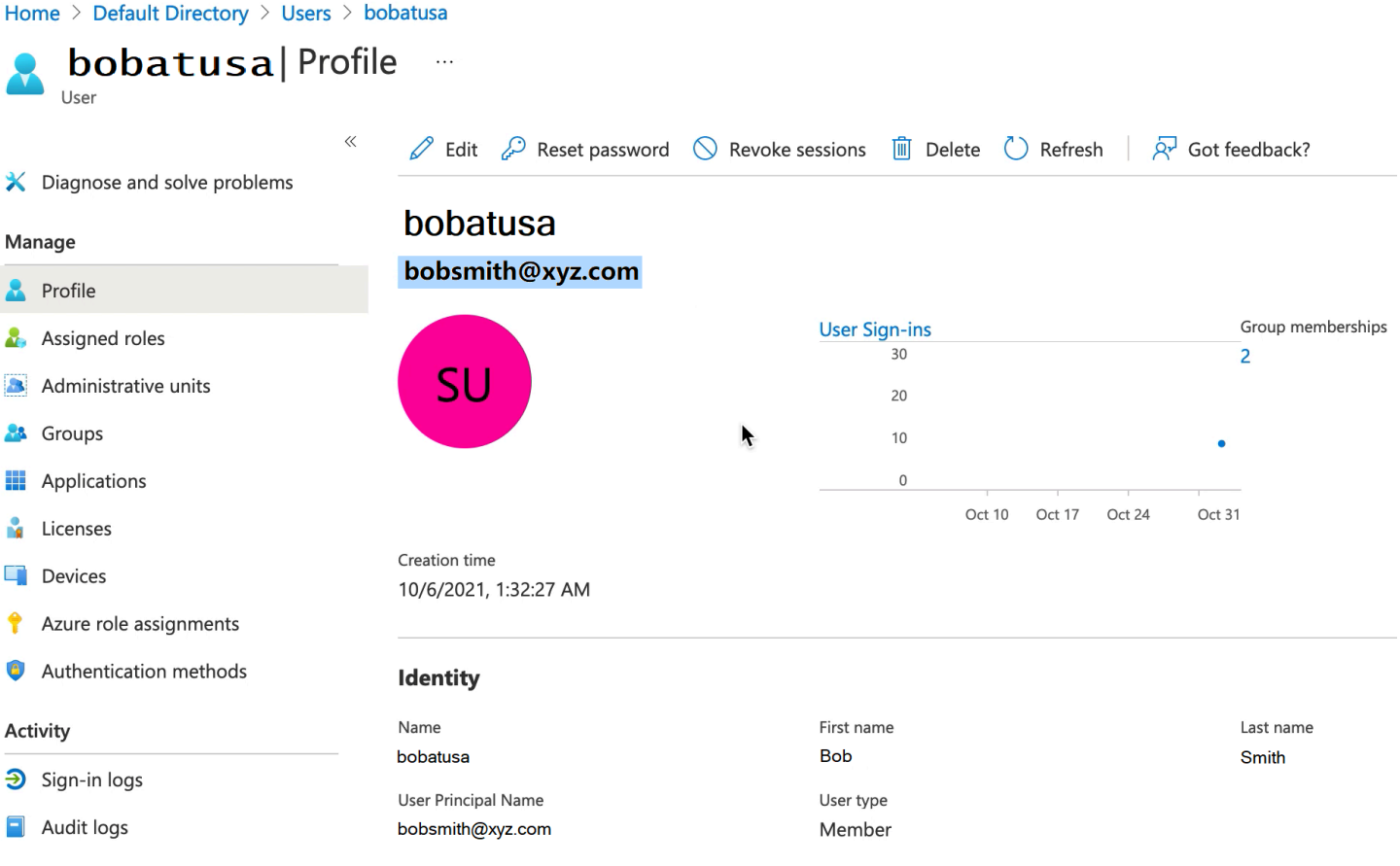
有关启用 Entra ID 域服务的信息，请参阅教程：创建和配置 Microsoft Entra Domain Services 托管域。

> **Note**
>
> 启用 Entra DS 时，请确保已为连接到 SFTP 传输服务器的资源组和 Entra 域进行了配置。



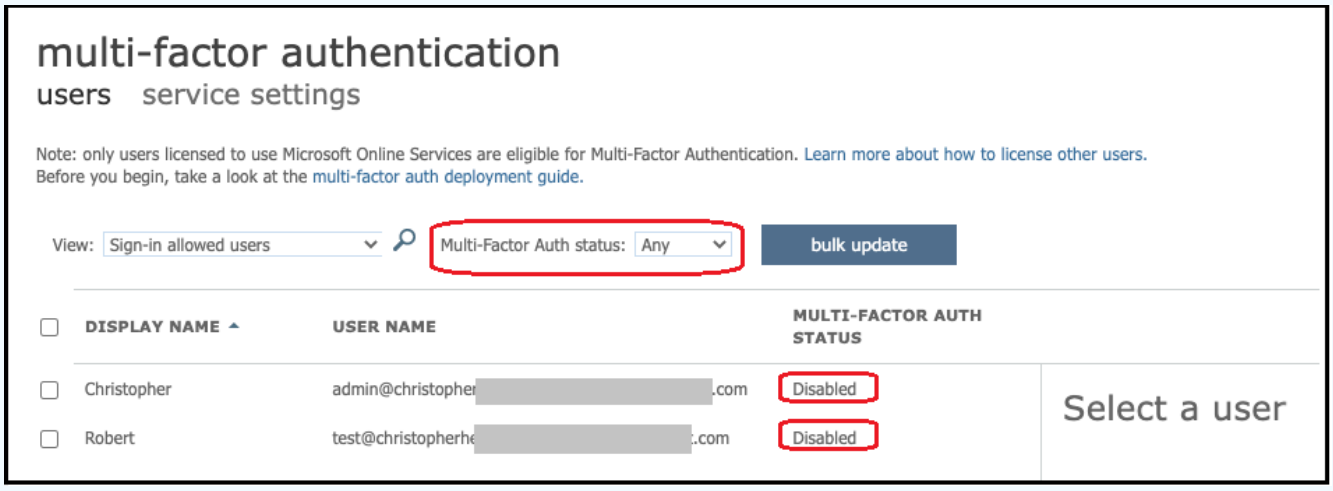
步骤 2：创建服务账号

Entra 必须有一个属于 Entra DS 中管理员组的服务帐户。此帐户与 Act Amazon ive Directory 连接器一起使用。请确保此账户与 Entra DS 同步。



Tip

使用 SFTP 协议的 Transfer Family 服务器不支持 Entra ID 的多重身份验证。在用户向 SFTP 进行身份验证后，Transfer Family 服务器无法提供 MFA 令牌。在尝试连接之前，请务必禁用 MFA。



步骤 3：使用 AD Connector 设置 Amazon 目录

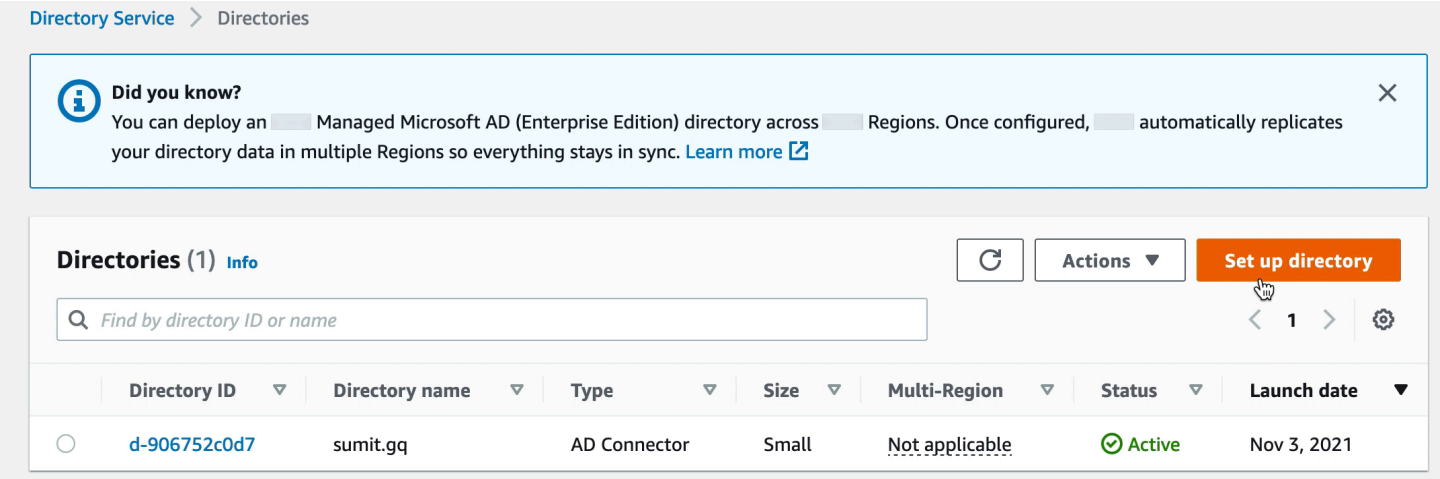
在您配置 Entra DS 并在您的 VPC 和 Entra Virtual 网络之间创建具有 IPSE Amazon C VPN 隧道的服务账户后，您可以通过从任何实例执行 ping Entra DS DNS IP 地址来测试连接。 Amazon EC2

在您确认连接处于活动状态后，您可以继续执行以下操作。

使用 AD Connector 设置您的 Amazon 目录

1. 打开 Directory Service 控制台并选择目录。
2. 选择设置目录。
3. 对于目录类型，请选择 AD Connector。
4. 选择目录大小，选择下一步，然后选择您的 VPC 和子网。
5. 选择 下一步，然后如下所示填写各字段：
   - 目录 DNS 名称：输入您用于 Entra DS 的域名。
   - DNS IP 地址：输入您的 Entra DS IP 地址。
   - 服务器账户用户名和密码：输入您在步骤 2：创建服务账户中创建的服务账户的详细信息。
6. 完成屏幕内容以创建目录服务。

现在，目录状态应为活动，并且可以与 SFTP 传输服务器一起使用了。



步骤 4：设置 Amazon Transfer Family 服务器

使用 SFTP 协议创建 Transfer Family 服务器，身份提供者类型为 Amazon Directory Service。从目录下拉列表中，选择您在步骤 3：使用 AD Connector 设置 Amazon 目录中添加的目录。

> **Note**
>
> 如果你在 Transfer Family 服务器中使用了 Microsoft AD Amazon 目录，则无法将其删除。必须先删除服务器，然后才能删除目录。

步骤 5：授予对组的访问权限

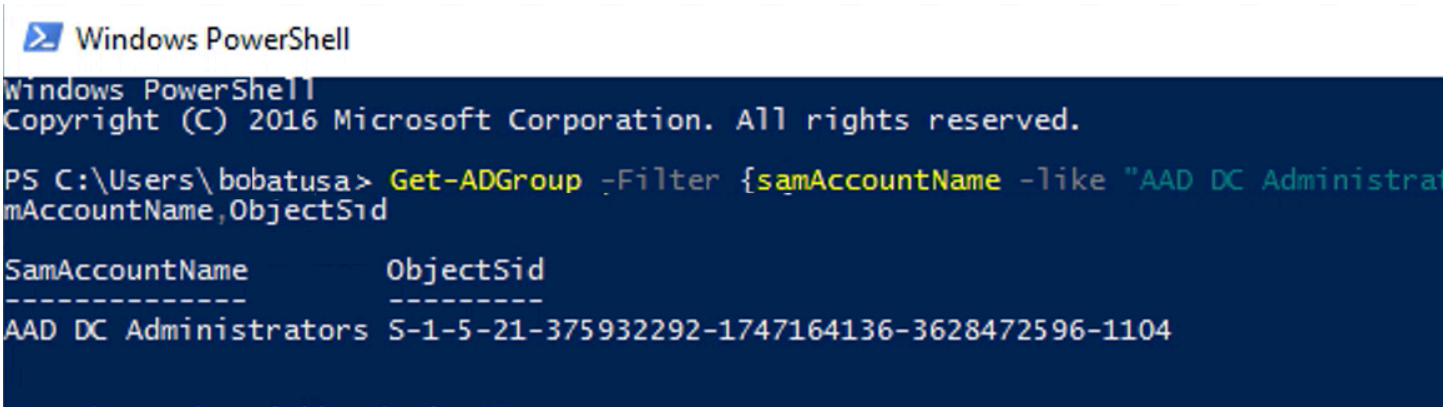
创建服务器后，必须使用已启用的协议选择目录中哪些组有权通过已启用的协议上传和下载文件 Amazon Transfer Family。您可以通过创建访问权限来实现此目的。

> **Note**
>
> 用户必须直接属于您授予访问权限的群组。例如，假设 Bob 是用户并属于 GroupA，而 groupA 本身包含在 groupB 中。
>
> - 如果您向 GroupA 授予访问权限，Bob 就会被授予访问权限。
> - 如果您授予对 GroupB（而不是 GroupA）的访问权限，则 Bob 没有访问权限。

要授予访问权限，您需要检索该组的 SID。

使用以下 Windows PowerShell 命令检索组的 SID，*YourGroupName*替换为该组的名称。

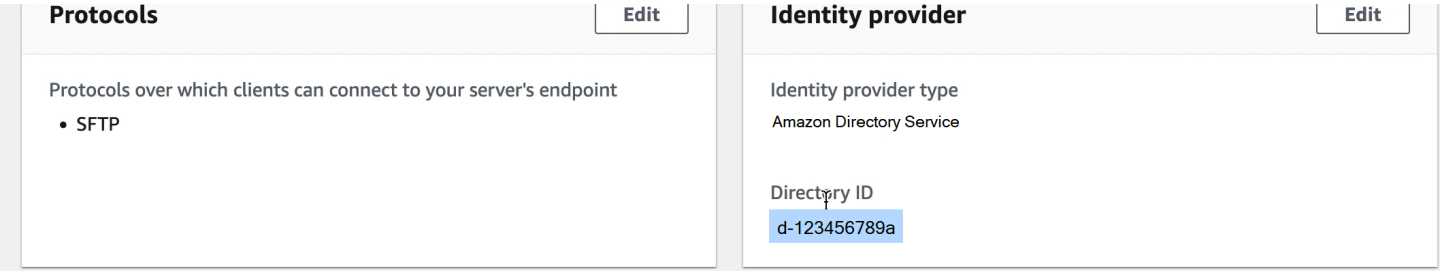
```
Get-ADGroup -Filter {samAccountName -like "YourGroupName*"} -Properties * | Select
 SamAccountName,ObjectSid
```

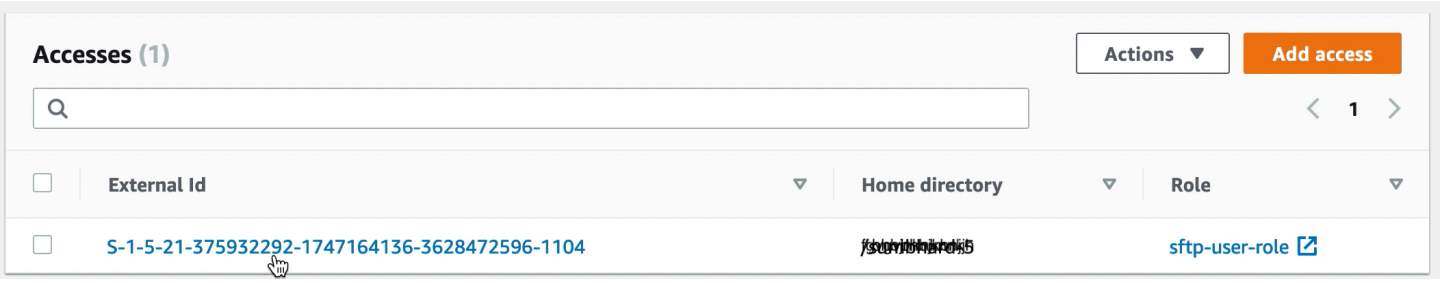


授予对组的访问权限

1. 打开 https://console.aws.amazon.com/transfer/。
2. 导航到您的服务器详细信息页面，然后在访问权限部分中，选择添加访问权限。
3. 输入您从上一个过程的输出中收到的 SID。
4. 在 “访问权限” 中，为群组选择一个 Amazon Identity and Access Management 角色。
5. 在策略部分，选择一个策略。默认值为 None（无）。
6. 对于主目录，选择与该组的主目录对应的 Amazon S3 存储桶。
7. 选择添加以创建关联。

您的 Transfer 服务器中的详细信息应类似于以下内容：





步骤 6：测试用户

您可以测试 (测试用户) 用户是否有权访问您的服务器的 Amazon Managed Microsoft AD 目录。用户必须正好属于端点配置页面的访问权限部分中列出的一个组（外部 ID）。如果用户不属于任何群组，或者属于多个群组，则不会向该用户授予访问权限。

使用逻辑目录简化您的 Transfer Family 目录结构

逻辑目录简化了您的 Amazon Transfer Family 服务器目录结构。使用逻辑目录，您可以创建具有用户友好名称的虚拟目录结构，用户在连接到 Amazon S3 存储桶或 Amazon EFS 文件系统时可以浏览该结构。这可以防止用户看到实际的目录路径、存储桶名称和文件系统名称。

> **Note**
>
> 您应该使用会话策略，以便您的最终用户只能执行您允许他们执行的操作。
> 您应该使用逻辑目录为最终用户创建用户友好的虚拟目录，并抽象存储桶名称。逻辑目录映射仅允许用户访问其指定的逻辑路径和子目录，禁止使用遍历逻辑根目录的相对路径。
> Transfer Family 会验证可能包含相对元素的每条路径，并在我们将这些路径传递给 Amazon S3 之前主动阻止解析这些路径；这样可以防止您的用户超越其逻辑映射。
> 尽管 Transfer Family 会阻止您的最终用户访问其逻辑目录之外的目录，但我们也建议您使用唯一的角色或会话策略在存储级别强制执行最低权限。

了解 chroot 和目录结构

chroot 操作允许您将用户的根目录设置为存储层次结构中的任何位置。这会将用户限制在他们配置的主目录或根目录中，从而阻止访问更高级别的目录。

假设一个 Amazon S3 用户仅限于`amzn-s3-demo-bucket/home/${transfer:UserName}`。如果没有 chroot，某些客户端可能会允许用户向上移至 /amzn-s3-demo-bucket/home，需要注销并登录才能返回到正确的目录。执行 chroot 操作可以防止出现此问题。

您可以跨多个存储桶和前缀创建自定义目录结构。如果您的工作流程需要仅靠存储桶前缀无法提供的特定目录布局，则此功能非常有用。您还可以链接到 Amazon S3 中的多个非连续位置，类似于在 Linux 文件系统中创建符号链接，其中您的目录路径引用文件系统中的不同位置。

使用逻辑目录的规则

本节介绍使用逻辑目录的一些规则和其他注意事项。

映射限制

- 如果`Entry`是，则只允许一个映射`"/"`（不允许重叠路径）。
- 对于自定义 IDP 和 AD 用户，逻辑目录支持最大 2.1 MB 的映射，为服务管理的用户支持最大 2,000 个条目的映射。您可以按如下方式计算映射大小：
  1. 用格式写出一个典型的映射`{"Entry":"/`*`entry-path`*`","Target":"/`*`target-path`*`"}`，其中*`entry-path`*和*`target-path`*是你将要使用的实际值。
  2. 计算该字符串中的字符，然后添加一 (1)。
  3. 将该数字乘以服务器的近似映射数。

如果您在步骤 3 中估计的数字小于 2.1 MB，则您的映射在可接受的限制范围内。

目标路径要求

- 如果存储桶或文件系统路径已根据用户名进行了参数化，则使用`${transfer:UserName}`变量。
- 只要关联的 IAM 角色具有访问这些存储位置的必要权限，就可以将目标配置为指向不同的 Amazon S3 存储桶或文件系统。
- 所有目标必须以正斜杠 (/) 开头，但不能以正斜杠 () 结尾。例如，`/amzn-s3-demo-bucket/images`是正确的，while `amzn-s3-demo-bucket/images` an `/amzn-s3-demo-bucket/images/` d 不是。

存储注意事项

- Amazon S3 是一个对象存储，其中的文件夹仅作为虚拟概念存在。使用 Amazon S3 存储时，即使没有带有尾部斜杠的零字节对象，Transfer Family 也会在 STAT 操作中将前缀报告为目录。在 STAT 操作中，带有尾部斜杠的正确零字节对象也被报告为目录。《亚马逊简单存储服务用户指南》中的使用文件夹在 Amazon S3 控制台中组织对象中描述了此行为。
- 对于需要区分文件和文件夹的应用程序，请使用亚马逊弹性文件系统 (Amazon EFS) 作为您的 Transfer Family 存储选项。
- 如果您为用户指定逻辑目录值，则使用的参数取决于用户的类型：
  - 对于服务托管的用户，请在 `HomeDirectoryMappings` 中提供逻辑目录值。
  - 对于自定义身份提供商用户，请在中提供逻辑目录值`HomeDirectoryDetails`。

用户目录值

- 用于指定逻辑目录值的参数取决于您的用户类型：
  - 对于服务托管的用户，请在 `HomeDirectoryMappings` 中提供逻辑目录值。
  - 对于自定义身份提供商用户，请在中提供逻辑目录值`HomeDirectoryDetails`。
- 使用 LOGICAL 时 HomeDirectoryType，您可以为服务托管用户、Active Directory 访问权限和自定义身份提供者实现指定一个 HomeDirectory值， HomeDirectoryDetails 这些实现将在响应中提供。如果未指定， HomeDirectory 则默认为`/`。

有关如何实现逻辑目录的详细信息，请参阅实现逻辑目录。

实现逻辑目录

> **Important**
>
> 根目录要求
>
> - 如果您未使用 Amazon S3 性能优化设置，则启动时必须存在根目录。
> - 对于 Amazon S3，这意味着创建一个以正斜杠 () / 结尾的零字节对象。
> - 为避免此要求，请考虑在创建或更新服务器时启用 Amazon S3 性能优化。
> - HomeDirectory 使用 LOGICAL 指定 a 时 HomeDirectoryType，该值必须映射到您的一个逻辑目录映射。该服务在用户创建和更新过程中都会对此进行验证，以防止配置失效。
>
> 逻辑主目录配置
> 使用 LOGICAL 作为您的时 HomeDirectoryType，请注意以下几点：
>
> - 该 HomeDirectory 值必须对应于您现有的逻辑目录映射之一。
> - 在用户创建和更新过程中，系统会自动对此进行验证。
> - 此验证可防止可能导致访问问题的配置。

启用逻辑目录

要为用户使用逻辑目录，请将`HomeDirectoryType`参数设置为`LOGICAL`。在创建新用户或更新现有用户时执行此操作。

```
"HomeDirectoryType": "LOGICAL"
```

`chroot`为用户启用

对于 chroot，创建一个由每个用户的单个 `Entry` 和 `Target` 配对组成的目录结构。Entry/代表根文件夹，而 Targ et 则指定存储桶或文件系统中的实际位置。

Example for Amazon S3

```
[{"Entry": "/", "Target": "/amzn-s3-demo-bucket/jane"}]
```

Example for Amazon EFS

```
[{"Entry": "/", "Target": "/fs-faa1a123/jane"}]
```

您可以像前面的示例一样使用绝对路径，也可以使用 ${transfer:UserName} 动态替换用户名，如下例所示。

```
[{"Entry": "/", "Target":
"/amzn-s3-demo-bucket/${transfer:UserName}"}]
```

在前面的示例中，用户被锁定到其根目录，且无法在层次结构中向上移动。

虚拟目录结构

对于虚拟目录结构，只要用户的 IAM 角色映射有权访问它们，您就可以创建多个 Entry Target 配对，目标位于您的 S3 存储桶或 EFS 文件系统的任意位置，包括跨多个存储桶或文件系统。

在以下虚拟结构示例中，当用户登录 Amazon SFTP 时，他们位于根目录中，子目录为/pics、/doc/reporting、和。/anotherpath/subpath/financials

> **Note**
>
> 除非您选择优化 Amazon S3 目录的性能（当您创建或更新服务器时），否则如果目录尚不存在，则用户或管理员需要创建这些目录。避免这个问题是考虑优化 Amazon S3 性能的理由。对于 Amazon EFS，您仍然需要管理员来创建逻辑映射或/目录。

```
[
{"Entry": "/pics", "Target": "/amzn-s3-demo-bucket1/pics"},
{"Entry": "/doc", "Target": "/amzn-s3-demo-bucket1/anotherpath/docs"},
{"Entry": "/reporting", "Target": "/amzn-s3-demo-bucket2/Q1"},
{"Entry": "/anotherpath/subpath/financials", "Target": "/amzn-s3-demo-bucket2/
financials"}]
```

Note

您只可以将文件上传到映射的特定文件夹。这意味着，在前面的示例中，您不能上传到 `/anotherpath` 或 `anotherpath/subpath` 目录；仅限 `anotherpath/subpath/financials`。您也无法直接映射到这些路径，因为不允许重叠路径。
例如，假设您创建以下映射：

```
{
   "Entry": "/pics",
   "Target": "/amzn-s3-demo-bucket/pics"
},
{
   "Entry": "/doc",
   "Target": "/amzn-s3-demo-bucket/mydocs"
},
{
   "Entry": "/temp",
   "Target": "/amzn-s3-demo-bucket2/temporary"
}
```

您只可以将文件上传到这些存储桶中。当您首次通过 `sftp` 连接时，您会被放到根目录 `/` 中。如果您尝试将文件上传到该目录，则上传将失败。以下命令显示了一个示例序列：

```
sftp> pwd
Remote working directory: /
sftp> put file
Uploading file to /file
remote open("/file"): No such file or directory
```

要上传到任何 `directory/sub-directory`，必须将路径明确映射到 `sub-directory`。

有关配置逻辑目录以及chroot为用户配置逻辑目录的更多信息，包括您可以下载和使用的 Amazon CloudFormation 模板，请参阅 Amazon 存储博客中的使用 chroot 和逻辑目录简化 Amazon SFTP 结构。

配置逻辑目录示例

在此示例中，我们创建一个用户并分配两个逻辑目录。以下命令使用逻辑目录 `pics` 和 `doc` 创建新用户（适用于现有的 Transfer Family 服务器）。

```
aws transfer create-user \
    --user-name marymajor \
    --server-id s-11112222333344445 \
    --role arn:aws:iam::1234abcd5678:role/marymajor-role \
    --home-directory-type LOGICAL \
    --home-directory-mappings "[{\"Entry\":\"/pics\", \"Target\":\"/amzn-s3-demo-
bucket1/pics\"}, {\"Entry\":\"/doc\", \"Target\":\"/amzn-s3-demo-bucket2/test/mydocs
\"}]" \
    --ssh-public-key-body file://~/.ssh/id_rsa.pub
```

如果 **marymajor** 是现有用户并且她的主目录类型是 PATH，则您可以使用与前一个命令类似的命令将其更改为 LOGICAL。

```
aws transfer update-user \
    --user-name marymajor \
    --server-id s-11112222333344445 \
    --role arn:aws:iam::1234abcd5678:role/marymajor-role \
    --home-directory-type LOGICAL \
    --home-directory-mappings "[{\"Entry\":\"/pics\", \"Target\":\"/amzn-s3-demo-
bucket1/pics\"}, {\"Entry\":\"/doc\", \"Target\":\"/amzn-s3-demo-bucket2/test/mydocs
\"}]"
```

请注意以下几点：

- 如果目录 /amzn-s3-demo-bucket1/pics 和 /amzn-s3-demo-bucket2/test/mydocs 尚未存在，则用户（或管理员）需要创建这些目录。

  > **Note**
  >
  > 如果您配置了优化的目录，则这些目录将由 Transfer Family 服务器自动创建。

- **marymajor**连接到服务器并运行`ls -l`命令时，Mary 会看到以下内容：

  ```
  drwxr--r--   1        -        -        0 Mar 17 15:42 doc
  drwxr--r--   1        -        -        0 Mar 17 16:04 pics
  ```

- **marymajor** 无法在此级别创建任何文件或目录。但是，在 pics 和 doc 中，她可以添加子目录。
- Mary 添加`pics`和添加到 Amazon S3 路径的文件将`doc`/amzn-s3-demo-bucket2/test/mydocs分别添加到 Amazon S3 路径/amzn-s3-demo-bucket1/pics和。

- 在此示例中，我们指定两个不同的存储桶来说明这种可能性。但是，您可以将同一个存储桶用于为用户指定的多个或所有逻辑目录。

此示例为逻辑主路径提供了另一种配置。

```
aws transfer create-user \
    --user-name marymajor \
    --server-id s-11112222333344445 \
    --role arn:aws:iam::1234abcd5678:role/marymajor-role \
    --home-directory-type LOGICAL \
    --home-directory /home/marymajor \
    --home-directory-mappings "[{\"Entry\":\"/home/marymajor/pics\", \"Target\":\"/
amzn-s3-demo-bucket1/pics\"}, {\"Entry\":\"/home/marymajor/doc\", \"Target\":\"/amzn-
s3-demo-bucket2/test/mydocs\"}]" \
    --ssh-public-key-body file://~/.ssh/id_rsa.pub
```

请注意以下几点：

- 映射提供了一个公共路径/home/marymajor，即两个逻辑路径的第一部分。然后可以将文件添加到pics和doc文件夹。
- 与前面的示例一样，主目录是只读的。/home/marymajor

为 Amazon EFS 配置逻辑目录

如果 Transfer Family 服务器使用 Amazon EFS，则必须先创建具有读写访问权限的用户主目录，然后用户才能在其逻辑主目录中工作。用户无法自己创建此目录，因为他们将缺乏 mkdir 对逻辑主目录的权限。

如果用户的主目录不存在，并且他们运行了 ls 命令，则系统会按如下方式做出响应：

```
sftp> ls
remote readdir ("/"): No such file or directory
```

对父目录具有管理访问权限的用户需要创建该用户的逻辑主目录。

自定义 Amazon Lambda 响应

您可以将逻辑目录与连接到自定义身份提供商的 Lambda 函数一起使用。为此，在 Lambda 函数中，将 HomeDirectoryType 指定为 **LOGICAL**，并为 HomeDirectoryDetails 参数添加 Entry 和 Target 值。例如：

```
HomeDirectoryType: "LOGICAL"
HomeDirectoryDetails: "[{\"Entry\": \"/\", \"Target\": \"/amzn-s3-demo-bucket/
theRealFolder"}]"
```

以下代码是来自自定义 Lambda 身份验证调用的成功响应示例。

```
aws transfer test-identity-provider \
    --server-id s-1234567890abcdef0 \
    --user-name myuser
{
    "Url": "https://a1b2c3d4e5.execute-api.us-east-2.amazonaws.com/prod/servers/
s-1234567890abcdef0/users/myuser/config",
    "Message": "",
    "Response": "{\"Role\": \"arn:aws:iam::123456789012:role/bob-usa-role\",
                  \"HomeDirectoryType\": \"LOGICAL\",
                  \"HomeDirectoryDetails\": \"[{\\\"Entry\\\":\\\"/myhome\\\",\\
\"Target\\\":\\\"/amzn-s3-demo-bucket/theRealFolder\\\"}]\",
                  \"PublicKeys\": \"[ssh-rsa myrsapubkey]\"}",
    "StatusCode": 200
}
```

> **Note**
>
> 仅当您使用 API Gateway 方法作为自定义身份提供商时，才会返回该 "Url": 行。

Transfer Family 网络应用程序

您可以创建 Web 应用程序以启用一个简单的界面，用于通过网络浏览器与 Amazon Simple Storage Service (S3) 进行数据传输。这不需要您创建或配置 Amazon Transfer Family 服务器。

在推出 Transfer Family 网络应用程序之前，最终用户需要使用客户端、定制解决方案或第三方解决方案来访问他们在 Amazon S3 中的数据。这是由于对客户和合作伙伴的安全要求严格，也因为客户应用程序对非技术用户来说很难操作。

随着 Web 应用程序的推出，您现在可以扩展品牌化、安全且高度可用的门户，供最终用户浏览、上传和下载 Amazon S3 中的数据。Web 应用程序与 Amazon IAM Identity Center Amazon S3 访问权限授予进行了原生集成。这意味着只有经过身份验证的用户才能查看他们有权访问的数据。Web 应用程序使用适用于 Amazon S3 的存储浏览器构建，在完全托管的产品中提供相同的最终用户功能，无需编写代码或托管自己的应用程序。

有关您在 Transf Amazon Web Services 服务 er Family 网络应用程序中使用的其他应用程序的更多信息，请参阅以下文档：

- 使用 Amazon 简单存储服务用户指南中的 S3 访问授权管理访问权限
- Amazon IAM Identity Center 用户指南
- Amazon S3 访问权限授予研讨会
- 宣布推出适用于完全托管的 Amazon S3 文件传输的 Amazon Transfer Family 网络应用程序

以下资源可帮助您开始使用 Transfer Family 网络应用程序。

- 用户指南详细介绍了如何在此处设置 Transfer Family 网络应用程序：教程：设置基本的 Transfer Family 网络应用程序。 step-by-step
- Amazon 入门资源中心在这里提供了一个教程：Amazon Transfer Family Web 应用程序入门。
-

Amazon Web Services 区域 适用于 Transfer Family 网络应用程序

Amazon Transfer Family 除墨西哥（中部）外，网络应用程序可在所有支持 Transfer Family 的区域（如Amazon Transfer Family 服务端点中所列）使用。

所有可用 Web 应用程序 Amazon Web Services 区域 的地方都支持 Web 应用程序的 VPC 终端节点。

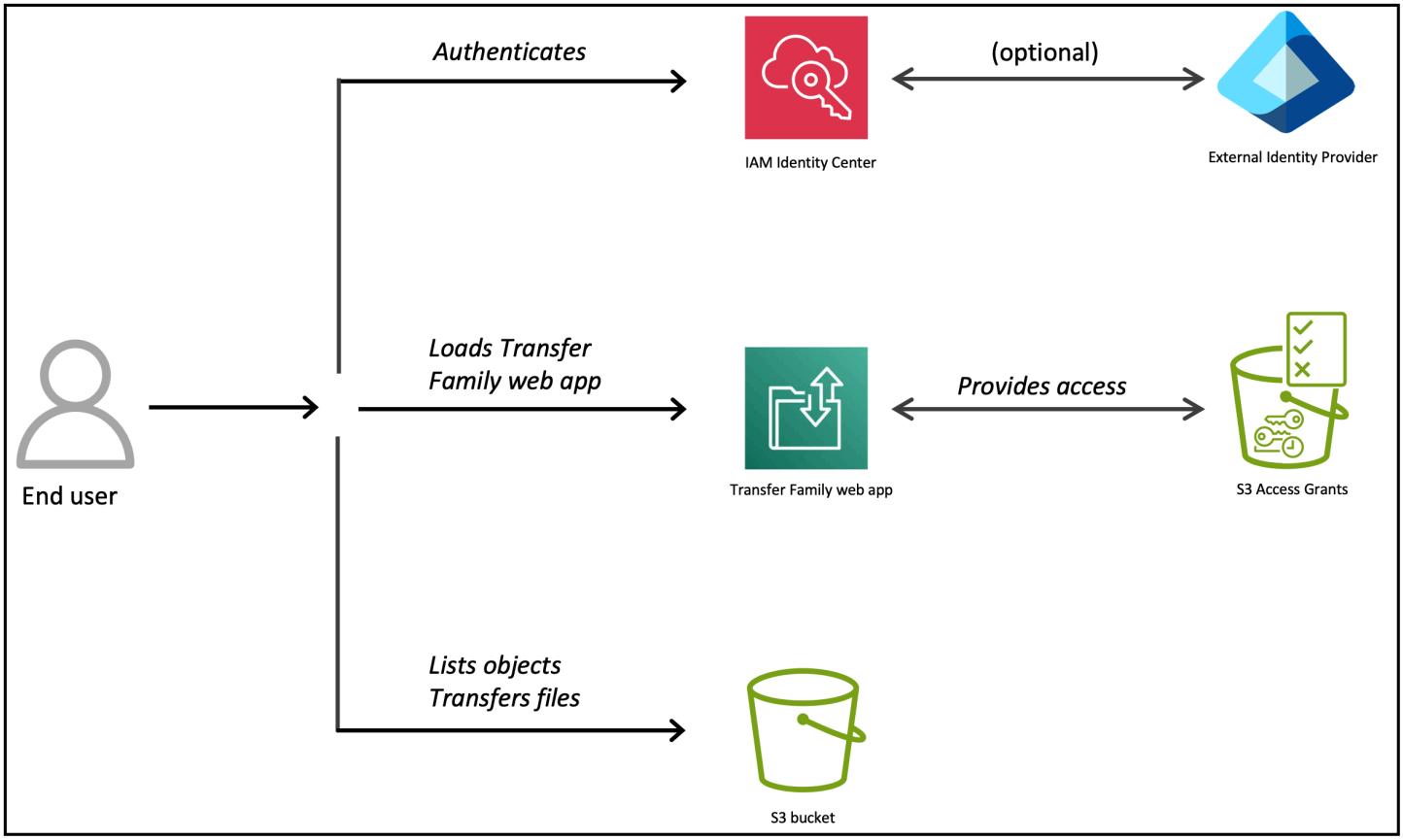
Amazon Transfer Family Web 应用程序的浏览器兼容性

Transfer Family 网络应用程序支持以下浏览器。

浏览器	版本	兼容性
Microsoft Edge	最新的 3 个版本	兼容
Mozilla Firefox	最新的 3 个版本	兼容
Google Chrome	最新的 3 个版本	兼容
Apple Safari	最新的 3 个版本	兼容

如何创建 Transfer Family 网络应用程序

下图说明了 Transfer Family 网络应用程序架构。



根据图表，你可以看到 Transfer Family 网络应用程序与以下内容交互 Amazon Web Services 服务：

- 用于存储的 Amazon S3 和用于获取会话凭证的 Amazon S3 访问权限。
- Amazon IAM Identity Center 作为联邦身份提供商。
- CloudFront 如果您为网络应用程序配置了自定义 URL，请使用亚马逊。

使用 Web 应用程序时，请注意以下限制。

- 每次查询的最大搜索结果数：10,000
- Transfer Family 网络应用程序使用的亚马逊 S3 存储桶必须与网络应用程序本身位于同一个账户中。目前不支持跨账户存储桶。
- 每次查询的最大搜索范围：10,000 个搜索文件
- 每个文件的最大上传大小：160 GB (149 GiB)
- 用于复制的最大文件大小：5.36 GB (5 GiB)
- 不支持以点 (.) 开头或结尾的文件夹名称

先决条件

在中 Amazon Identity and Access Management，配置必要的角色。粘贴我们在说明中提供的代码块。有关配置必要角色的信息，请参阅为 Transfer Family 网络应用程序配置 IAM 角色。

- 创建身份持有者角色。
- 创建一个 IAM 角色以供 S3 访问权限授予使用。S3 访问权限授予以此 IAM 角色向注册的 Amazon S3 位置的被授权者提供临时证书。

创建 Transfer Family 网络应用程序的流程

要创建 Web 应用程序并让最终用户启动并运行，您需要执行以下任务：

1. 将 IAM 身份中心配置为您的联合身份提供商。在 IAM 身份中心执行以下任务。有关配置 IAM 身份中心的更多详细信息，请参阅为 Transfer Family 网络应用程序配置您的身份提供商。
    a. 如果您还没有 IAM 身份中心实例，请创建一个。
    b. 确定您的身份来源。它可以是默认 IAM 身份中心目录或第三方提供商（例如 Okta）。
    c. 创建或识别将使用您的 Web 应用程序的用户或群组。
    d. 如果您使用 IAM Identity Center 目录作为身份源，请记下您创建的用户或群组 IDs 。以后使用 S3 访问权限授予创建访问权限时，您需要它们。

2. 在 Amazon S3 中，配置亚马逊 S3 访问授权。有关 S3 Access Grants 的更多信息，请参阅为 Transfer Family 网络应用程序配置 Amazon S3 访问授权。
   - 如果您还没有 S3 访问权限授予实例，请创建该实例 Amazon Web Services 区域。
   - 使用 IAM 角色注册您的位置。
   - 创建访问授权。
3. 在 Transfer Family 中，执行以下任务。
   a. 创建 Transfer Family 网络应用程序。有关如何创建 Transfer Family 网络应用程序的更多信息，请参阅配置 Transfer Family 网络应用程序。

      > **Important**
      > 为您的网络应用程序使用的所有 Amazon S3 存储桶设置跨源资源共享 (CORS)。有关设置 CORS 的信息，请参阅为您的存储桶设置跨源资源共享 (CORS)。

   b. 将用户或群组分配给 Web 应用程序。有关如何分配用户和群组的更多信息，请参阅在 Transfer Family 网络应用中分配或添加用户或群组。
   c. （可选）使用自定义 URL 更新 Web 应用程序的访问端点。有关创建自定义 URL 的信息，请参阅使用自定义 URL 更新您的访问终端节点。
   d. 为您的最终用户提供访问终端节点 URL，以便他们可以登录您的 Web 应用程序并与之交互。

为 Transfer Family 网络应用程序配置您的身份提供商

以下部分介绍如何配置您的身份提供商。

首先，你必须有身份来源。您可以使用 IAM 身份中心目录或外部身份提供商。 Amazon Directory Service for Microsoft Active Directory Transfer Family 使用 IAM Identity Center 作为联合身份提供商，这是一个存储用户证书并对多个组织中的用户进行身份验证的系统。

如果您未使用 IAM 身份中心目录作为身份源，请参阅以下主题：

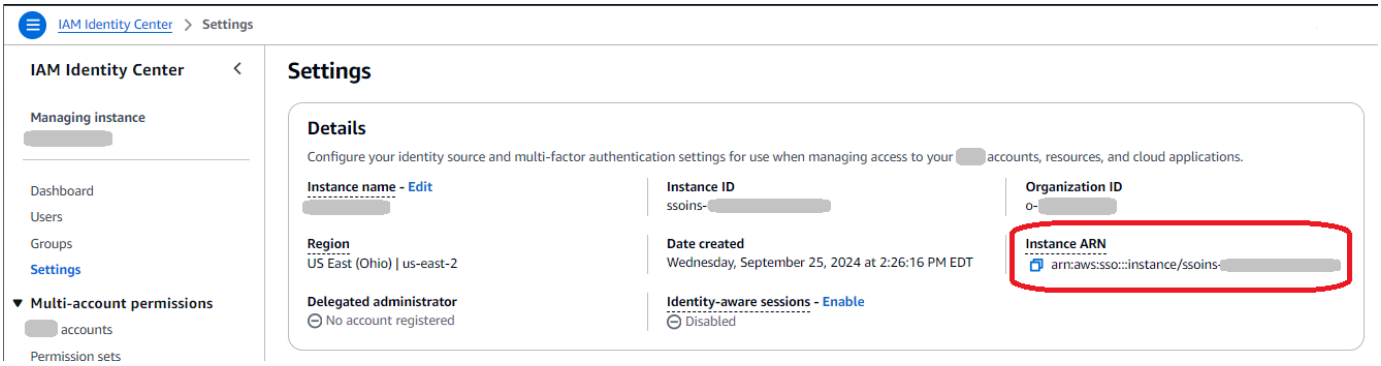
- 管理外部身份提供商
- Connect 连接到微软 AD 目录
- IAM 身份中心的组织和账户实例
- IAM 身份中心身份源教程

> **Note**
>
> 每个实例只能在 IAM Identity Center 中拥有一个身份源 Amazon Web Services 区域。有关详细信息，请参阅 IAM 身份中心先决条件和注意事项。

如果您计划使用 IAM Identity Center 目录作为身份源，并且想要快速设置，则可以跳过此主题，转到创建 Transfer Family 网络应用程序通过向导创建 IAM Identity Center 实例。

配置 Amazon IAM Identity Center 为与 Transfer Family 网络应用程序一起使用

1. 登录 Amazon Web Services 管理控制台 并打开 Amazon IAM Identity Center 控制台，网址为https://console.aws.amazon.com/singlesignon/。
2. 您可以创建和使用账户实例或组织实例 Amazon IAM Identity Center。
   - 有关账户实例的详细信息，请参阅创建账户实例 Amazon IAM Identity Center。使用 IAM 身份中心的账户实例，您可以部署支持的 Amazon 托管应用程序和基于 OpenID Connect (OIDC) 的客户托管应用程序。账户实例利用 IAM Identity Center 员工身份和访问门户功能 Amazon Web Services 账户，支持在单个账户中隔离部署应用程序。
   - 有关组织实例的详细信息，请参阅 IAM 身份中心的组织实例。您可以使用单个组织实例集中管理用户和群组的访问权限。
3. 在 IAM 身份中心设置页面上，记下您的实例 ARN。创建 Amazon S3 访问权限授予实例时，您将需要此值。



4. 创建一个或多个用户以及群组（可选），以与您的 Transfer Family 网络应用程序配合使用。如果您使用 IAM Identity Center 目录作为身份提供商，也可以直接从 Web 应用程序本身添加用户。有关更多信息，请参阅 在 Transfer Family 网络应用中分配或添加用户或群组。

为 Transfer Family 网络应用程序配置 IAM 角色

您将需要两个角色：一个用作 Web 应用程序的身份持有者角色，另一个用于配置访问授权。身份持有者角色是在其会话中包含经过身份验证的用户的身份的角色。它用于代表用户向 S3 访问授权请求数据访问权限。

> **Note**
>
> 您可以跳过创建身份持有者角色的过程。有关让 Transfer Family 服务创建身份持有者角色的信息，请参阅创建 Transfer Family 网络应用程序。
> 您可以跳过创建访问权限授予角色的过程。在创建访问权限的过程中，在注册 S3 位置的步骤中，选择创建新角色。

创建身份持有者角色

1. 登录 Amazon Web Services 管理控制台 并打开 IAM 控制台，网址为https://console.aws.amazon.com/iam/。
2. 选择角色，然后选择创建角色。
3. 选择 “自定义信任策略”，然后粘贴以下代码。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service":"transfer.amazonaws.com"
            },
            "Action": [
                "sts:AssumeRole",
                "sts:SetContext"
            ]
        }
    ]
}
```

4. 选择 “下一步”，然后跳过 “添加权限”，然后再次选择 “下一步”。
5. 例如，输入名称web-app-identity-bearer。

6. 选择创建角色以创建身份持有者角色。
7. 从列表中选择您刚刚创建的角色，然后在 “权限策略” 面板中，选择 “添加权限” > “创建内联策略”。
8. 在策略编辑器中，选择 JSON，然后粘贴到以下代码块中。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetDataAccess",
                "s3:ListCallerAccessGrants",
                "s3:ListAccessGrantsInstances"
            ],
            "Resource": "*"
        }
    ]
}
```

9. 在策略名称中输入`AllowS3AccessGrants`，然后选择创建策略。

接下来，您将创建 S3 访问权限授予的角色来向被授权者提供临时证书。

> **Note**
>
> 如果您允许服务为您创建身份持有者角色，则该角色会混淆副手保护。因此，它的代码与此处显示的不同。

创建访问权限授予角色

1. 登录 Amazon Web Services 管理控制台 并打开 IAM 控制台，网址为https://console.aws.amazon.com/iam/。
2. 选择角色，然后选择创建角色。此角色应有权在中访问您的 S3 数据 Amazon Web Services 区域。
3. 选择 “自定义信任策略”，然后粘贴以下代码。

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "access-grants.s3.amazonaws.com"
            },
            "Action": [
                "sts:AssumeRole",
                "sts:SetContext"
            ]
        }
    ]
}
```

4. 选择 “下一步” 添加最低限度政策，如注册位置中所述。尽管不建议这样做，但您可以添加 AmazonS3 FullAccess 托管政策，该政策可能过于宽松，无法满足您的需求。
5. 选择 “下一步”，然后输入名称（例如`access-grants-location`）。
6. 选择创建角色以创建角色。

> **Note**
>
> 如果您允许服务为您创建访问权限授予角色，则该角色会混淆副手保护。因此，它的代码与此处显示的不同。

配置 Transfer Family 网络应用程序

本节介绍创建 Transfer Family 网络应用程序的过程。要分配可以使用它的用户和群组，请参阅在 Transfer Family 网络应用中分配或添加用户或群组。

> **Note**
>
> 重复这些步骤以添加其他 Web 应用程序。您可以重复使用之前创建的 IAM 角色。确保将新 Web 应用程序的访问端点添加到每个存储桶的跨源资源共享 (CORS) 策略中。

创建 Transfer Family 网络应用程序

> **Note**
>
> 如果您没有使用身份提供商的 IAM Identity Center 目录，则在您已设置 IAM Identity Center 并配置第三方身份提供商之前，请不要尝试创建 Web 应用程序，如中所述为 Transfer Family 网络应用程序配置您的身份提供商。

完成以下步骤即可创建 Transfer Family 网络应用程序。

创建 Transfer Family 网络应用程序

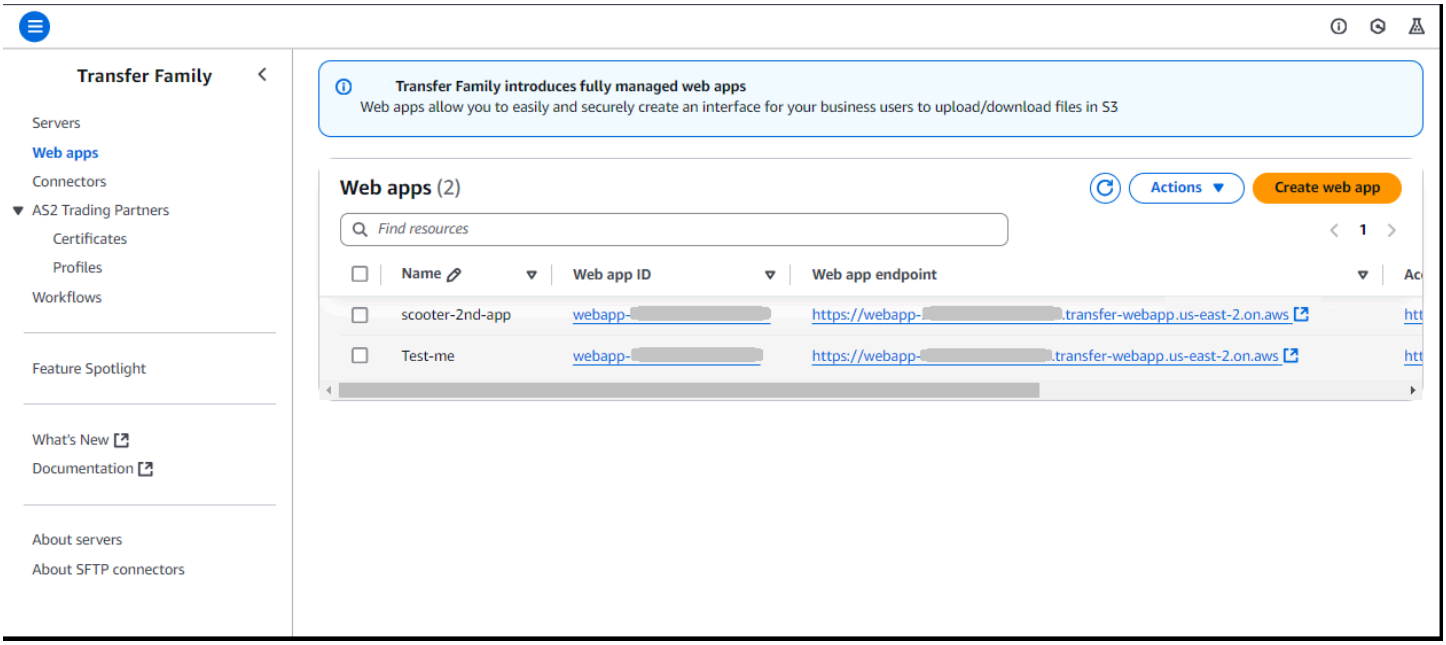
1. 登录 Amazon Web Services 管理控制台 并打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在左侧导航窗格中，选择 Web 应用程序。
3. 选择创建 Web 应用程序。

   对于身份验证访问，窗格填充如下。

   - 如果您已经在中创建了组织或账户实例 Amazon IAM Identity Center，则会看到以下消息：您的 Amazon Transfer Family 应用程序已连接到 IAM Identity Center 的账户实例。
   - 如果您已经拥有账户实例并且是组织实例的成员，则可以选择连接哪个实例。
   - 如果您还没有账户实例，或者您是组织实例的成员，则可以选择创建账户实例。
4. 对于端点类型，选择可公开访问的端点类型。有关 VPC 托管的端点，请参阅 在 VPC 中创建 Transfer Family 网络应用程序。
5. 在权限类型窗格中，您可以使用先前创建的角色，也可以让服务为您创建一个角色。

   - 如果您已经创建了身份持有者角色，请选择 “使用现有角色”，然后从 “选择现有角色” 菜单中选择您的角色。
   - 要让服务为您创建角色，请选择创建并使用新的服务角色。
6. 在 Web 应用程序单位窗格中，选择一个值。一个 Web 应用程序单元允许来自多达 250 个独特会话的 Web 应用程序活动。创建 Web 应用程序时，您可以根据预期的峰值工作量配置所需的单元数量。更改您的 Web 应用程序单位会影响您的账单。有关定价的信息，请参阅Amazon Transfer Family 定价。
7. 如果您在中使用 Transfer Family Amazon GovCloud (US) Region，则可以在 “启用 FIPS” 窗格中选中 “启用 FIPS 端点” 复选框。对于所有其他选项 Amazon Web Services 区域，此选项不可用。

8. （可选）添加标签以帮助您整理 Web 应用程序。我们建议您添加一个以 Name 作为键并以描述性名称作为值的标签。
9. 选择下一步。在此屏幕上，您可以选择为 Web 应用程序提供标题。如果您不提供标题，则会提供 Transfer Web App 的默认标题。您也可以上传徽标和网站图标的图片文件。
10. 选择 “下一步”，然后选择 “创建 Web 应用程序”。



> **Note**
>
> 请务必为从 Web 应用程序终端节点访问的所有存储分区设置跨源资源共享 (CORS) 策略。

在 VPC 中创建 Transfer Family 网络应用程序

本节介绍在 VPC 中创建 Transfer Family 网络应用程序的过程。您可以将 Web 应用程序的终端节点托管在虚拟私有云 (VPC) 中，用于向 Amazon S3 存储桶传输数据和从中传输数据，而无需通过公共互联网。要分配可以使用您的 Web 应用程序的用户和群组，请参阅[在 Transfer Family 网络应用中分配或添加用户或群组]。

> **Note**
>
> 为了确保在使用 Transfer Family 网络应用程序 VPC 终端节点时的私密 end-to-end数据流，您必须实现三个额外的组件。首先，为 Amazon S3 控制 API 操作设置 PrivateLink 终端节点，这

是调用 Amazon S3 访问授权 API 所必需的。其次，使用 Amazon S3 网关终端节点（用于来自您的 VPC 内部的流量）或 PrivateLink Amazon S3 接口终端节点（用于通过 VPN 或 Direct Connect 来自本地网络的流量）为访问 Amazon S3 数据配置终端节点。第三，将存储桶策略更新为仅允许来自这些 VPC 终端节点的流量，从而锁定您的 Amazon S3 存储桶访问权限。这种组合可确保所有数据传输都保留在您的专用网络基础设施中，并且永远不会通过公共互联网。

创建 Transfer Family 网络应用程序

先决条件

- Amazon IAM Identity Center 使用已配置的身份提供商进行设置。请参阅为 Transfer Family 网络应用程序配置您的身份提供商。
- VPC 和网络组件已设置。请参阅创建 VPC。
- 为 Amazon S3 控制操作设置的 API 终端节点。请参阅访问 Amazon S3 接口终端节点。
- 为 Amazon S3（网关或接口）设置的 VPC 终端节点。请参阅 Amazon S3 的 VPC 终端节点类型。如果您使用的是接口终端节点，则必须启用私有 DNS。有关示例，请参阅引入对 Amazon S3 的私有 DNS 支持 Amazon PrivateLink。

> **Note**
>
> Amazon IAM Identity Center 不支持 VPC 终端节点；所有身份验证请求都通过公共互联网传输。此外，Transfer Family 网络应用程序需要互联网访问才能加载静态内容（例如 JavaScript CSS 和 HTML 文件）。公共互联网访问的要求与数据访问是分开的。您的 VPC 终端节点可确保连接通过您的 VPC 基础设施进行路由。

创建 Transfer Family 网络应用程序

1. 登录 Amazon Web Services 管理控制台 并打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在左侧导航窗格中，选择 Web 应用程序。
3. 选择创建 Web 应用程序。对于身份验证访问，窗格填充如下。

- 如果您已经在中创建了组织或账户实例 Amazon IAM Identity Center，则会看到以下消息：您的 Amazon Transfer Family 应用程序已连接到 IAM Identity Center 的账户实例。
- 如果您已经拥有账户实例并且是组织实例的成员，则可以选择连接哪个实例。
- 如果您还没有账户实例，或者您是组织实例的成员，则可以选择创建账户实例。

4. 在终端节点配置部分，选择您的用户访问您的 Web 应用程序的方式：

- 可公开访问：您可以通过 HTTPS 通过公众访问您的 Web 应用程序终端节点。此选项不需要任何 VPC 配置，因此设置起来很简单，适用于供广泛公众使用的应用程序。
- VPC 托管：您的网络应用程序终端节点托管在您的虚拟私有云 (VPC) 中，通过您的 VPC 网络或 VPN 连接提供私有网络 Amazon Direct Connect访问权限。此选项通过网络隔离增强了安全性，建议用于内部应用程序。

> **Note**
>
> 您必须具有双堆栈 VPC 配置。有关更多信息，请参阅 Amazon Virtual Private Cloud 用户指南中的双栈 VPC 配置示例。

配置 VPC 托管终端节点时，您需要指定：

- VPC：选择一个现有 VPC 或创建一个新的 VPC。“创建 VPC” 按钮可用。
- 可用区：选择要部署终端节点的可用区。
- 子网：在每个选定的可用区内选择子网。
- 安全组：选择或创建安全组以根据源 IP 地址控制访问权限。如果未指定，则使用 VPC 的默认安全组。通过 VPC 控制台管理安全组。将您的 VPC 安全组配置为允许通过 TCP 端口 443 通过 HTTPS 从您的网络发送的入站流量。这是 IAM 身份中心身份验证和加载 Web 应用程序静态内容所必需的。

> **Note**
>
> 无法为 VPC 终端节点自定义访问终端节点。要添加自定义 URL，请使用公共端点。

创建后步骤

- 请务必为从 Web 应用程序终端节点访问的所有存储分区设置跨源资源共享 (CORS) 策略。请参阅跨源资源共享 (CORS) 政策。
- 更新您的存储桶策略，仅允许来自您的 VPC 的流量通过您的 VPC 终端节点。请参阅限制对特定 VPC 端点的访问。
- 向 Transfer Family 网络应用程序分配或添加用户或群组。请参阅在 Transfer Family 网络应用中分配或添加用户或群组。

跨源资源共享 (CORS) 政策

您必须为 Web 应用程序使用的所有存储分区设置跨源资源共享 (CORS)。有关 CORS 的更多信息，请参阅 为您的存储桶设置跨源资源共享 (CORS)。

> **Important**
>
> 在使用以下示例策略之前，请将 Allowed Origin 替换为您的访问终端节点。否则，当您的最终用户尝试访问您的 Web 应用程序上的某个位置时，他们将收到错误消息。

策略示例：

```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "GET",
      "PUT",
      "POST",
      "DELETE",
      "HEAD"
    ],
    "AllowedOrigins": [
      "https://vpce-1234567-example.vpce-mq.transfer-webapp.us-east-1.on.aws"
    ],
    "ExposeHeaders": [
      "last-modified",
```

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

限制对特定 VPC 端点的访问

下面是限制仅从 ID 为 amzn-s3-demo-bucket 的 VPC 端点访问特定存储桶 vpce-1a2b3c4d 的 Amazon S3 存储桶策略示例。如果未使用指定的端点，则该策略会拒绝对存储桶的所有访问。aws:SourceVpce 条件指定端点。aws:SourceVpce 条件不需要 VPC 端点资源的 ARN，而只需要 VPC 端点 ID。有关更新存储桶策略以仅允许来自您的 VPC 的流量的更多信息，请参阅使用存储桶策略控制来自 VPC 终端节点的访问。有关在策略中使用条件的更多信息，请参阅使用条件键的存储桶策略示例。作为应用此策略的先决条件，您应该创建一个 Amazon S3 VPC 终端节点。

> **Important**
>
> 在使用以下示例策略之前，将 VPC 端点 ID 替换为适合您的使用案例的值。否则，您将无法访问您的存储桶。

```
{
  "Version":"2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPCE-only",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket",
                   "arn:aws:s3:::amzn-s3-demo-bucket/*"],
```

```
      "Condition": {
        "StringNotEquals": {
          "aws:SourceVpce": "vpce-1a2b3c4d"
        }
      }
    }
  ]
}
```

在 Transfer Family 网络应用中分配或添加用户或群组

创建 Transfer Family 网络应用程序后，您可以分配随后可以访问该网络应用程序的用户和群组。您可以检索已创建并存储在 IAM Identity Center 中的用户，也可以直接添加新用户（如果您使用 IAM Identity Center 目录作为身份提供商）。如果您添加新用户，他们也会被添加到您的 IAM 身份中心实例中。

注意以下几点：

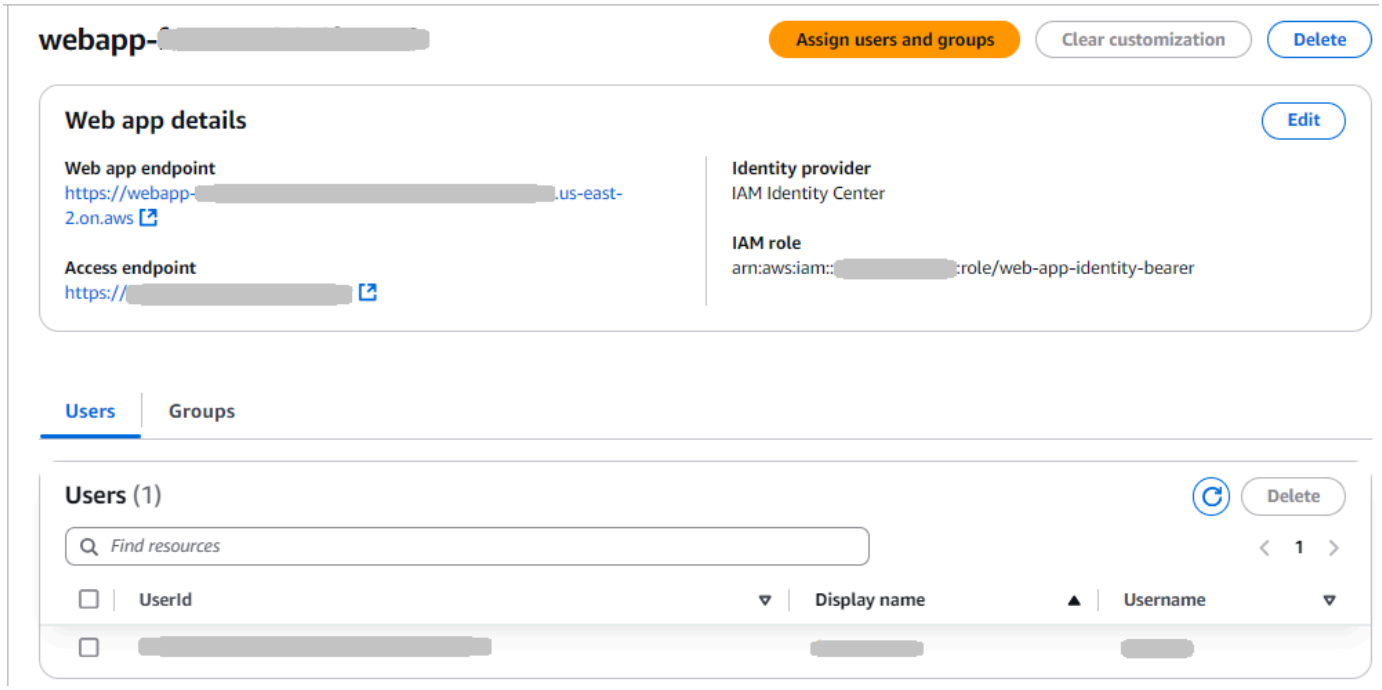
- 只有当您使用 IAM Identity Center 目录作为身份源并拥有适当权限时，您才能添加新用户。如果您是组织实例的成员，则可能没有添加用户的必要权限。

> **Note**
>
> 如果您不向应用程序分配用户或群组，则当您的用户尝试登录您的 Web 应用程序时，他们将收到错误消息。

- 如果您创建新用户，则还必须为该用户创建 S3 访问授权，以便他们可以访问您的 Web 应用程序上的数据。
- 创建新用户后，该用户会收到一封来自 IAM Identity Center 的入职电子邮件，其中包含操作说明。

将用户分配给 Transfer Family 网络应用程序

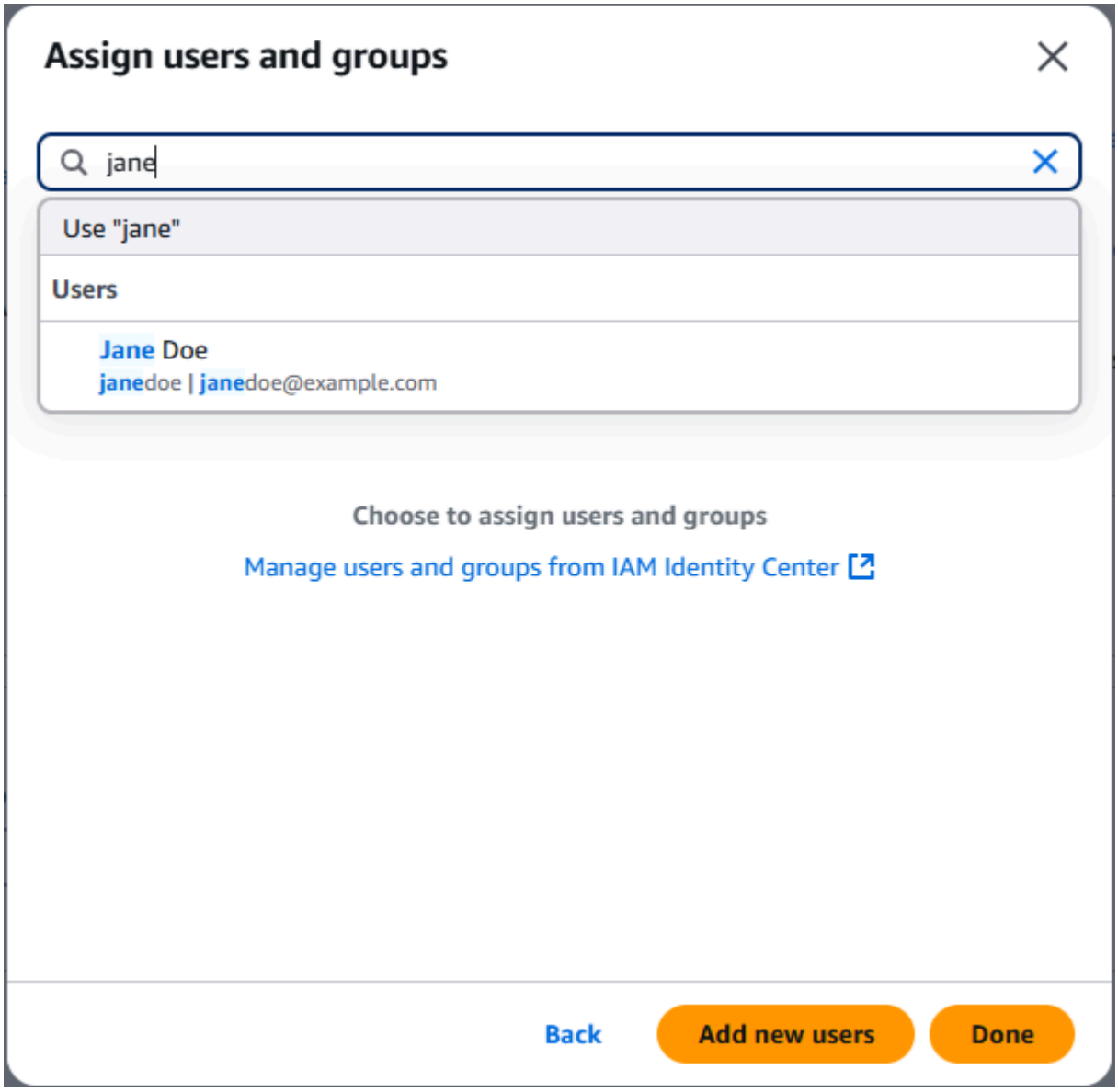
1. 导航到您的 Web 应用程序列表，然后选择要编辑的列表。
2. 选择分配用户和组。



3. 要分配您之前在 IAM Identity Center 中创建的用户，请选择分配现有用户和群组。要创建新用户，请跳至步骤 4。

   a. 将出现一个信息屏幕。选择 Get started（开始）以继续。

   b. 搜索用户。请注意，在您开始输入搜索条件之前，不会显示任何用户。如果显示名称不同，则必须按显示名称进行搜索，而不是按用户名进行搜索。只返回完全匹配的结果。如果您找不到您的用户，请导航到 IAM Identity Center 管理控制台，找到该用户，然后将其显示名称复制并粘贴到此处。



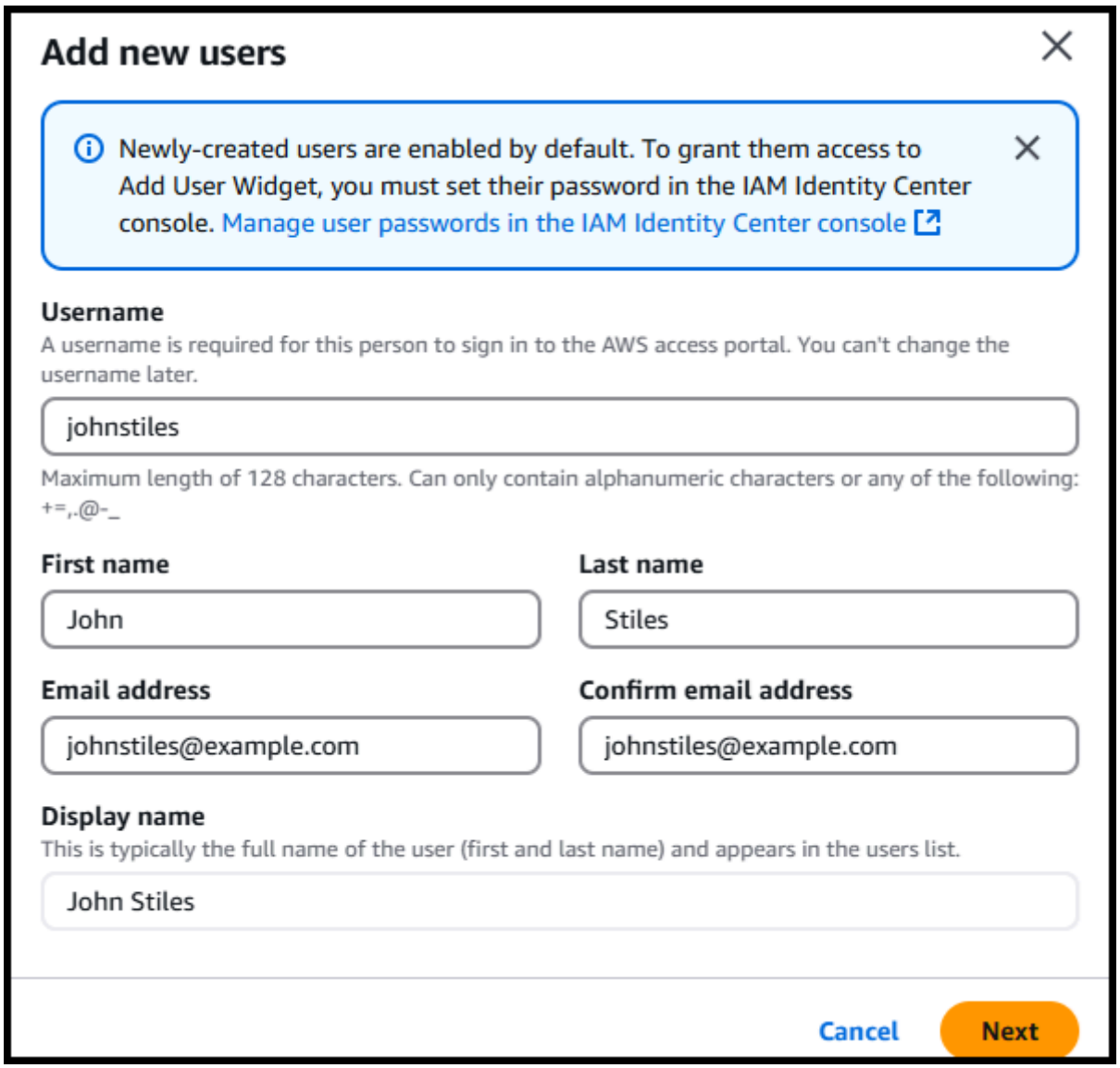
c. 选择要添加的用户和群组，然后选择分配。

4. 要创建新用户，请选择添加并分配新用户。

a. 将出现一个信息屏幕。选择 Get started（开始）以继续。

b. 选择添加新用户。

c. 在对话框中输入以下用户详细信息：用户名、名字和姓氏以及电子邮件地址。



d. 选择 “下一步”，然后选择 “添加” 以添加用户并关闭对话框，或者选择 “添加新用户” 以创建其他用户。

为您的存储桶设置跨源资源共享 (CORS)

您必须为 Web 应用程序使用的所有存储分区设置跨源资源共享 (CORS)。CORS 配置是定义规则的文档，这些规则用于识别您将允许访问存储桶的来源。有关 CORS 的更多信息，请参阅配置跨域资源共享 (CORS)。

> **Important**
>
> 如果您未设置 CORS，则最终用户在尝试访问您的 Web 应用程序上的位置时会收到错误消息。

为您的 Amazon S3 存储桶设置跨源资源共享 (CORS)

1. 登录 Amazon Web Services 管理控制台 并打开 Amazon S3 控制台，网址为https://console.aws.amazon.com/s3/。
2. 从左侧导航面板中选择 Buckets，在搜索对话框中搜索您的存储桶，然后选择权限选项卡。
3. 在跨源资源共享 (CORS) 中，选择编辑并粘贴以下代码。*WebAppEndpoint*替换为您的 Web 应用程序的实际访问端点。这可以是创建 Web 应用程序时创建的 VPC 托管或公共访问终端节点，也可以是自定义访问终端节点（如果您创建一个）。确保不要在尾部输入斜杠，因为这样做会导致用户尝试登录您的 Web 应用程序时出错。

   - 不正确的例子：`https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws/`
   - 正确的例子：
     - `https://webapp-c7bf3423.transfer-webapp.us-east-2.on.aws`
     - `https://vpce-05668789767a-fh45z079.vpce-mq.transfer-webapp.us-east-1.on.aws`

   如果您要将存储桶重复用于多个 Web 应用程序，请将其终端节点添加到列表中。`AllowedOrigins`

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

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

4. 选择 “保存更改” 以更新 CORS。

要测试您的 CORS 配置，请参阅测试 CORS。

为 Transfer Family 网络应用程序配置 Amazon S3 访问授权

本主题介绍如何使用 Amazon S3 访问授权添加访问授权。此访问授权定义了直接向公司目录中的用户和群组访问您的数据的权限 just-in-time，并根据授权提供最低权限的临时证书。S3 访问权限授予实例中的个人授权允许公司目录中的特定用户或群组在您的 S3 访问权限授予实例中注册的位置内获得访问权限。有关更多详细信息，请参阅 Amazon S3 用户指南中的 S3 访问权限授予概念。

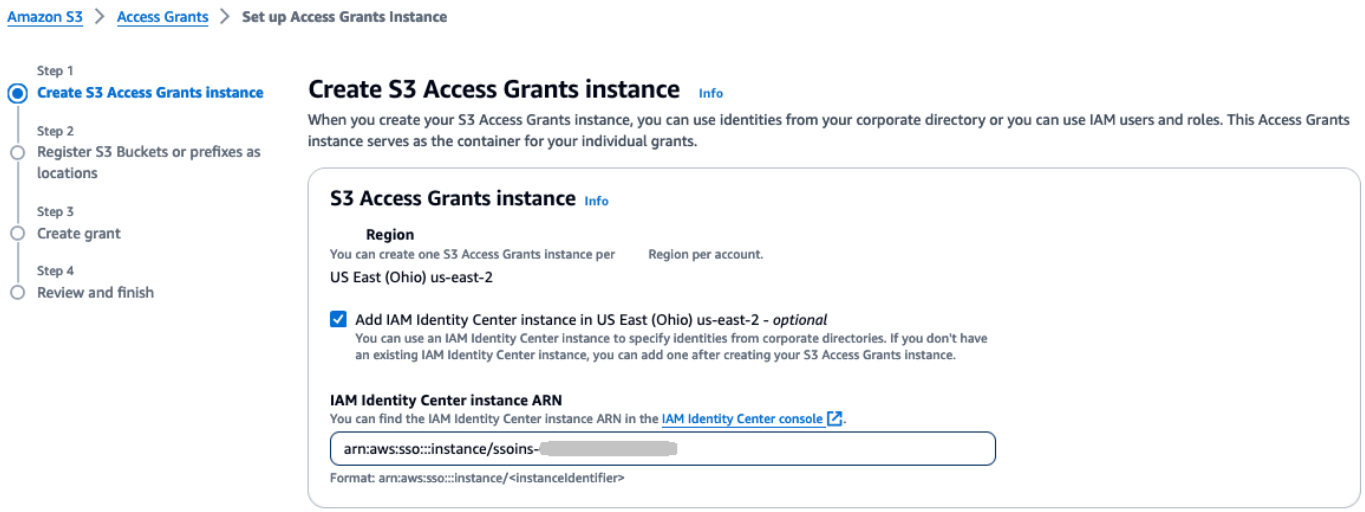
> **Note**
>
> 除了 Transfer Family 网络应用程序外，您不能将 IAM 身份中心目录与 S3 访问权限授予一起使用。

您必须为身份传播指定 Amazon S3 访问授权。Amazon S3 访问权限授予存储您的最终用户必须访问的数据。当您的最终用户登录您的 Transfer Family 网络应用程序时，S3 访问权限授予会将用户的身份传递给受信任的应用程序。本节介绍如何添加和配置 Amazon S3 访问授权实例，然后为 Amazon S3 存储桶添加和配置访问授权。

> **Note**
>
> 准备好您的 IAM Identity Center 实例 ARN 和用户或群组 ID，因为您需要它们来完成访问权限的设置。

使用 Amazon S3 访问授权创建授权

1. 登录 Amazon Web Services 管理控制台 并打开 Amazon S3 控制台，网址为 https://console.aws.amazon.com/s3/。
2. 创建存储分区，或记下现有存储分区以用于您的 Web 应用程序。有关创建存储桶的信息，请参阅 Amazon S3 用户指南。
3. 从左侧导航窗格中选择 “访问授权”。
4. 选择创建 S3 访问权限授予实例，并提供以下信息。
   - 在 “您的*your-Region*位置*your-Region*” 中选择 “添加 IAM 身份中心实例” Amazon Web Services 区域。如果您没有使用 IAM Identity Center 作为身份提供商，请清除此框。
   - 粘贴您的 IAM 身份中心实例 ARN。



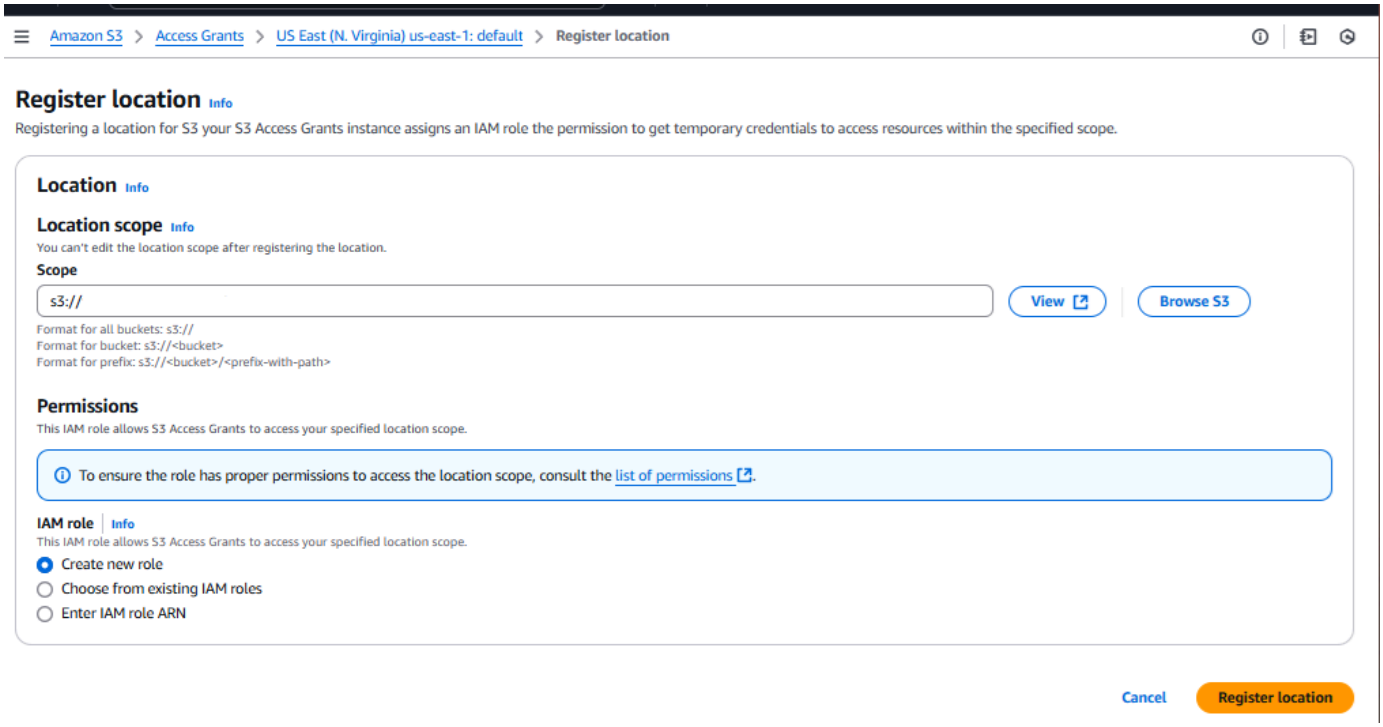
选择下一步以继续。

5. 将 S3 存储桶或前缀注册为位置。我们建议您注册默认位置`s3://`，并将其映射到 IAM 角色。此默认路径上的位置可以访问您账户中的所有 Amazon S3 存储桶。 Amazon Web Services 区域 创建访问权限时，您可以将范围缩小到默认位置内的存储桶、前缀或对象。

提供以下信息：

- 对于范围，请浏览存储桶或输入存储桶的名称以及可选的前缀。
- 对于 IAM 角色，选择创建新角色让服务创建角色。

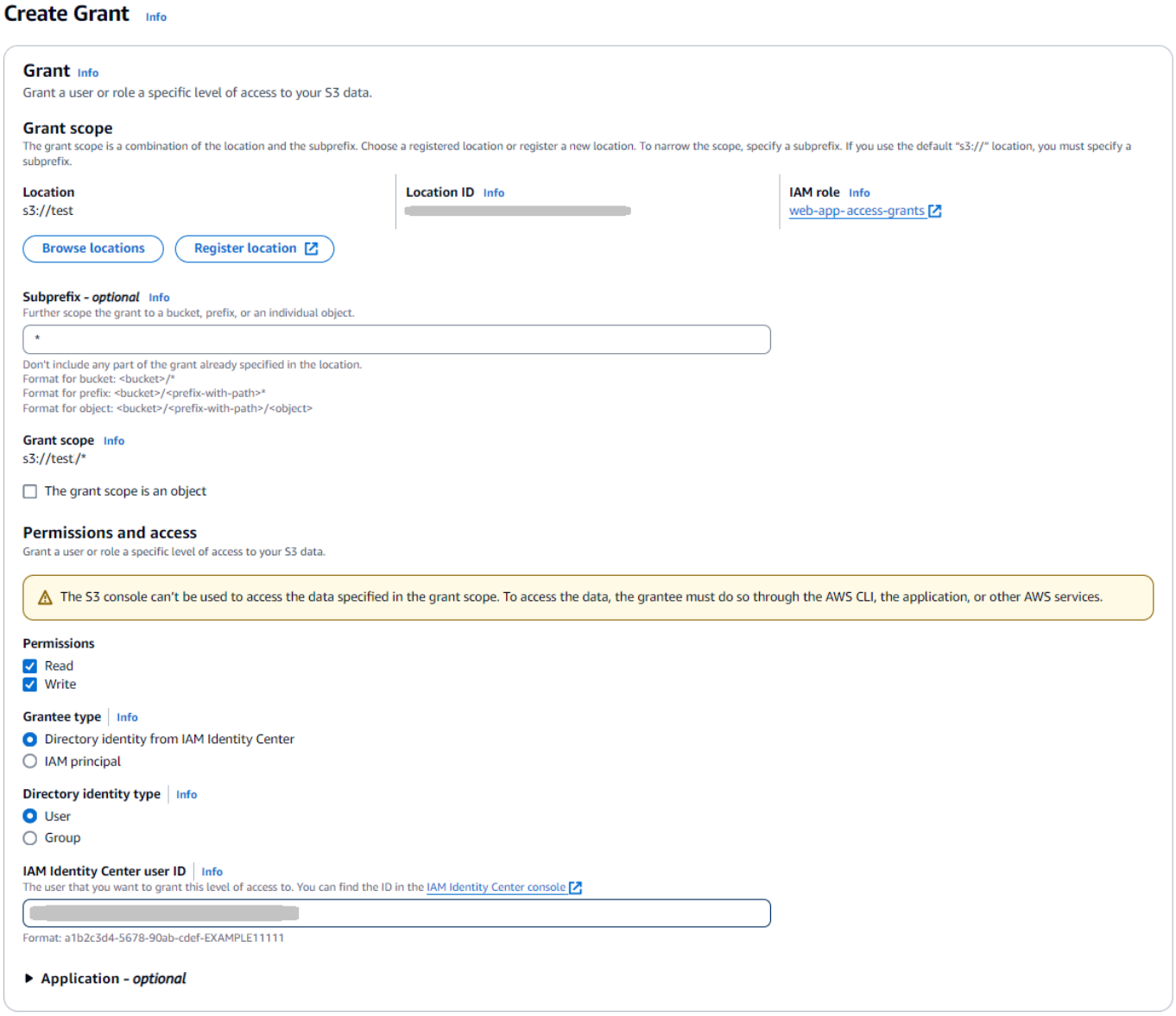
  或者，您可以自己创建角色（如所述）为 Transfer Family 网络应用程序配置 IAM 角色，然后在此处输入其 ARN。



选择下一步以继续。

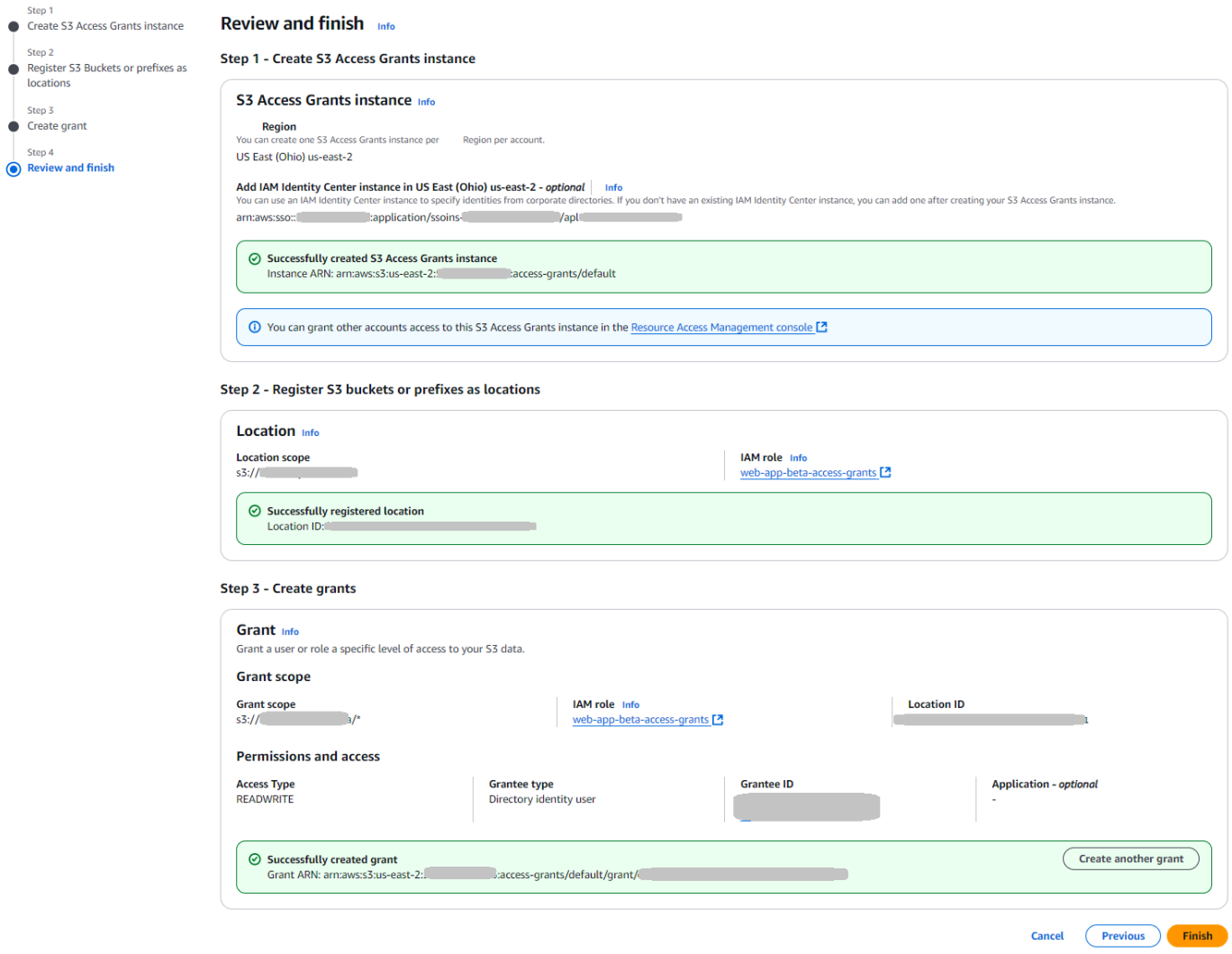
6. 在 “创建授权” 屏幕中，提供以下详细信息。

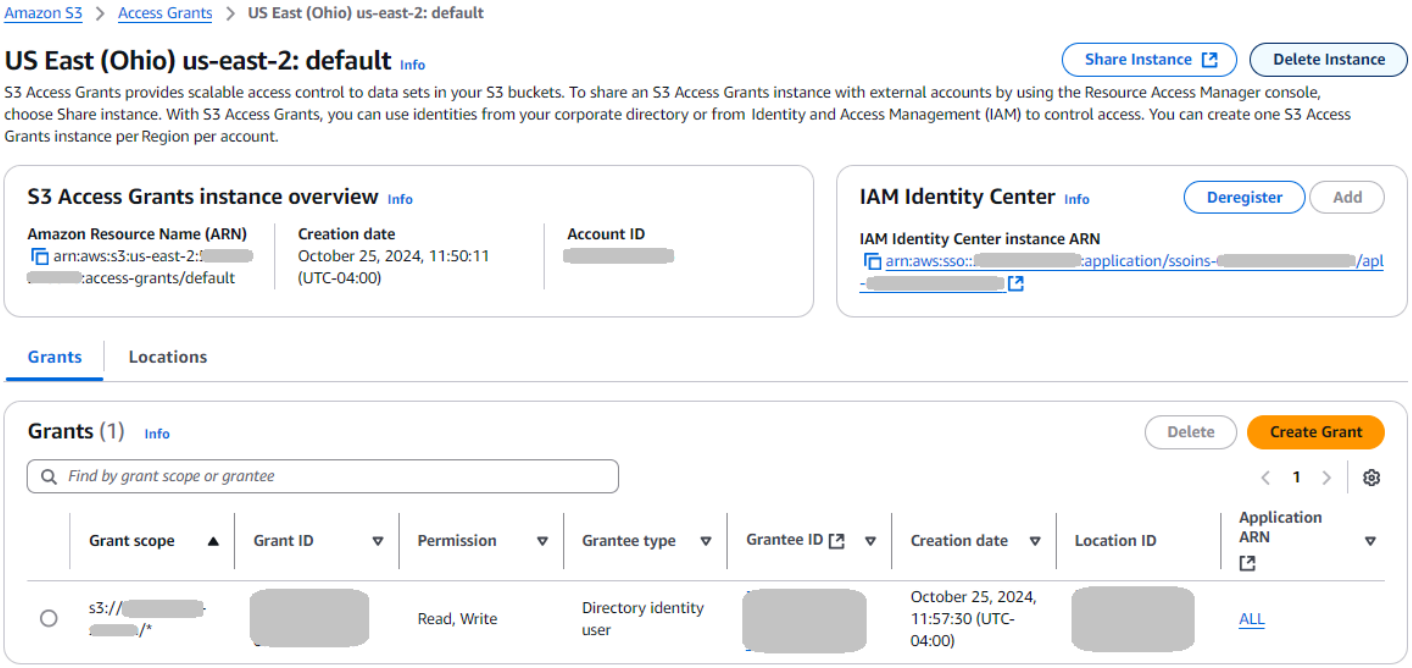
- 在 “权限” 中，选择 “读取” 和 “写入”。访问权限可以是只读或读写，但不支持只写。
- 对于被授权者类型，请从 IAM 身份中心选择目录身份。
- 对于 “目录” 身份类型，选择 “用户” 或 “组”，具体取决于您要立即注册的类型。
- 在 IAM 身份中心 user/group ID 中，粘贴您的用户或群组的 ID。此 ID 可在 IAM Identity Center 控制台中找到，也可以在你的 Transfer Family 网络应用程序的用户和群组表中找到。



选择下一步。

7. 查看屏幕上的设置。如果一切正确，请选择 “完成” 以创建访问授权。或者，您可以选择 “取消” 或 “上一步” 进行更改。


Step 1
Create S3 Access Grants instance
Step 2
Register S3 Buckets or prefixes as locations
Step 3
Create grant
Step 4
Review and finish
Review and finish Info
Step 1 - Create S3 Access Grants instance
S3 Access Grants instance Info
Region
You can create one S3 Access Grants instance per Region per account.
US East (Ohio) us-east-2
Add IAM Identity Center instance in US East (Ohio) us-east-2 - optional Info
You can use an IAM Identity Center instance to specify identities from corporate directories. If you don't have an existing IAM Identity Center instance, you can add one after creating your S3 Access Grants instance.
arn:aws:sso::[redacted]:application/ssoins-[redacted]/apl[redacted]
Successfully created S3 Access Grants instance
Instance ARN: arn:aws:s3:us-east-2:[redacted]:access-grants/default
You can grant other accounts access to this S3 Access Grants instance in the Resource Access Management console
Step 2 - Register S3 buckets or prefixes as locations
Location Info
Location scope
s3://[redacted]
IAM role Info
web-app-beta-access-grants
Successfully registered location
Location ID:[redacted]
Step 3 - Create grants
Grant Info
Grant a user or role a specific level of access to your S3 data.
Grant scope
Grant scope
s3://[redacted]a/*
IAM role Info
web-app-beta-access-grants
Location ID
[redacted]
Permissions and access
Access Type
READWRITE
Grantee type
Directory identity user
Grantee ID
[redacted]
Application - optional
-
Successfully created grant
Grant ARN: arn:aws:s3:us-east-2:[redacted]:access-grants/default/grant/[redacted]
Create another grant
Cancel
Previous
Finish



这就完成了 Web 应用程序的设置。您配置的用户和群组可以在接入点访问 Web 应用程序、登录以及上传和下载文件。

使用自定义 URL 更新您的访问终端节点

使用您的 Web 应用程序创建的默认访问端点包含服务生成的标识符。为了提供品牌体验，您可能需要为用户提供一个自定义网址，以访问您的 Transfer Family 网络应用程序。本主题介绍如何使用自定义 URL 更新您的访问终端节点。

> **Note**
>
> 无法为 VPC 终端节点自定义访问终端节点。要添加自定义 URL，请使用公共端点。

> **Note**
>
> 以下过程依赖于您使用推荐的CloudFormation 堆栈模板。您无需使用模板：您可以直接使用CloudFront 控制台创建发行版。
> 但是，所提供的模板简化了流程，并且可以更轻松地避免错误配置。如果您不使用该 Amazon CloudFormation 模板，请务必遵循以下准则：
>
> - O rigin 请求策略应将查询字符串和 Cookie 转发到源，而不应将`Host`标头转发到源。

- 缓存策略不应在缓存密钥中包含Host标头。

自定义您的 Web 应用程序网址

1. 使用 Transfer Family 提供的 Amazon CloudFormation 模板CloudFormation 堆栈模板创建 CloudFront 分配。

   a. 在 https://console.aws.amazon.com/cloudformation 上打开 Amazon CloudFormation 控制台。

   b. 选择创建堆栈并指定以下内容。

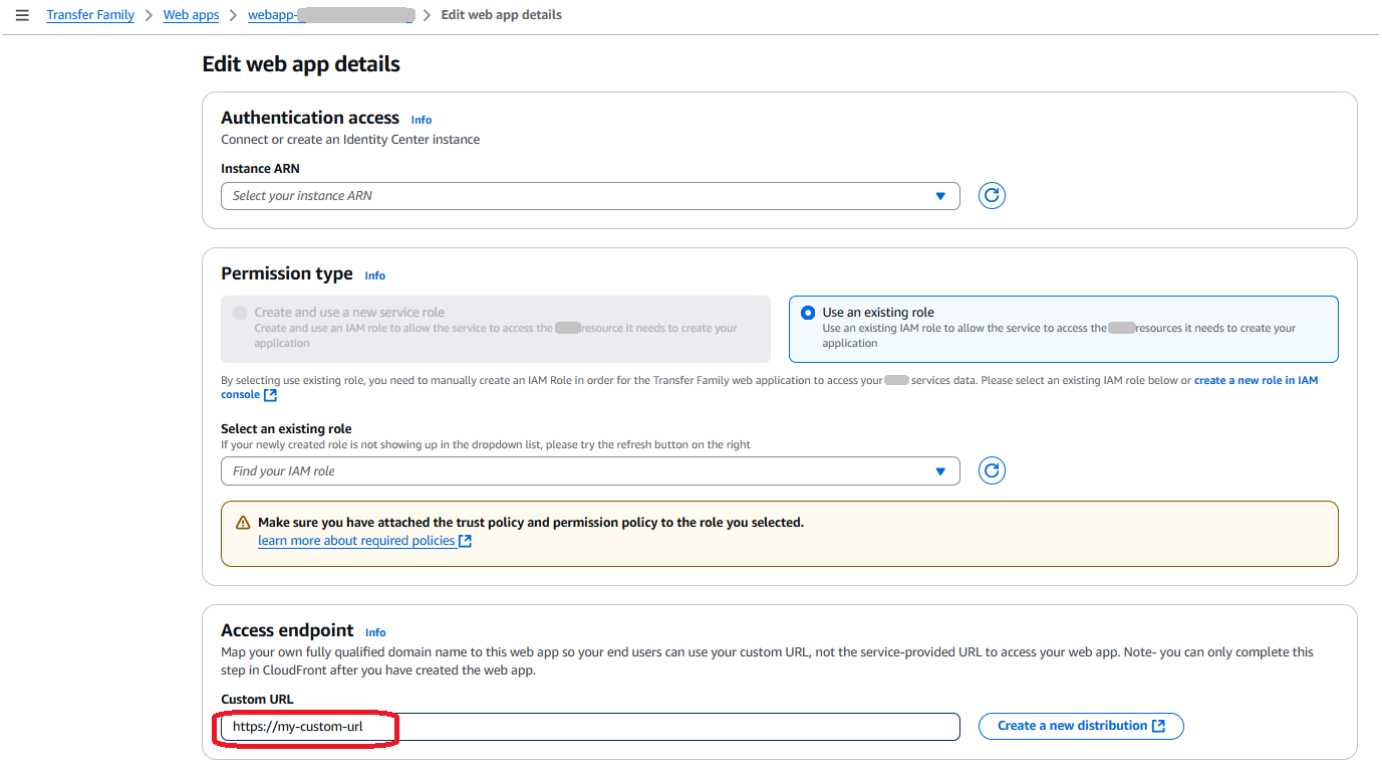
      - 在“先决条件-准备模板”部分，选择选择现有模板。
      - 在指定模板部分，选择上传模板文件。
      - 保存CloudFormation 堆栈模板文件，然后将其上传到此处。

   c. 选择“下一步”并提供以下信息。

      - WebAppEndpoint: 从你的 Web 应用程序中复制值
      - AccessEndpoint: 提供您要使用的自定义域名
      - AcmCertificateArn: 为存储在中的公共或私有 SSL/TLS 证书提供 ARN Amazon Certificate Manager

   d. 完成向 Amazon CloudFormation 导直到创建新堆栈。

2. 在您的 Web 应用程序中，编辑 A ccess 端点，将自定义 UR L 更新为您要使用的网址。



3. 创建 DNS 记录，将自定义域名的流量路由到 CloudFront分配。如果您使用的是 Route 53 作为该区域，则可以为 CloudFront 分配名称创建别名或别名记录（例如 xxxx .cloudfront.net）。有关将 Amazon Route 53 与配合使用的信息 CloudFront，请参阅[配置 Amazon Route 53 以将流量路由到 CloudFront分配](#)。
4. 将默认访问端点替换为`AllowedOrigins`代码块中的以下行，从而更新您的跨源资源共享策略：

```
"https://custom-url"
```

您需要对您的 Web 应用程序使用的每个存储分区进行此更改。

更新后，CORS 政策的`AllowedOrigins`部分应如下所示：

```
"AllowedOrigins": [
    "https://custom-url"],
```

每个 Transfer AllowedOrigins Family 网络应用程序只需要输入一个条目。

有关更多详细信息，请参阅[为您的 Amazon S3 存储桶设置跨源资源共享 (CORS)](#) 过程。

现在，您可以访问您的自定义访问终端节点，并与您的最终用户共享此链接。

CloudTrail 登录 Transfer Family 网络应用程序

CloudTrail 是 Amazon Web Services 服务 用来记录你内部所采取的操作的 Amazon Web Services 账户。它持续监控和记录控制台登录、 Amazon Command Line Interface 命令和操作等活动的 API 操作。 SDK/API 这使您可以记录谁在何时何地采取了什么行动。 CloudTrail 通过提供 Amazon 环境中所有活动的历史记录，帮助审计、访问管理和监管合规性。

对于 Transfer Family 网络应用程序，您可以跟踪用户执行的身份验证事件和数据访问操作。要启用全面日志记录，您需要：

1. 配置 CloudTrail 为记录管理事件以跟踪身份验证活动。
2. 启用 Amazon S3 数据事件以跟踪通过您的网络应用程序执行的文件操作。

另请参阅

- CloudTrail IAM 身份中心的用例
- 了解 IAM 身份中心登录事件
- CloudTrail 用户身份元素
- 为 S3 存储桶和对象启用 CloudTrail 事件记录
- 亚马逊 S3 CloudTrail 活动

启用 Amazon S3 数据事件

要跟踪通过 Transfer Family 网络应用程序在 Amazon S3 存储桶上执行的文件操作，您需要为这些存储桶启用数据事件。数据事件提供对象级 API 活动，对于跟踪 Web 应用程序用户执行的文件上传、下载和其他操作特别有用。

要为您的 Transfer Family 网络应用程序启用 Amazon S3 数据事件，请执行以下操作：

1. 打开 CloudTrail 控制台，网址为https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，选择 T ra ils，然后选择现有跟踪或创建新跟踪。
3. 在高级事件选择器下，选择编辑。
4. 选择添加高级事件选择器。
5. 对于第一个字段选择器：
   - 将 “字段” 设置为 `eventCategory`
   - 将运算符设置为等于

- 将 “值” 设置为 Data

6. 选择添加字段，对于第二个字段选择器：
   - 将 “字段” 设置为 resources.type
   - 将运算符设置为等于
   - 将 “值” 设置为 AWS::S3::Object
7. （可选）要仅记录特定存储桶的事件，请选择添加字段并添加：
   - 将 “字段” 设置为 resources.ARN
   - 将运算符设置为开头为
   - 将 “值” 设置为 arn:aws:s3:::your-bucket-name/
8. 选择保存更改。

或者，您可以使用传统数据事件配置：

1. 在数据事件下，选择编辑。
2. 对于数据事件类型，选择 S3 存储桶和对象事件。
3. 选择要为其记录数据事件的 Amazon S3 存储桶。您可以选择 “所有当前和将来的 S3 存储桶”，也可以指定单个存储桶。
4. 选择是记录读取事件、写入事件还是同时记录两者。
5. 选择保存更改。

启用数据事件后，您可以在为配置的 Amazon S3 存储桶中访问这些日志 CloudTrail。日志包括诸如执行操作的用户、操作时间戳、受影响的特定对象以及帮助跟踪通过 Transfer Family 网络应用程序执行userId的操作的onBehalfOf字段等详细信息。

查找和查看您的日志

您可以通过多种方式查找和查看 Transfer Family 网络应用程序的 CloudTrail 日志：

使用控制 CloudTrail 台

查看最近事件的最快方法：

1. 打开 CloudTrail 控制台，网址为https://console.aws.amazon.com/cloudtrail/。
2. 选择事件历史记录。
3. 按以下条件筛选事件：

- 事件源：signin.amazonaws.com用于 Web 应用程序事件
- 事件源：s3.amazonaws.com用于文件操作

4. 单击任何事件可查看详细信息。

访问 Amazon S3 中的日志

要访问存储在 Amazon S3 中的完整日志文件，请执行以下操作：

1. 识别您的 CloudTrail 跟踪的 Amazon S3 存储桶：

```
aws cloudtrail describe-trails --query 'trailList[*].[Name,S3BucketName]' --output
 table
```

2. 导航到 Amazon S3 中的日志文件：

```
aws s3 ls s3://your-cloudtrail-bucket/AWSLogs/account-id/CloudTrail/region/YYYY/MM/
DD/
```

3. 下载并搜索您的网络应用程序 ID 的日志文件：

```
aws s3 cp s3://your-cloudtrail-bucket/AWSLogs/account-id/CloudTrail/region/YYYY/MM/
DD/ . --recursive
gunzip *.json.gz
grep -l "webapp-1a2b3c4d5e6f7g8h9" *.json
```

Amazon CLI 用于搜索事件

使用以下方式搜索特定的 Web 应用程序事件 Amazon CLI：

```
aws logs filter-log-events \
  --log-group-name /aws/cloudtrail/your-trail-name \
  --filter-pattern "webapp-1a2b3c4d5e6f7g8h9" \
  --start-time $(date -d "1 day ago" +%s)000
```

或者搜索身份验证事件：

```
aws logs filter-log-events \
  --log-group-name /aws/cloudtrail/your-trail-name \
  --filter-pattern "UserAuthentication" \
```

```
  --start-time $(date -d "1 day ago" +%s)000
```

身份验证日志示例

CloudTrail 记录 Transfer Family 网络应用程序的身份验证事件，这可以帮助您跟踪成功和失败的登录尝试。这些日志对于安全监控和合规性特别有用。

主题

- 证书验证日志条目示例
- 登录身份验证的日志条目示例
- 的日志条目示例 ListCallerAccessGrants
- GetDataAccess事件日志条目示例

证书验证日志条目示例

以下示例显示了在身份验证过程中发生的凭据验证事件的 CloudTrail 日志条目。

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "123456789012",
        "arn": "",
        "accountId": "123456789012",
        "accessKeyId": "",
        "userName": "demo-user-2",
        "onBehalfOf": {
            "userId": "f12bb510-a011-702f-10dd-5607e2776dbc",
            "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/
d-9a670c546e"
        },
        "credentialId": "58138a11-87e5-401d-8f0b-7161c9389112"
    },
    "eventTime": "2025-08-08T15:29:30Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialVerification",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "192.0.2.224",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36",
```

```
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "f304a48b-7b6d-41c8-b136-4f49c91c1f31",
        "CredentialType": "PASSWORD"
    },
    "requestID": "ff936828-4a81-453c-802d-81368b6bca1a",
    "eventID": "70cb7008-493d-42c2-a9eb-38bf168af6a8",
    "readOnly": false,
    "eventType": "Amazon ServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "serviceEventDetails": {
        "CredentialVerification": "Success"
    },
    "eventCategory": "Management"
}
```

此事件提供了有关身份验证过程中的凭证验证步骤的更多详细信息，显示了使用的特定凭据 ID 和身份验证工作流程 ID。

登录身份验证的日志条目示例

以下示例显示了使用 IAM Identity Center CloudTrail 登录 Web 应用程序期间成功进行用户身份验证事件的日志条目。

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "123456789012",
        "arn": "",
        "accountId": "123456789012",
        "accessKeyId": "",
        "userName": "demo-user-2",
        "onBehalfOf": {
            "userId": "f12bb510-a011-702f-10dd-5607e2776dbc",
            "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/
d-9a670c546e"
        },
        "credentialId": "b41f0a02-1635-4d07-a414-aecf9e14b906"
    },
    "eventTime": "2025-08-07T14:09:07Z",
```

```
    "eventSource": "signin.amazonaws.com",
    "eventName": "UserAuthentication",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "192.0.2.14",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "7a4ef12c-7c4b-4bc3-b5bd-c2469afcc795",
        "LoginTo": "https://example.awsapps.com/start/",
        "CredentialType": "PASSWORD"
    },
    "requestID": "fc91bcf0-ac53-4454-a1a0-fb911eacc095",
    "eventID": "18522007-1e60-4a71-b2b5-150baf504ab3",
    "readOnly": false,
    "eventType": "Amazon ServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "serviceEventDetails": {
        "UserAuthentication": "Success"
    },
    "eventCategory": "Management"
}
```

在此示例中，请注意以下重要字段：

- `eventSource`：显示 “signin.amazonaws.com”，表示这是一个 IAM 身份中心身份验证事件。
- `userIdentity.onBehalfOf`：包含网络应用程序用户的用户 ID 和身份存储 ARN。
- `additionalEventData.LoginTo`：显示正在访问的 IAM 身份中心应用程序 URL。
- `additionalEventData.CredentialType`：表示使用的身份验证方法（密码）。
- `serviceEventDetails`：显示身份验证结果（成功）。

的日志条目示例 ListCallerAccessGrants

以下示例显示了一个事件的 CloudTrail 日志条目，该 ListCallerAccessGrants 事件在 Transfer Family 网络应用查询用户的可用访问权限时发生。

```
{
    "eventVersion": "1.11",
    "userIdentity": {
```

```
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEID:aws-transfer",
        "arn": "arn:aws:sts::123456789012:assumed-role/Amazon
 TransferWebAppIdentityBearer-us-east-2/aws-transfer",
        "accountId": "123456789012",
        "accessKeyId": "ASIAEXAMPLEKEY",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEID",
                "arn": "arn:aws:iam::123456789012:role/service-role/Amazon
 TransferWebAppIdentityBearer-us-east-2",
                "accountId": "123456789012",
                "userName": "Amazon TransferWebAppIdentityBearer-us-east-2"
            },
            "attributes": {
                "creationDate": "2025-08-08T15:29:34Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "transfer.amazonaws.com",
        "onBehalfOf": {
            "userId": "f12bb510-a011-702f-10dd-5607e2776dbc",
            "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/
d-9a670c546e"
        }
    },
    "eventTime": "2025-08-08T15:29:35Z",
    "eventSource": "s3.amazonaws.com",
    "eventName": "ListCallerAccessGrants",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "transfer.amazonaws.com",
    "userAgent": "transfer.amazonaws.com",
    "requestParameters": {
        "Host": "123456789012.s3-control.dualstack.us-east-2.amazonaws.com",
        "allowedByApplication": "true",
        "maxResults": "100"
    },
    "responseElements": null,
    "additionalEventData": {
        "SignatureVersion": "SigV4",
        "CipherSuite": "TLS_AES_128_GCM_SHA256",
        "bytesTransferredIn": 0,
        "AuthenticationMethod": "AuthHeader",
```

```
        "x-amz-id-2": "1g34AaAELn/
fntxwrifVsr41VDl8dp5ygWFasHJFNVq5FDCWYfX0ye7s4tWHEJC8ppI5lLePYLIcw3iTXAgn5Q==",
        "bytesTransferredOut": 462
    },
    "requestID": "48485MTZEDWT0ANT",
    "eventID": "3de5dd60-b7cf-474c-a1ab-631467c1a5c3",
    "readOnly": true,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "Amazon:S3::AccessGrantsInstance",
            "ARN": "arn:aws:s3:us-east-2:123456789012:access-grants/default"
        }
    ],
    "eventType": "Amazon ApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```


在此示例中，请注意以下重要字段：

- `eventName`：显示这是一个查询可用的 S3 访问权限 ListCallerAccessGrants 的事件。
- `requestParameters.allowedByApplication`：表示查询已筛选为应用程序允许的授权。
- `requestParameters.maxResults`：显示响应中要返回的最大授权数量。
- `userIdentity.onBehalfOf`：将请求链接到特定的 Web 应用程序用户。

此事件有助于跟踪 Transfer Family 网络应用何时查询用户可以访问的 S3 资源，从而可以查看访问授权发现操作。

GetDataAccess事件日志条目示例

以下示例显示了事件的 CloudTrail 日志条目，该 GetDataAccess 事件在 Transfer Family Web 应用程序代表用户请求 S3 资源的访问权限时发生。


```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROASEQRAEABP7ADWEZA5:aws-transfer",
```

```
        "arn": "arn:aws:sts::123456789012:assumed-role/AWSTransferWebAppIdentityBearer-
ap-southeast-1/aws-transfer",
        "accountId": "123456789012",
        "accessKeyId": "ASIAEXAMPLEKEY",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROASEQRAEABP7ADWEZA5",
                "arn": "arn:aws:iam::123456789012:role/service-role/
AWSTransferWebAppIdentityBearer-ap-southeast-1",
                "accountId": "123456789012",
                "userName": "AWSTransferWebAppIdentityBearer-ap-southeast-1"
            },
            "attributes": {
                "creationDate": "2025-05-08T16:09:05Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "transfer.amazonaws.com",
        "onBehalfOf": {
            "identityStoreArn": "arn:aws:identitystore::123456789012:identitystore/
d-9667b0da7a",
            "userId": "191a35ec-10a1-70c1-e4ab-e2802411e13e"
        }
    },
    "eventTime": "2025-05-08T16:10:25Z",
    "eventSource": "s3.amazonaws.com",
    "eventName": "GetDataAccess",
    "awsRegion": "ap-southeast-1",
    "sourceIPAddress": "transfer.amazonaws.com",
    "userAgent": "transfer.amazonaws.com",
    "requestParameters": {
        "Host": "123456789012.s3-control.dualstack.ap-southeast-1.amazonaws.com",
        "durationSeconds": 900,
        "permission": "READWRITE",
        "target": "s3://amzn-s3-demo-bucket/users/john.doe/documents/*"
    },
    "responseElements": null,
    "additionalEventData": {
        "AuthenticationMethod": "AuthHeader",
        "CipherSuite": "TLS_AES_128_GCM_SHA256",
        "SignatureVersion": "SigV4",
        "bytesTransferredIn": 0,
        "bytesTransferredOut": 2244,
```

```
        "x-amz-id-2": "8ce8sZOgNwsaj9w1mzagyA
+csONjYl8FgEw4FGpE8DARi90aNC0RFWlTYNEn7ChqE9RCJrTzMvS+ru7Vz2xXHrkQt/1uQ9exZTZdlhX+/fM="
    },
    "requestID": "BXGSKKQXCWS5RAHB",
    "eventID": "c11db1d1-dfb8-431e-8625-48eba2ebadfe",
    "readOnly": true,
    "resources": [
        {
            "type": "Amazon:S3::AccessGrantsInstance",
            "ARN": "arn:aws:s3:ap-southeast-1:123456789012:access-grants/default",
            "accountId": "123456789012"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```


在此示例中，请注意以下重要字段：

- `eventName`：显示这是一个 Transfer Family 请求 S3 资源的访问权限时发生 GetDataAccess 的事件。
- `userIdentity.onBehalfOf`：包含身份存储 ARN 和用户 ID，将访问请求关联到特定 Web 应用用户。
- `requestParameters.target`：显示请求访问的 S3 路径模式。
- `requestParameters.permission`：表示请求的访问类型（读写、读或写）。
- `requestParameters.durationSeconds`：显示访问权限的有效期（通常为 900 秒/15 分钟）。
- `sourceIPAddress`和`userAgent`：两者都显示 “transfer.amazonaws.com”，表示这是内部服务请求。

GetDataAccess 事件对于跟踪 Transfer Family 网络应用程序用户何时被授予访问特定 S3 资源的权限特别有用，可帮助您监控访问模式并确保获得适当的授权。

查看 CloudTrail 日志条目

您可以通过多种方式查看和分析您的 Transfer Family 网络应用程序的 CloudTrail 日志条目：

使用控制 CloudTrail 台

CloudTrail 控制台提供了一个用户友好的界面，用于查看和筛选日志条目：

1. 打开 CloudTrail 控制台，网址为https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，选择事件历史记录。
3. 使用筛选选项缩小事件范围：
   - 将事件来源设置为，`transfer.amazonaws.com`以便仅查看 Transfer Family 事件。
   - 按事件名称筛选以查看特定的操作，例如`UserAuthentication`.
   - 使用时间范围来关注特定时间段内的事件。
4. 点击任何事件可查看其详细信息。

访问 Amazon S3 中的日志

如果您已将 CloudTrail 跟踪配置为将日志传输到 Amazon S3 存储桶，则可以直接访问原始日志文件：

1. 打开 Amazon S3 控制台，网址为 https://console.aws.amazon.com/s3/。
2. 导航到存储 CloudTrail 日志的存储桶和前缀。
3. 日志按年、月、日和地区进行组织。导航到相应的目录。
4. 下载并打开 JSON 格式的日志文件。

对 Web 应用程序进行故障排除

> **Note**
>
> 这些疑难解答提示适用于网络应用程序管理员，而不是最终用户。对于最终用户，如果您遇到任何问题，请联系您的 Web 应用程序管理员。以下段落中您的所有实例均指向 Web 应用程序管理员。

对网络错误进行故障排除

描述

您的最终用户在加载 Web 应用程序端点时会看到网络横幅网络错误。

原因

最常见的问题如下：

- 管理员未分配尝试登录新应用程序的用户。
- 管理员未向您的 IAM 角色添加必要的操作。
- 您会看到分配给您的用户的 S3 访问权限列表，但是您的 Amazon S3 存储桶的 CORS 配置不正确。

解决方案

- 在 IAM Identity Center 中，确保将用户分配到正确的应用程序。或者，如果您分配了群组，请确保尝试登录的用户属于正确的群组。在 Transfer Family 网络应用中分配或添加用户或群组中对此进行了描述。
- 检查您的角色是否包含针对`sts:AssumeRole`和操作的自定义信任策略中的必要`sts:SetContext`操作。为 Transfer Family 网络应用程序配置 IAM 角色中对此进行了描述。
- 查看您的 Web 应用程序使用的所有存储分区的 CORS 政策。为您的 Amazon S3 存储桶设置跨源资源共享 (CORS) 中对此进行了介绍。

对配置的存储桶未显示进行故障排除

描述

一切似乎都配置正确，但是 Amazon S3 存储桶未出现在网络应用程序中。

原因

一个可能的原因是 Amazon S3 存储桶与网络应用程序不在同一个账户中。

解决方案

确保 Amazon S3 存储桶与网络应用程序位于同一个账户中。目前不支持跨账户存储桶。

排查自定义 URL 错误

描述

当您的最终用户登录 Web 应用程序时，他们会收到错误消息 “授权失败：缺少授权码”。

原因

如果您 CloudFront 直接使用而不是提供的 Amazon CloudFormation 模板，则可能错误地将原始请求策略配置为不转发查询字符串。

解决方案

更新您的源站请求政策，将查询字符串和 Cookie 转发到源。

描述

当您的最终用户尝试访问 Transfer Family 网络应用程序时，他们会收到 404 响应。

原因

如果您 CloudFront 直接使用而不是提供的 Amazon CloudFormation 模板，则可能错误地将缓存策略配置为在缓存密钥中包含Host标头，或者错误配置了原始请求策略以转发标头。Host

解决方案

- 确保您的缓存策略不在缓存密钥中包含Host标头
- 请确保您的原始请求策略不会转发标Host头。

对其他错误进行故障排除

描述

您的最终用户无法登录，或者无法查看任何存储桶或文件，或者您会收到其他错误。

原因

一个可能的原因是，IAM 身份中心实例 ARN 与您的授权 ARN 或您的网络应用程序 IAM 身份中心实例 ARN 的值不匹配。

解决方案

检查以下项目以查看它们是否匹配。

- 在 IAM 身份中心中，导航到设置并查看实例 ARN。

```
arn:aws:sso:::instance/ssoins-instance-identifier
```

- 在 Amazon S3 中，导航到访问授权并查看您的 IAM 身份中心实例 AR N。

```
arn:aws:sso::account-id:application/ssoins-instance-identifier/apl-1234567890abcdef0
```

- 在 Transfer Family 中，导航到您的网络应用程序详情页面并查看其实例 ARN。

```
arn:aws:sso:::instance/ssoins-instance-identifier
```

这三个位置的*instance-identifier*值必须相同。

Web 应用程序中出现重复的 S3 存储桶

描述

用户可以在 Transfer Family 网络应用程序界面中多次看到相同的 S3 存储分区。

原因

当用户属于多个 Active Directory 群组，这些群组对同一 S3 存储桶有重复的授权时，就会发生这种情况。无论用户是否向同一个存储桶位置分配了多个授权，Web 应用程序都会列出与该用户关联的所有顶级授权（UID 或 GID）。

解决方案

要解决此问题，管理员应删除重复的授权，以便每个用户对每个 S3 位置只有一个授权。查看您的 S3 访问权限授权配置，并整合不同的 Active Directory 组中同一存储桶的重复授权。

Transfer Family 网络应用程序的最终用户说明

> **Note**
>
> 在本主题中，这些信息适用于正在与 Web 应用程序交互的最终用户。本主题中的所有实例均指最终用户。

本主题介绍如何访问您有权使用的 Amazon Transfer Family Web 应用程序，并介绍如何与之交互。

Web 应用程序配额

使用 Web 应用程序时，请注意以下限制。

- 每次查询的最大搜索结果数：10,000
- Transfer Family 网络应用程序使用的亚马逊 S3 存储桶必须与网络应用程序本身位于同一个账户中。目前不支持跨账户存储桶。
- 每次查询的最大搜索范围：10,000 个搜索文件
- 每个文件的最大上传大小：160 GB (149 GiB)
- 用于复制的最大文件大小：5.36 GB (5 GiB)
- 不支持以点 (.) 开头或结尾的文件夹名称

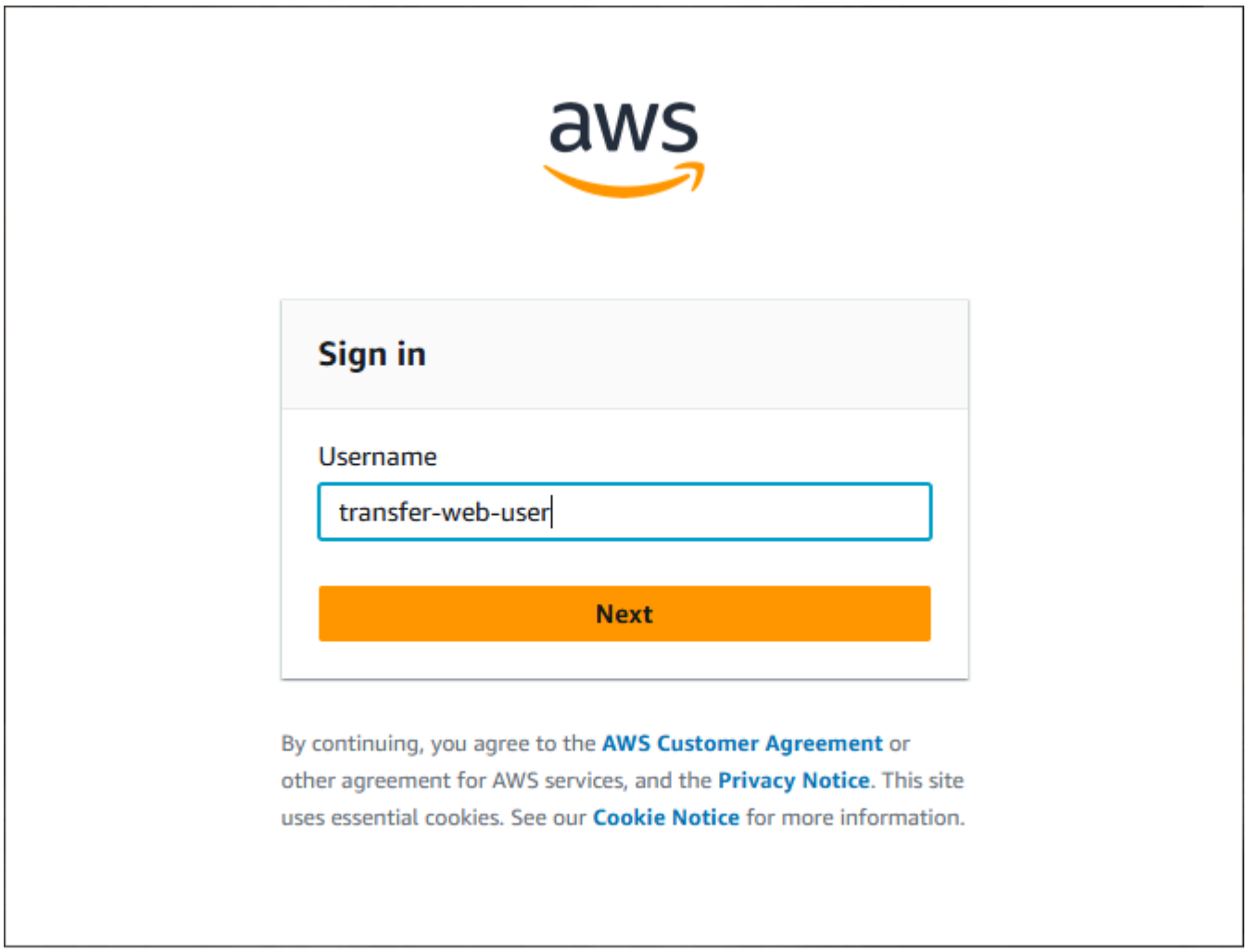
IAM 身份中心用户的用户体验

本节介绍您的组织使用 IAM Identity Center 配置其用户时的用户体验。

访问 Transfer Family 网络应用程序

1. 你应该会收到一封来自 no-reply@login.awsapps.com 的电子邮件，标题为 “邀请加入” Amazon IAM Identity Center。接受邀请以激活您的用户帐户。
2. 在消息中，选择您的 Amazon 访问门户 URL 下方的 URL。

   这会将您带到 Amazon 登录屏幕。



3. 输入您的凭据并选择登录。

   这会将您带到 Amazon Web Services 访问门户，其中显示了可用应用程序的列表。

4. 为您的 Transfer Family 网络应用程序选择应用程序。

第三方身份提供商用户的用户体验

如果您的组织未使用 Amazon IAM Identity Center 来配置其用户，则您的入职体验将取决于他们用来配置最终用户的身份提供商应用程序。进行身份验证并登录后，您的 Web 应用程序界面将与下一节中描述的界面相同。

> **Note**
>
> 如果用户属于对同一 Amazon S3 存储桶拥有权限的多个 Amazon Directory 群组，则该存储桶会在 Web 应用程序界面中多次出现。之所以出现这种情况，是因为 Web 应用程序列出了与用

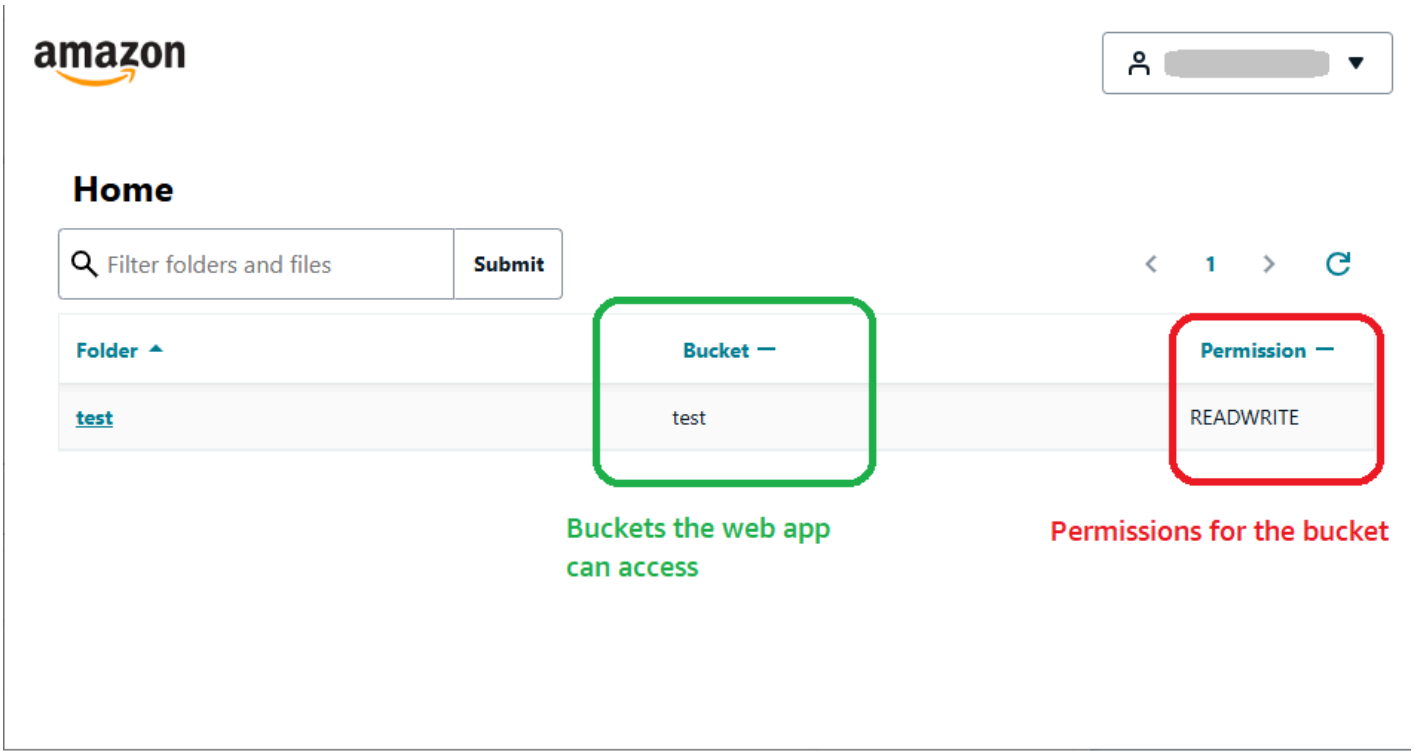
户的 UID 或 GID 关联的所有顶级授权，包括对同一个存储桶的重复授权。为防止重复上架商品，管理员可以整合多项授权，这样每位用户在每个 Amazon S3 地点只能获得一项授权。

Transfer Family 最终用户界面

经过身份验证并登录后，您可以与 Web 应用程序进行交互。

有四个主要观点。

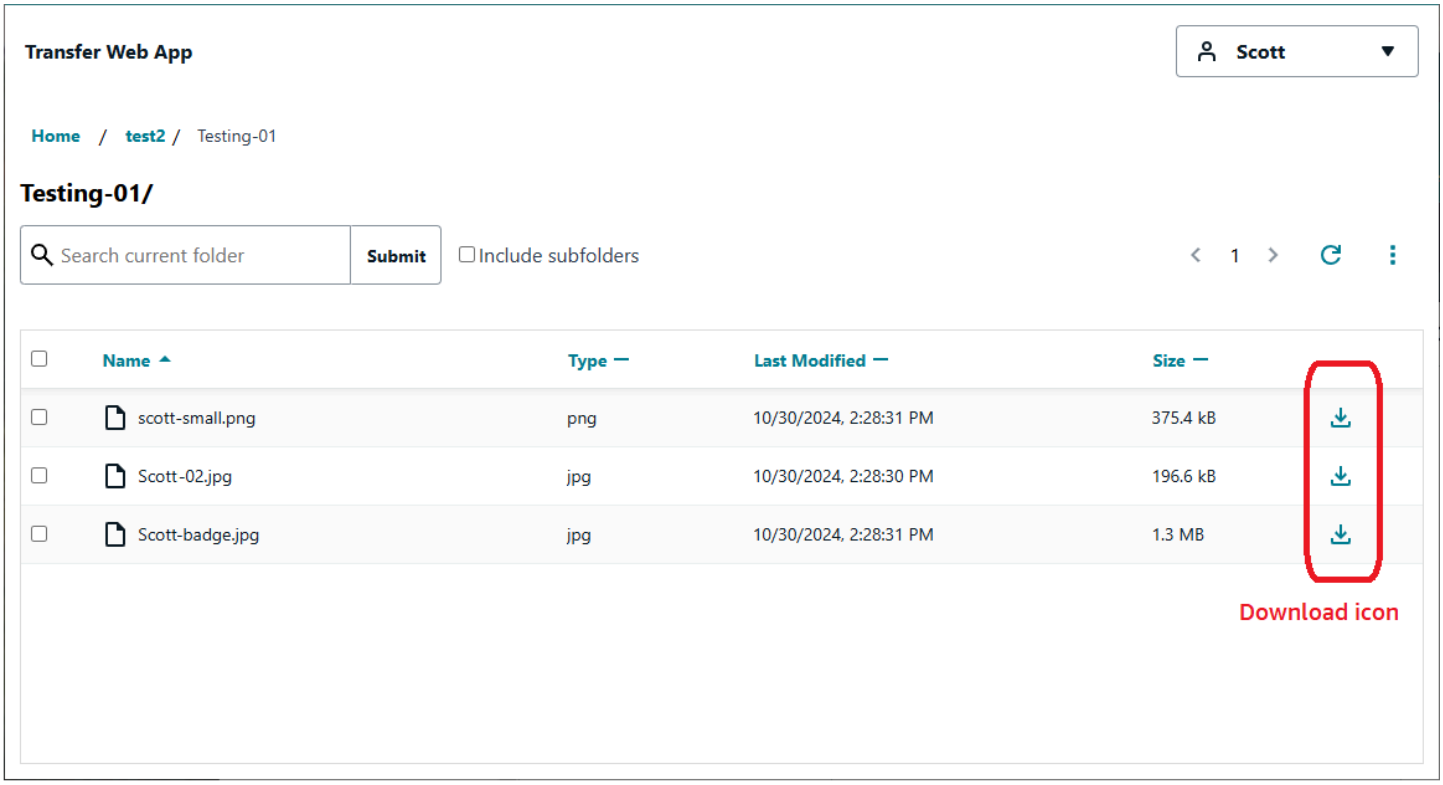
- 主页：您的主页列出了您可以访问的 S3 位置以及每个位置的权限。S3 位置是 S3 存储桶或前缀，您可以在使用 S3 访问权限授权时对其进行定义。这是用户的初始视图，它显示了您的最终用户有权访问的根级 S3 资源以及每个 S3 位置的权限。



- 位置详细信息：此视图可让用户浏览 S3 中的文件和文件夹，以及上传或下载文件。
- 位置操作：选择某项操作（例如“上传”）后，它会打开文件位置的另一个视图。
- 垂直省略号：垂直省略号图标可打开“操作”菜单。

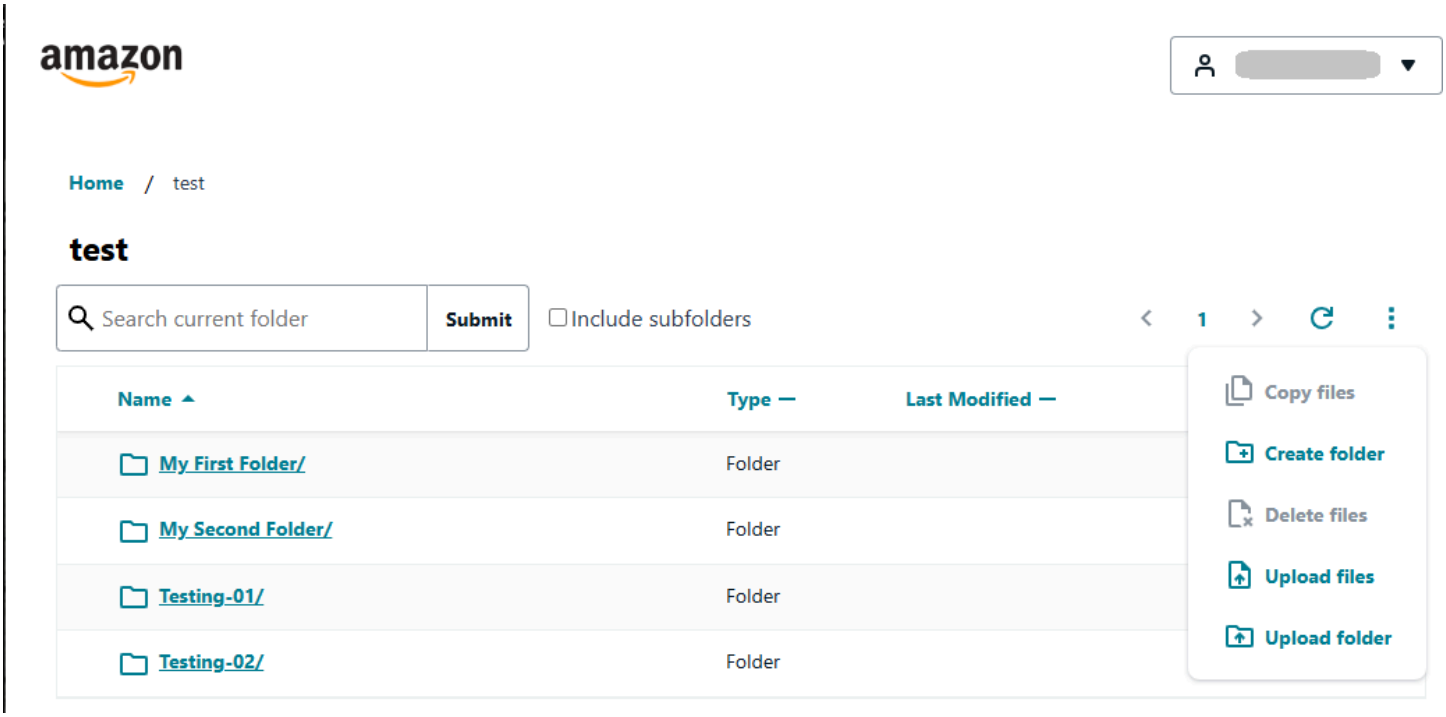
可用操作

大多数操作都可从“操作”菜单中找到。对于另一个主要操作，即下载文件，请在选择文件后使用下载图标（当前，您一次只能下载一个文件）。



在文件夹中，使用 “操作” 菜单执行以下任一任务：

- 将一个或多个文件复制到其他位置。
- 创建一个文件夹。
- 删除一个或多个文件。
- 上传一个或多个文件。
- 上传整个文件夹（如果有的话，包括子文件夹）。
- 选择一个文件夹并导航到该文件夹。然后，您可以执行先前列出的任何操作。
- 按页面排序。
- 按每个文件夹和子文件夹的文件或文件夹名称进行筛选。


amazon
Home / test
test
Search current folder
Submit
Include subfolders
1
Name
Type
Last Modified
My First Folder/
Folder
My Second Folder/
Folder
Testing-01/
Folder
Testing-02/
Folder
Copy files
Create folder
Delete files
Upload files
Upload folder

Amazon Transfer Family SFTP 连接器

Amazon Transfer Family SFTP 连接器与远程 SFTP 服务器建立连接，以便使用 SFTP 协议在 Amazon 存储和远程服务器之间传输文件。您可以将文件从 Amazon S3 发送到合作伙伴拥有的外部 SFTP 服务器，将文件从合作伙伴的 SFTP 服务器检索到 Amazon S3，或者在远程服务器上列出、删除、重命名或移动文件。SFTP 连接器支持两种出口类型：服务托管（使用托 Amazon 管基础设施）和 VPC（使用 Amazon VPC Lattice 通过您的 VPC 路由）。使用 SFTP 连接器，您可以在中构建自动化、事件驱动的文件传输工作流程。 Amazon

主题

- 创建 SFTP 连接器
- SFTP 连接器的 VPC 连接
- 使用 SFTP 连接器
- 监控 SFTP 连接器
- 管理 SFTP 连接器
- SFTP 连接器的扩展和配额
- 使用 SFTP 连接器的参考架构

创建 SFTP 连接器

本主题介绍如何创建 SFTP 连接器。每个连接器都提供与一台远程 SFTP 服务器连接的功能。您可以执行以下高级任务来配置 SFTP 连接器。

> **Note**
>
> 有关通过您的虚拟私有云路由流量的基于 VPC 的连接器，请参阅。使用基于 VPC 的出口创建一个 SFTP 连接器

1. 将连接器的身份验证凭据存储在中 Amazon Secrets Manager。
2. 通过指定密钥 ARN、远程服务器的 URL 或资源配置 ARN、包含连接器支持的算法的安全策略以及其他配置设置来创建连接器。
3. 创建连接器后，您可以对其进行测试以确保它可以与远程 SFTP 服务器建立连接。

选择 SFTP 连接器出口类型

创建 SFTP 连接器时，可以在 “服务托管” 和 “VPC Lattice” 之间选择出口类型。

- 服务托管（默认）：连接器使用 NAT 网关和拥有的 IP 地址通过 Amazon Transfer Family 公共互联网路由连接。该服务为您的连接器提供 3 个静态 IP 地址，这些地址需要在远程服务器上列入许可名单才能建立连接。
- VPC Lattice：连接器使用 Amazon VPC Lattice 通过您的 VPC 环境路由流量。在以下情况下，对 SFTP 连接器使用 VPC 连接：
  - 私有 SFTP 服务器：连接到只能从您的 VPC 访问的 SFTP 服务器
  - 本地连接：通过 Amazon Direct Connect 或 Amazon Virtual Private Network 连接连接到本地 SFTP 服务器
  - 自定义 IP 地址：向远程服务器提供您自己的 NAT 网关和弹性 IP 地址
  - 集中式安全控制：通过组织的中央 ingress/egress 控制进行文件传输

以下矩阵可帮助您为用例选择正确的连接器类型。

SFTP 连接器出口类型矩阵

能力	出口类型 = 服务托管	出口类型 = VPC 格子
连接到公共托管（可访问互联网）的 SFTP 服务器	支持	支持 [1]
连接到私有托管（本地）SFTP 服务器	不支持	支持 [2]
连接到私有托管（vpC 内）SFTP 服务器	不支持	支持
提供给远程 SFTP 服务器的静态 IP 地址	通过服务提供的静态 IP 地址提供支持	通过客户拥有的静态 IP 地址提供支持
可用带宽	每个账户 50 MBPS	更高的带宽，可从客户拥有的资源网关和 NAT 网关获得
通过客户自有的 NAT 网关和网络防火墙将流量路由到互联网	不支持。NAT 网关由 Transfer Family 服务拥有和管理。	支持

[1] 如果出口类型 = VPC Lattice，则使用出口中的出口基础设施（NAT 网关）设置支持与公共托管服务器的连接。 VPCs

[2] 如果出口类型 = VPC Lattice，则使用您的 VPC 中的现有网络（例如 Amazon Direct Connect 或 VPN）支持与私有托管服务器的连接。

主题

- 在 Secrets Manager 中存储 SFTP 连接器的身份验证凭证
- 使用服务管理的出口创建一个 SFTP 连接器
- 使用基于 VPC 的出口创建一个 SFTP 连接器
- 测试 SFTP 连接器

在 Secrets Manager 中存储 SFTP 连接器的身份验证凭证

您可以使用 Secrets Manager 来存储 SFTP 连接器的用户凭证。创建密钥时，必须提供用户名。此外，您可以提供密码、私钥或两者兼而有之。有关更多信息，请参阅 SFTP 连接器配额。

> **Note**
>
> 当你在 Secret Amazon Web Services 账户 s Manager 中存储密钥时，会产生费用。有关定价的信息，请参阅Amazon Secrets Manager 定价。

若要在 Secrets Manager 中存储 SFTP 连接器的用户凭证

1. 登录 Amazon Web Services 管理控制台 并打开 Amazon Secrets Manager 控制台，网址为https://console.aws.amazon.com/secretsmanager/。
2. 在左侧导航窗格中，选择密钥。
3. 在密钥页面，选择存储新密钥。
4. 在选择密钥类型页面上，对于密钥类型，选择其他类型密钥。
5. 提供您的密钥 key/value 信息：您需要提供用户名以及私钥或密码。

    a. 在键/值对部分，选择键/值选项卡。

    - 键 — 输入**`Username`**。
    - valu e-输入有权连接到合作伙伴服务器的用户的姓名。

b. 如果要提供密钥对，请选择添加行，然后在键/值对部分，选择键/值选项卡。

- 键 — 输入 **PrivateKey**。
- 值 — 粘贴您的私钥。

提示：您输入的私钥数据必须与在远程 SFTP 服务器上为该用户存储的公钥相对应。

> **Note**
>
> 无法使用受密码保护的私钥通过 SFTP 连接器进行身份验证。 Amazon Transfer Family

有关如何生成 public/private 密钥对的详细信息，请参阅在 macOS、Linux 或 Unix 系统创建 SSH 密钥。

c. 如果要提供密码，请选择添加行，然后在键/值对部分中，选择键/值选项卡。

- 键 — 输入 **Password**。
- 值 — 输入用户的密码。

6. 选择下一步。
7. 在配置密钥页面，输入密钥的名称和描述。建议对名称使用前缀 **aws/transfer/**。例如，您可以将密钥命名为 **aws/transfer/connector-1**。
8. 选择下一步，接受配置轮换页面的默认设置。然后选择下一步。
9. 在审核页面，选择存储以创建和存储密钥。

使用服务管理的出口创建一个 SFTP 连接器

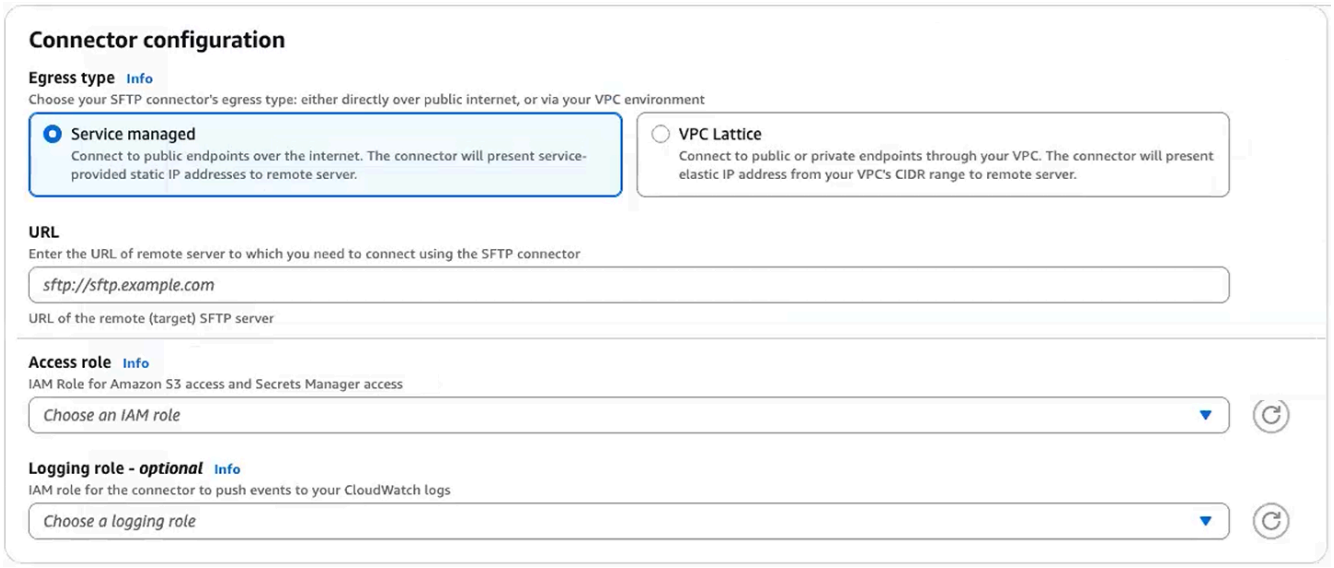
此过程说明如何使用 Amazon Transfer Family 控制台或 Amazon CLI创建 SFTP 连接器。

Console

若要创建 SFTP 连接器

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在左侧导航窗格中，选择 SFTP 连接器，然后选择创建 SFTP 连接器。

3. 在 “连接器配置” 部分中，对于 “出站类型”，选择 “服务管理”。此选项使用 Amazon Transfer Family 托管出口基础架构。Transfer Family 服务为每个 SFTP 连接器提供和管理静态 IP 地址。
4. 在连接器配置部分中，提供以下信息：



- 在 URL 中，输入远程 SFTP 服务器的 URL。例如 `sftp://AnyCompany.com`，此 URL 的格式必须为 `sftp://`*`partner-SFTP-server-url`*。

> **Note**
>
> （可选）您可以在 URL 中提供端口号。格式为 `sftp://`*`partner-SFTP-server-url`*`:`*`port-number`*。默认端口号（未指定端口时）为端口 22。

- 对于访问角色，请选择要使用的 (IAM) 角色的 Amazon 资源名称 Amazon Identity and Access Management (ARN)。
  - 确保此角色提供对 **`StartFileTransfer`** 请求中所使用文件位置父目录提供读取和写入权限。
  - 请确保此角色为 **`secretsmanager:GetSecretValue`** 提供访问密钥的权限。

> **Note**
>
> 在策略中，您必须为密钥指定 ARN。ARN 包含机密名称，但在名称后面附加了六个随机的字母数字字符。密钥的 ARN 格式如下。

```
arn:aws:secretsmanager:region:account-id:secret:aws/
transfer/SecretName-6RandomCharacters
```

- 此角色还应包含一个信任关系，从而允许服务器在为用户的传输请求提供服务时访问您的资源。有关建立信任关系的详细信息，请参阅 建立信任关系。

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
        "Sid": "AllowListingOfUserFolder",
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket"
        ]
    },
    {
        "Sid": "HomeDirObjectAccess",
        "Effect": "Allow",
        "Action": [
            "s3:PutObject",
            "s3:GetObject",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion",
            "s3:GetObjectVersion",
            "s3:GetObjectACL",
            "s3:PutObjectACL"
        ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    },
    {
        "Sid": "GetConnectorSecretValue",
        "Effect": "Allow",
        "Action": [
            "secretsmanager:GetSecretValue"
        ],
```

```
        "Resource": "arn:aws:secretsmanager:us-
west-2:111122223333:secret:aws/transfer/SecretName-6RandomCharacters"
    }
  ]
}
```

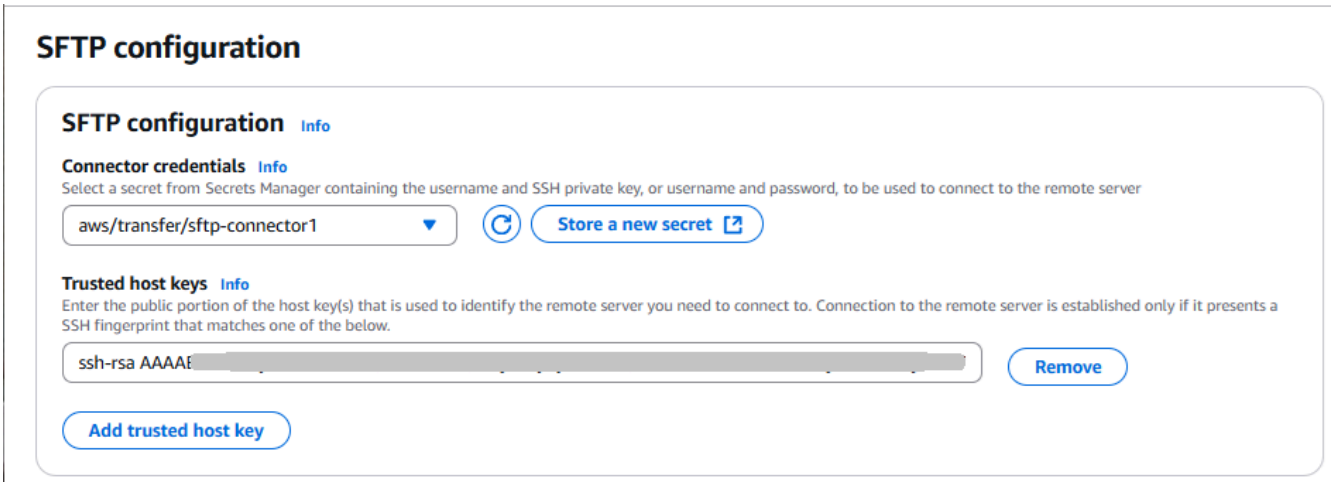
> **Note**
>
> 对于访问角色，该示例授予对单个密钥的访问权限。但是，您可以使用通配符，如果您想为多个用户和密钥重复使用相同的 IAM 角色，这样可以节省工作量。例如，以下资源语句为名称以 aws/transfer 开头的所有密钥授予权限。
>
> ```
> "Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/
> transfer/*"
> ```
>
> 您也可以将包含您的 SFTP 凭据的密钥存储在另一个 Amazon Web Services 账户中。有关启用跨账户秘密访问的详细信息，请参阅其他账户中用户的 Amazon Secrets Manager 密钥权限。

5. 完成连接器配置：

   - （可选）对于日志记录角色，选择连接器用于将事件推送到 CloudWatch 日志的 IAM 角色。以下示例策略列出了记录 SFTP 连接器事件的必要权限。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:DescribeLogStreams",
                "logs:CreateLogGroup",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/transfer/*"
        }
    ]
}
```

6. 在 SFTP 配置面板中提供以下信息：



- 对于 Connector 凭据，从下拉列表中选择包含 SFTP 用户私钥或密码的密钥的名称。Amazon Secrets Manager 您必须创建密钥并以特定方式存储它。有关更多信息，请参阅 在 Secrets Manager 中存储 SFTP 连接器的身份验证凭证 。
- （可选）您可以选择创建连接器，同时将`TrustedHostKeys`参数留空。但是，除非您在连接器的配置中提供此参数，否则您的连接器将无法使用远程服务器传输文件。您可以在创建连接器时输入可信主机密钥，也可以稍后使用`TestConnection`控制台操作或 API 命令返回的主机密钥信息更新您的连接器。也就是说，对于受信任的主机密钥文本框，您可以执行以下任一操作：
  - 在创建连接器时提供可信主机密钥。粘贴用于标识外部服务器的主机密钥的公共部分。您可以添加多个密钥，方法是选择“添加可信主机密钥”来添加其他密钥。您可以对 SFTP 服务器使用 `ssh-keyscan` 命令以检索必要的密钥。有关 Transfer Family 支持的受信任主机密钥的格式和类型的详细信息，请参阅 SFTPConnectorConfig。
  - 创建连接器时，请将可信主机密钥文本框留空，稍后再使用此信息更新您的连接器。如果您在创建连接器时没有主机密钥信息，则可以暂时将此参数留空，然后继续创建连接器。创建连接器后，使用新连接器的 ID 在连接器的详细信息页面中 Amazon CLI 或从连接器的详细信息页面运行`TestConnection`命令。如果成功，`TestConnection`将返回必要的主机密钥信息。然后，您可以使用控制台（或通过运行`UpdateConnector` Amazon CLI 命令）编辑连接器，并添加运行时返回的主机密钥信息`TestConnection`。

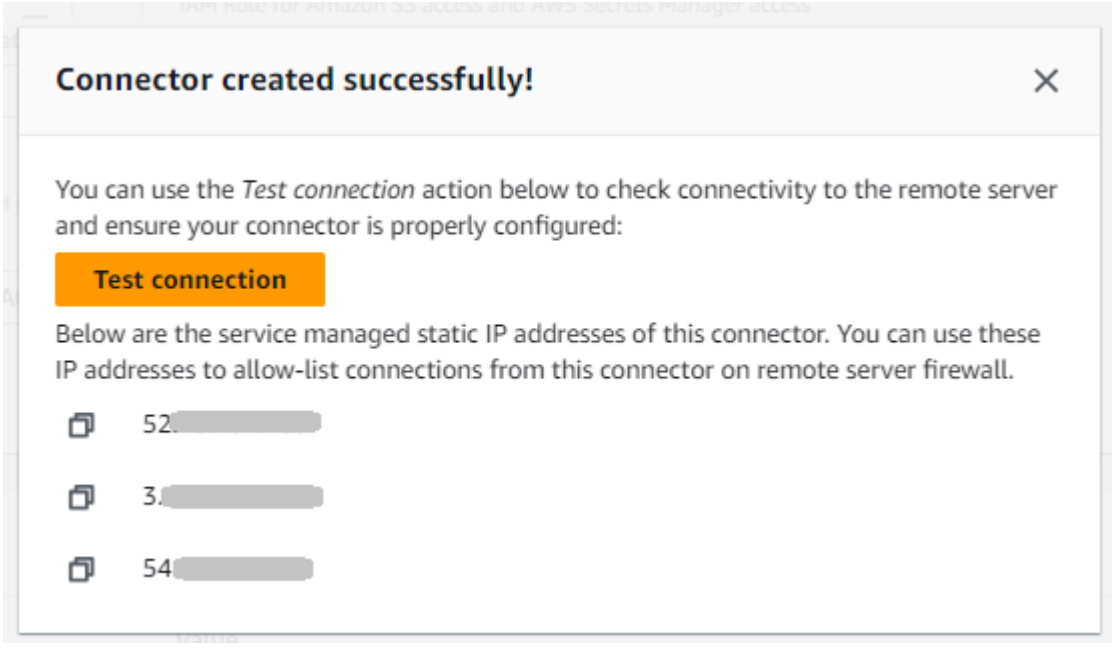
> **Important**
>
> 如果您通过运行`TestConnection`来检索远程服务器的主机密钥，请确保对返回的密钥执行 out-of-band验证。

您必须接受新密钥为可信密钥，或者使用以前从正在连接的远程 SFTP 服务器的所有者那里收到的已知指纹来验证所提供的指纹。

- （可选）在“最大并发连接数”中，从下拉列表中选择您的连接器创建到远程服务器的并发连接数。控制台上的默认选择为 5。

  此设置指定您的连接器可以同时与远程服务器建立的活动连接的数量。创建并行连接可以通过启用 parallel 操作来提高连接器性能。

7. 在“加密算法选项”部分，从“安全策略”字段的下拉列表中选择一个安全策略。安全策略允许您选择连接器支持的加密算法。有关可用安全策略和算法的详细信息，请参阅Amazon Transfer Family SFTP 连接器的安全策略。
8. （可选）对于标签部分的键和值，以键/值对格式输入一个或多个标签。
9. 确认所有设置后，选择创建 SFTP 连接器以创建 SFTP 连接器。如果成功创建了连接器，则会出现一个屏幕，其中包含分配的静态 IP 地址列表和“测试连接”按钮。使用按钮测试新连接器的配置。



“连接器”页面会出现，其中新 SFTP 连接器的 ID 已添加到列表中。要查看连接器的详细信息，请参阅 查看 SFTP 连接器详细信息。

CLI

可使用 create-connector 命令创建连接器。要使用此命令创建 SFTP 连接器，必须提供以下信息。

- 远程 SFTP 服务器的 URL。例如 `sftp://AnyCompany.com`，此 URL 的格式必须为 `sftp://partner-SFTP-server-url`。
- 访问角色。选择 Amazon Identity and Access Management IAM 角色的 Amazon 资源名称 (ARN)。
  - 确保此角色提供对 **`StartFileTransfer`** 请求中所使用文件位置父目录提供读取和写入权限。
  - 请确保此角色为 **`secretsmanager:GetSecretValue`** 提供访问密钥的权限。

> **Note**
>
> 在策略中，您必须为密钥指定 ARN。ARN 包含机密名称，但在名称后面附加了六个随机的字母数字字符。密钥的 ARN 格式如下。
>
> ```
> arn:aws:secretsmanager:region:account-id:secret:aws/
> transfer/SecretName-6RandomCharacters
> ```

- 此角色还应包含一个信任关系，从而允许服务器在为用户的传输请求提供服务时访问您的资源。有关建立信任关系的详细信息，请参阅 建立信任关系。

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
        "Sid": "AllowListingOfUserFolder",
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket"
        ]
    },
    {
        "Sid": "HomeDirObjectAccess",
        "Effect": "Allow",
        "Action": [
            "s3:PutObject",
            "s3:GetObject",
```

```
            "s3:DeleteObject",
            "s3:DeleteObjectVersion",
            "s3:GetObjectVersion",
            "s3:GetObjectACL",
            "s3:PutObjectACL"
        ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    },
    {
        "Sid": "GetConnectorSecretValue",
        "Effect": "Allow",
        "Action": [
            "secretsmanager:GetSecretValue"
        ],
        "Resource": "arn:aws:secretsmanager:us-west-2:111122223333:secret:aws/
transfer/SecretName-6RandomCharacters"
    }
  ]
}
```

> **Note**
>
> 对于访问角色，该示例授予对单个密钥的访问权限。但是，您可以使用通配符，如果您想为多个用户和密钥重复使用相同的 IAM 角色，这样可以节省工作量。例如，以下资源语句为名称以 `aws/transfer` 开头的所有密钥授予权限。
>
> ```
> "Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/
> *"
> ```
>
> 您也可以将包含您的 SFTP 凭据的密钥存储在另一个 Amazon Web Services 账户中。有关启用跨账户秘密访问的详细信息，请参阅其他账户中用户的 Amazon Secrets Manager 密钥权限。

- （可选）为连接器选择用于将事件推送到 CloudWatch 日志的 IAM 角色。以下示例策略列出了记录 SFTP 连接器事件的必要权限。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
```

```
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:DescribeLogStreams",
                "logs:CreateLogGroup",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/transfer/*"
        }
    ]
}
```

- 提供以下 SFTP 配置信息。
  - 中包含 SFTP 用户的私钥或密码 Amazon Secrets Manager 的密钥的 ARN。
  - 用于识别外部服务器的主机密钥的公共部分。如果您愿意，可以提供多个可信的主机密钥。

  提供 SFTP 信息的最简单方法是将其保存到文件中。例如，将以下示例文本复制到名为 `testSFTPConfig.json` 的文件中。

```
// Listing for testSFTPConfig.json
{
   "UserSecretId": "arn:aws::secretsmanager:us-east-2:123456789012:secret:aws/
transfer/example-username-key",
   "TrustedHostKeys": [
      "sftp.example.com ssh-rsa AAAAbbbb...EEEE="
   ]
}
```

- 为连接器指定安全策略，输入安全策略名称。

> **Note**
>
> `SecretId`可以是整个 ARN，也可以是密钥的名称（*`example-username-key`*在前面的列表中）。

然后运行以下命令来创建连接器：

```
aws transfer create-connector --url "sftp://partner-SFTP-server-url" \
--access-role your-IAM-role-for-bucket-access \
```

```
--logging-role arn:aws:iam::your-account-id:role/service-role/
AWSTransferLoggingAccess \
--sftp-config file:///path/to/testSFTPConfig.json \
--security-policy-name security-policy-name \
--maximum-concurrent-connections integer-from-1-to-5
```

当您描述 VPC 出口类型连接器时，响应将包含新字段：

```
{
   "Connector": {
      "AccessRole": "arn:aws:iam::123456789012:role/connector-role",
      "Arn": "arn:aws:transfer:us-east-1:123456789012:connector/
c-1234567890abcdef0",
      "ConnectorId": "c-1234567890abcdef0",
      "Status": "ACTIVE",
      "EgressConfig": {
        "VpcLattice": {
          "ResourceConfigurationArn": "arn:aws:vpc-lattice:us-
east-1:123456789012:resourceconfiguration/rcfg-12345678",
          "PortNumber": 22
        }
      },
      "EgressType": "VPC",
      "ServiceManagedEgressIpAddresses": null,
      "SftpConfig": {
         "TrustedHostKeys": [ "ssh-rsa AAAAB3NzaC..." ],
         "UserSecretId": "aws/transfer/connector-secret"
      },
      "Url": "sftp://my.sftp.server.com:22"
   }
}
```

请注意，ServiceManagedEgressIpAddresses对于 VPC 出口类型连接器，该值为空，因为流量通过您的 VPC 而不是 Amazon 托管基础设施路由。

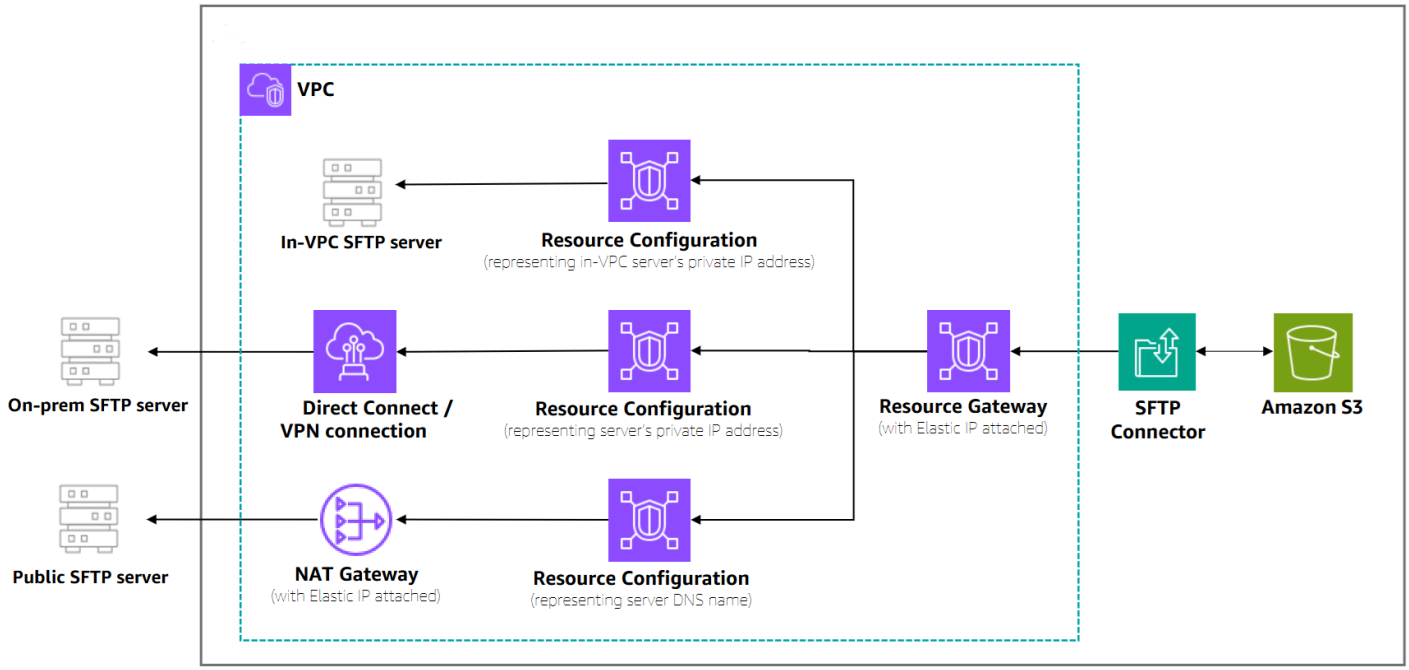
使用基于 VPC 的出口创建一个 SFTP 连接器

本主题提供创建具有 VPC 连接的 SFTP 连接器的 step-by-step说明。支持 vpc_Lattice 的连接器使用 Amazon VPC Lattice 通过您的虚拟私有云路由流量，从而实现与私有终端节点的安全连接或使用您自己的 NAT 网关访问互联网。

何时使用 VPC 连接

在以下情况下，对 SFTP 连接器使用 VPC 连接：

- 私有 SFTP 服务器：连接到只能从您的 VPC 访问的 SFTP 服务器。
- 本地连接：通过 Di Amazon rect Connect 或 Amazon Site-to-Site VPN 连接连接到本地 SFTP 服务器。
- 自定义 IP 地址：使用您自己的 NAT 网关和弹性 IP 地址，包括 BYOIP 场景。
- 集中式安全控制：通过组织的中央 ingress/egress 控制进行文件传输。



支持 vpc_lattice 的 SFTP 连接器的先决条件

在创建支持 vpc_lattice 的 SFTP 连接器之前，必须满足以下先决条件：

基于 VPC 的连接的工作原理

VPC Lattice 使您能够安全地与其他 Amazon 服务共享 VPC 资源。 Amazon Transfer Family 使用服务网络来简化资源共享过程。关键组件包括：

- 资源网关：用作您的 VPC 的访问点。你可以在你的 VPC 中创建它，至少有两个可用区。
- 资源配置：包含要连接的 SFTP 服务器的私有 IP 地址或公有 DNS 名称。

创建支持 vpc_Lattice 的连接器时， Amazon Transfer Family 使用正向访问会话 (FAS) 临时获取您的凭证，并将您的资源配置与我们的服务网络相关联。

必需的设置步骤

1. VPC 基础设施：确保您的 VPC 配置正确，其中包含满足您的 SFTP 服务器连接要求所需的子网、路由表和安全组。
2. 资源网关：使用 VPC Lattice `create-resource-gateway` 命令在您的 VPC 中创建资源网关。资源网关必须与至少两个可用区中的子网关联。有关更多信息，请参阅 Amazon VPC Lattice 用户指南中的资源网关。
3. 资源配置：使用 VPC Lattic `create-resource-configuration` e 命令创建代表目标 SFTP 服务器的资源配置。您可以指定下列之一：
   - 私有端点的私有 IP 地址
   - 公共终端节点的公有 DNS 名称（公共终端节点不支持 IP 地址）
4. 身份验证凭证： Amazon Secrets Manager 如中所述，将 SFTP 用户凭据存储在中。在 Secrets Manager 中存储 SFTP 连接器的身份验证凭证

> **Important**
>
> 资源网关和资源配置必须在同一个 Amazon 账户中创建。创建资源配置时，必须先设置资源网关。

有关 VPC 资源配置的更多信息，请参阅 Amazon VPC Lattice 用户指南中的资源配置。

> **Note**
>
> 在 Amazon VPC Lattice 资源可用 Amazon Web Services 区域 的地方，可以使用 SFTP 连接器的 VPC 连接。有关更多信息，请参阅 VPC 莱迪思。 FAQs可用区支持因地区而异，资源网关至少需要两个可用区。

创建支持 vpc_lattice 的 SFTP 连接器

完成先决条件后，您可以使用 Amazon 管理控制台或 Amazon SDKs创建具有 VPC 连接的 Amazon CLI SFTP 连接器。

Console

创建支持 vpc_lattice 的 SFTP 连接器

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在左侧导航窗格中，选择 SFTP 连接器，然后选择创建 SFTP 连接器。
3. 在连接器配置部分中，对于出口类型，选择 VPC Lat t ice。

   此选项使用 Amazon VPC Lattice 通过您的 VPC 路由流量，实现跨虚拟私有云资源访问。您可以使用此选项连接到私有托管的服务器终端节点，通过 VPC 的安全控制来路由流量，或者使用自己的 NAT 网关和弹性 IP 地址。远程 SFTP 服务器的地址以您的 VPC 中的资源配置表示。有关资源配置的更多信息，请参阅 Amazon VPC Lattice 用户指南中的 VPC 资源的资源配置。
4. 完成连接器配置：

   - 对于访问角色，请选择要使用的 (IAM) 角色的 Amazon 资源名称 Amazon Identity and Access Management (ARN)。
     - 确保此角色提供对 **StartFileTransfer** 请求中所使用文件位置父目录提供读取和写入权限。
     - 请确保此角色为 **secretsmanager:GetSecretValue** 提供访问密钥的权限。

     > **Note**
     >
     > 在策略中，您必须为密钥指定 ARN。ARN 包含机密名称，但在名称后面附加了六个随机的字母数字字符。密钥的 ARN 格式如下。
     >
     > ```
     > arn:aws:secretsmanager:region:account-id:secret:aws/
     > transfer/SecretName-6RandomCharacters
     > ```

   - 此角色还应包含一个信任关系，从而允许服务器在为用户的传输请求提供服务时访问您的资源。有关建立信任关系的详细信息，请参阅 建立信任关系。

     ```
     {
       "Version":"2012-10-17",
       "Statement": [
         {
             "Sid": "AllowListingOfUserFolder",
             "Action": [
     ```

```
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket"
        ]
    },
    {
        "Sid": "HomeDirObjectAccess",
        "Effect": "Allow",
        "Action": [
            "s3:PutObject",
            "s3:GetObject",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion",
            "s3:GetObjectVersion",
            "s3:GetObjectACL",
            "s3:PutObjectACL"
        ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
    },
    {
        "Sid": "GetConnectorSecretValue",
        "Effect": "Allow",
        "Action": [
            "secretsmanager:GetSecretValue"
        ],
        "Resource": "arn:aws:secretsmanager:us-
west-2:111122223333:secret:aws/transfer/SecretName-6RandomCharacters"
    }
  ]
}
```

> **Note**
>
> 对于访问角色，该示例授予对单个密钥的访问权限。但是，您可以使用通配符，如果您想为多个用户和密钥重复使用相同的 IAM 角色，这样可以节省工作量。例如，以下资源语句为名称以 aws/transfer 开头的所有密钥授予权限。
>
> ```
> "Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/
> transfer/*"
> ```

您也可以将包含您的 SFTP 凭据的密钥存储在另一个 Amazon Web Services 账户中。有关启用跨账户秘密访问的详细信息，请参阅其他账户中用户的 Amazon Secrets Manager 密钥权限。

- 对于资源配置 ARN，请输入指向您的 SFTP 服务器的 VPC Lattice 资源配置的 ARN：

```
arn:aws:vpc-lattice:region:account-id:resourceconfiguration/rcfg-12345678
```

- （可选）对于日志记录角色，选择连接器用于将事件推送到 CloudWatch 日志的 IAM 角色。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:DescribeLogStreams",
                "logs:CreateLogGroup",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/transfer/*"
        }
    ]
}
```

5. 在 SFTP 配置面板中提供以下信息：

   - 对于连接器凭据，请选择中 Amazon Secrets Manager 包含 SFTP 用户私钥或密码的密钥的名称。
   - 对于受信任的主机密钥，请粘贴用于标识外部服务器的主机密钥的公共部分，或者将其留空，以便以后使用`TestConnection`命令进行配置。

     由于此主机密钥用于 VPC_LATTICE 连接器，因此请删除密钥中的主机名

   - （可选）在 “最大并发连接数” 中，选择您的连接器创建到远程服务器的并发连接数（默认为 5）。

6. 在加密算法选项部分，从下拉列表中选择一个安全策略。
7. （可选）在 “标签” 部分中，将标签添加为键值对。

8. 选择创建 SFTP 连接器以创建支持 vpc_Lattice 的 SFTP 连接器。

在配置资源关联PENDING时，连接器的创建状态将为，这通常需要几分钟。状态更改为后ACTIVE，连接器就可以使用了。

CLI

使用以下命令创建支持 vpc_lattice 的 SFTP 连接器：

```
aws transfer create-connector \
    --url "sftp://my.sftp.server.com:22" \
    --access-role arn:aws:iam::123456789012:role/TransferConnectorRole \
    --sftp-config UserSecretId=my-secret-id,TrustedHostKeys="ssh-rsa AAAAB3NzaC..."
 \
    --egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-
east-1:123456789012:resourceconfiguration/rcfg-1234567890abcdef0} \
    --security-policy-name TransferSecurityPolicy-2024-01
```

VPC 连接的关键参数是`--egress-config`，它指定了定义您的 SFTP 服务器目标的资源配置 ARN。

监控 VPC 连接器状态

支持 vpc_Lattice 的连接器具有异步设置过程。创建后，监视连接器状态：

- 待处理：连接器正在配置中。服务网络配置正在进行中，通常需要几分钟。
- 激活：连接器已准备就绪，可以传输文件。
- 错误：连接器配置失败。查看错误详细信息以获取疑难解答信息。

使用`describe-connector`以下命令检查连接器状态：

```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

在 PENDING 状态下，`test-connection`API 将返回 “连接器不可用”，直到配置完成。

限制和注意事项

- 公共终端节点：通过 VPC 连接到公共终端节点时，必须在资源配置中提供 DNS 名称。不支持公有 IP 地址。

- 区域可用性：VPC 连接仅在部分区域提供 Amazon Web Services 区域。不支持跨区域资源共享。
- 可用区要求：资源网关必须与至少两个可用区中的子网关联。并非所有可用区在每个区域都支持 VPC Lattice。
- 连接限制：每个资源最多 350 个连接，TCP 连接的空闲超时时间为 350 秒。

成本考虑因素

Amazon Transfer Family 除常规服务费外，不收取任何额外费用。但是，如果客户使用自己的 NAT 网关访问互联网，则可能需要向 Amazon VPC Lattice 收取与共享其亚马逊虚拟私有云资源相关的额外费用；如果客户使用自己的 NAT 网关访问互联网，则可能需要支付 NAT 网关费用。

要了解完整的 Amazon Transfer Family 定价信息，请参阅定Amazon Transfer Family 价页面。

SFTP 连接器的 VPC 连接示例

本节提供了在各种场景中创建具有 VPC 连接的 SFTP 连接器的示例。在使用这些示例之前，请确保您已按照 VPC 连接文档中所述完成了 VPC 基础设施设置。

示例：私有端点连接

此示例说明如何创建 SFTP 连接器，该连接器可连接到只能从您的 VPC 访问的私有 SFTP 服务器。

先决条件

1. 在您的 VPC 中创建资源网关：

```
aws vpc-lattice create-resource-gateway \
    --name my-private-server-gateway \
    --vpc-identifier vpc-1234567890abcdef0 \
    --subnet-ids subnet-1234567890abcdef0 subnet-0987654321fedcba0
```

2. 为您的私有 SFTP 服务器创建资源配置：

```
aws vpc-lattice create-resource-configuration \
    --name my-private-server-config \
    --resource-gateway-identifier rgw-1234567890abcdef0 \
    --resource-configuration-definition ipResource={ipAddress="10.0.1.100"} \
    --port-ranges 22
```

创建支持 vpc_lattice 的连接器

1. 创建具有 VPC 连接的 SFTP 连接器：

```
aws transfer create-connector \
    --access-role arn:aws:iam::123456789012:role/TransferConnectorRole \
    --sftp-config UserSecretId=my-private-server-credentials,TrustedHostKeys="ssh-
rsa AAAAB3NzaC..." \
    --egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-
east-1:123456789012:resourceconfiguration/rcfg-1234567890abcdef0,PortNumber=22}
```

2. 监视连接器状态，直到它变成ACTIVE：

```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

远程 SFTP 服务器将看到来自您的 VPC CIDR 范围内的资源网关 IP 地址的连接。

示例：通过 VPC 的公共终端节点

此示例说明如何通过您的 VPC 将连接路由到公有 SFTP 服务器，以利用集中式安全控制并使用您自己的 NAT 网关 IP 地址。

先决条件

1. 在您的 VPC 中创建资源网关（与私有终端节点示例相同）。
2. 使用公共 SFTP 服务器的 DNS 名称为其创建资源配置：

```
aws vpc-lattice create-resource-configuration \
    --name my-public-server-config \
    --resource-gateway-identifier rgw-1234567890abcdef0 \
    --resource-configuration-definition dnsResource={domainName="sftp.example.com"}
 \
    --port-ranges 22
```

> **Note**
>
> 对于公共终端节点，必须使用 DNS 名称，而不是 IP 地址。

创建连接器

- 创建 SFTP 连接器：

```
aws transfer create-connector \
    --access-role arn:aws:iam::123456789012:role/TransferConnectorRole \
    --sftp-config UserSecretId=my-public-server-credentials,TrustedHostKeys="ssh-
rsa AAAAB3NzaC..." \
    --egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-
east-1:123456789012:resourceconfiguration/rcfg-0987654321fedcba0,PortNumber=22}
```

流量将从连接器流向您的资源网关，然后通过您的 NAT 网关到达公共 SFTP 服务器。远程服务器会将您的 NAT 网关的弹性 IP 地址视为来源。

示例：跨账户私有终端节点

此示例说明如何使用资源共享以不同的 Amazon 账户连接到私有 SFTP 服务器。

> **Note**
>
> 如果您已经通过其他机制（例如）启用了跨VPC资源共享 Amazon Transit Gateway，则无需配置此处所述的资源共享。SFTP 连接器会自动使用现有的路由机制，例如 Transit Gateway 路由表。您只需要在创建 SFTP 连接器的同一个帐户中创建资源配置即可。

账户 A（资源提供者）-共享资源配置

1. 在账户 A 中创建资源网关和资源配置（与前面的示例相同）。
2. 使用 Resource Access Manager 与账户 B 共享 Amazon 资源配置：

```
aws ram create-resource-share \
    --name cross-account-sftp-share \
    --resource-arns arn:aws:vpc-lattice:us-
east-1:111111111111:resourceconfiguration/rcfg-1234567890abcdef0 \
    --principals 222222222222
```

账户 B（资源使用者）-接受并使用共享

1. 接受资源共享邀请：

```
aws ram accept-resource-share-invitation \
    --resource-share-invitation-arn arn:aws:ram:us-east-1:111111111111:resource-
share-invitation/invitation-id
```

2. 在账户 B 中创建 SFTP 连接器：

```
aws transfer create-connector \
    --access-role arn:aws:iam::222222222222:role/TransferConnectorRole \
    --sftp-config UserSecretId=cross-account-server-
credentials,TrustedHostKeys="ssh-rsa AAAAB3NzaC..." \
    --egress-config VpcLattice={ResourceConfigurationArn=arn:aws:vpc-lattice:us-
east-1:111111111111:resourceconfiguration/rcfg-1234567890abcdef0,PortNumber=22}
```

账户 B 中的连接器现在可以通过共享资源配置访问账户 A 中的专用 SFTP 服务器。

常见故障排除场景

以下是创建启用 vpc_Lattice 的连接器时常见问题的解决方案：

- 连接器停留在 PENDING 状态：检查您的资源网关是否处于活动状态，并且子网位于支持的可用区。如果连接器仍处于 PENDING 状态，请UpdateConnector使用最初使用的相同配置参数进行调用。这会触发一个可能解决问题的新状态事件。
- 连接超时：验证安全组规则允许端口 22 上的流量以及您的 VPC 路由是否正确。
- DNS 解析问题：对于公共终端节点，请确保您的 VPC 通过 NAT 网关或 Internet Gateway 实现互联网连接。
- 跨账户访问被拒绝：验证资源共享是否被接受以及资源配置 ARN 是否正确。如果在原始账户创建资源共享时将适当的权限策略附加到资源配置中，则需要以下权限：`vpc-lattice:AssociateViaAWSService`、`vpc-lattice:AssociateViaAWSService-EventsAndStates`、`vpc-lattice:CreateServiceNetworkResourceAssociation`、`vpc-lattice:GetResourceConfiguration`。

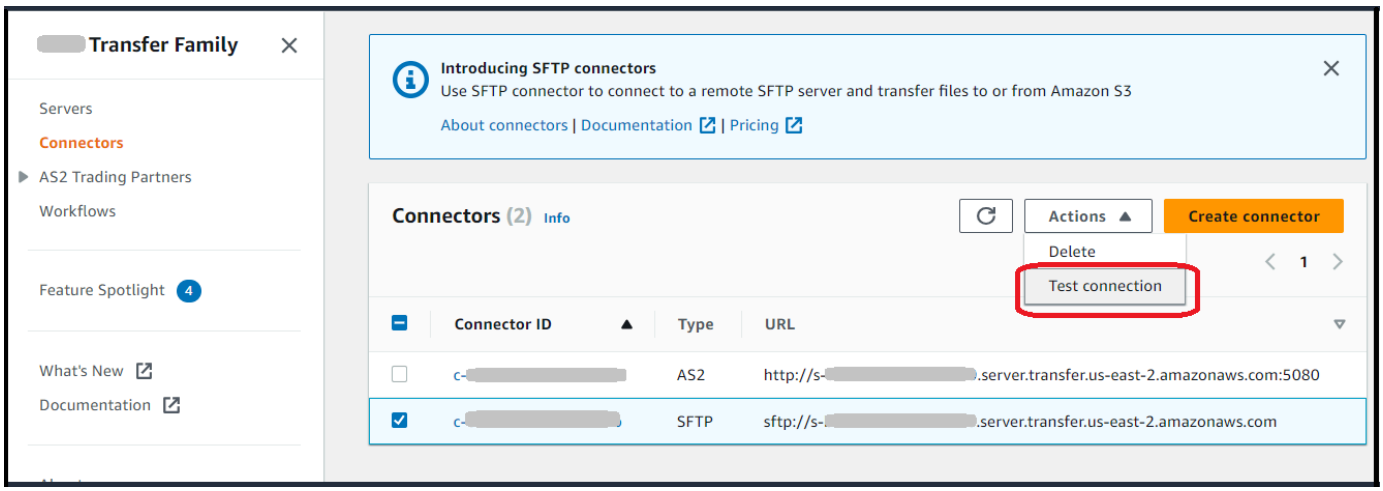
测试 SFTP 连接器

创建 SFTP 连接器后，我们建议您在尝试使用新连接器传输任何文件之前对其进行测试。

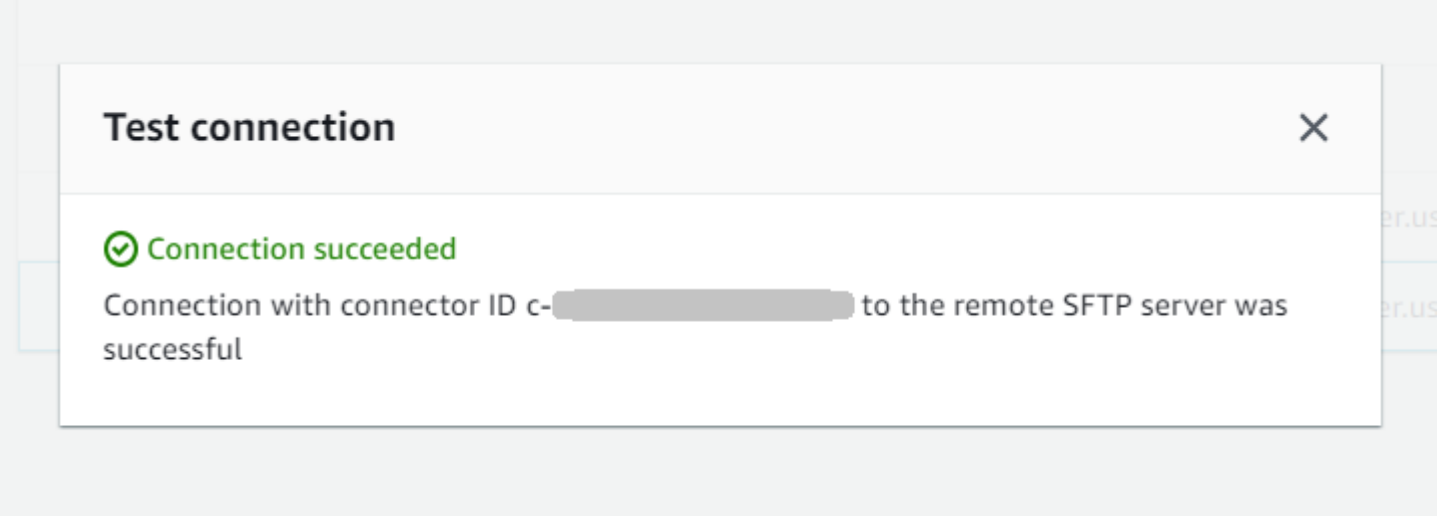
若要测试 SFTP 连接器

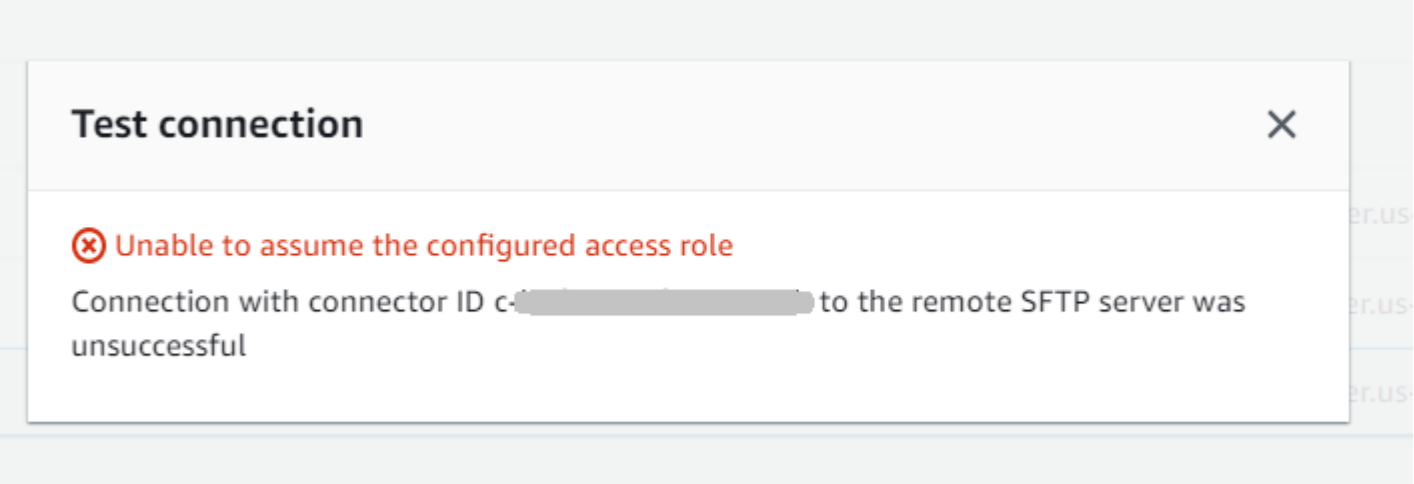
1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。

2. 在左侧导航窗格中，选择 SFTP 连接器，然后选择一个连接器。
3. 从操作菜单中选择测试连接。



系统会返回一条消息，指示测试是通过还是失败。如果测试失败，系统会根据测试失败的原因提供错误消息。





> **Note**
>
> 要使用 API 测试您的连接器，请参阅 TestConnection API 文档。

SFTP 连接器的 VPC 连接

Amazon Transfer Family SFTP 连接器支持使用 Amazon VPC Lattice 通过您的 VPC 环境连接到远程 SFTP 服务器。这使您能够连接私有托管的 SFTP 服务器或通过 VPC 的安全控制来路由互联网流量，并使用自己的 NAT 网关和弹性 IP 地址。

出口类型

SFTP 连接器可以使用以下两种出口类型之一：

- 服务托管（默认）：连接器使用 NAT 网关和拥有的 IP 地址通过 Amazon Transfer Family 公共互联网路由连接。
- VPC_LATTICE：连接器使用跨虚拟私有网络资源访问通过您的 VPC 环境路由流量。

何时使用 VPC 连接

在以下情况下，对 SFTP 连接器使用 VPC 连接：

- 私有 SFTP 服务器：连接到只能从您的 VPC 访问的 SFTP 服务器。
- 本地连接：通过 Di Amazon rect Connect 或 Amazon Site-to-Site VPN 连接连接到本地 SFTP 服务器。
- 自定义 IP 地址：使用您自己的 NAT 网关和弹性 IP 地址，包括 BYOIP 场景。

- 集中式安全控制：通过组织的中央 ingress/egress 控制进行文件传输。

要求

在创建支持 vpc_lattice 的 SFTP 连接器之前，您需要：

- VPC 和相关基础设施（子网、路由表、安全组）
- 您的 VPC 中的资源网关（至少两个可用区）
- 指定目标 SFTP 服务器的资源配置

有关详细的设置说明，请参阅创建支持 vpc_lattice 的 SFTP 连接器。而且，有关示例，请参阅SFTP 连接器的 VPC 连接示例。

使用 SFTP 连接器

本主题介绍如何使用 SFTP 连接器执行支持的文件操作。您还可以在 Amazon Transfer Family 控制台上选择连接器的详细信息，找到用于执行这些操作的示例命令https://console.aws.amazon.com/transfer/。

创建 SFTP 连接器后，您可以使用它在与之关联的远程 SFTP 服务器上执行以下文件操作。

- 将文件从 Amazon S3 发送到远程 SFTP 服务器。
- 将文件从远程 SFTP 服务器检索到 Amazon S3。
- 列出远程 SFTP 服务器上某个目录中的文件和子文件夹。
- 删除、重命名或移动远程 SFTP 服务器上的文件和目录。

有关创建连接器的详细信息，请参阅 创建 SFTP 连接器。

主题

- 传输文件
- 列出远程目录的内容
- 移动、重命名或删除远程服务器上的文件或目录

传输文件

主题

- 使用 SFTP 连接器发送和检索文件

使用 SFTP 连接器发送和检索文件

要使用 SFTP 连接器发送和检索文件，您可以使用 StartFileTransferAPI 操作并指定以下参数，具体取决于您是发送文件（出站传输）还是接收文件（入站传输）。请注意，每个StartFileTransfer请求可以包含 10 个不同的路径。

> **Note**
>
> 默认情况下，SFTP 连接器一次处理一个文件，按顺序传输文件。您可以选择让连接器与支持来自同一用户的并发会话的远程服务器创建并行会话，并行处理最多 5 个文件，从而提高传输性能。
>
> 要为任何连接器启用并发连接，可以在创建或更新连接器时编辑 “最大并发连接数” 设置。有关更多信息，请参阅 使用服务管理的出口创建一个 SFTP 连接器。

- 出站传输
  - `send-file-paths` 包含一到十个源文件路径，用于将文件传输到合作伙伴的 SFTP 服务器。
  - `remote-directory-path` 是客户的 SFTP 服务器上向其发送文件的远程路径。
- 入站传输
  - `retrieve-file-paths` 包含一到十条远程路径。每个路径都指定了将文件从合作伙伴的 SFTP 服务器传输到您的 Transfer Family 服务器的位置。
  - `local-directory-path` 是存储文件的 Amazon S3 位置（存储桶和可选前缀）。

要发送文件，请指定 `send-file-paths` 和 `remote-directory-path` 参数。您最多可以为 `send-file-paths` 参数指定 10 个文件。以下示例命令将位于 Amazon S3 存储空间中的名为 `/amzn-s3-demo-source-bucket/file1.txt` 和 `/amzn-s3-demo-source-bucket/file2.txt` 的文件发送到合作伙伴的 SFTP 服务器上的 `/tmp` 目录。要使用此示例命令，请将 *amzn-s3-demo-source-bucket* 替换为您自己的存储桶。

```
aws transfer start-file-transfer --send-file-paths /amzn-s3-demo-source-bucket/
file1.txt /amzn-s3-demo-source-bucket/file2.txt \
    --remote-directory-path /tmp --connector-id c-1111AAAA2222BBBB3 --region us-east-2
```

要检索文件，请指定retrieve-file-paths和local-directory-path参数。以下示例检索合作伙伴的 SFTP 服务器/my/remote/file2.txt上的文件/my/remote/file1.txt，并将其放置在 Amazon S3 位置 /amzn-s3-demo-bucket/ 中。*prefix*要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws transfer start-file-transfer --retrieve-file-paths /my/remote/file1.txt  /my/
remote/file2.txt \
   --local-directory-path /amzn-s3-demo-bucket/prefix --connector-id
 c-2222BBBB3333CCCC4 --region us-east-2
```

前面的示例指定了 SFTP 服务器上的绝对路径。您也可以使用相对路径：即相对于 SFTP 用户主目录的路径。例如，如果 SFTP 用户是 marymajor，而他们在 SFTP 服务器上的主目录是 /users/marymajor/，则以下命令会将 /amzn-s3-demo-source-bucket/file1.txt 发送到 /users/marymajor/test-connectors/file1.txt

```
aws transfer start-file-transfer --send-file-paths /amzn-s3-demo-source-bucket/
file1.txt \
   --remote-directory-path test-connectors --connector-id c-2222BBBB3333CCCC4 --
region us-east-2
```

列出远程目录的内容

在从远程 SFTP 服务器检索文件之前，可以检索远程 SFTP 服务器上目录的内容。为此，你可以使用StartDirectoryListingAPI 操作。

以下示例列出了远程 SFTP 服务器上该home文件夹的内容，该内容是在连接器的配置中指定的。结果将放入 Amazon S3 位置/amzn-s3-demo-bucket/connector-files和名为的文件中c-AAAA1111BBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json。

```
aws transfer start-directory-listing  \
   --connector-id c-AAAA1111BBBB2222C  \
   --output-directory-path /amzn-s3-demo-bucket/example/connector-files  \
   --remote-directory-path /home
```

此 Amazon CLI 命令返回列表 ID 和包含结果的文件的名称。

```
{
    "ListingId": "6666abcd-11aa-22bb-cc33-0000aaaa3333",
    "OutputFileName": "c-AAAA1111BBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json"
}
```

> **Note**
>
> 输出文件的命名约定为*connector-ID*-*listing-ID*.json。

JSON 文件包含以下信息：

- filePath：远程文件的完整路径，相对于远程服务器上 SFTP 连接器的列出请求目录。
- modifiedTimestamp：上次修改文件的时间，以秒为单位，采用协调世界时 (UTC) 格式。该字段是可选的。如果远程文件属性不包含时间戳，则文件列表中将省略该时间戳。
- size: 文件的大小，以字节为单位。该字段是可选的。如果远程文件属性不包含文件大小，则会将其从文件列表中省略。
- path：远程目录的完整路径，相对于远程服务器上的 SFTP 连接器的列出请求目录。
- truncated: 一个标志，指示列表输出是否包含远程目录中包含的所有项目。如果您的truncated输出值为 true，则可以增加可选max-items输入属性中提供的值，以便能够列出更多项目（允许的最大列表大小为 10,000 个）。

以下是输出文件 (c-AAAA1111BBBB2222C-6666abcd-11aa-22bb-cc33-0000aaaa3333.json) 内容的示例，其中远程目录包含两个文件和两个子目录（路径）。

```
{
    "files": [
        {
            "filePath": "/home/what.txt",
            "modifiedTimestamp": "2024-01-30T20:34:54Z",
            "size" : 2323
        },
        {
            "filePath": "/home/how.pgp",
            "modifiedTimestamp": "2024-01-30T20:34:54Z",
            "size" : 4691
        }
    ],
    "paths": [
        {
            "path": "/home/magic"
        },
        {
            "path": "/home/aws"
```

```
        },
    ],
    "truncated": "false"
}
```

移动、重命名或删除远程服务器上的文件或目录

主题

- 移动或重命名远程 SFTP 服务器上的文件或目录
- 删除远程 SFTP 服务器上的文件或目录

移动或重命名远程 SFTP 服务器上的文件或目录

您可以使用 SFTP 连接器移动或重命名远程 SFTP 服务器上的文件和目录。请注意，远程服务器需要支持这些操作才能成功使用连接器进行处理。

一些常见的用例如下。

- 远程服务器每小时生成或接收一个新文件，文件名相同，但时间戳不同。要使主文件夹保持最新状态（使其仅包含最新文件），您可以使用连接器将较旧的文件移至已存档文件夹。
- 您可以使用连接器列出远程目录中的所有文件，然后将所有文件传输到本地存储。然后，您可以使用连接器将文件移动到远程服务器上的已存档文件夹。

您必须对要处理的每个文件或目录使用`StartRemoteMove`调用，因为该命令将单个源文件和目标文件或目录作为参数。但是，您可以通过让连接器创建与远程服务器的并发会话来提高性能，这些会话支持来自同一用户的并行会话以及 move/rename 最多 5 个并行文件。

以下示例将远程 SFTP 服务器上的文件从移动`/source/folder/sourceFile`到`/destination/targetFile`，并返回该操作的唯一标识符。

```
aws transfer --connector-id c-AAAA1111BBBB2222C start-remote-move \
   --source-path /source/folder/sourceFile --target-path /destination/targetFile
```

> **Note**
>
> 对于这些 move/rename 操作，Transfer Family 使用标准`SFTP SSH_FXP_RENAME`命令来执行 move/rename 操作。

删除远程 SFTP 服务器上的文件或目录

您可以使用 SFTP 连接器删除远程 SFTP 服务器上的文件或目录。请注意，远程服务器需要支持这些操作才能成功使用连接器进行处理。

> **Note**
>
> 只有空目录才支持远程目录的删除操作。

一些常见的用例如下。

- 您可以使用连接器从远程 SFTP 服务器检索文件，将其存储在 Amazon S3 存储桶中，然后对其进行加密。最后，您可以使用连接器删除远程服务器上未加密的文件。
- 您可以使用连接器列出远程目录中的所有文件，然后将所有文件传输到本地存储。然后，您可以使用连接器删除您传输的所有文件。如果您愿意，也可以删除远程目录。

您必须对要删除的每个文件或目录使用`StartRemoteDelete`调用，因为该命令将单个文件或目录作为参数。但是，您可以让连接器与支持来自同一用户的并发会话的远程服务器创建并行会话，并行删除最多 5 个 files/directories 会话，从而提高性能。

以下示例删除远程 SFTP 服务器上路径中的一个文件`/delete/folder/deleteFile`，并返回该操作的唯一标识符。

```
aws transfer start-remote-delete --connector-id c-AAAA1111BBBB2222C \
   --delete-path /delete/folder/deleteFile
```

> **Note**
>
> 对于删除操作，Transfer Family 使用标准`SSH_FXP_REMOVE`命令删除文件和`SSH_FXP_RMDIR`删除目录。

监控 SFTP 连接器

您可以使用以下任何一种方法来监控连接器操作的状态。选择满足您需求的方法。

使用连接器 API 查询文件传输请求的状态

要跟踪文件传输操作的进度，您可以使用 ListFileTransferResultsAPI 操作，该操作会返回有关在特定文件传输操作中传输的每个文件状态的实时更新和详细信息。您可以通过提供其连接器 ID 和传输 ID 来指定文件传输。以下示例返回连接器 ID a-11112222333344444 和传输 aa1b2c3d4-5678-90ab-cdef-EXAMPLE11111 ID 的文件列表。

```
aws transfer list-file-transfer-results --connector-id a-11112222333344444 --transfer-
id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

> **Note**
>
> 文件传输结果将在您调用 ListFileTransferResults API 操作后 7 天内公布。

您还可以查看使用 SFTP 连接器的文件传输请求的日志和事件。中描述了 Transfer Family 的亚马逊 EventBridge 活动SFTP 连接器事件。有关如何查看 Transfer Famil CloudWatch y 日志条目，请参阅查看 Transfer Family 日志流。

在亚马逊上查看 SFTP 连接器事件 EventBridge

对于 SFTP 连接器执行的每项操作，Transfer Family 都会自动生成事件并将其发送到您的亚马逊 EventBridge 账户中的默认事件总线。这些事件包含有关操作的详细元数据，包括操作状态。您可以在中订阅这些事件 EventBridge，根据操作状态等特定事件条件应用过滤器，并根据状态自动触发下游操作。有关 SFTP 连接器操作生成的事件的详细信息，请参阅SFTP 连接器事件。

在亚马逊上查看 SFTP 连接器日志 CloudWatch

所有 SFTP 连接器操作都会生成详细的日志。 CloudWatch有关 SFTP 连接器生成的日志条目的示例，请参阅SFTP 连接器的日志条目示例。

监控 VPC 出口类型连接器

除了标准服务托管连接器之外，VPC 出口类型连接器还提供其他监控功能和注意事项：

连接器状态监控

VPC_LATTICE 连接器包含其他信息，可帮助您监控配置和运行状态：

- EgressType 字段：显示 VPC VPC_LATTICE 出口类型连接器
- EgressConfig 字段：包含资源配置 ARN 和端口信息

使用 `describe-connector` API 监控连接器状态：

```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

VPC 莱迪思成本监控

VPC 出口类型连接器会产生额外的 VPC 莱迪思费用，您应监控这些费用：

- 资源提供商费用：作为资源提供者，您需要支付0.006/GB的数据处理费用（由VPC Lattice直接计费）
- 资源使用者费用：Trans Amazon fer Family 吸收了 0.01 美元/GB 的资源消耗成本（前 1 PB）
- NAT 网关费用：对于通过 VPC 访问的公共终端节点，可能会收取额外的 NAT 网关和数据传输费用
- T@@ ransfer Family 费用：仍然收取 0.40 美元/GB 的标准数据处理费

通过成本和账单控制台，通过VPC Lattice服务进行筛选，监控VPC Lattice的使用情况和 Amazon 成本。

VPC 连接器的网络监控

监控 VPC 出口类型连接器的网络活动和性能：

- VPC 流日志：启用 VPC 流日志以监控资源网关和 SFTP 服务器之间的网络流量模式
- VPC Lattice 访问日志：VPC Lattice 提供显示 source/destination IP 地址、连接时间和数据传输量的访问日志
- 安全组监控：监控安全组规则和流量模式，确保适当的网络访问控制
- DNS 解析监控：监控服务网络端点的 DNS 解析时间和故障

VPC 莱迪思访问日志条目示例：

```
{
  "eventTimestamp": "2025-01-16T20:59:08.531Z",
  "serviceNetworkArn": "arn:aws:vpc-lattice:us-east-1:123456789012:servicenetwork/
sn-1234567890abcdef0",
  "sourceVpcArn": "arn:aws:ec2:us-east-1:123456789012:vpc/vpc-12345678",
```

```
  "resourceConfigurationArn": "arn:aws:vpc-lattice:us-
east-1:123456789012:resourceconfiguration/rcfg-12345678",
  "protocol": "tcp",
  "sourceIpPort": "10.0.1.100:33760",
  "destinationIpPort": "10.0.2.200:22",
  "gatewayIpPort": "10.0.1.150:1769",
  "resourceIpPort": "10.0.2.200:22"
}
```

通过监控进行故障排除

使用监控数据对常见的 VPC 连接器问题进行故障排除：

- 待处理状态：监控 DNS 解析进度，等待激活状态后再尝试传输
- 连接超时：查看 VPC 流日志和安全组规则中是否存在端口 22 上被封锁的流量
- 传输失败：查看 CloudWatch 日志以获取详细的错误消息，查看VPC Lattice访问日志以了解网络级别的问题
- 性能问题：监控 VPC Lattice 访问日志，了解连接时间和吞吐量指标

管理 SFTP 连接器

本主题介绍如何查看和更新 SFTP 连接器。

> **Note**
>
> 系统会自动为每个连接器分配静态 IP 地址，这些地址在连接器的生命周期内保持不变。这允许您连接仅接受来自已知 IP 地址的入站连接的远程 SFTP 服务器。您的连接器会分配一组静态 IP 地址，这些地址由您 Amazon Web Services 账户中使用相同协议（SFTP 或 AS2）的所有连接器共享。
>
> 对于启用 vpc_lattice 的连接器，远程 SFTP 服务器将看到来自您的 VPC CIDR 范围的 IP 地址，而不是服务管理的 IP 地址。 Amazon Transfer Family

更新 SFTP 连接器

要更改连接器的现有参数值，可以运行 `update-connector` 命令。以下命令将区域 *region-id* 中连接器 *connector-id* 的密钥更新为 *secret-ARN*。要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。

```
aws transfer update-connector --sftp-config '{"UserSecretId":"secret-ARN"}' \
   --connector-id connector-id --region region-id
```

更新 VPC 连接设置

您可以更新现有连接器的 VPC 连接设置，包括在服务管理和 VPC 出口类型之间切换或更改资源配置 ARN。

要将连接器从服务托管切换到 VPC 出口，请执行以下操作：

```
aws transfer update-connector \
   --connector-id connector-id \
   --egress-type VPC \
   --egress-config ResourceConfigurationArn=resource-configuration-arn
```

要更新启用 vpc_lattice 的连接器的资源配置 ARN，请执行以下操作：

```
aws transfer update-connector \
   --connector-id connector-id \
   --egress-config ResourceConfigurationArn=new-resource-configuration-arn
```

> **Note**
>
> 更新 VPC 连接设置时，在重新配置PENDING过程中，连接器状态将更改为。使用describe-connector命令监控连接器状态。

查看 SFTP 连接器详细信息

您可以在 Amazon Transfer Family 控制台中找到 SFTP 连接器的详细信息和属性列表。

要查看连接器详细信息

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在左侧导航窗格中，选择连接器。
3. 在“连接器 ID”列中选择标识符以查看所选连接器的详细信息页面。

您可以通过在连接器详细信息页面上选择编辑来更改 SFTP 连接器的属性。

监控 VPC 连接器状态

启用 vpc_Lattice 的连接器包括其他状态信息，可帮助您监控配置过程：

- 状态：节目PENDINGACTIVE、或 ERRORED
- EgressType: 节目VPC或 SERVICE_MANAGED
- EgressConfig: 包含 VPC 连接器的资源配置 ARN
- 错误：如果连接器ERRORED处于状态，则提供详细的错误信息

对于 VPC 连接器，该ServiceManagedEgressIpAddresses字段将为空，因为流量会改用您的 VPC IP 地址。

> **Note**
>
> 你可以通过运行以下 Amazon Command Line Interface (Amazon CLI) 命令来获取其中的大部分信息，尽管格式不同。要使用此示例命令，请将 *user input placeholders* 替换为您自己的信息。
>
> ```
> aws transfer describe-connector --connector-id your-connector-id
> ```
>
> 有关更多信息，请参阅《 API 参考》中的 DescribeConnector。

SFTP 连接器的扩展和配额

主题

- SFTP 连接器配额
- 扩展您的 SFTP 连接器

SFTP 连接器配额

SFTP 连接器有以下配额。

> **Note**
>
> SFTP 连接器的更多服务配额列在Amazon Transfer Family 终端节点和配额中。Amazon Web Services 一般参考

SFTP 连接器配额

Name	默认值	可调整
每秒最大测试连接事务数 (TPS)	每账户每秒 1 个请求	否
待处理文件传输的最大队列大小	1000	否
最大文件大小	150 千兆字节 (GiB)	否
每个文件的最大传输时间	12 小时	否
每个文件的最大请求等待时间	12 小时	否
每个账户的连接器的最大带宽（SFTP 和 AS2连接器均构成此值）	50 MBps	不可以
目录列出操作的最大项目数	10000	否
每次`StartFileTransfer` 请求的最大文件数	10	否
每秒`StartDirectoryListing` 请求的最大事务数	3	是

> **Note**
>
> 默认情况下，SFTP 连接器一次处理一个文件，按顺序传输文件。您可以选择让连接器与支持来自同一用户的并发会话的远程服务器创建并行会话，并行处理最多 5 个文件，从而提高传输性能。

要为任何连接器启用并发连接，可以在创建或更新连接器时编辑 “最大并发连接数” 设置。有关更多信息，请参阅 使用服务管理的出口创建一个 SFTP 连接器。

为了存储 SFTP 连接器的凭证，每个 Secrets Manager 密钥都有与之关联的配额。如果您出于多种目的使用同一个密钥来存储多种类型的密钥，则可能会遇到这些配额。

- 单个密钥的总长度：12,000 个字符
- **`Password`**字符串的最大长度：1024 个字符
- **`PrivateKey`**字符串的最大长度：8192 个字符
- **`Username`**字符串的最大长度：100 个字符

扩展您的 SFTP 连接器

本节介绍如何扩展 Amazon Transfer Family SFTP 连接器工作负载的注意事项。当你想使用 SFTP 连接器扩展工作负载时，你需要考虑以下三个配额。

- 最大队列大小。这是指连接器队列中已请求的最大待处理操作数。待处理操作是指之前提交的任何尚未完成的转移请求，无论成功还是失败。

  待处理请求的最大队列深度目前设置为每个连接器 1,000（如Amazon Transfer Family 服务配额中所定义）。当您在短时间内请求数千次传输操作时，您的工作负载可能会超过此服务限制，并且您将收到一条`ThrottlingException`消息，消息显示已超出最大待处理请求数。如果您的工作负载受此配额限制，请通过联系Transfer Family服务团队 Amazon Web Services 支持 或您的客户团队，讨论您的可扩展性要求。

  您也可以采取以下任一或两项操作。

  - 将您的文件卷分发到多个连接器上。
  - 让您的连接器与远程服务器创建并行会话，以并行处理来自队列的多个请求。
- 并发会话数。默认情况下，SFTP 连接器一次传输一个文件，按顺序从其队列中传输文件。

  您可以选择让连接器并行传输多个文件，从而提高传输性能。您可以与支持来自同一用户的并发会话的远程服务器创建并行会话，并行处理最多 5 个文件。创建 SFTP 连接器时，请在创建或更新连接器时为 “最大并发连接数” 设置选择一个不超过 5 的值。有关更多信息，请参阅 使用服务管理的出口创建一个 SFTP 连接器。
- **`StartFileTransfer`**请求的速率。每个 SFTP 连接器最多可以请求每秒 100 个文件路径进行传输。请求的文件路径将添加到您的连接器队列中进行处理。无论单个`StartFileTransfer`命令中

提供的文件数量如何，您都可以递归地使用该`StartFileTransfer`命令为每个连接器请求每秒 100 个文件路径。

使用 SFTP 连接器的参考架构

本节列出了可用于使用 SFTP 连接器配置自动文件传输工作流程的参考资料。您可以使用 Amazon 中的 SFTP 连接器事件设计自己的事件驱动架构 EventBridge，在文件传输操作与中的预处理和后处理操作之间进行协调。 Amazon

博客文章

以下博客文章提供了使用 SFTP 连接器构建 MFT 工作流程的参考架构，包括在使用 SFTP 连接器将文件发送到远程 SFTP 服务器之前使用 PGP 加密文件：使用 SFTP 连接器和 PGP 加密架构安全且合规的托管文件传输。 Amazon Transfer Family

研讨会

- 以下研讨会提供了配置 SFTP 连接器以及使用连接器从远程 SFTP 服务器发送或检索文件的动手实验：Transfer F amily-S FTP 研讨会。
- 以下研讨会提供动手实验来构建全自动和事件驱动的工作流程，包括将文件传输到外部 SFTP 服务器或从外部 SFTP 服务器传输到 Amazon S3，以及这些文件的常见预处理和后处理：事件驱动的 MFT 研讨会。

  该视频提供了本次研讨会的详细介绍。

Solutions

Amazon Transfer Family 提供了以下解决方案：

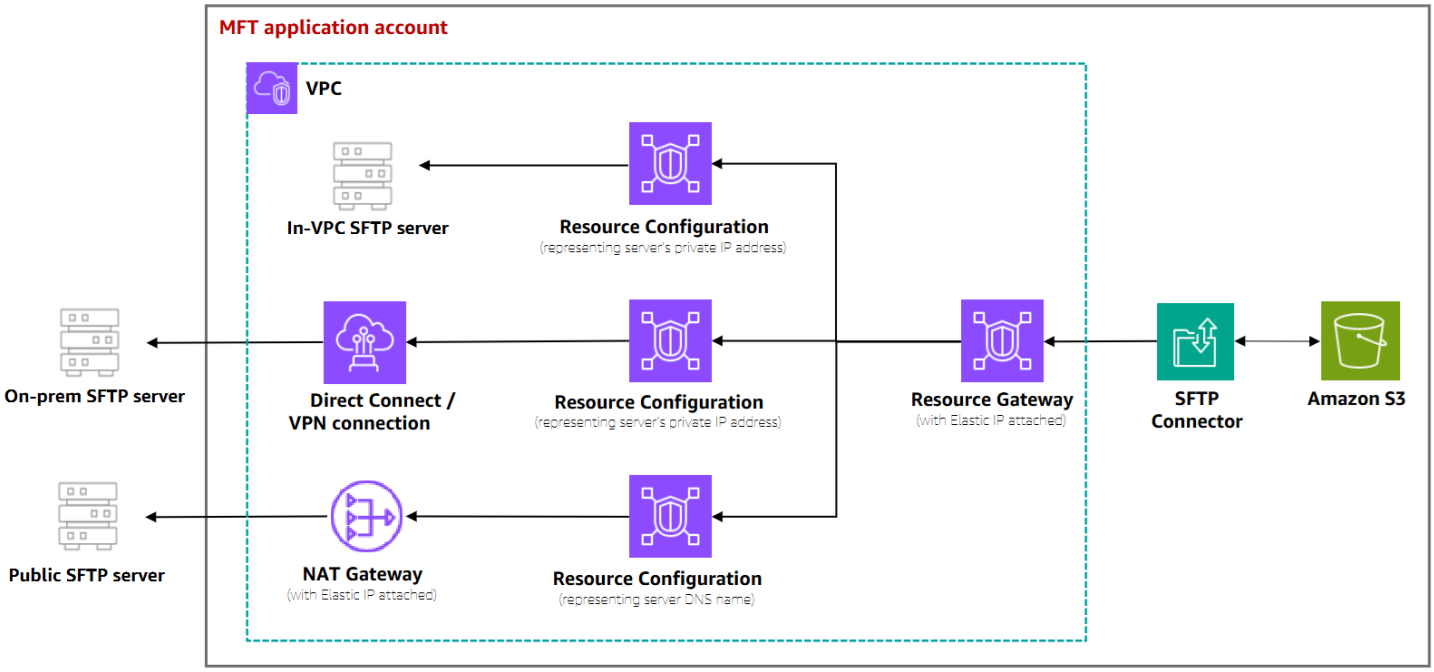
- 文件传输同步解决方案提供了一个参考架构，可以自动使用 SFTP 连接器将远程 SFTP 目录（包括整个文件夹结构）与本地 Amazon S3 存储桶同步。它协调列出远程目录、检测更改以及传输新文件或修改文件的过程。
- S@@ erverlessland-远程 SFTP 服务器和 S3 之间的选择性文件传输；使用 Amazon Transfer Family提供了列出存储在远程 SFTP 位置的文件以及将选择性文件传输到 Amazon S3 的示例模式。

VPC 参考架构

以下参考架构显示了部署启用 vpc_Lattice 的 SFTP 连接器的常见模式。这些示例可帮助您了解在整体 Amazon 架构中需要在何处创建 VPC Lattice 资源。

具有共享出口基础设施的单一账户

在此架构中，出口基础设施（NAT 网关、VPN 隧道或 Direct Connect）是在与您的 SFTP 连接器相同的账户内的 VPC 中配置的。所有连接器都可以共享同一个资源网关和 NAT 网关。

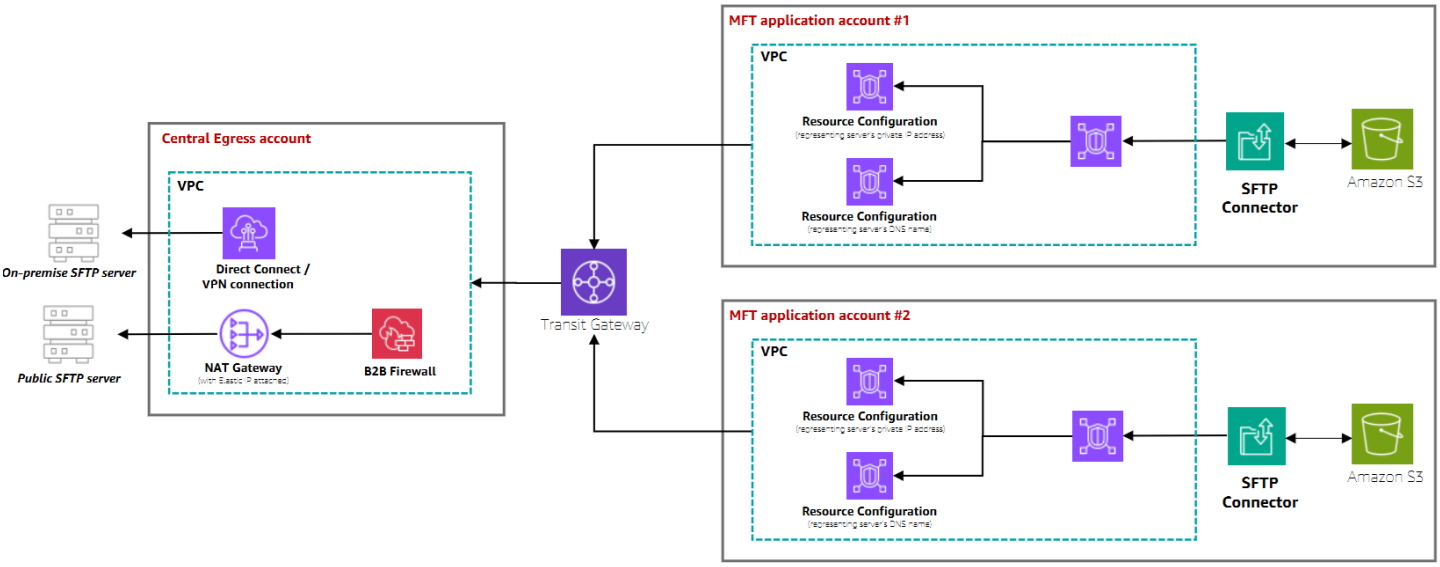


在以下情况下，此模式最为理想：

- 所有 SFTP 连接器都在一个连接器中进行管理 Amazon Web Services 账户
- 出口基础设施是在 VPC 中设置的，账户与 SFTP 连接器相同

具有集中式出口基础设施的跨账户

在此架构中，出口基础设施（NAT 网关、VPN 隧道、Direct Connect 或 B2B 防火墙）是在网络团队管理的中央出口账户中配置的。SFTP 连接器是在 MFT 管理员团队管理的 MFT 应用程序帐户中创建的。跨账户联网是使用 Transit Gateway 建立的，以遵守现有的联网规则。



在以下情况下，此模式最为理想：

- 网络基础设施由一个单独的团队通过一个专门的账户进行管理
- 在创建 SFTP 连接器的账户和设置 Egress 基础设施的账户之间，您已有路由（例如 Amazon Transit Gateway ）。SFTP 连接器将能够利用连接这两个账户的现有路由。
- 需要集中式安全控制和 B2B 防火墙
- 您需要保持网络团队和应用团队之间的职责分离

Amazon Transfer Family 对于 AS2

适用性声明 2 (AS2) 是 RFC 定义的文件传输规范，其中包括强大的消息保护和验证机制。保护传输中的有效 AS2 载荷使用带有加密和数字签名的加密消息语法 (CMS) 来提供数据保护和对等身份验证。已签名的消息处置通知（MDN）响应有效负载提供消息已接收并成功解密的验证（不可否认性）。

该 AS2 协议对于具有合规性要求的工作流程至关重要，这些工作流程依赖于在协议中内置数据保护和安全功能。 Amazon Transfer Family AS2 端点已通过 Drummond 认证，使零售、生命科学、制造业、金融服务和公用事业等行业的客户能够安全地与其业务合作伙伴进行交易。

当你 AS2 与 Transfer Family 一起使用时，可以在以下版本中 Amazon 本地访问已处理的数据：

- 处理、分析和机器学习
- 与企业资源规划 (ERP) 系统集成
- 与客户关系管理 (CRM) 系统集成

要与具有 AS2启用服务器的合作伙伴交换文件，您必须：

- 生成用于加密的公私密钥 pair
- 生成用于签名的公私密钥 pair
- 与您的伴侣交换公钥

> **Important**
>
> 目前不支持 HTTPS AS2 服务器端点。您应对终止 TLS 负责。

Transfer Family 提供了一个你可以参加的研讨会，在研讨会中，你可以将 Transfer Family 端点配置为 AS2 已启用，也可以配置 Transfer Famil AS2 y 连接器。您可以在此处查看本次研讨会的详细信息。

有关在 Transfer Family AS2 中进行配置的 step-by-step说明，请参阅以下内容：

1. 导入 AS2 证书
2. 创建 AS2 个人资料
3. 创建 AS2 服务器

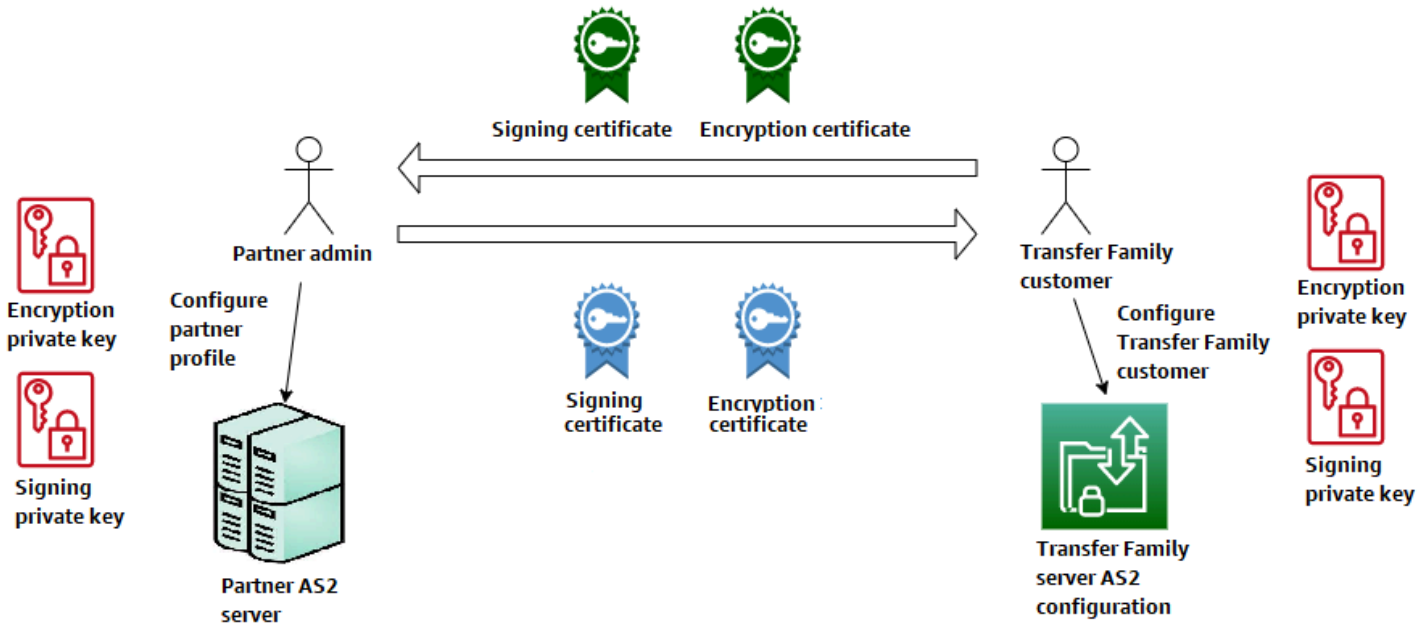
4. 创建 AS2 协议
5. 配置 AS2 连接器

有关完整示例，请参阅设置 AS2 配置。

> **Note**
>
> 要显示对 AS2 Terraform 模板的支持，请在 Transfer Family Ter raf orm 模板功能请求中添加竖起大拇指的反应 (#)。您也可以添加评论来描述您的用例。

AS2 用例

如果您是想要与具有 AS2启用服务器的合作伙伴交换文件的 Amazon Transfer Family 客户，则设置中最复杂的部分涉及生成一个用于加密的公私密钥对，另一个用于与合作伙伴签署和交换公钥。



Amazon Transfer Family 与一起使用时，请考虑以下变体 AS2。

> **Note**
>
> 贸易伙伴是与该合作伙伴资料关联的合作伙伴。
> 下表中所有提及 MDN 的内容均假定已签名 MDNs。

AS2 用例

仅限入站的使用案例

- 将加密的 AS2 消息从交易伙伴传输到 Transfer Family 服务器。

  在此情况下，您可以执行以下操作：

  1. 为您的贸易伙伴和您自己创建档案。
  2. 创建使用该 AS2协议的 Transfer Family 服务器。
  3. 创建协议并将其添加到您的服务器。
  4. 导入带有私钥的证书并将其添加到您的个人资料中，然后将公钥导入您的合作伙伴资料进行加密。
  5. 拿到这些物品后，将证书的公有密钥发送给您的交易伙伴。

  现在，您的合作伙伴可以向您发送加密消息，您可以将其解密并存储在您的 Amazon S3 存储桶中。
- 将加密的 AS2 消息从交易伙伴传输到 Transfer Family 服务器并添加签名。

  在这种情况下，您仍然只进行入站传输，但现在您希望让您的合作伙伴签署他们发送的消息。在这种情况下，请导入贸易伙伴的签名公钥（作为添加到合作伙伴资料中的签名证书）。
- 将加密的 AS2 消息从交易伙伴传输到 Transfer Family 服务器，然后添加签名和发送 MDN 响应。

  在这种情况下，您仍然只进行入站传输，但是现在，除了接收已签名的有效负载外，您的交易伙伴还希望接收签名的 MDN 响应。

  1. 导入您的公有和私有签名密钥（作为签名证书导入您的配置文件中）。
  2. 将公开签名密钥发送给您的贸易伙伴。

仅限出站的使用案例

- 将加密的 AS2 消息从 Transfer Family 服务器传输给交易伙伴。

  这种情况与仅限入站传输的用例类似，不同之处在于您无需向 AS2服务器添加协议，而是创建连接器。在这种情况下，您可以将贸易伙伴的公钥导入他们的个人资料中。
- 将加密的 AS2 消息从 Transfer Family 服务器传输给贸易伙伴并添加签名。

  您仍然只进行出站转账，但现在您的贸易伙伴希望您在发送给他们的消息上签名。

1. 导入您的签名私有密钥（作为签名证书添加至您的配置文件中）。
2. 将您的公钥发送给您的贸易伙伴。

- 将加密的 AS2 消息从 Transfer Family 服务器传输到交易伙伴，然后添加签名并发送 MDN 响应。

  您仍然只能进行出站转账，但是现在，除了发送已签名的有效载荷外，您还希望收到贸易伙伴签名的 MDN 响应。

  1. 您的贸易伙伴向您发送他们的公开签名密钥。
  2. 导入您的贸易伙伴的公钥（作为添加到您的合作伙伴资料中的签名证书）。

入站和出站使用案例

- 在 Transfer Family 服务器和交易伙伴之间双向传输加密 AS2 消息。

  在此情况下，您可以执行以下操作：

  1. 为您的贸易伙伴和您自己创建档案。
  2. 创建使用该 AS2协议的 Transfer Family 服务器。
  3. 创建协议并将其添加到您的服务器。
  4. 创建连接器。
  5. 导入带有私钥的证书并将其添加到您的个人资料中，然后将公钥导入您的合作伙伴资料进行加密。
  6. 从您的贸易伙伴那里接收公钥并将其添加到他们的个人资料中进行加密。
  7. 拿到这些物品后，将证书的公有密钥发送给您的交易伙伴。

  现在，您和您的交易伙伴可以交换加密消息，并且双方都可以对其进行解密。您可以将接收的消息存储在 Amazon S3 存储桶中，且您的合作伙伴可以解密和存储您发送给他们的消息。
- 在 Transfer Family 服务器和贸易伙伴之间双向传输加密 AS2 消息并添加签名。

  现在您和您的合作伙伴想要签名消息。

  1. 导入您的签名私有密钥（作为签名证书添加至您的配置文件中）。
  2. 将您的公钥发送给您的贸易伙伴。
  3. 导入贸易伙伴的签名公钥并将其添加到他们的个人资料中。
- 在 Transfer Family 服务器和交易伙伴之间双向传输加密 AS2 消息，添加签名并发送 MDN 响应。

  现在，您想交换签名的有效负载，并且您和您的交易伙伴都想要 MDN 响应。

  1. 您的贸易伙伴向您发送他们的公开签名密钥。
  2. 导入贸易伙伴的公钥（作为合作伙伴资料的签名证书）。
  3. 将您的公钥发送给您的贸易伙伴。

AS2 CloudFormation 模板

本主题提供有关 Amazon CloudFormation 模板的信息，您可以使用这些模板来快速部署 AS2 服务器和配置 Amazon Transfer Family。这些模板可以自动执行设置过程，并帮助您实施 AS2 文件传输的最佳实践。

- 有关基本 AS2 模板的描述，请参见 使用模板创建演示 Transfer Family AS2 堆栈
- 中描述了用于自定义 HTTP 标头的 AS2 为 AS2 消息自定义 HTTP 标头模板。

自定义模板 AS2

您可以自定义提供的模板以满足您的特定要求：

1. 从 S3 网址下载模板。
2. 修改 YAML 代码以调整配置，例如：
   - 安全设置和证书配置
   - 网络架构和 VPC 设置
   - 存储选项和文件处理
   - 监控和通知首选项
3. 将修改后的模板上传到自己的 S3 存储桶。
4. 使用 Amazon CloudFormation 控制台部署自定义模板或 Amazon CLI。

> **Important**
>
> 自定义模板时，请确保保持资源之间的依赖关系并遵循安全最佳实践。

测试您的 AS2 部署

使用模板部署 AS2 服务器后，您可以测试配置：

1. 查看 CloudFormation 堆栈输出以获取示例命令和端点信息。
2. 使用 Amazon CLI 发送测试文件：

```
aws s3api put-object --bucket your-bucket-name --key test.txt --body test.txt
```

```
aws transfer start-file-transfer --connector-id your-connector-id --send-file-
paths /your-bucket-name/test.txt
```

3. 验证目标 S3 存储桶中的文件传输。
4. 检查 CloudWatch 日志是否成功处理和 MDN 响应。

要进行更全面的测试，可以考虑使用第三方 AS2 客户端将文件发送到您的 Transfer Famil AS2 y 服务器。

AS2 模板部署的最佳实践

使用 AS2 CloudFormation 模板时，请遵循以下最佳实践：

安全性

- 使用强证书并定期轮换。
- 实施最低权限的 IAM 策略。
- 使用安全组限制网络访问。

可靠性

- 跨多个可用区部署。
- 对失败的传输实施监控和警报。
- 为失败的传输设置自动重试。

性能

- 为您的传输量选择合适的实例类型。
- 实施 S3 生命周期策略以实现高效的文件管理。
- 监控和优化网络配置。

成本优化

- 对可变的工作负载使用自动缩放。
- 为较旧的文件实现 S3 存储类别。

根据实际使用情况监控和调整资源。

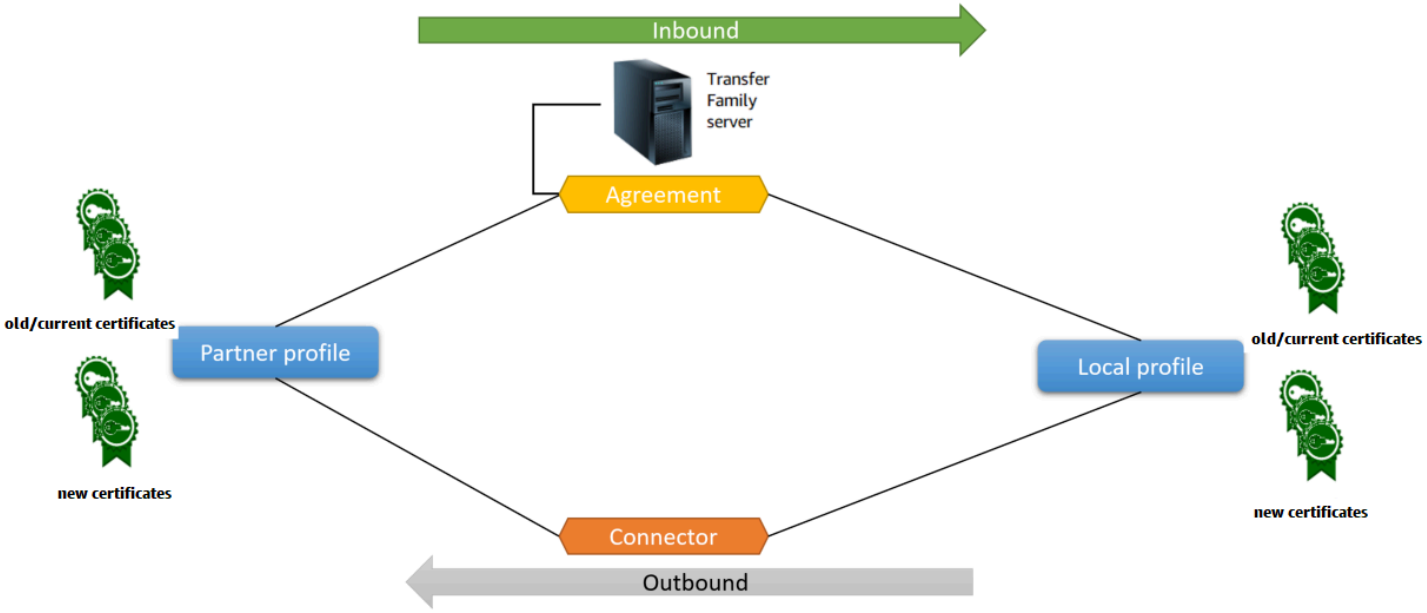
正在配置 AS2

要创建 AS2启用了的服务器，还必须指定以下组件：

- 协议 — 双边贸易伙伴协议或伙伴关系，定义交换消息（文件）的双方之间的关系。为了定义协议，Transfer Family 结合了服务器、本地配置文件、合作伙伴配置文件和证书信息。Tran AS2 sfer Family 入站流程使用协议。
- 证书-公钥 (X.509) 证书用于 AS2 通信以进行消息加密和验证。证书也用于连接器端点。
- 本地档案和合作伙伴档案 — 本地资料定义本地（AS2已启用 Transfer Family 服务器）组织或 “派对”。同样，合作伙伴配置文件定义了 Transfer Family 外部的远程合作伙伴组织。

虽然并非所有 AS2启用了连接器的服务器都需要连接器，但对于出站传输，则需要连接器。连接器捕获出站连接的参数。要将文件发送到客户的外部非 Amazon 服务器，则需要使用连接器。

下图显示了入站和出站流程中涉及的 AS2 对象之间的关系。



有关 AS2 配置示 end-to-end例，请参阅设置 AS2 配置。

主题

- AS2 配置
- AS2 配额和限制

- AS2 特性和功能

AS2 配置

本主题介绍使用适用性声明 2 (AS2) 协议的传输支持的配置、特性和功能，包括接受的密码和摘要。

签名、加密、压缩、MDN

对于入站和出站传输，以下项目为必需或可选项目：

- 加密 - 必需（对于 HTTP 传输，这是目前唯一支持的传输方法）。只有通过终止 TLS 的代理（例如应用程序负载均衡器(ALB)）转发且 `X-Forwarded-Proto: https` 标头存在的情况下，才会接受未加密的消息。
- 签名 - 可选
- 压缩 - 可选（目前唯一支持的压缩算法是 ZLIB）
- 邮件处置通知 (MDN) - 可选

密码

入站和出站传输均支持以下密码：

- AES128_CBC
- AES192_CBC
- AES256_CBC
- 3DES（仅用于向后兼容）

摘要

支持以下摘要：

- 入站签名和 MDN — SHA1、、 SHA256、 SHA384 SHA512
- 出站签名和 MDN — SHA1、、 SHA256、 SHA384 SHA512

MDN

对于 MDN 响应，支持某些类型，如下所示：

- 入站传输 - 同步和异步
- 出站传输 - 仅限同步
- 简单邮件传输协议（SMTP）（电子邮件 MDN）– 不支持

Transports

- 入站传输 – HTTP 是目前唯一支持的传输，您必须明确指定。

> **Note**
>
> 如果您需要使用 HTTPS 进行入站传输，则可以在应用程序负载均衡器或网络负载均衡器上终止 TLS。通过 HTTPS 接收 AS2 消息中对此进行了描述。

- 出站传输 - 如果您提供 HTTP URL，则还必须指定加密算法。如果您提供 HTTPS URL，则可以选择为加密算法指定 NONE。

AS2 配额和限制

本节讨论配额和限制 AS2

主题

- AS2 配额
- 处理密钥的限额
- 已知限制条件

AS2 配额

AS2 文件传输有以下配额。要申请增加可调整的限额，请参阅 Amazon Web Services 一般参考 中的 Amazon Web Services 服务 限额。

AS2 配额

名称	默认值	可调整
每秒接收的最大入站文件数	100	否
每秒发送的最大出站文件数	100	否

名称	默认值	可调整
并发入站文件的最大数量	400	否
并发出站文件的最大数量	400	否
入站文件的最大大小（未压缩）	1 GB	否
出站文件的最大大小（未压缩）	1 GB	否
每个出站请求的最大文件数	10	否
每秒最大出站请求数	100	否
每秒最大入站请求数	100	否
每个账户的最大出站带宽（出站 SFTP 和 AS2请求均构成此值）	每秒 50 MB	否
每个账户的最大协议数量	100	是
每个账户的最大连接器数量（SFTP 和 AS2 连接器均构成此限制）	100	是
每个合作伙伴资料的最大证书数量	10	否
每个账户的最大证书数	1000	是
每个账户的最大合作伙伴配置文件数	1000	是

处理密钥的限额

Amazon Transfer Family Amazon Secrets Manager 代表使用基本身份验证的 AS2 客户拨打电话。此外，Secrets Manager 还会拨打电话 Amazon KMS。

> **Note**
>
> 这些配额并不特定于你对 Transfer Family 的密钥的使用：它们是在你的所有服务之间共享的 Amazon Web Services 账户。

对于 Secrets Manager`GetSecretValue`，适用的配额是组合速率 DescribeSecret 和 GetSecretValue API 请求，如Amazon Secrets Manager 配额中所述。

Secrets Manager **`GetSecretValue`**

名称	值	说明
和 GetSecretValue API 请求 DescribeSecret 的合并速率	每个受支持的区域：每秒 1 万个	`DescribeSecret` 和 `GetSecretValue` API 操作的每秒最大事务总和。

对于 Amazon KMS，以下配额适用`Decrypt`。有关详细信息，请参阅每个 Amazon KMS API 操作的请求配额

Amazon KMS **`Decrypt`**

限额名称	默认值（每秒请求数）

加密操作（对称）请求速率	这些共享配额因请求中使用的 Amazon KMS 密钥类型 Amazon Web Services 区域 和密钥类型而异。每个配额都单独计算。
	• 5500（共享）
	• 在以下区域中为 10000（共享）：
	  • 美国东部（俄亥俄），us-east-2
	  • 亚太地区（新加坡），ap-southeast-1
	  • 亚太区域（悉尼），ap-southeast-2
	  • 亚太区域（东京），ap-northeast-1
	  • 欧洲（法兰克福），eu-central-1
	  • 欧洲（伦敦），eu-west-2
	• 在以下区域中为 50000（共享）：

限额名称	默认值（每秒请求数）
	• 美国东部（弗吉尼亚北部），us-east-1 • 美国西部（俄勒冈），us-west-2 • 欧洲（爱尔兰），eu-west-1
自定义密钥存储请求限额 Note 此限额仅适用于使用外部密钥存储的情况。	自定义密钥存储请求限额是针对每个自定义密钥存储单独计算的。 • 每个 Amazon CloudHSM 密钥库有 1,800（共享） • 每个外部密钥存储 1800 次（共享）

已知限制条件

- 不支持服务器端 TCP 保持活动状态。除非客户端发送保持活动状态的数据包，否则连接将在处于非活动状态 350 秒后超时。
- 要使有效协议被服务接受并显示在 Amazon CloudWatch 日志中，消息必须包含有效的 AS2 标头。
- 从 Amazon Transfer Family for 接收消息的服务器 AS2 必须支持 R FC 6211 中定义的用于验证消息签名的加密消息语法 (CMS) 算法保护属性。某些较早的 IBM Sterling 产品不支持此属性。
- 重复的消息 IDs 会导致已处理/警告：重复的文档消息。
- AS2 证书的密钥长度必须至少为 2048 位，最多为 4096 位。
- MDNs 向贸易伙伴的 HTTPS 终端节点发送 AS2 消息或异步消息时，消息或 MDNs 必须使用由公开信任的证书颁发机构 (CA) 签署的有效 SSL 证书。目前仅支持出站传输自签名证书。
- 端点必须支持 TLS 版本 1.2 协议和安全策略允许的加密算法（如 Amazon Transfer Family 服务器的安全策略 中所述）。
- 目前不支持 AS2 版本 1.2 中的多个附件和证书交换消息 (CEM)。
- 基本身份验证目前仅支持出站消息。
- 您可以将文件处理工作流程附加到使用该 AS2 协议的 Transfer Family 服务器：但是， AS2 消息不会执行附加到服务器的工作流程。

AS2 特性和功能

下表列出了使用的 Transfer Family 资源可用的特性和功能 AS2。

AS2 features

Transfer Family 为以下用户提供以下功能 AS2。

功能	由... 支持 Amazon Transfer Family
德拉蒙德认证	是
Amazon CloudFormation 支持	是
亚马逊 CloudWatch指标	是
SHA-2 加密算法	是
对亚马逊 S3 的支持	是
Amazon EFS 支持	否
定时消息	是 [1]
Amazon Transfer Family 托管工作流程	否
证书交换消息 (CEM)	否
双向 TLS (mTLS)	否
Support 支持自签名证书	是

1. 通过使用 Amazon 的计划 Amazon Lambda 功能提供出站预设消息 EventBridge

AS2 发送和接收功能

下表列出了 Amazon Transfer Family AS2 发送和接收功能。

能力	入站：通过服务器接收	出站：使用连接器发送
TLS 加密传输 (HTTPS)	是 [1]	是
非 TLS 传输 (HTTP)	是	是 [2]
同步 MDN	支持	是

能力	入站：通过服务器接收	出站：使用连接器发送
消息压缩	支持	是
异步 MDN	是	否
静态 IP 地址	支持	是
自带 IP 地址	是	否
多个文件附件	否	否
基本身份验证	否	是
AS2 重启	不适用	否
AS2 可靠性	否	否
每封邮件的自定义主题	不适用	否

1. Network Load Balancer (NLB) 或应用程序负载均衡器 (ALB) 提供入站 TLS 加密传输

2. 只有启用加密后，出站非 TLS 传输才可用

管理 AS2 证书

本主题讨论如何导入和管理 AS2 证书。导入证书是 Transfer Family AS2 流程的第一步。

1. 导入证书
2. 创建 AS2 个人资料
3. 创建 AS2 服务器
4. 创建 AS2 协议
5. 配置 AS2 连接器

导入 AS2 证书

Transf AS2 er Family 流程使用证书密钥对传输的信息进行加密和签名。合作伙伴可以为两个目的使用相同的密钥，也可以为每个目的使用单独的密钥。如果您的通用加密密钥由受信任的第三方托管，以便

在发生灾难或安全漏洞时可以对数据进行解密，我们建议您使用单独的签名密钥。通过使用单独的签名密钥（您不托管），您不会损害数字签名的不可否认性功能。

> **Note**
>
> AS2 证书的密钥长度必须至少为 2048 位，最多为 4096 位。

以下几点详细说明了在此过程中如何使用 AS2 证书。

- 入境 AS2
  - 交易伙伴发送签名证书的公有密钥，该密钥将导入至合作伙伴配置文件中。
  - 本地方发送用于其加密和签名证书的公有密钥。然后，合作伙伴导入一个或多个私有密钥。本地方可以发送单独的证书密钥进行签名和加密，也可以选择将相同的密钥用于两种用途。
- 出境 AS2
  - 合作伙伴发送其加密证书的公有密钥，该密钥将导入至合作伙伴配置文件中。
  - 本地方发送证书的公有密钥进行签名，并导入证书的私有密钥进行签名。
  - 如果您使用的是 HTTPS，则可以导入自签名的传输层安全 (TLS) 证书。

有关如何创建证书的详细信息，请参阅 the section called “步骤 1：为创建证书 AS2”。

此步骤说明了如何使用 Transfer Family 控制台导入证书。如果要 Amazon CLI 改用，请参阅the section called “第 2 步：将证书作为 Transfer Family 证书资源导入”。

指定 AS2启用了的证书

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在左侧导航窗格的AS2 贸易伙伴下，选择证书。
3. 选择导入证书。
4. 在证书配置部分的证书描述中，输入一个易于识别的证书名称。确保您可以通过其描述来识别证书的用途。此外，选择证书的角色。
5. 在证书使用部分中，选择此证书的用途。它可以用于加密、签名或两者兼而有之。

   提示：如果您为使用选择加密和签名，Transfer Family 会创建两个相同的证书（每个证书都有自己的 ID）：一个使用值为，另一个使用值为SIGNING。ENCRYPTION
6. 在证书内容部分，提供交易伙伴提供的公有证书，或本地证书的公有和私有密钥。

在证书内容部分填写相应的详细信息。

- 如果选择自签名证书，则不提供证书链。
- 将证书文本及其链粘贴到证书和证书链字段中。
- 如果此证书是本地证书，请粘贴其私有密钥。

7. 选择导入证书以完成该流程并保存导入证书的详细信息。

> **Note**
>
> TLS 证书只能作为合作伙伴的公共证书导入。如果您选择合作伙伴提供的公共证书，然后为使用选择传输层安全 (TLS)，则会收到警告。此外，TLS 证书必须是自签名的（也就是说，您必须选择自签名证书才能导入 TLS 证书）。

AS2 证书轮换

通常，证书的有效期为六个月至一年。您可能已经设置想要保留更长时间的配置文件。为此，Transfer Family 提供了证书轮换功能。您可以为一个配置文件指定多个证书，以便您可以连续多年使用该配置文件。Transfer Family 使用证书进行签名（可选）和加密（必填）。如果您愿意，可以为这两个目的指定一个证书。

证书轮换是将即将过期的旧证书替换为较新的证书的过程。过渡是渐进的，以避免协议中的合作伙伴尚未为出站传输配置新证书，或者可能在使用新证书的时期发送使用旧证书签名或加密的有效负载，从而避免中断传输。新旧证书均有效的中间期称为宽限期。

X.509 证书有 `Not Before` 日期和 `Not After` 日期。但是，这些参数可能无法为管理员提供足够的控制。Transfer Family 提供 `Active Date` 和 `Inactive Date` 设置以控制哪些证书用于出站负载，哪些证书被接受用于入站负载。

证书到期监控

Transfer Famil CloudWatch y `DaysUntilExpiry` 在导入证书后会发布亚马逊指标。该指标显示当前日期与证书`InactiveDate`上指定的日期之间的天数。该指标位于 CloudWatch指标控制面板的`Transfer` Amazon 命名空间下。

此指标将始终有一个指标维度 CertificateId，如果客户在证书上提供了描述维度，则可以选择包含描述维度。有关 CloudWatch 指标维度的更多信息，请参阅 CloudWatch API 参考中的维度。

> **Note**
>
> 导入 Transfer Family 证书后，可能需要整整一天的时间才能将该指标发送到客户账户。

您可以使用此指标创建 CloudWatch 警报，在证书即将到期时通知您。

出站证书选择使用转移日期之前的最大值作为 `Inactive Date`。入站流程接受 `Not Before` 和 `Not After` 范围内的证书，以及 `Active Date` 和 `Inactive Date` 范围内的证书。

证书轮换示例

下表描述了为单个配置文件配置两个证书的一种可能方法。

两个证书轮换

Name	NOT BEFORE（由证书颁发机构控制）	ACTIVE DATE（由 Transfer Family 设置）	INACTIVE DATE（由 Transfer Family 设置）	NOT AFTER（由证书颁发机构设置）
证书 1（旧证书）	2019-11-01	2020-01-01	2020-12-31	2024-01-01
证书 2（新证书）	2020-11-01	2020-06-01	2021-06-01	2025-01-01

注意以下几点：

- 为证书指定 `Active Date` 和 `Inactive Date` 时，该范围必须介于 `Not Before` 和 `Not After` 之间。
- 我们建议您为每个配置文件配置多个证书，确保所有证书的有效日期范围涵盖您要使用该配置文件的时间。
- 我们建议您在旧证书变为非活动状态和新证书处于活动状态之间指定一段宽限时间。在前面的示例中，第一个证书直到 2020 年 12 月 31 才处于非活动状态，而第二个证书在 2020 年 6 月 1 日生效，提供了 6 个月的宽限期。在 2020 年 6 月 1 日至 2020 年 12 月 31 日期间，两个证书均处于活动状态。

创建 AS2 个人资料

本主题讨论如何创建用于 AS2 流程的配置文件。本地配置文件定义本地（AS2已启用 Transfer Family 服务器）组织或 “派对”。同样，合作伙伴配置文件定义了 Transfer Family 外部的远程合作伙伴组织。

1. 导入 AS2 证书
2. 创建 AS2 个人资料
3. 创建 AS2 服务器
4. 创建 AS2 协议
5. 配置 AS2 连接器

使用此步骤创建本地和合作伙伴配置文件。此过程说明了如何使用 Transfer Family 控制台创建 AS2 配置文件。如果要改用 Amazon CLI ，请参阅 the section called “第 3 步：为您和您的贸易伙伴创建档案”。

创建个人 AS2 资料

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在左侧导航窗格的 “AS2 贸易伙伴” 下，选择个人资料，然后选择创建个人资料。
3. 在配置文件配置部分，输入配置文件的 AS2 ID。此值用于 AS2 特定于协议的 HTTP 标头，`as2-from`并`as2-to`用于标识交易伙伴关系，后者决定要使用的证书，依此类推。
4. 在配置文件类型部分，选择本地配置文件或合作伙伴配置文件。
5. 在证书部分，从下拉菜单中选择一个或多个证书。

   提示：如果要导入未在下拉菜单中列出的证书，请选择导入新证书。这将在导入证书屏幕上打开一个新的浏览器窗口。有关导入证书的步骤，请参阅导入 AS2 证书。
6. （可选）在标签部分中，指定一个或多个键值对以帮助标识此配置文件。
7. 选择创建配置文件以完成该流程并保存新的配置文件。

创建 AS2 服务器

本主题提供使用控制台或 Amazon CloudFormation 模板创建 AS2启用的 Transfer Family 服务器的说明。有关 AS2 配置示 end-to-end例，请参阅设置 AS2 配置。创建 AS2 服务器后，可以向服务器添加协议。

1. 导入 AS2 证书
2. 创建 AS2 个人资料
3. 创建 AS2 服务器
4. 创建 AS2 协议
5. 配置 AS2 连接器

主题

- 使用 Tran AS2 sfer Family 控制台创建服务器
- 使用模板创建演示 Transfer Family AS2 堆栈
- 创建 AS2 协议

使用 Tran AS2 sfer Family 控制台创建服务器

此过程说明了如何使用 Transfer AS2 Family 控制台创建支持该功能的服务器。如果要 Amazon CLI 改用，请参阅the section called “步骤 4：创建使用该 AS2协议的 Transfer Family 服务器”。

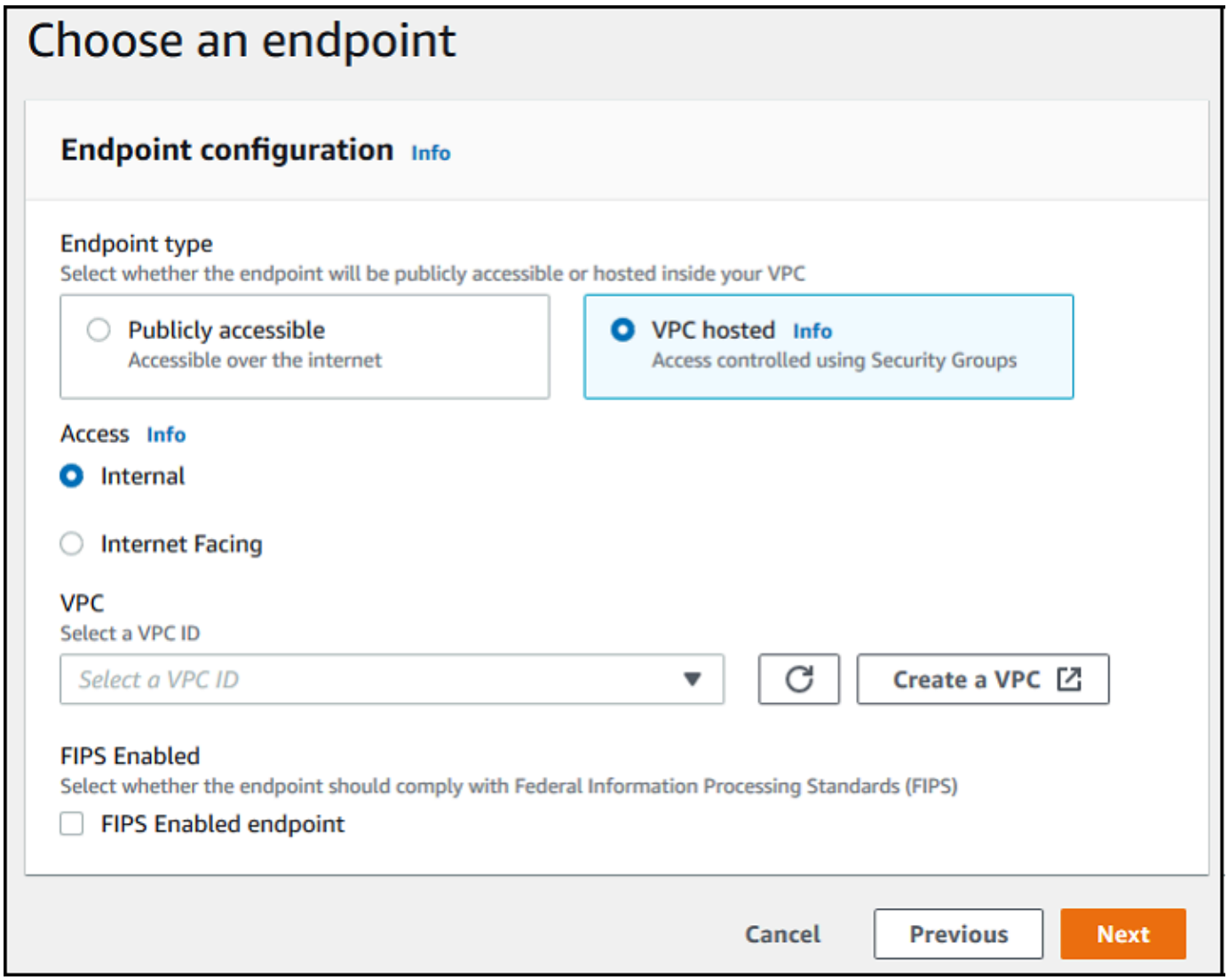
> **Note**
>
> 您可以将文件处理工作流程附加到使用该 AS2 协议的 Transfer Family 服务器：但是， AS2 消息不会执行附加到服务器的工作流程。

创建 AS2启用了-的服务器

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在左侧的导航窗格中，选择服务器，然后选择创建服务器。
3. 在 “选择协议” 页上，选择 AS2（适用性声明 2），然后选择下一步。
4. 在选择身份提供商页面上，选择下一步。

   > **Note**
   >
   > 对于 AS2，您无法选择身份提供商，因为该 AS2 协议不支持基本身份验证。相反，您可以通过虚拟私有云 (VPC) 安全组控制访问权限。

5. 在选择端点页面上，执行以下操作：



a. 对于端点类型，选择托管服务器端点的 VPC 托管。有关设置 VPC 主机端点的信息，请参阅在虚拟私有云中创建服务器。

> **Note**
>
> 该 AS2协议不支持可公开访问的端点。要使您的 VPC 端点可通过互联网访问，请在访问权限下选择面向互联网，然后提供您的弹性 IP 地址。

b. 对于访问权限，请选择下列选项之一：

- 内部 — 选择此选项可在您的 VPC 和 VPC 连接的环境中提供访问权限，例如通过 Amazon Direct Connect 或 VPN 的本地数据中心。

- 面向互联网 — 选择此选项可通过互联网以及您的 VPC 和 VPC 连接的环境（例如本地数据中心或 VPN）提供访问权限。 Amazon Direct Connect

  如果您选择面向互联网，请在出现提示时提供您的弹性 IP 地址。

c. 对于 VPC，选择现有 VPC 或选择创建 VPC 以创建新的 VPC。

d. 对于启用 FIPS，请清除启用 FIPS 端点复选框。

> **Note**
>
> 该协议不支持启用 FIPS 的端点。 AS2

e. 选择下一步。

6. 在选择域页面上，选择 Amazon S3 以使用所选协议将文件作为对象存储和访问。

   选择下一步。

7. 在配置其他详细信息页面上，选择所需的设置。

> **Note**
>
> 如果您同时配置任何其他协议 AS2，则所有其他详细设置均适用。但是，对于该 AS2 协议，唯一适用的设置是CloudWatch 日志和标签部分中的设置。
> 尽管设置 CloudWatch 日志记录角色是可选的，但我们强烈建议您对其进行设置，以便您可以查看消息状态并解决配置问题。

8. 在查看并创建页面上，查看您的选择以确保它们正确无误。

   - 如果要编辑任何设置，请选择要更改步骤旁边的编辑。

   > **Note**
   >
   > 如果您编辑某个步骤，我们建议您在选择编辑的步骤之后查看每个步骤。

   - 如果没有任何更改，请选择创建服务器来创建您的服务器。您将转至如下所示的服务器页面，其中列出了您的新服务器。

     您的新服务器状态更改为在线可能需要几分钟时间。到时候，您的服务器可以执行用户的文件操作。

使用模板创建演示 Transfer Family AS2 堆栈

我们提供了一个独立的 Amazon CloudFormation 模板来快速创建 AS2支持的 Transfer Family 服务器。该模板为服务器配置公有 Amazon VPC 端点、证书、本地和合作伙伴配置文件、协议和连接器。

基本 AS2 服务器模板创建以下资源：

- 一台 AS2启用了 Transfer Family 的服务器，带有 VPC 终端节点
- 带有证书的本地和合作伙伴 AS2 档案
- 个人资料之间的协议
- 用于文件存储的 Amazon S3 存储桶
- 所需的 IAM 角色和策略
- CloudWatch 日志配置

在使用此模板之前，请注意以下事项：

- 如果您根据此模板创建堆栈，则需为使用的 Amazon 资源计费。
- 该模板会创建多个证书并将其放入其中 Amazon Secrets Manager 以安全地存储它们。如果您愿意，您可以从 Secrets Manager 中删除这些证书，因为使用此服务需要付费。在 Secrets Manager 中删除这些证书不会将其从 Transfer Family 服务器中删除。因此，演示堆栈的功能不受影响。但是，对于要用于生产 AS2 服务器的证书，您可能需要使用 Secrets Manager 来管理和定期轮换存储的证书。
- 我们建议您仅将模板用作基础，主要用于演示目的。如果您想在生产环境中使用此演示堆栈，我们建议您修改模板的 YAML 代码以创建更强大的堆栈。例如，创建生产级证书，并创建可在生产中使用的 Amazon Lambda 函数。

使用模板创建 AS2启用了 Transfer Family CloudFormation 服务器

1. 在 https://console.aws.amazon.com/cloudformat ion 上打开 Amazon CloudFormation 控制台。
2. 在左侧导航窗格中，选择堆栈。
3. 选择创建堆栈，然后选择使用新资源（标准）。
4. 在 “先决条件-准备模板” 部分，选择 “选择现有模板”。
5. 复制此链接、AS2 演示模板，然后将其粘贴到 Amazon S3 网址字段中。
6. 选择下一步。
7. 在指定堆栈详细信息页面上，命名您的堆栈，然后指定以下参数：

- 在下方 AS2，输入本地 AS2 ID 和合作伙伴 AS2 ID 的值，或者分别接受默认值和。`local` `partner`
- 在网络下，输入安全组入口 CIDR IP 的值，或接受默认值 `0.0.0.0/0`。

> **Note**
>
> 此值采用 CIDR 格式，指定允许向 AS2 服务器传入流量使用哪些 IP 地址。默认值 `0.0.0.0/0` 允许所有 IP 地址。

- 在常规下，输入前缀的值，或接受默认值 `transfer-as2`。此前缀位于堆栈创建的任何资源名称之前。例如，如果您使用默认前缀，则会将您的 Amazon S3 存储桶命名为 `transfer-as2-`*`amzn-s3-demo-bucket`*。

8. 选择下一步。在配置堆栈选项页面上，再次选择下一步。
9. 查看您正在创建的堆栈的详细信息，然后选择创建堆栈。

> **Note**
>
> 在页面底部的能力下，您必须确认这 Amazon CloudFormation 可能会创建 Amazon Identity and Access Management (IAM) 资源。

创建堆栈后，您可以使用 Amazon Command Line Interface (Amazon CLI) 将测试 AS2 消息从伙伴服务器发送到本地 Transfer Family 服务器。将创建用于发送测试消息的示例 Amazon CLI 命令以及堆栈中的所有其他资源。

要使用此示例命令，请转到堆栈的 “输出” 选项卡，然后复制 TransferExampleAs2Com mand。然后，您可以使用 Amazon CLI运行该命令。如果您尚未安装 Amazon CLI，请参阅Amazon Command Line Interface 用户指南 Amazon CLI中的安装或更新最新版本的。

此示例命令采用以下格式：

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key test.txt && aws transfer start-file-transfer --region aws-region --connector-id TransferConnectorId --send-file-paths /amzn-s3-demo-bucket/test.txt
```

> **Note**
>
> 此命令的版本包含堆栈中 *amzn-s3-demo-bucket* 和 *TransferConnectorId* 资源的实际值。

此示例命令由两个单独的命令组成，这两个命令使用 && 字符串链接在一起。

第一个命令在您的存储桶中创建一个新的空文本文件：

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key test.txt
```

然后，第二个命令使用连接器将文件从合作伙伴配置文件发送到本地配置文件。Transfer Family 服务器已设置协议，允许本地配置文件接受来自合作伙伴配置文件的消息。

```
aws transfer start-file-transfer --region aws-region --connector-id TransferConnectorId
 --send-file-paths /amzn-s3-demo-bucket/test.txt
```

运行命令后，您可以转到您的 Amazon S3 存储桶 (*amzn-s3-demo-bucket*) 并查看其内容。如果命令成功，您应看到存储桶中有以下对象：

- `processed/` – 此文件夹包含一个 JSON 文件，该文件描述传输的文件和 MDN 响应。
- `processing/` – 此文件夹暂时包含正在处理的文件，但在传输完成后，此文件夹应为空。
- *server-id*`/` – 此文件夹根据您的 Transfer Family 服务器 ID 命名。它包含`from-`*partner*（此文件夹根据合作伙伴的 AS2 ID 动态命名），该文件夹本身包含`failed/processed/`、和`processing/`文件夹。/*server-id*`/from-`*partner*`/processed/` 文件夹包含传输的文本文件的副本以及相应的 JSON 和 MDN 文件。
- `test.txt` – 此对象是传输的（空）文件。

创建 AS2 协议

协议与 Transfer Family 服务器相关联。它们为使用该 AS2 协议通过Transfer Family交换消息或文件的贸易伙伴以及入站传输（将 AS2 文件从合作伙伴拥有的外部来源发送到Transfer Family服务器）提供了详细信息。

此过程说明了如何使用 Transfer Family 控制台创建 AS2 协议。如果要 Amazon CLI 改用，请参阅the section called “第 5 步：创建您与合作伙伴之间的协议”。

要为 Transfer Family 服务器创建协议

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在左侧导航窗格中，选择 Servers，然后选择使用该 AS2 协议的服务器。

   或者，只要您至少有一台使用该协议的 Transfer Family 服务器，请从 “AS2 交易伙伴” 菜单中选择 “协议” 以接收消息。 AS2 然后，在创建协议屏幕中，选择要与该协议关联的 AS2 服务器。
3. 在服务器详细信息页面上，向下滚动到协议部分。
4. 选择添加协议。
5. 填写协议参数，如下所示：

   a. 在协议配置部分中，输入描述性名称。确保您可以通过协议名称来识别协议的目的。此外，还要设置协议的状态：活动（默认选中）或非活动。

   b. 在通信配置部分，选择本地配置文件和合作伙伴配置文件。此外，还要选择是否强制执行消息签名。

      - 默认情况下，“强制消息签名” 处于启用状态，这意味着 Transfer Family 会拒绝您的交易伙伴为此协议发送的未签名消息。
      - 清除此设置可允许 Transfer Family 接受交易伙伴为本协议发送的未签名消息。

   c. 在收件箱目录配置部分，提供以下信息。

      - 确定是否选择指定单独的目录来存储您的 AS2 消息、MDN 文件和 JSON 状态文件。
        - 如果选择此选项，则可以为负载文件、失败文件、MDN 文件、状态文件和临时文件指定单独的位置。
        - 如果清除此选项，则所有 AS2 文件都会进入您为基目录指定的位置。
      - 对于 S3 存储桶，请选择一个 Amazon S3 存储桶。
      - 在 P refix 中，您可以输入用于在存储桶中存储文件的前缀（文件夹）。

        例如，如果您**amzn-s3-demo-bucket**为存储桶和**incoming**前缀输入，则您的 AS2文件将保存到该文件/**amzn-s3-demo-bucket**/incoming夹。
      - 对于 Amazon IAM 角色，请选择可以访问您指定的存储桶的角色。
      - 在 “保留文件名” 中，选择是否为传入的 AS2 邮件负载保留原始文件名。
        - 如果您选择此设置，则在将文件保存到 Amazon S3 中时，您的交易伙伴提供的文件名将被保留。

- 如果清除此设置，则在 Transfer Family 保存文件时，会调整文件名，如中所述文件名和位置。

d. （可选）在标签部分中，添加标签。

e. 输入协议的所有信息后，选择创建协议。

新协议显示在服务器详细信息页面的协议部分。

配置 AS2 连接器

连接器的目的是在贸易伙伴之间建立出站传输关系，即将 AS2 文件从 Transfer Family 服务器发送到合作伙伴拥有的外部目的地。对于连接器，您可以指定本地方、远程合作伙伴及其证书（通过创建本地和合作伙伴配置文件）。

有了连接器后，您可以将信息传输给您的交易伙伴。为每 AS2 台服务器分配了三个静态 IP 地址。AS2 连接器使用这些 IP 地址 MDNs 向您的贸易伙伴发送异步信息 AS2。

> **Note**
>
> 交易伙伴收到的消息大小将与 Amazon S3 中的对象大小不匹配。之所以出现这种差异，是因为 AS2 邮件在发送前会将文件封装在信封中。因此，即使文件是以压缩方式发送的，文件大小也可能会增加。因此，请确保交易伙伴的最大文件大小大于您发送的文件的大小。

1. 导入 AS2 证书
2. 创建 AS2 个人资料
3. 创建 AS2 服务器
4. 创建 AS2 协议
5. 创建 AS2 连接器

创建 AS2 连接器

此过程说明如何使用 Amazon Transfer Family 控制台创建 AS2 连接器。如果要 Amazon CLI 改用，请参阅the section called “第 6 步：创建您与合作伙伴之间的连接器”。

创建 AS2 连接器

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在左侧导航窗格中，从 “AS2 贸易伙伴” 菜单中选择 “要发送消息的连接器”，然后选择 “创建 AS2 连接器”。
3. 在连接器配置部分中，指定以下信息：

   - URL — 输入出站连接的 URL。
   - 访问角色-选择要使用的 (IAM) 角色的亚马逊资源名称 Amazon Identity and Access Management (ARN)。确保角色提供对 `StartFileTransfer` 请求中所使用文件位置父目录的读取和写入访问权限。此外，确保角色对拟定发送 `StartFileTransfer` 的父目录提供读取和写入访问权限。

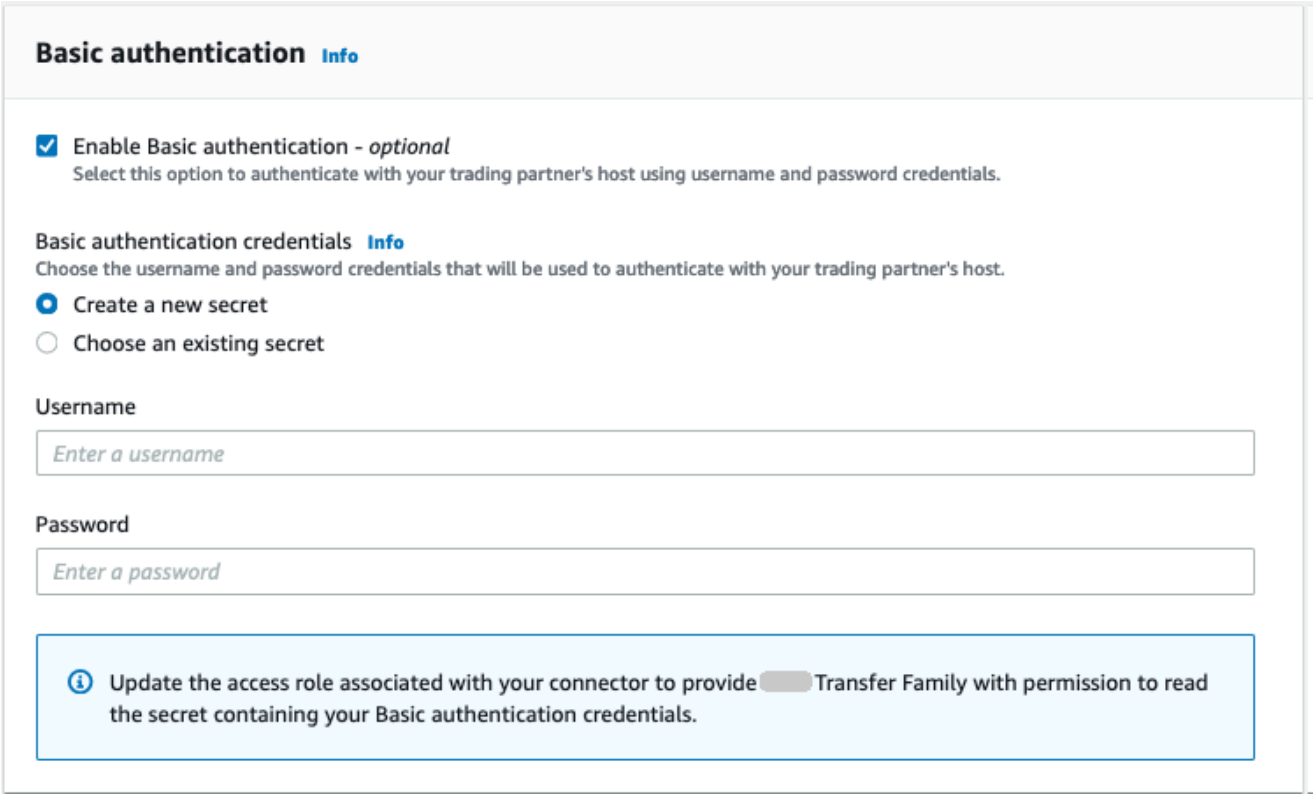
     > **Note**
     >
     > 如果您对连接器执行基本身份验证，则访问角色需要密钥的 `secretsmanager:GetSecretValue` 权限。如果使用客户管理的密钥而不是 in 对密钥进行加密 Amazon Secrets Manager，则该角色还需要`kms:Decrypt`获得该密钥的权限。 Amazon 托管式密钥 如果您使用前缀 `aws/transfer/` 命名您的密钥，则可以使用通配符 (*) 添加必要的权限，如创建密钥的权限示例中所示。

   - 日志角色（可选）-选择连接器用于将事件推送到 CloudWatch日志的 IAM 角色。
4. 在AS2 配置部分，选择本地和合作伙伴配置文件、加密和签名算法，以及是否压缩传输的信息。注意以下几点：

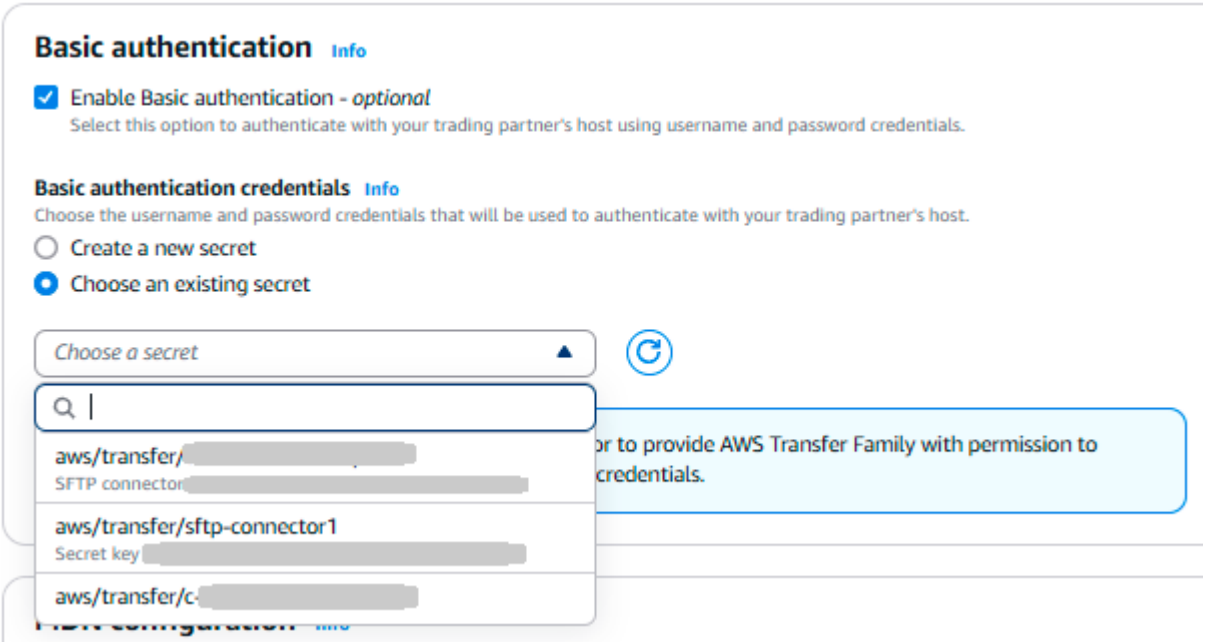
   - 默认情况下，保留 S3 内容类型参数处于启用状态。

     设置后，Transfer Famil `Content-Type` y 使用与 S3 中的对象关联的 Amazon S3，而不是根据文件扩展名映射内容类型。如果您希望服务根据文件扩展名映射 AS2 消息的内容类型，而不是使用 S3 对象中的内容类型，请清除此设置。
   - 对于加密算法，`DES_EDE3_CBC`除非必须支持需要加密算法的旧版客户端，否则不要选择，因为这是一种较弱的加密算法。
   - 在使用连接器发送的 AS2 邮件中，主题用作 `subject` HTTP标头属性。
   - 如果您选择创建不使用加密算法的连接器，则必须指定HTTPS为您的协议。
5. 在基本身份验证部分中，指定以下信息：

- 要将登录凭证与出站消息一起发送，请选择启用基本身份验证。如果您不想在出站消息中发送任何凭证，请清除启用基本身份验证。
- 如果您使用的是身份验证，请选择或创建密钥。
  - 要创建新密钥，请选择创建新密钥，然后输入用户名和密码。这些凭证必须与连接到合作伙伴端点的用户相匹配。



  - 要使用现有密钥，请选择选择现有秘钥，然后从下拉菜单中选择密钥。有关在 Secrets Manager 中创建格式正确的密钥的详细信息，请参阅 为 AS2连接器启用基本身份验证。



6. 在 MDN 配置部分中，指定以下信息：

   - 请求 MDN — 您可以选择要求您的贸易伙伴在成功收到您的消息后向他们发送 MDN。 AS2
   - 已签名 MDN — 您可以选择要求对其 MDNs 进行签名。只有选择了请求 MDN，此选项才可用。

7. 确认所有设置后，选择创建 AS2 连接器以创建连接器。

连接器页面会出现，其中新连接器的 ID 已添加到列表中。要查看连接器的详细信息，请参阅 查看 AS2 连接器详细信息。

AS2 连接器算法

创建 AS2 连接器时，会将以下安全算法附加到该连接器。

Type	算法
TLS 密码	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

Type	算法
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

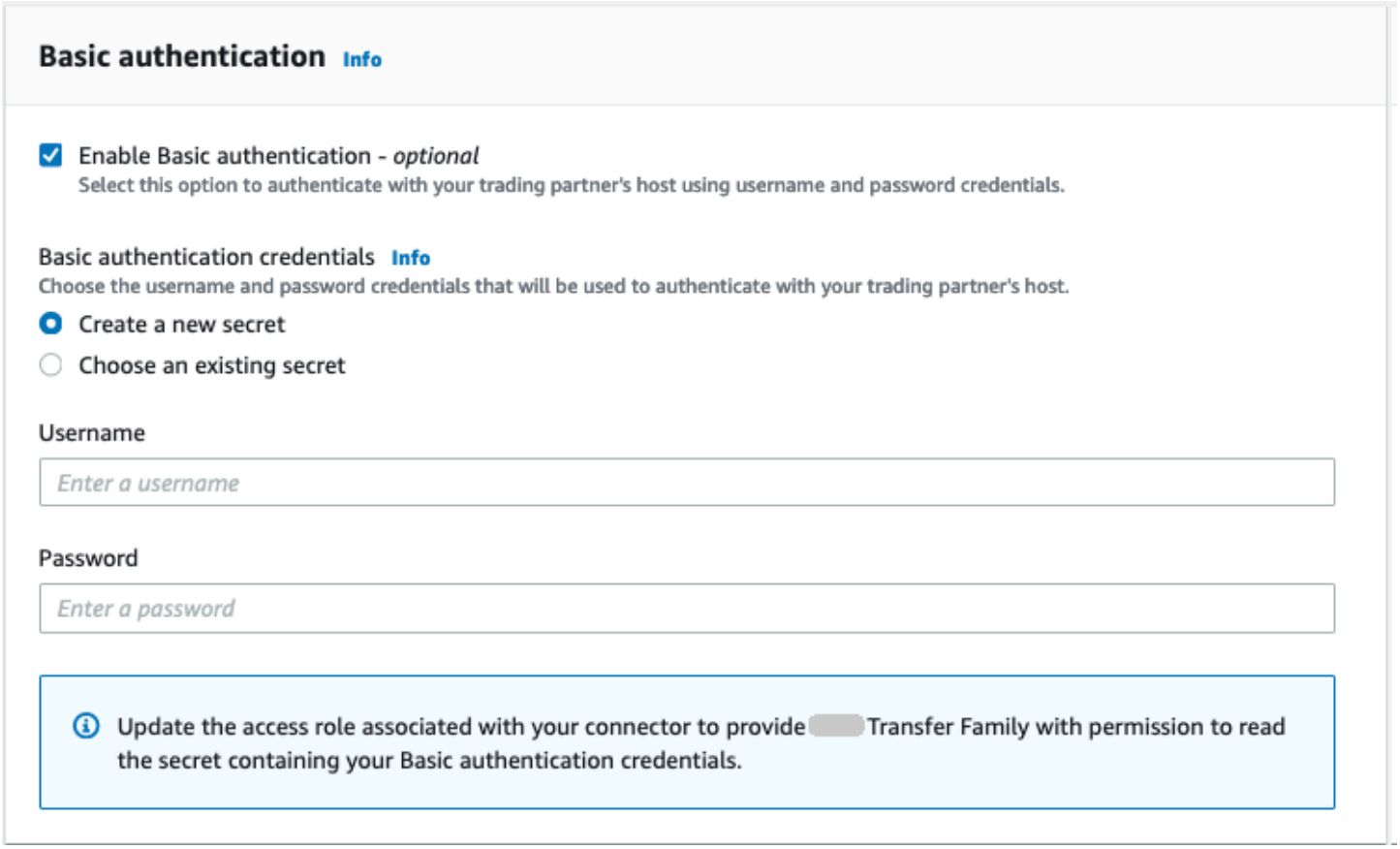
AS2 连接器的基本身份验证

创建或更新使用该 AS2 协议的 Transfer Family 服务器时，可以为出站邮件添加基本身份验证。可以通过为连接器添加身份验证信息来完成此操作。

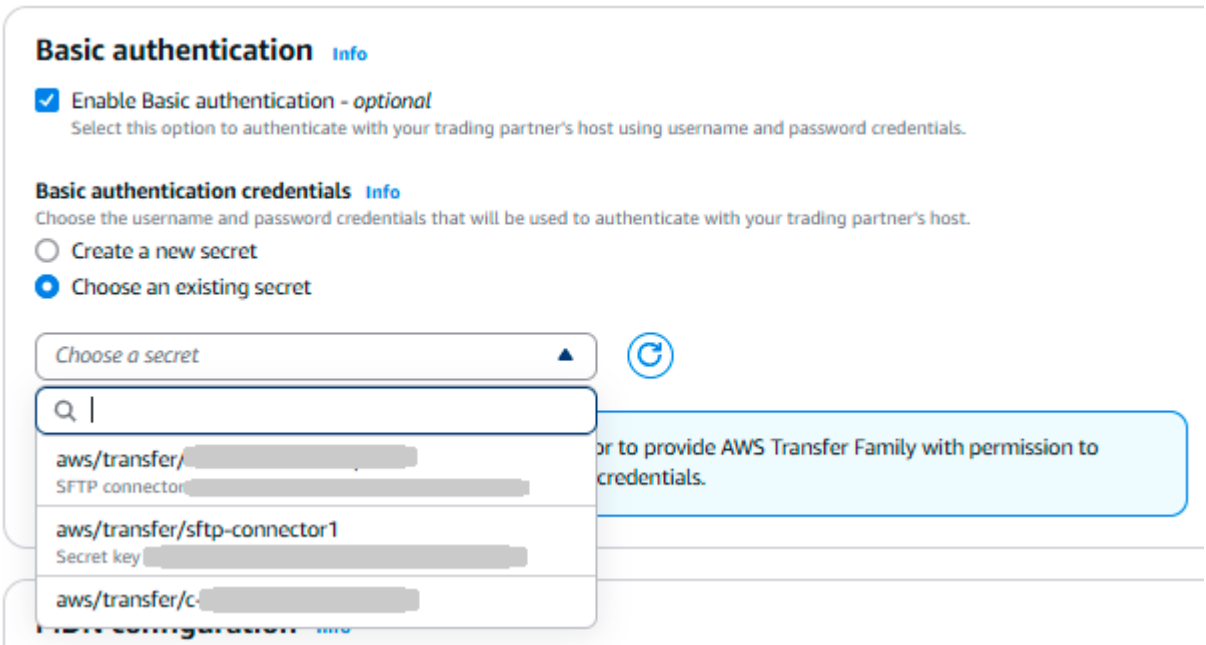
> **Note**
>
> 仅当您使用 HTTPS 时，基本身份验证才可用。

要对连接器使用身份验证，请在“基本身份验证”部分中选择“启用基本身份验证”。启用基本身份验证后，您可以选择创建新密钥，或使用现有密钥。无论哪种情况，密钥中的凭据都与使用此连接器的出站邮件一起发送。这些凭证必须与试图连接到贸易伙伴的远程端点的用户相匹配。

以下屏幕截图显示选中了“启用基本身份验证”，并选择了“创建新密钥”。做出这些选择后，您可以输入密钥的用户名和密码。



以下屏幕截图显示选中了“启用基本身份验证”，并选择了“创建现有密钥”。您的密钥必须为正确格式，如 为 AS2连接器启用基本身份验证 所述。



为 AS2连接器启用基本身份验证

为 AS2 连接器启用基本身份验证后，您可以在 Transfer Family 控制台中创建新密钥，也可以使用在中创建的密钥 Amazon Secrets Manager。无论哪种情况，您的密钥都存储在 Secrets Manager 中。

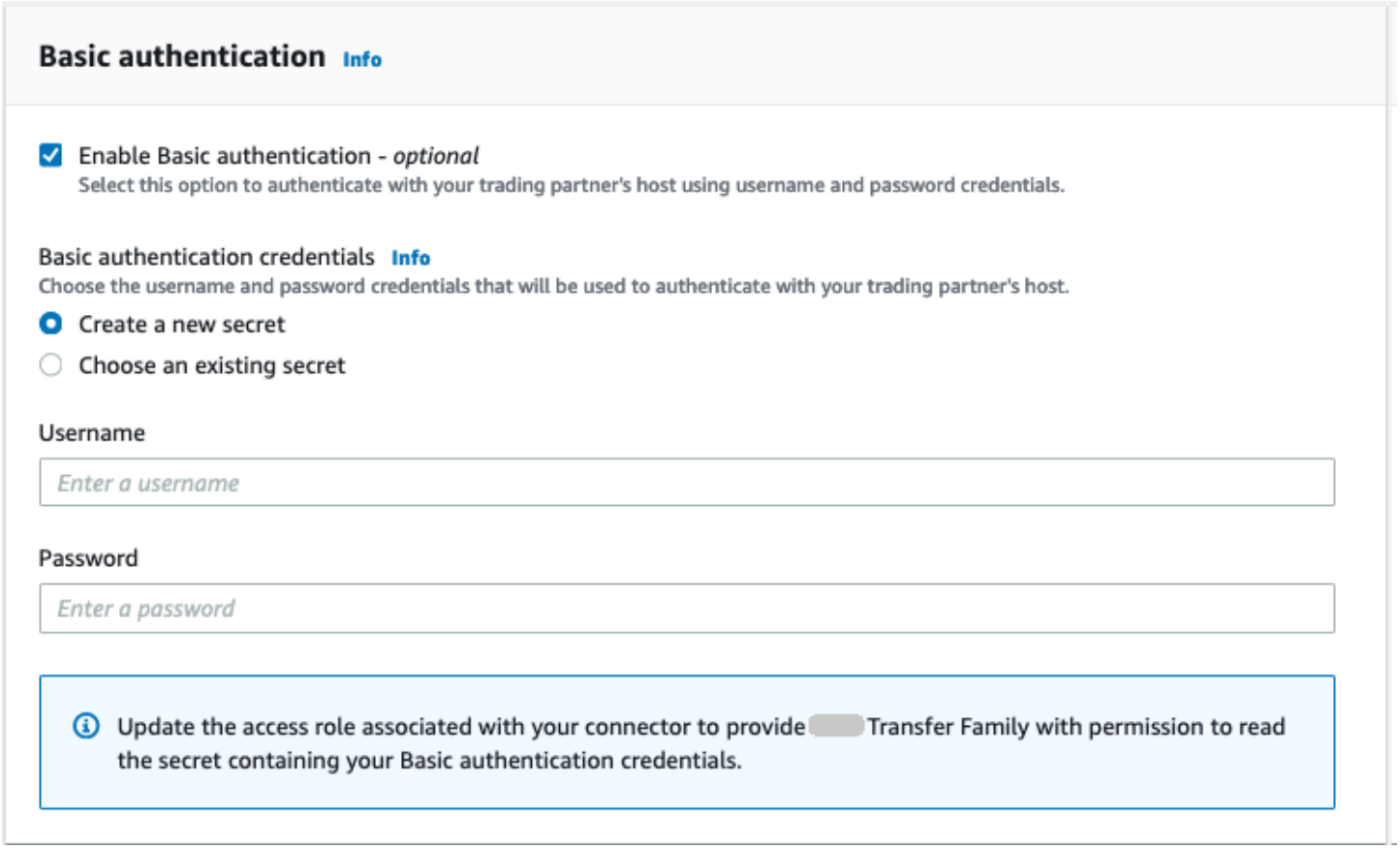
主题

- 在控制台中创建新的密钥
- 使用现有 密钥
- 在中创建密钥 Amazon Secrets Manager

在控制台中创建新的密钥

当您在控制台中创建连接器时，您可以创建一个新的密钥。

要创建新密钥，请选择创建新密钥，然后输入用户名和密码。这些凭证必须与连接到合作伙伴端点的用户相匹配。

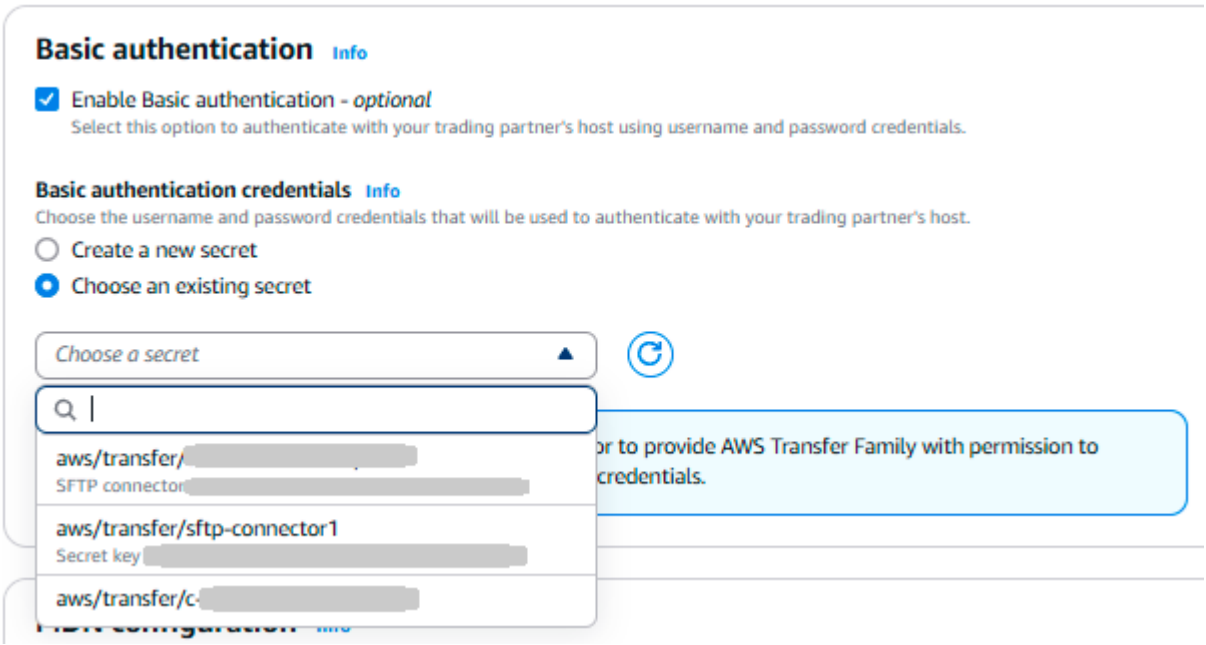


> **Note**
>
> 当您在控制台中创建新密钥时，密钥的名称将遵循以下命名约定：**`/aws/transfer/connector-id`**，其中*`connector-id`*是您正在创建的连接器的 ID。当您试图在 Amazon Secrets Manager中定位密钥时，请考虑这一点。

使用现有 密钥

当您在控制台中创建连接器时，您可以指定一个现有密钥。

要使用现有密钥，请选择选择现有秘钥，然后从下拉菜单中选择密钥。有关在 Secrets Manager 中创建格式正确的密钥的详细信息，请参阅 在中创建密钥 Amazon Secrets Manager。



在中创建密钥 Amazon Secrets Manager

以下过程介绍如何创建用于 AS2 连接器的相应密钥。

> **Note**
>
> 仅当您使用 HTTPS 时，基本身份验证才可用。

将用户凭据存储在 Secrets Manager 中以进行 AS2 基本身份验证

1. 登录 Amazon Web Services 管理控制台 并打开 Amazon Secrets Manager 控制台，网址为https://console.aws.amazon.com/secretsmanager/。
2. 在左侧导航窗格中，选择密钥。
3. 在密钥页面，选择存储新密钥。
4. 在选择密钥类型页面上，对于密钥类型，选择其他类型密钥。
5. 在键/值对部分，选择键/值选项卡。
   - 键 — 输入**Username**。
   - 值 — 输入有权连接到合作伙伴服务器的用户名。
6. 如果要提供密码，请选择添加行，然后在键/值对部分中，选择键/值选项卡。

   选择添加行，然后在键/值对部分选择键/值选项卡。
   - 键 — 输入 **Password**。
   - 值 — 输入用户的密码。
7. 如果要提供私钥，请选择添加行，然后在密钥/值对部分，选择密钥/值选项卡。
   - 键 — 输入 **PrivateKey**。
   - 值 — 输入用户的私有密钥。此值必须以 OpenSSH 格式存储，并且必须与在远程服务器中为该用户存储的公有密钥相对应。
8. 选择下一步。
9. 在配置密钥页面，输入密钥的名称和描述。建议对名称使用前缀 **aws/transfer/**。例如，您可以将密钥命名为 **aws/transfer/connector-1**。
10. 选择下一步，接受配置轮换页面的默认设置。然后选择下一步。
11. 在审核页面，选择存储以创建和存储密钥。

创建密钥后，您可以在创建连接器时选择密钥（请参阅 配置 AS2 连接器）。在启用基本身份验证的步骤中，从可用密钥的下拉列表中选择密钥。

查看 AS2 连接器详细信息

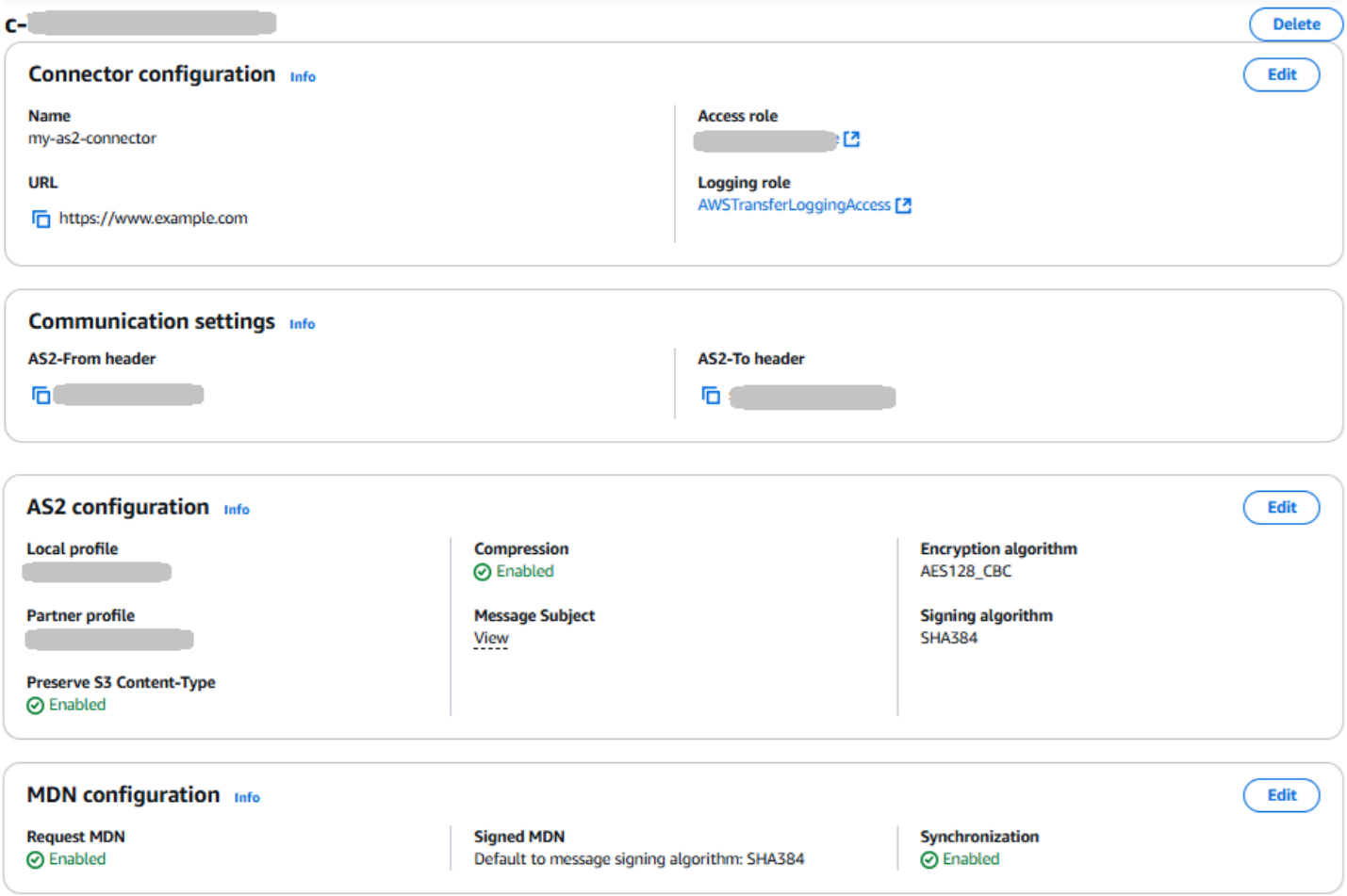
您可以在 Amazon Transfer Family 控制台中找到 AS2 Amazon Transfer Family 连接器的详细信息和属性列表。 AS2 连接器的属性包括其 URL、角色、配置文件 MDNs、标签和监控指标。

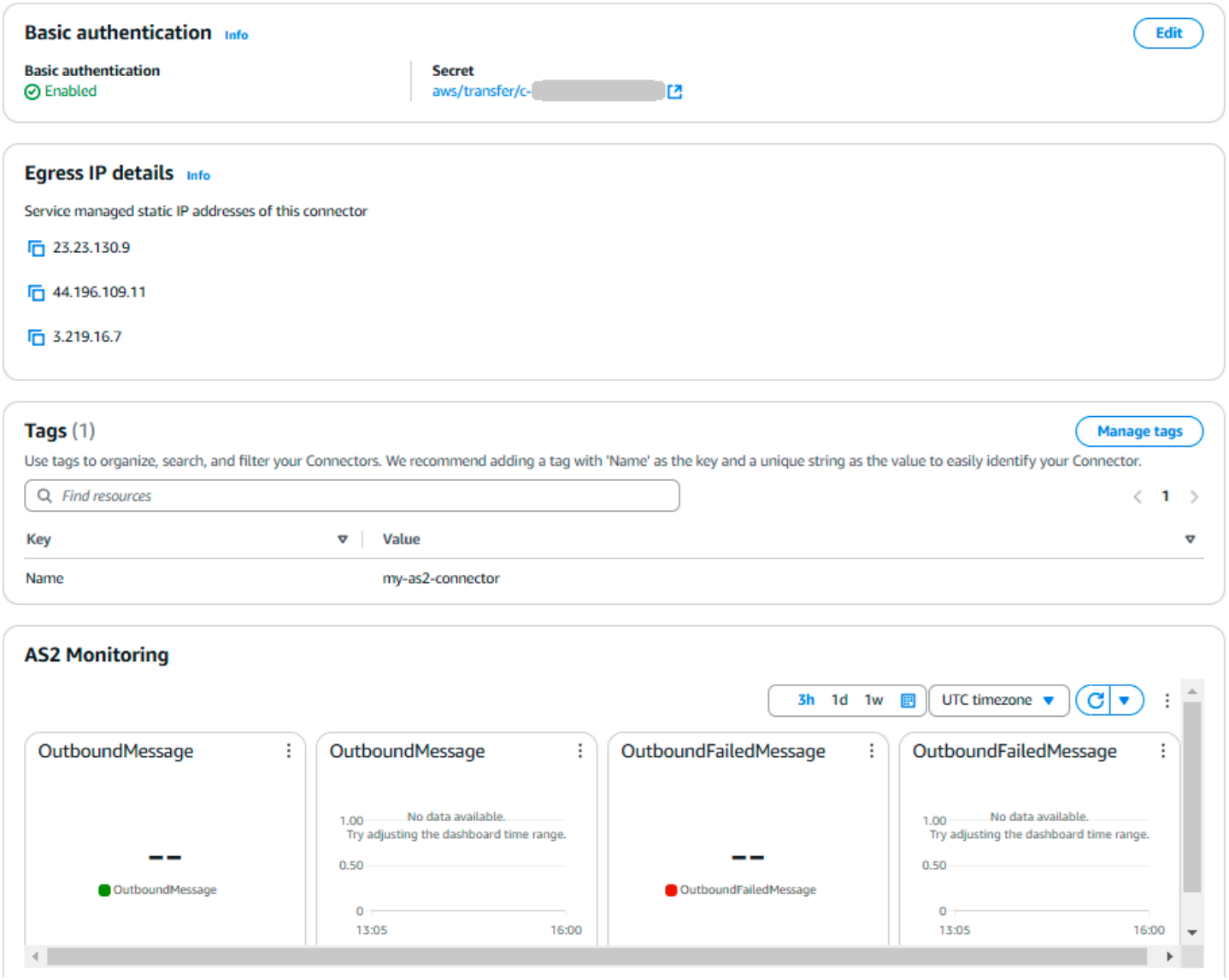
这是查看连接器详细信息的过程。

要查看连接器详细信息

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在左侧导航窗格中，选择连接器。
3. 在“连接器 ID”列中选择标识符以查看所选连接器的详细信息页面。

通过选择 “编辑”，可以在 AS2 连接器的详细信息页面上更改连接器的属性。





> **Note**
>
> 你可以通过运行以下命令来获取其中的大部分信息，尽管格式不同 Amazon Command Line Interface（Amazon CLI 命令：
>
> ```
> aws transfer describe-connector --connector-id your-connector-id
> ```
>
> 有关更多信息，请参阅《API 参考》中的 DescribeConnector。

发送和接收 AS2 消息

本节介绍发送和接收 AS2 消息的过程。它还提供与 AS2 消息相关的文件名和位置的详细信息。

下表列出了 AS2 消息的可用加密算法以及何时可以使用这些算法。

加密算法	HTTP	HTTPS	注意
AES128_CBC	支持	是	
AES192_CBC	支持	是	
AES256_CBC	支持	是	
DES_ _ EDE3 CBC	支持	是	只有在必须支持需要此算法的旧版客户端时才使用此算法，因为它是一种弱加密算法。
NONE	否	是	如果您要向 Transfer Family 服务器发送消息，则只能选择NONE是否使用应用程序负载均衡器 (ALB)。

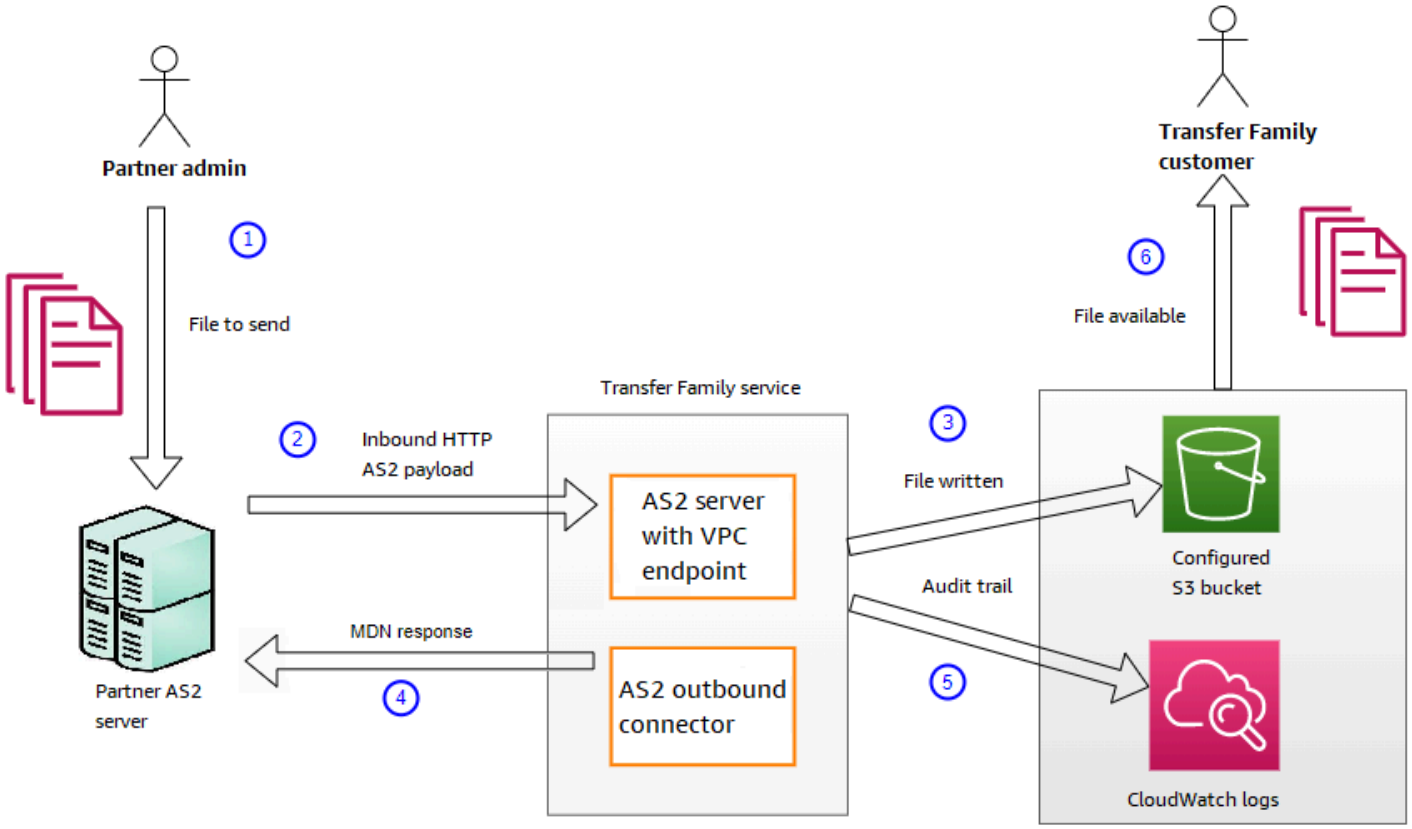
主题

- 接收 AS2 消息流程
- 通过 HTTPS 发送和接收 AS2 消息
- 使用 AS2连接器传输文件
- 文件名和位置
- 状态代码
- 示例 JSON 文件

接收 AS2 消息流程

入站流程定义为正在传输到 Amazon Transfer Family 服务器的消息或文件。入站消息的顺序如下：

1. 管理员或自动流程在合作伙伴的远程 AS2 服务器上启动 AS2 文件传输。
2. 合作伙伴的远程 AS2 服务器对文件内容进行签名和加密，然后向托管在 Transfer Family 上的 AS2 入站端点发送 HTTP POST 请求。
3. Transfer Family 使用服务器、合作伙伴、证书和协议的配置值，解密并验证有效负载。 AS2 文件内容存储在已配置的 Amazon S3 文件存储中。
4. 已签名的 MDN 响应应与 HTTP 响应内联返回，或者通过单独的 HTTP POST 请求异步返回原始服务器。
5. 审计记录已写入Amazon， CloudWatch 其中包含有关交易所的详细信息。
6. 解密后的文件位于名为 `inbox/processed` 的文件夹中。



通过 HTTPS 发送和接收 AS2 消息

本节介绍如何配置使用该 AS2 协议通过 HTTPS 发送和接收消息的 Transfer Family 服务器。

主题

- 通过 HTTPS 发送 AS2 消息
- 通过 HTTPS 接收 AS2 消息

通过 HTTPS 发送 AS2 消息

要使用 HTTPS 发送 AS2 消息，请使用以下信息创建一个连接器：

- 对于网址，请指定 HTTPS URL
- 对于加密算法，请选择任何可用的算法。

> **Note**
>
> 要在不使用加密（即您选择NONE加密算法）的情况下向 Transfer Family 服务器发送消息，则必须使用应用程序负载均衡器 (ALB)。

- 提供连接器的其余值，如 配置 AS2 连接器 中所述。

通过 HTTPS 接收 AS2 消息

Amazon Transfer Family AS2 服务器目前仅通过端口 5080 提供 HTTP 传输。但是，您可以使用自己选择的端口和证书在您的 Transfer Family 服务器 VPC 终端节点前的网络或应用程序负载均衡器上终止 TLS。通过这种方法，您可以让传入的 AS2 消息使用 HTTPS。

先决条件

- VPC 必须与您的 Transfer Amazon Web Services 区域 Family 服务器位于同一个服务器中。
- 您的 VPC 的子网必须位于您要在其中使用服务器的可用区内。

> **Note**
>
> 每台 Transfer Family 服务器最多可以支持三个可用区。

- 在与您的服务器相同的区域中最多分配三个弹性 IP 地址。或者，您可以选择自带 IP 地址范围（BYOIP）。

> **Note**
>
> 弹性 IP 地址的数量必须与您用于服务器端点的可用区域数量相匹配。

您可以配置网络负载平衡 (NLB) 或 Application Load Balancer (ALB)。下表列出了每种方法的优缺点。

下表提供了使用 NLB 与 ALB 终止 TLS 时的功能差异。

功能	Network Load Balancer (NLB)	Application Load Balancer (ALB)
延迟	由于它在网络层运行，因此延迟更低。	由于它在应用层运行，因此延迟更高。
支持静态 IP	可以附加可以是静态的弹性 IP 地址。	无法附加弹性 IP 地址：提供其基础 IP 地址可以更改的域。
高级路由	不支持高级路由。	支持高级路由。 AS2无需加密即可注入所需的`X-Forwarded-Proto` 标头。 developer.mozilla.org 网站上的 X-Forwarded-Proto 中描述了这个标题。
TLS/SSL 终止	支持 TLS/SSL 终止	支持 TLS/SSL 终止
双向 TLS (mTLS)	Transfer Family 目前不支持将 NLB 用于 mTL	对 mTLS 的 Support

Configure NLB

此过程介绍如何在您的 VPC 中设置面向互联网的网络负载均衡器 (NLB)。

创建网络负载均衡器并将服务器的 VPC 端点定义为负载均衡器的目标

1. 打开亚马逊弹性计算云控制台，网址为https://console.aws.amazon.com/ec2/。

2. 在导航窗格中，选择负载均衡器，然后选择创建负载均衡器。
3. 在网络负载均衡器下，选择创建。
4. 在基本配置部分，输入以下信息：
   - 对于名称，为负载均衡器输入一个描述性名称。
   - 对于 Scheme，选择 Internet-facing。
   - 对于 IP address type（IP 地址类型），选择 IPv4。
5. 在网络映射部分中，输入以下信息：
   - 对于 VPC，请选择您已创建的虚拟私有云 (VPC)。
   - 在映射下，选择与公有子网关联的可用区，这些子网位于您用于服务器端点的同一 VPC 中。
   - 对于每个子网IPv4 的地址，选择您分配的弹性 IP 地址之一。
6. 在侦听器和路由部分中，输入以下信息：
   - 对于协议，选择 TLS。
   - 对于端口，输入 **5080**。
   - 对于默认操作，选择创建目标组。有关创建新目标组的详细信息，请参阅 创建目标组。

   创建目标组后，在默认操作字段中输入其名称。
7. 在安全侦听器设置部分，在默认证书区域中选择您的 SSL/TLS 证书。
8. 选择创建负载均衡器以创建您的 NLB。
9. （可选，但推荐）打开网络负载均衡器的访问日志以保持完整的审计跟踪记录，如网络负载均衡器的访问日志中所述。

   我们建议执行此步骤，因为 TLS 连接已在 NLB 终止。因此，反映在您的 Transfer Family AS2 CloudWatch 日志组中的源 IP 地址是 NLB 的私有 IP 地址，而不是交易伙伴的外部 IP 地址。

Configure ALB

此过程介绍如何在您的 VPC 中设置应用程序负载均衡器 (ALB)。

创建 Application Load Balancer 并将服务器的 VPC 终端节点定义为负载均衡器的目标

1. 打开亚马逊弹性计算云控制台，网址为https://console.aws.amazon.com/ec2/。

2. 在导航窗格中，选择负载均衡器，然后选择创建负载均衡器。
3. 在应用程序负载均衡器下，选择创建。
4. 在 ALB 控制台中，在端口 443 (HTTPS) 上创建一个新的 HTTP 监听器。
5. （可选）。如果要设置相互身份验证 (mTLS)，请配置安全设置和信任存储。

   a. 将您的 SSL/TLS 证书附加到监听器。

   b. 在“客户证书处理”下，选择相互身份验证 (mTLS)。

   c. 选择“使用信任存储进行验证”。

   d. 在“高级 mTLS 设置”下，通过上传您的 CA 证书来选择或创建信任存储。
6. 创建一个新的目标组，并将 Transfer Family AS2 服务器端点的私有 IP 地址添加为端口 5080 上的目标。有关创建新目标组的详细信息，请参阅 创建目标组。
7. 为目标组配置运行状况检查，使其在端口 5080 上使用 HTTP 协议。
8. 创建新规则，将 HTTPS 流量从侦听器转发到目标组。
9. 将侦听器配置为使用您的 SSL/TLS 证书。

设置负载均衡器后，客户端通过自定义端口侦听器与负载均衡器进行通信。然后，负载均衡器通过端口 5080 与服务器通信。

创建目标组

1. 在前面的过程中选择创建目标组后，您将进入新目标组的指定组详细信息页面。
2. 在基本配置部分，输入以下信息。

   - 在选择目标类型中，选择 IP 地址。
   - 对于目标组名称，输入目标组的名称。
   - 对于协议，您的选择取决于您使用的是 ALB 还是 NLB。
     - 对于 Network Load Balancer (NLB)，请选择 TCP
     - 对于 Application Load Balancer (ALB)，请选择 HTTP
   - 对于端口，输入 **`5080`**。
   - 对于 IP address type（IP 地址类型），选择 IPv4。
   - 对于 VPC，请选择您为 Transfer Family AS2 服务器创建的 VPC。
3. 在健康检查部分，选择健康检查协议。

   - 对于 ALB，请选择 HTTP

- 对于 NLB，请选择 TCP

4. 选择下一步。
5. 在注册目标页面，输入以下信息：
   - 对于网络，请确认已指定您为 Transfer Family AS2 服务器创建的 VPC。
   - 对于IPv4 地址，请输入 Trans IPv4 fer Family AS2 服务器端点的私有地址。

     如果您的服务器有多个端点，请选择添加 IPv4 地址以添加另一行用于输入其他 IPv4 地址。重复此过程，直到输入服务器所有端点的私有 IP 地址。
   - 确保端口设置为 **`5080`**。
   - 选择包含如下待处理事项，将您的条目添加到审核目标部分。
6. 在查看目标部分，查看您的 IP 目标。
7. 选择创建目标组，然后返回之前创建 NLB 的过程，并在指示的位置输入新的目标组。

测试从弹性 IP 地址访问服务器

使用弹性 IP 地址或网络负载均衡器的 DNS 名称通过自定义端口连接到服务器。

> **Important**
>
> 使用负载均衡器上配置的子网的网络访问控制列表（网络 ACLs），管理从客户端 IP 地址对服务器的访问。网络 ACL 权限是在子网级别设置的，因此这些规则适用于使用该子网的所有资源。您无法使用安全组控制来自客户端 IP 地址的访问，因为负载均衡器的目标类型设置为 IP 地址而不是实例。因此，负载均衡器不保留源 IP 地址。如果网络负载均衡器的运行状况检查失败，则意味着负载均衡器无法连接到服务器端点。要对此问题进行故障排除，请检查以下步骤：
>
> - 确认服务器端点的关联安全组允许来自负载均衡器上配置的子网的入站连接。负载均衡器必须能够通过端口 5080 连接到服务器端点。
> - 确认服务器的状态为联机。

使用 AS2连接器传输文件

AS2 连接器在贸易伙伴之间建立关系，以便将 AS2 消息从 Transfer Family 服务器传输到合作伙伴拥有的外部目的地。

您可以使用 Transfer Family 通过引用连接器 ID 和文件路径来发送 AS2 消息，如以下 `start-file-transfer` Amazon Command Line Interface (Amazon CLI) 命令所示：

```
aws transfer start-file-transfer --connector-id c-1234567890abcdef0 \
--send-file-paths "/amzn-s3-demo-source-bucket/myfile1.txt" "/amzn-s3-demo-source-bucket/myfile2.txt"
```

要获取连接器详细信息，请运行以下命令：

```
aws transfer list-connectors
```

该`list-connectors`命令会返回连接器 IDs URLs、以及连接器的 Amazon 资源名称 (ARNs)。

要返回特定连接器的属性，请使用要使用的 ID 运行以下命令：

```
aws transfer describe-connector --connector-id your-connector-id
```

该`describe-connector`命令返回连接器的所有属性，包括其 URL、角色、配置文件、邮件处置通知 (MDNs)、标签和监控指标。

您可以通过查看 JSON 和 MDN 文件来确认合作伙伴已成功接收文件。这些文件是根据 文件名和位置 中描述的约定命名的。如果您在创建连接器时配置了日志记录角色，则还可以检查 CloudWatch 日志中的 AS2 消息状态。

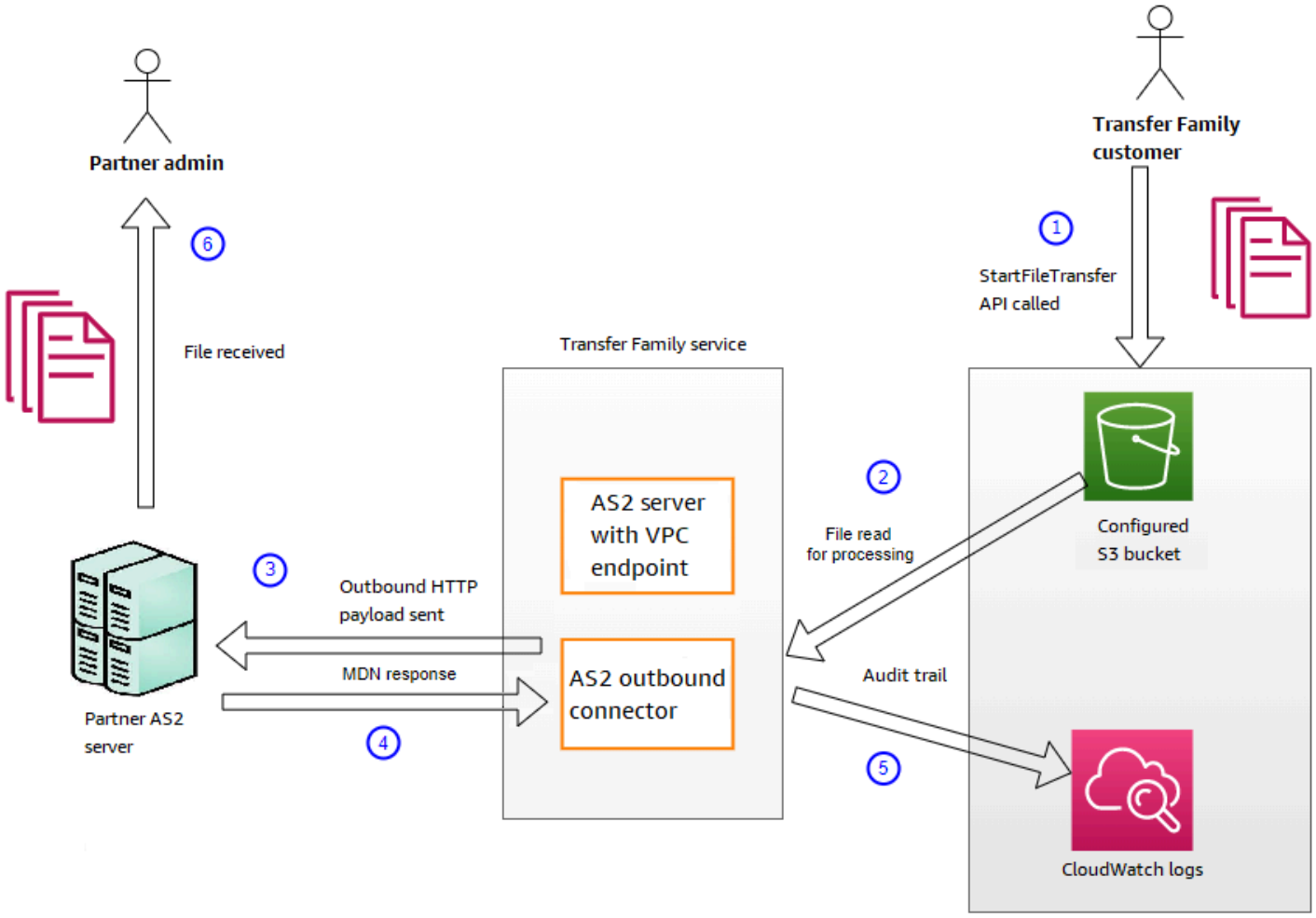
要查看 AS2 连接器详细信息，请参阅查看 AS2 连接器详细信息。有关创建 AS2连接器的更多信息，请参见配置 AS2 连接器。

发送出 AS2 站消息

出站进程定义为从 Amazon 外部客户端或服务发送的消息或文件。出站消息的顺序如下：

1. 管理员调用 `start-file-transfer` Amazon Command Line Interface (Amazon CLI) 命令或 `StartFileTransfer` API 操作。此操作引用 `connector` 配置。
2. Transfer Family 检测到新的文件请求并定位该文件。文件经过压缩、签名和加密。
3. 传输 HTTP 客户端执行 HTTP POST 请求，将有效负载传输到合作伙伴的 AS2 服务器。
4. 该流程返回已签名的 MDN 响应，该响应与 HTTP 响应（同步 MDN）内联。
5. 当文件在不同的传输阶段之间移动时，该流程会向客户提供 MDN 响应接收和处理详细信息。

6. 远程 AS2 服务器将解密并经过验证的文件提供给合作伙伴管理员。



AS2 处理支持许多 RFC 4130 协议，重点是常见用例以及与现有 AS2支持服务器实现的集成。有关支持的配置详细信息，请参阅 AS2 配置。

文件名和位置

本节讨论传输的文件命名惯例。 AS2

对于入站文件传输，需要注意以下方面：

- 您可以在协议中指定基本目录。基本目录是 Amazon S3 存储桶名称和前缀（如果有）的组合。例如 **/amzn-s3-demo-bucket**/AS2-folder。
- 如果成功处理了传入的文件，则该文件（以及相应的 JSON 文件）将保存至该 /processed 文件夹。例如 **/amzn-s3-demo-bucket**/AS2-folder/processed。

JSON 文件包含以下字段：

- agreement-id
- as2-from
- as2-to
- as2-message-id
- transfer-id
- client-ip
- connector-id
- failure-message
- file-path
- message-subject
- mdn-message-id
- mdn-subject
- requester-file-name
- requester-content-type
- server-id
- status-code
- failure-code
- transfer-size

- 如果无法成功处理传入文件，则该文件（以及相应的 JSON 文件）将保存至该 /failed 文件夹。例如 /amzn-s3-demo-bucket/AS2-folder/failed。
- 传输的文件存储在 processed 文件夹中，名为 *original_filename*.*messageId*.*original_extension*。也就是说，传输的消息 ID 会附加到文件名之后，在文件的原始扩展名之前。
- 已创建 JSON 文件并将其另存为 *original_filename*.*messageId*.*original_extension*.json。除了要添加的消息 ID 外，还会在传输的文件名后面附加该字符串 .json。
- 消息处置通知 (MDN) 文件已创建并另存为 *original_filename*.*messageId*.*original_extension*.mdn。除了要添加的消息 ID 外，还会在传输的文件名后面附加该字符串 .mdn。
- 如果存在名为 ExampleFileInS3Payload.dat 的入站文件，则会创建以下文件：

- File — ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.
- JSON — ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.
- MDN — ExampleFileInS3Payload.c4d6b6c7-23ea-4b8c-9ada-0cb811dc8b35@44313c54b0a46a36.

对于出站传输，命名类似，不同之处在于没有传入的消息文件，而且，已传输消息的传输 ID 会添加到文件名中。传输 ID 由 StartFileTransfer API 操作返回（或者当其他流程或脚本调用此操作时）。

- transfer-id 是与文件传输关联的标识符。作为 StartFileTransfer 调用一部分的所有请求共享 transfer-id。
- 基本目录与您用于源文件的路径相同。也就是说，基目录是您在 StartFileTransfer API 操作或start-file-transfer Amazon CLI 命令中指定的路径。例如：

  ```
  aws transfer start-file-transfer --send-file-paths /amzn-s3-demo-bucket/AS2-folder/file-to-send.txt
  ```

  如果运行此命令，MDN 和 JSON 文件将保存在 /amzn-s3-demo-bucket/AS2-folder/processed 中（对于成功传输）或 /amzn-s3-demo-bucket/AS2-folder/failed（对于不成功传输）。
- 已创建 JSON 文件并将其另存为 *original_filename*.*transferId*.*messageId*.*original_extension*.json。
- 已创建 MDN 文件并将其另存为 *original_filename*.*transferId*.*messageId*.*original_extension*.mdn。
- 如果存在名为 ExampleFileOutTestOutboundSyncMdn.dat 的出站文件，则会创建以下文件：
  - JSON — ExampleFileOutTestOutboundSyncMdn.dedf4601-4e90-4043-b16b-579af35e0d83.fbe18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa.dat.j
  - MDN — ExampleFileOutTestOutboundSyncMdn.dedf4601-4e90-4043-b16b-579af35e0d83.fbe18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa.dat.m

您还可以查看 CloudWatch 日志以查看转账的详细信息，包括任何失败的转账。

状态代码

下表列出了您或您的合作伙伴发送 AS2 消息时可以记录到 CloudWatch 日志中的所有状态代码。不同的消息处理步骤适用于不同的消息类型，并且仅用于监控。“已完成” 和 “失败” 状态表示处理的最后一步，在 JSON 文件中可见。

代码	描述	处理完成了吗？
处理	该消息正在转换为其最终格式。例如，解压缩和解密步骤都具有此状态。	否
MDN_TRANSM	消息处理正在发送 MDN 响应。	否
MDN_RECEIVE	消息处理正在收到 MDN 响应。	否
COMPLETED	消息处理已成功完成。此状态包括为入站消息或出站消息的 MDN 验证发送 MDN 的时间。	是
FAILED	消息处理失败。有关错误代码的列表，请参阅AS2 错误代码。	是

示例 JSON 文件

本部分列出了入站和出站传输的示例 JSON 文件，包括传输成功和传输失败的示例文件。

传输成功的示例出站文件：

```
{
  "requester-content-type": "application/octet-stream",
  "message-subject": "File xyzTest from MyCompany_OID to partner YourCompany",
  "requester-file-name": "TestOutboundSyncMdn-9lmCr79hV.dat",
  "as2-from": "MyCompany_OID",
  "connector-id": "c-c21c63ceaaf34d99b",
  "status-code": "COMPLETED",
```

```
  "disposition": "automatic-action/MDN-sent-automatically; processed",
  "transfer-size": 3198,
  "mdn-message-id": "OPENAS2-11072022063009+0000-df865189-1450-435b-9b8d-
d8bc0cee97fd@PartnerA_OID_MyCompany_OID",
  "mdn-subject": "Message be18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa has been
 accepted",
  "as2-to": "PartnerA_OID",
  "transfer-id": "dedf4601-4e90-4043-b16b-579af35e0d83",
  "file-path": "/amzn-s3-demo-bucket/as2testcell0000/openAs2/
TestOutboundSyncMdn-9lmCr79hV.dat",
  "as2-message-id": "fbe18db8-7361-42ff-8ab6-49ec1e435f34@c9c705f0baaaabaa",
  "timestamp": "2022-07-11T06:30:10.791274Z"
}
```

传输失败的示例出站文件：

```
{
  "failure-code": "HTTP_ERROR_RESPONSE_FROM_PARTNER",
  "status-code": "FAILED",
  "requester-content-type": "application/octet-stream",
  "subject": "Test run from Id da86e74d6e57464aae1a55b8596bad0a to partner
 9f8474d7714e476e8a46ce8c93a48c6c",
  "transfer-size": 3198,
  "requester-file-name": "openAs2TestOutboundWrongAs2Ids-necco-3VYn5n8wE.dat",
  "as2-message-id": "9a9cc9ab-7893-4cb6-992a-5ed8b90775ff@718de4cec1374598",
  "failure-message": "http://Test123456789.us-east-1.elb.amazonaws.com:10080 returned
 status 500 for message with ID 9a9cc9ab-7893-4cb6-992a-5ed8b90775ff@718de4cec1374598",
  "transfer-id": "07bd3e07-a652-4cc6-9412-73ffdb97ab92",
  "connector-id": "c-056e15cc851f4b2e9",
  "file-path": "/amzn-s3-demo-bucket-4c1tq6ohjt9y/as2IntegCell0002/openAs2/
openAs2TestOutboundWrongAs2Ids-necco-3VYn5n8wE.dat",
  "timestamp": "2022-07-11T21:17:24.802378Z"
}
```

传输成功的示例进站文件：

```
{
  "requester-content-type": "application/EDI-X12",
  "subject": "File openAs2TestInboundAsyncMdn-necco-5Ab6bTfCO.dat sent from MyCompany
 to PartnerA",
  "client-ip": "10.0.109.105",
  "requester-file-name": "openAs2TestInboundAsyncMdn-necco-5Ab6bTfCO.dat",
  "as2-from": "MyCompany_OID",
```

```
  "status-code": "COMPLETED",
  "disposition": "automatic-action/MDN-sent-automatically; processed",
  "transfer-size": 1050,
  "mdn-subject": "Message Disposition Notification",
  "as2-message-id": "OPENAS2-11072022233606+0000-5dab0452-0ca1-4f9b-b622-
fba84effff3c@MyCompany_OID_PartnerA_OID",
  "as2-to": "PartnerA_OID",
  "agreement-id": "a-f5c5cbea5f7741988",
  "file-path": "processed/openAs2TestInboundAsyncMdn-
necco-5Ab6bTfCO.OPENAS2-11072022233606+0000-5dab0452-0ca1-4f9b-b622-
fba84effff3c@MyCompany_OID_PartnerA_OID.dat",
  "server-id": "s-5f7422b04c2447ef9",
  "timestamp": "2022-07-11T23:36:36.105030Z"
}
```

传输失败的示例进站文件：

```
{
  "failure-code": "INVALID_REQUEST",
  "status-code": "FAILED",
  "subject": "Sending a request from InboundHttpClientTests",
  "client-ip": "10.0.117.27",
  "as2-message-id": "testFailedLogs-TestRunConfig-Default-inbound-direct-
integ-0c97ee55-af56-4988-b7b4-a3e0576f8f9c@necco",
  "as2-to": "0beff6af56c548f28b0e78841dce44f9",
  "failure-message": "Unsupported date format: 2022/123/456T",
  "agreement-id": "a-0ceec8ca0a3348d6a",
  "as2-from": "ab91a398aed0422d9dd1362710213880",
  "file-path": "failed/01187f15-523c-43ac-9fd6-51b5ad2b08f3.testFailedLogs-
TestRunConfig-Default-inbound-direct-integ-0c97ee55-af56-4988-b7b4-a3e0576f8f9c@necco",
  "server-id": "s-0582af12e44540b9b",
  "timestamp": "2022-07-11T06:30:03.662939Z"
}
```

为 AS2 消息自定义 HTTP 标头

向贸易伙伴发送 AS2 消息时，您可能需要自定义 HTTP 标头以满足特定要求或增强与合作伙伴 AS2 服务器配置的兼容性。此 Amazon CloudFormation 模板创建了一个基础架构，用于为通过发送的 AS2 消息启用自定义 HTTP 标头 Amazon Transfer Family。它设置了充当代理的 Amazon API Gateway 和 Lambda 函数，允许动态修改交易伙伴 AS2 服务器所需的标头。

使用此模板执行以下操作：

- 向出站 AS2 消息添加自定义 HTTP 标头
- 使用自定义值覆盖默认标题值

> **Important**
>
> 覆盖默认标头值时要小心，因为这可能会导致发送失败：需要一些 AS2 标头。

- 确保与具有特定标题要求的贸易伙伴兼容

模板概述

该模板创建了以下主要组件：

- 用于处理和转发消息的 Lambda 函数 AS2
- 用于公开 Lambda 函数的亚马逊 API Gateway
- Lambda 函数的 IAM 角色和权限
- 支持 HTTPS 的条件资源

模板文件可在此处获得：动态 HTTP 标头模板。

工作方式

1. Amazon API Gateway 接收来自的传入 AS2 消息 Amazon Transfer Family。
2. 该请求被转发到 Lambda 函数。
3. Lambda 函数处理请求，根据需要添加或修改标头。
4. 然后，修改后的请求会被转发到合作伙伴的 AS2 服务器。
5. 来自合作伙伴服务器的响应将通过 Lambda 和 Amazon API Gateway 返回到。 Amazon Transfer Family

主要功能

- 动态标题修改：允许自定义主题标题和添加其他必需的标题。
- P@@ rotocol Support：可同时使用 HTTP 和 HTTPS 协议。
- 灵活配置：允许指定合作伙伴主机、端口和路径。

实施详情

该模板实现了以下关键组件：

Lambda 函数

该解决方案的核心是一个 Node.js Lambda 函数，该函数：

- 接收来自亚马逊 API Gateway 的请求
- 根据配置和传入的请求数据修改标头
- 将修改后的请求转发到合作伙伴的服务器 AS2
- 同时处理 HTTP 和 HTTPS 协议
- 包括错误处理和日志记录

Amazon API Gateway

HTTP API 设置为：

- 接收传入的 AS2 消息
- 将请求路由到 Lambda 函数
- 将回复返回到 Amazon Transfer Family

模板参数

按如下方式输入模板参数信息。请注意，所有这些参数都是字符串。

- `Environment`: 此参数用于命名模板创建的资源：无论它们是用于开发环境还是生产环境。有效值为 dev 和 prod。
- `PartnerHost`： AS2 伙伴服务器的 IP 地址或主机名。
- `PartnerPort`: AS2 伙伴服务器的端口号。如果未指定，则 HTTP 的默认值为 80，HTTPS 的默认值为 443。
- `PartnerPath`: 伙伴服务器上 AS2 终端节点的路径
- `ProtocolType`：用于 AS2 通信的协议：有效值为 HTTP 和 HTT PS。

有条件的资源

为了支持 HTTPS，模板会有条件地创建：

- 用于 CA 证书的 Lambda 层
- Lambda 函数中特定于 HTTPS 的配置

部署和使用

使用 CloudFormation 模板自定义 AS2 HTTP 标头

1. 在 https://console.aws.amazon.com/cloudformation 上打开 Amazon CloudFormation 控制台。
2. 在左侧导航窗格中，选择堆栈。
3. 选择创建堆栈，然后选择使用新资源（标准）。
4. 在 “先决条件-准备模板” 部分，选择 “选择现有模板”。
5. 复制此链接，即动态 HTTP 标头模板，然后将其粘贴到 Amazon S3 网址字段中。
6. 选择下一步。
7. 在参数详细信息中填写您的信息。详情请参阅模板参数。
8. 选择下一步。在配置堆栈选项页面上，再次选择下一步。
9. 查看您正在创建的堆栈的详细信息，然后选择创建堆栈。

> **Note**
>
> 在页面底部的能力下，您必须确认这 Amazon CloudFormation 可能会创建 Amazon Identity and Access Management (IAM) 资源。

部署此 Amazon CloudFormation 堆栈后：

1. 请注意堆栈输出中提供的 Amazon API Gateway 终端节点网址。
2. 更新您的现有 Amazon Transfer Family 连接器以使用这个新的 Amazon API Gateway 终端节点。
3. 现在，该解决方案将处理 AS2 消息，根据配置添加或修改标头。

> **Warning**
>
> 仅修改主题标题或添加合作伙伴明确期望的标题。更改其他标头可能会导致传输失败。

监控 AS2 使用情况

您可以使用Amazon CloudWatch 和Amazon监控 AS2 活动 Amazon CloudTrail。要查看其他 Transfer Family 服务器指标，请参阅 Amazon Amazon Transfer Family 服务器 CloudWatch 登录

AS2 指标

指标	描述
`InboundMessage`	成功从交易伙伴处收到的 AS2 消息总数。 单位：计数 时间：5 分钟
`InboundFailedMessage`	未成功从贸易伙伴处收到的 AS2 消息总数。也就是说，交易伙伴发送了一条消息，但是 Transfer Family 服务器无法成功处理该消息。 单位：计数 时间：5 分钟
`OutboundMessage`	从 Transfer Family 服务器成功发送给交易伙伴的 AS2 消息总数。 单位：计数 时间 = 5 分钟
`OutboundFailedMessage`	未成功发送给贸易伙伴的 AS2 消息总数。也就是说，它们是从 Transfer Family 服务器发送的，但交易伙伴没有成功接收。 单位：计数

指标	描述
	时间：5 分钟
DaysUntilExpiry	证书到期前的天数由导入时证书上的InactiveDate 设置决定。 单位：计数 尺寸：CertificateId ，Description （如果提供） 周期：1 天 有关更多信息，请参阅 AS2 证书轮换。

AS2 状态码

下表列出了您或您的合作伙伴发送 AS2 消息时可以记录到 CloudWatch 日志中的所有状态代码。不同的消息处理步骤适用于不同的消息类型，并且仅用于监控。“已完成” 和 “失败” 状态表示处理的最后一步，在 JSON 文件中可见。

代码	描述	处理完成了吗？
处理	该消息正在转换为其最终格式。例如，解压缩和解密步骤都具有此状态。	否
MDN_TRANSM	消息处理正在发送 MDN 响应。	否
MDN_RECEIVE	消息处理正在收到 MDN 响应。	否
COMPLETED	消息处理已成功完成。此状态包括为入站消息或出站消息的 MDN 验证发送 MDN 的时间。	是

代码	描述	处理完成了吗？
FAILED	消息处理失败。有关错误代码的列表，请参阅AS2 错误代码。	是

AS2 错误代码

下表列出并描述了您可能从 AS2文件传输中收到的错误代码。

AS2 错误代码

代码	错误	描述和解决方法
ACCESS_DENIED	• 访问遭拒绝。检查您的访问角色具有必要的权限。 • 文件路径无效 *send-file-path* • 无法通过以下方式获取凭证 ErrorCode：*error-code*	在处理其中任何一个 SendFilePaths 都无效或格式错误的 StartFileTransfer 请求时发生。也就是说，路径缺少 Amazon S3 存储桶名称，或者路径包含无效字符。如果 Transfer Family 未能担任访问角色或日志记录角色，也会发生这种情况。 确保路径包含有效的 Amazon S3 存储桶名称和密钥名称。
AGREEMENT_NOT_FOUND	未找到协议。	要么找不到协议，要么该协议与非活动配置文件相关联。 在 Transfer Family 服务器中更新协议，使其包含活动的配置文件。
CONNECTOR_NOT_FOUND	找不到连接器或相关配置。	要么找不到连接器，要么该连接器与非活动配置文件相关联。

代码	错误	描述和解决方法
		更新连接器以包含活动配置文件。
CREDENTIALS_RETRIEVAL_FAILED	1. 在 Secrets Manager 中找不到密钥。 2. 无法访问 Secrets Manager。 3. 无法解密 Secrets Manager 中的密钥。 4. 由于节流，无法获取密钥值。	对于 AS2 基本身份验证，密钥的格式必须正确。以下解决方案对应于上一栏中列出的错误。 1. 确保密钥 ID 正确无误。 2. 确保访问角色具有读取密钥的相应权限。访问权限角色必须提供对 StartFileTransfer 请求中所使用文件位置父目录的读取和写入权限。此外，确保角色对拟定发送 StartFileTransfer 的父目录提供读取和写入访问权限。 3. 如果使用客户管理的密钥作为密钥，请确保访问角色拥有对 Amazon Key Management Service (Amazon KMS) 密钥的权限。 4. 有关适用的限额，请参阅 处理密钥的限额。
DECOMPRESSION_FAILED	无法解压缩消息。	要么发送的文件已损坏，要么压缩算法无效。 重新发送消息并验证使用了 ZLIB 压缩，或者在未启用压缩的情况下重新发送消息。

代码	错误	描述和解决方法
DECRYPT_FAILED	无法解密消息。*message-ID* 确保合作伙伴拥有正确的公共加密密钥。	解密失败。 确认合作伙伴使用有效证书发送了有效负载，并且使用有效加密算法执行了加密。
DECRYPT_FAILED_INVALID_SMIME_FORMAT	无法解析封装的 mimePart。	MIME 有效负载要么已损坏，要么采用不支持的 SMIME 格式。 发送者应确保他们使用的格式受到支持，然后重新发送有效负载。
DECRYPT_FAILED_NO_DECRYPTION_KEY_FOUND	未找到匹配的解密密钥。	没有为合作伙伴配置文件分配与消息匹配的证书，或者与消息匹配的证书现已过期或不再有效。 您必须更新合作伙伴配置文件并确保其中包含有效的证书。
DECRYPT_FAILED_UNSUPPORTED_ENCRYPTION_ALG	使用不支持的算法请求了 SMIME Payload 解密，编号为：。*encryption-ID*	远程发送方发送了使用不支持的加密算法的 AS2 有效负载。 发件人必须选择 Amazon Transfer Family支持的加密算法。
DUPLICATE_MESSAGE	重复或双重处理步骤。	有效负载具有重复的处理步骤。例如，有两个加密步骤。 只需一步即可重新发送消息，完成签名、压缩和加密。

代码	错误	描述和解决方法
ENCRYPT_FAILED_NO_ENCRYPTION_KEY_FOUND	在配置文件中找不到有效的公共加密证书：*local-profile-ID*	Transfer Family 正在尝试加密出站消息，但找不到本地配置文件的加密证书。 解决办法选项： • 确保本地配置文件附有用于加密的证书和私钥。 • 确保加密证书当前处于活动状态。
ENCRYPTION_FAILED	无法加密文件*file-name* 。	要发送的文件不可用于加密。 确认文件位于预期 AS2 位置并且 Amazon Transfer Family 有权读取该文件。
FILE_SIZE_TOO_LARGE	文件太大。	当发送或接收超过文件大小限制的文件时，就会发生这种情况。
HTTP_ERROR_RESPONSE_FROM_PARTNER	*partner-URL* ID 为 = *message-ID* 的消息返回状态 400。	与合作伙伴的 AS2 服务器通信返回了意外的 HTTP 响应代码。 合作伙伴可能能够从其 AS2 服务器日志中提供更多诊断。
INSUFFICENT_MESSAGE_SECURITY_UNENCRYPTED	需要加密。	合作伙伴向 Transfer Family 发送了一封未加密的消息，但该消息不受支持。发件人必须使用加密的有效负载。
INVALID_ENDPOINT_PROTOCOL	仅支持 HTTP 和 HTTPS。	您必须在 AS2 连接器配置中指定 HTTP 或 HTTPS 作为协议。

代码	错误	描述和解决方法
INVALID_REQUEST	1. 消息标题有问题。 2. 无法解析密钥 JSON。 密钥 JSON 与预期格式不符。 3. 密钥必须是 JSON 字符串。 4. 用户名不得包含冒号。 用户名不得包含控制字符。 用户名只能包含 ASCII 字符。 密码不得包含控制字符。 密码只能包含 ASCII 字符。	此错误有多种原因。以下解决方案对应于上一栏中列出的错误。 1. 选中 as2-from 和 as2-to 字段。确保 MDN 格式的原始消息 ID 准确无误。还要确保消息 ID 格式不缺少任何 AS2 标题。 2. 确保密钥值与记录的格式相匹配，如 为 AS2连接器启用基本身份验证 中所述。 3. 确保密钥以字符串形式提供，而不是以二进制形式提供。 4. 对用户名或密码进行必要的更正。
INVALID_URL_FORMAT	网址格式无效：*URL*	当您使用配置了格式错误的 URL 的连接器发送出站消息时，就会发生这种情况。 确保为连接器配置了有效的 HTTP 或 HTTPS URL。
MDN_RESPONSE_INDICATES_AUTHENTICATION_FAILED	不适用	接收方无法对发送者进行身份验证。交易伙伴向 Transfer Family 返回 MDN，其带有处置修饰符 错误：authentication-failed。

代码	错误	描述和解决方法
MDN_RESPONSE_INDICATES_DECOMPRESSION_FAILED	不适用	当接收者无法解压缩消息内容时，就会发生这种情况。交易伙伴向 Transfer Family 返回 MDN，其带有处置修饰符 错误：decompression-failed。
MDN_RESPONSE_INDICATES_DECRYPTION_FAILED	不适用	接收者无法解密消息内容。交易伙伴向 Transfer Family 返回 MDN，其带有处置修饰符 错误：authentication-failed。
MDN_RESPONSE_INDICATES_INSUFFICIENT_MESSAGE_SECURITY	不适用	接收者希望对消息进行签名或加密，但事实并非如此。贸易伙伴向 Transfer Family 返回带有处置修饰符的 MDN 错误：insufficient-message-security。 在连接器上启用签名 and/or 加密，以符合交易伙伴的期望。
MDN_RESPONSE_INDICATES_INTEGRITY_CHECK_FAILED	不适用	接收者无法验证内容的完整性。贸易伙伴向 Transfer Family 返回带有处置修饰符的 MDN 错误： integrity-check-failed。
PATH_NOT_FOUND	无法创建目录*file-path* 。找不到父路径。	Transfer Family 正在尝试在客户的 Amazon S3 存储桶中创建目录，但未找到该存储桶。 确保 StartFileTransfer 命令中提到的每个路径都包含现有存储桶的名称。

代码	错误	描述和解决方法
SEND_FILE_NOT_FOUND	*file-path* 未找到文件路径。	Transfer Family 在发送文件操作中找不到该文件。 检查配置的主目录和路径有效，以及 Transfer Family 具有该文件的读取权限。
SERVER_NOT_FOUND	找不到与消息关联的服务器。	Transfer Family 在收到消息时找不到服务器。如果在处理传入消息的过程中删除了服务器，则可能会发生这种情况。
SERVER_NOT_ONLINE	服务器*server-ID* 未联机。	Transfer Family 服务器处于脱机状态。 启动服务器，使其可以接收和处理消息。
SIGNING_FAILED	对文件签名失败。	要发送的文件不可用于签名，或者无法进行签名。 确认文件位于预期 AS2 位置并且 Amazon Transfer Family 有权读取该文件。
SIGNING_FAILED_NO_SIGNING_KEY_FOUND	找不到个人资料的证书:*local-profile-ID* .	正在尝试对出站消息进行签名，但找不到本地配置文件的签名证书。 解决办法选项： • 确保本地配置文件附有证书和用于签名的私钥。 • 确保签名证书当前处于活动状态。

代码	错误	描述和解决方法
UNABLE_RESOLVE_HOST_TO_IP_ADDRESS	无法将主机名解析为 IP 地址。	Transfer Family 无法在 AS2 连接器中配置的公共 DNS 服务器上执行 DNS 到 IP 地址的解析。 更新连接器以指向有效的合作伙伴 URL。
UNABLE_TO_CONNECT_TO_REMOTE_HOST_OR_IP	与端点的连接超时。	Transfer Family 无法与配置的伙伴的 AS2 服务器建立套接字连接。 检查合作伙伴的 AS2 服务器在配置的 IP 地址上是否可用。
UNABLE_TO_RESOLVE_HOSTNAME	无法解析主机名*hostname*。	Transfer Family 服务器无法使用公共 DNS 服务器解析伙伴的主机名。 检查配置的主机已注册以及 DNS 记录有时间发布。
VERIFICATION_FAILED	AS2 消息签名验证失败*message-ID* 或 MIC 代码不匹配。	检查发件人的签名证书与远程配置文件的签名证书相匹配。还要检查 MIC 算法是否兼容 Amazon Transfer Family。

代码	错误	描述和解决方法
VERIFICATION_FAILED_NO_MATCHING_KEY_FOUND	• 在配置文件中找不到与消息签名匹配的公共证书:*partner-profile-ID* 。 • 无法为不存在的配置文件获取证书:。*partner-profile-ID* • 在配置文件中找不到有效的证书:*partner-profile-ID* 。	Amazon Transfer Family 正在尝试验证收到的消息的签名，但找不到与合作伙伴配置文件匹配的签名证书。 解决办法选项： • 确保合作伙伴配置文件附有签名证书。 • 确保证书当前处于活动状态。 • 确保证书是合作伙伴的正确签名证书。

证书到期监控

Amazon Transfer Family 自动监控 AS2 证书的到期日期，并发布 Amazon CloudWatch 指标以帮助您跟踪证书何时接近到期。这使您可以主动管理证书续订并避免服务中断。

DaysUntilExpiry 指标

当您导入证书以供 AS2 使用时，Transfer Family 会自动创建一个名为的 CloudWatch 指标`DaysUntilExpiry`。此指标根据`InactiveDate`您在导入证书时指定的时间，跟踪证书到期前的剩余天数。

指标详情：

- 指标名称：`DaysUntilExpiry`
- 命名空间：`AWS/Transfer`
- 尺寸：`CertificateId`（始终存在），`Description`（如果在导入证书时提供）
- 单位：计数（天）
- 频率：每日发布

> **Important**
>
> 导入证书后，Transfer Family 可能需要整整一天的时间才能将该指标发送到您的账户。

随着证书的失效日期临近，该指标值每天减少一个。例如，如果证书的到期时间为 30 天，则该指标将显示 30 天，然后在第二天显示 29 天，依此类推。

证书监控的最佳实践

设置证书过期监控时，请遵循以下最佳实践：

- 设置多个警报阈值：为不同的时间段（例如，到期前 30 天、14 天和 7 天）创建警报，以便为证书续订提供充足的时间。
- 使用适当的统计数据：在创建警报时使用`Maximum`统计数据以确保捕获最新的指标值。
- 配置适当的警报操作：设置通知以提醒可以续订证书的相应团队成员。
- 测试您的警报：定期测试您的通知系统，确保警报正确传送。
- 记录您的流程：保留有关您的证书续订流程以及谁负责不同证书的文档。

警报配置示例

以下是针对不同通知场景的一些警报配置示例：

30 天到期警告

创建警报，当证书距离到期时间不超过 30 天时触发：

- 指标： DaysUntilExpiry
- 统计数据：Maximum
- 周期：1 天
- 阈值：30
- 比较：小于或等于阈值
- 缺失数据处理：将缺失的数据视为良好（不是泄露）

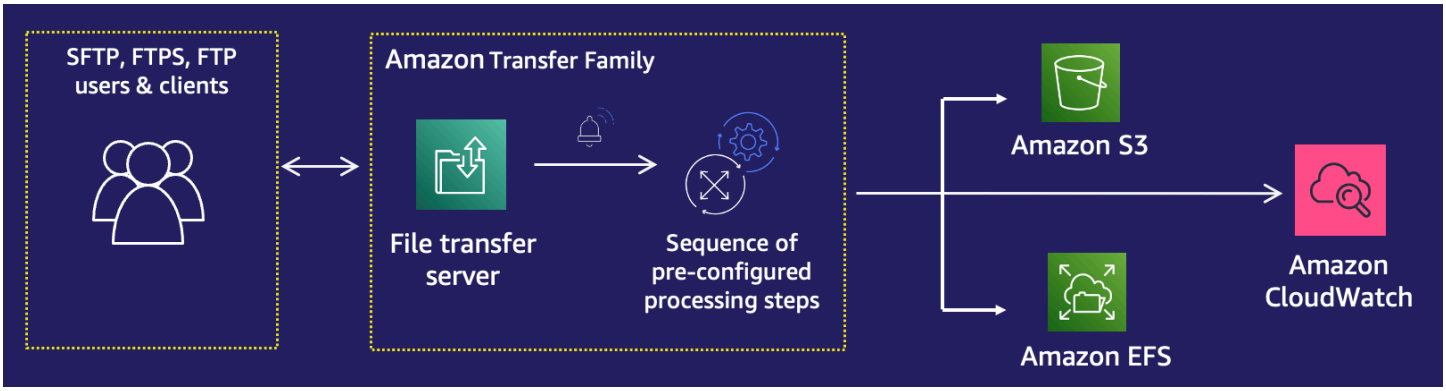
严重的 7 天到期警告

创建临界警报，当证书距离到期时间不超过 7 天时触发：

- 指标： DaysUntilExpiry
- 统计数据：Maximum
- 周期：1 天
- 阈值：7
- 比较：小于或等于阈值
- 缺失数据处理：将缺失的数据视为良好（不是泄露）

Amazon Transfer Family 托管工作流程

Amazon Transfer Family 支持文件处理的托管工作流程。借助托管工作流程，您可以在通过 SFTP、FTPS 或 FTP 传输文件后启动工作流程。使用此功能，您可以协调文件处理所需的所有必要步骤，从而安全且经济高效地满足 business-to-business (B2B) 文件交换的合规性要求。此外，您还可以从 end-to-end审计和可见性中受益。



通过协调文件处理任务，托管工作流可帮助您在下游应用程序使用数据之前对其进行预处理。此类文件处理任务可能包括：

- 将文件移动到用户特定的文件夹。
- 作为工作流的一部分对文件进行解密。
- 标记文件
- 通过创建 Amazon Lambda 函数并将其附加到工作流程来执行自定义处理。
- 文件成功传输后发送通知。（有关详细介绍此用例的博客文章，请参阅使用 Amazon Transfer Family 托管工作流程自定义文件传送通知。）

要快速复制和标准化组织中多个业务部门的常见上传后文件处理任务，您可以使用基础设施即代码 (IaC) 来部署工作流程。您可以指定要在完整上传的文件上启动托管工作流程。对于因会话过早断开连接而仅部分上传的文件，您也可以指定不同的托管工作流程。内置的异常处理功能可帮助您对文件处理结果做出快速反应，同时让您能够控制如何处理故障。此外，每个工作流程步骤都会生成详细的日志，您可以对其进行审核以跟踪数据沿袭。

要开始使用 ，请执行以下任务：

1. 根据您的要求将工作流程设置为包含预处理操作，例如复制、标记和其他步骤。有关详细信息，请参阅 创建工作流。

2. 配置执行角色，Transfer Family 会使用该角色来运行工作流程。有关详细信息，请参阅 适用于工作流程的 IAM 策略。
3. 将工作流程映射到服务器，以便在文件到达时，实时评估和启动此工作流程中指定的操作。有关详细信息，请参阅 配置和运行工作流程。

相关信息

- 要监控您的工作流程执行情况，请参阅 使用 T CloudWatch ransfer Family 服务器的指标。
- 有关详细的执行日志和故障排除信息，请参阅 使用 Amazon 解决与工作流程相关的错误 CloudWatch。
- Transfer Family 提供了一篇博客文章和一个研讨会，引导你完成文件传输解决方案的构建。该解决方案利用托管 SFTP/FTPS 终端节点 Amazon Transfer Family ，利用 Amazon Cognito 和 DynamoDB 进行用户管理。

  该博客文章可在使用 Amazon Cognito 作为身份提供商 Amazon Transfer Family 和 Amazon S3 上找到。您可以在此处查看研讨会的详细信息。
-
- 以下研讨会提供动手实验来构建全自动和事件驱动的工作流程，包括将文件传输到外部 SFTP 服务器或从外部 SFTP 服务器传输到 Amazon S3，以及这些文件的常见预处理和后处理：事件驱动的 MFT 研讨会。

  该视频提供了本次研讨会的详细介绍。

主题

- 创建工作流
- 使用预定义的步骤
- 使用自定义文件处理步骤
- 适用于工作流程的 IAM 策略
- 工作流程的异常处理
- 监控工作流程执行情况
- 通过模板创建工作流
- 从 Transfer Family 服务器中移除工作流
- 托管工作流限制和局限性

有关托管工作流程入门的更多帮助，请参阅使用工作 Amazon Transfer Family 流程构建云原生文件传输平台博客文章。

创建工作流

您可以使用创建托管工作流程 Amazon Web Services 管理控制台，如本主题所述。为了使工作流程创建过程尽可能简单，控制台中的大多数部分都提供了上下文帮助面板。

工作流程有两种步骤：

- 标称步骤 — 标称步骤是要应用于传入文件的文件处理步骤。如果您选择多个标称步骤，每个步骤将按线性序列处理。
- 异常处理步骤 — 异常处理程序是文件处理步骤，可在任何标称步骤失败或导致验证错误时 Amazon Transfer Family 执行。

创建工作流

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在左侧导航窗格中，选择工作流。
3. 在 工作流页面，选择 创建工作流。
4. 在创建工作流页面，输入描述。此描述显示在“工作流程”页面上。
5. 在标称步骤部分中，选择添加步骤。添加一个或多个步骤。
    a. 从可用选项中选择步骤类型。有关各种作业状态的更多信息，请参阅 the section called “使用预定义的步骤”。
    b. 选择“下一步”，然后为该步骤配置参数。
    c. 选择“下一步”，然后查看该步骤的详细信息。
    d. 选择“创建步骤”以添加该步骤并继续。
    e. 根据需要继续添加步骤。工作流中的最大步骤数为 8。
    f. 添加完所有必需的标称步骤后，向下滚动到“异常处理程序 - 可选”部分，然后选择“添加步骤”。

> **Note**
>
> 为便于您实时了解故障，我们建议您设置异常处理程序和步骤，以便在工作流程失败时执行。

6. 要配置异常处理程序，请按照与前面所述相同的方式添加步骤。如果某个文件导致任何步骤引发异常，则会逐一调用您的异常处理程序。
7. （可选）向下滚动到“标签”部分，然后为您的工作流程添加标签。
8. 检查配置并选择创建工作流。

> **Important**
>
> 创建工作流程后，您将无法对其进行编辑，因此请务必仔细查看配置。

配置和运行工作流程

在运行工作流程之前，您需要将其与 Transfer Family 服务器相关联。

将 Transfer Family 配置为对上传的文件运行工作流程

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在左侧导航窗格中，选择服务器。
   - 要将工作流程添加到现有服务器，请选择要用于工作流程的服务器。
   - 或者，创建一个新服务器并向其添加工作流程。有关更多信息，请参阅 配置 SFTP、FTPS 或 FTP 服务器端点。
3. 在服务器的详细信息页面上，向下滚动到其他详细信息部分，然后选择编辑。

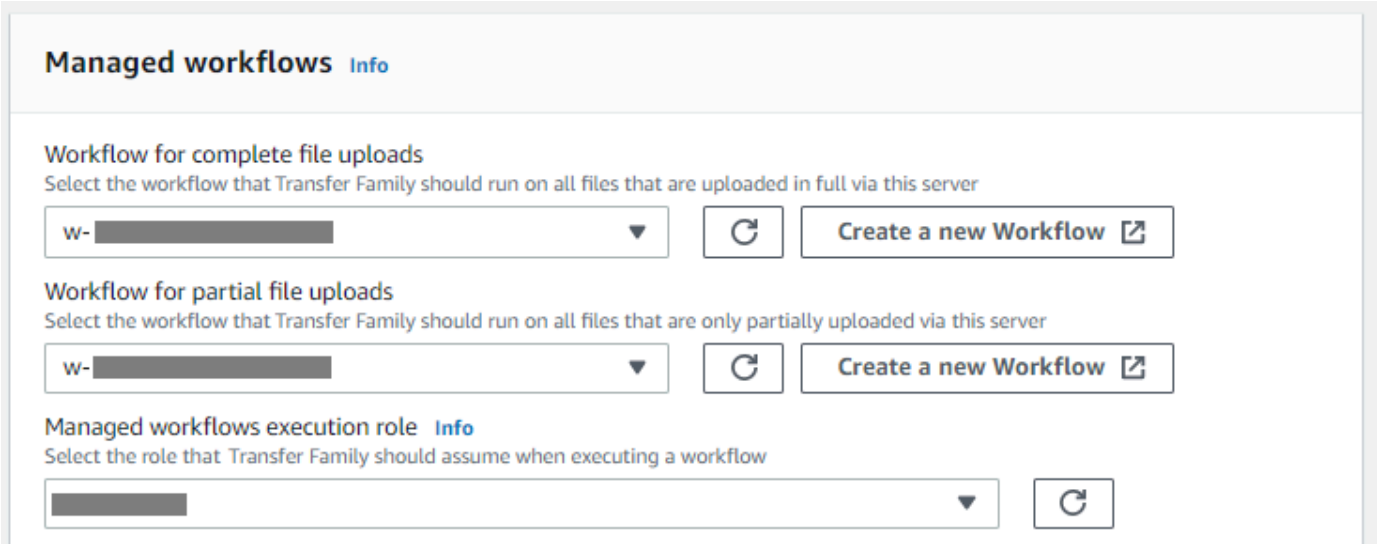
> **Note**
>
> 默认情况下，服务器没有任何关联的工作流程。您可以使用“其他详细信息”部分将工作流与所选服务器相关联。

4. 在编辑其他详细信息页面的托管工作流程部分，选择要在所有上传中运行的工作流程。

> **Note**
>
> 如果您还没有工作流，请选择“创建新的工作流程”来创建工作流程。

a. 选择要使用的工作流程 ID。

b. 选择执行角色。这是 Transfer Family 在执行工作流程步骤时所扮演的角色。有关更多信息，请参阅 适用于工作流程的 IAM 策略。选择 Save。



> **Note**
>
> 如果您不想再将工作流程与服务器关联，则可以移除关联。有关更多信息，请参阅 从 Transfer Family 服务器中移除工作流。

要执行工作流程

要执行工作流程，您需要将文件上传到您配置了关联工作流程的 Transfer Family 服务器。

> **Note**
>
> 无论何时从服务器上移除工作流程并用新的工作流程替换它，或者更新服务器配置（这会影响工作流程的执行角色），都必须等待大约 10 分钟才能执行新的工作流程。Transfer Family 服务器会缓存工作流程细节，服务器需要 10 分钟才能刷新其缓存。
> 此外，您必须注销所有活动的 SFTP 会话，然后等待 10 分钟重新登录才能看到更改。

Example

```
# Execute a workflow
> sftp bob@s-1234567890abcdef0.server.transfer.us-east-1.amazonaws.com

Connected to s-1234567890abcdef0.server.transfer.us-east-1.amazonaws.com.
sftp> put doc1.pdf
Uploading doc1.pdf to /amzn-s3-demo-bucket/home/users/bob/doc1.pdf
doc1.pdf                                                                    100% 5013KB
 601.0KB/s   00:08
sftp> exit
>
```

文件上传后，会对您的文件执行定义的操作。例如，如果您的工作流程包含复制步骤，则该文件将会被复制到您在该步骤中定义的位置。您可以使用 Amaz CloudWatch on Logs 来跟踪已执行的步骤及其执行状态。

查看工作流详细信息

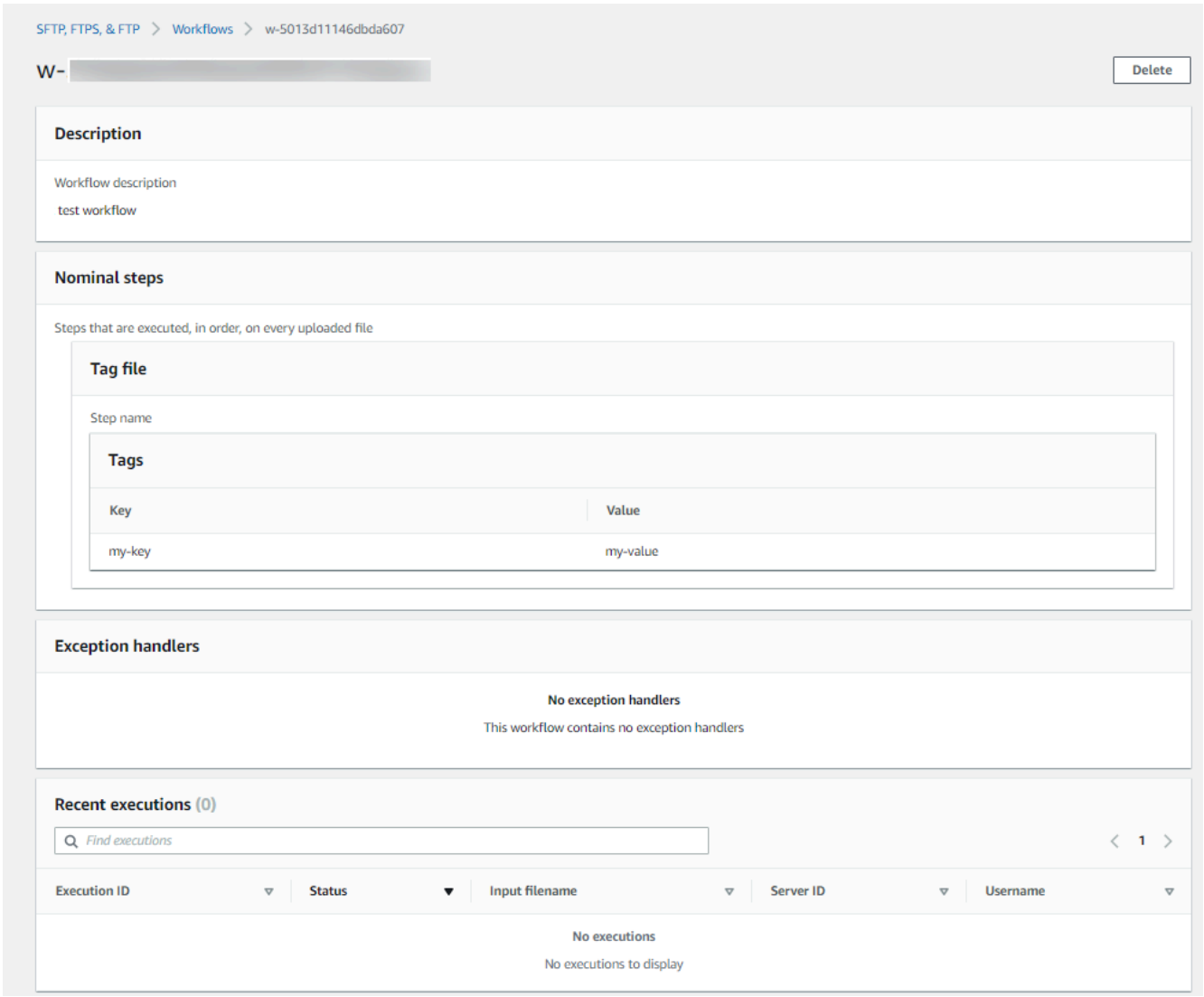
您可以查看有关先前创建的工作流程或工作流程执行的详细信息。要查看这些详细信息，您可以使用控制台或 Amazon Command Line Interface (Amazon CLI)。

Console

查看工作流详细信息

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在左侧导航窗格中，选择工作流。
3. 在“工作流程”页面上，选择一个工作流程。

   工作流程详细信息页面随即打开。



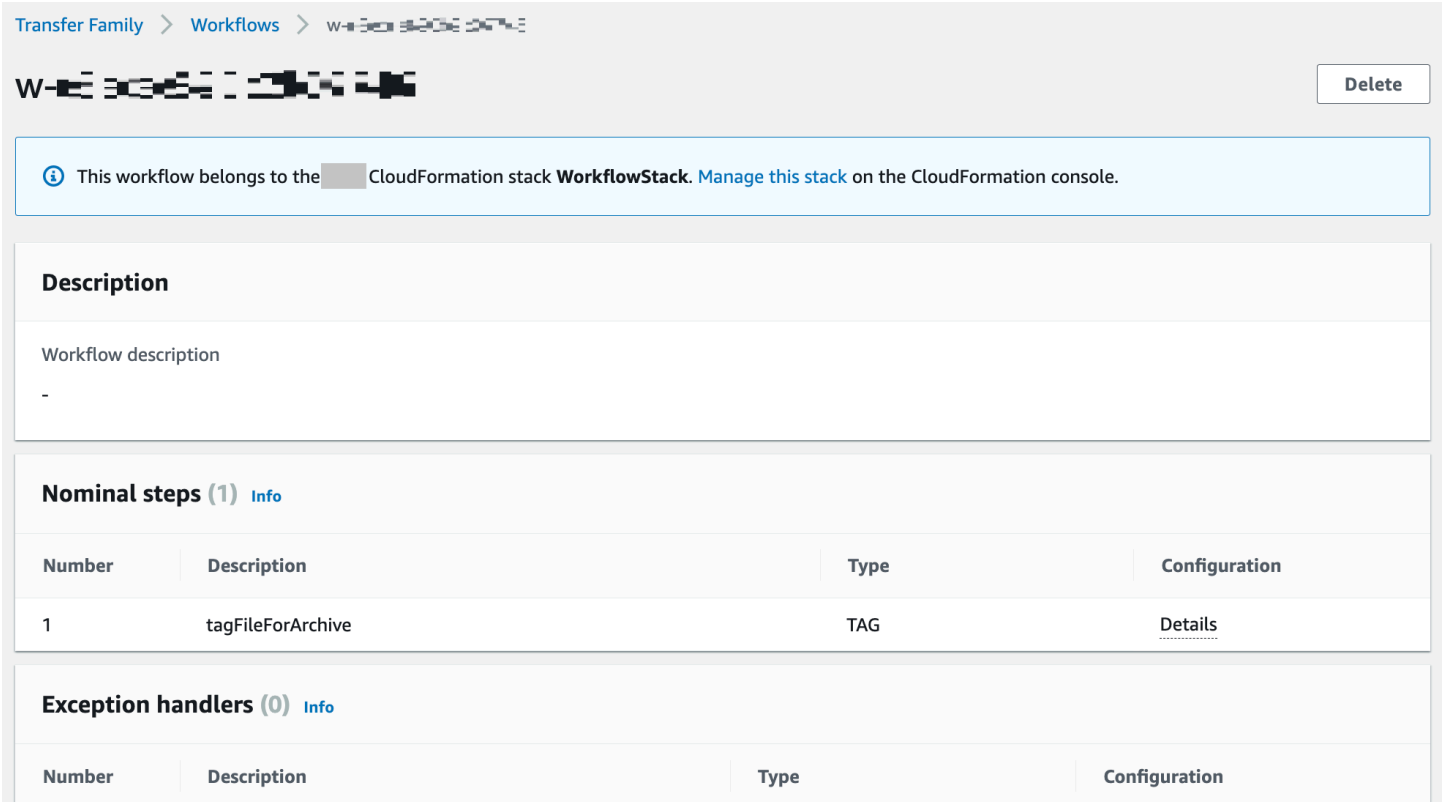
CLI

要查看工作流详细信息，请使用 `describe-workflow` CLI 命令，如以下示例所示。将工作流程 ID *w-1234567890abcdef0* 替换为您自己的值。有关更多信息，请参阅 Amazon CLI 命令引用中的 describe-workflow。

```
# View Workflow details
> aws transfer describe-workflow --workflow-id w-1234567890abcdef0
{
    "Workflow": {
        "Arn": "arn:aws:transfer:us-east-1:111122223333:workflow/
w-1234567890abcdef0",
        "WorkflowId": "w-1234567890abcdef0",
        "Name": "Copy file to shared_files",
```

```
        "Steps": [
            {
                "Type": "COPY",
                "CopyStepDetails": {
                "Name": "Copy to shared",
                "FileLocation": {
                    "S3FileLocation": {
                        "Bucket": "amzn-s3-demo-bucket",
                        "Key": "home/shared_files/"
                    }
                }
                }
            }
        ],
        "OnException": {}
    }
}
```

如果您的工作流程是作为 Amazon CloudFormation 堆栈的一部分创建的，则可以使用 Amazon CloudFormation 控制台 (https://console.aws.amazon.com/cloudformation) 管理工作流程。



使用预定义的步骤

创建工作流程时，可以选择添加本主题中讨论的以下预定义步骤之一。您还可选择添加自己的自定义文件处理步骤。有关更多信息，请参阅 the section called “使用自定义文件处理步骤”。

主题

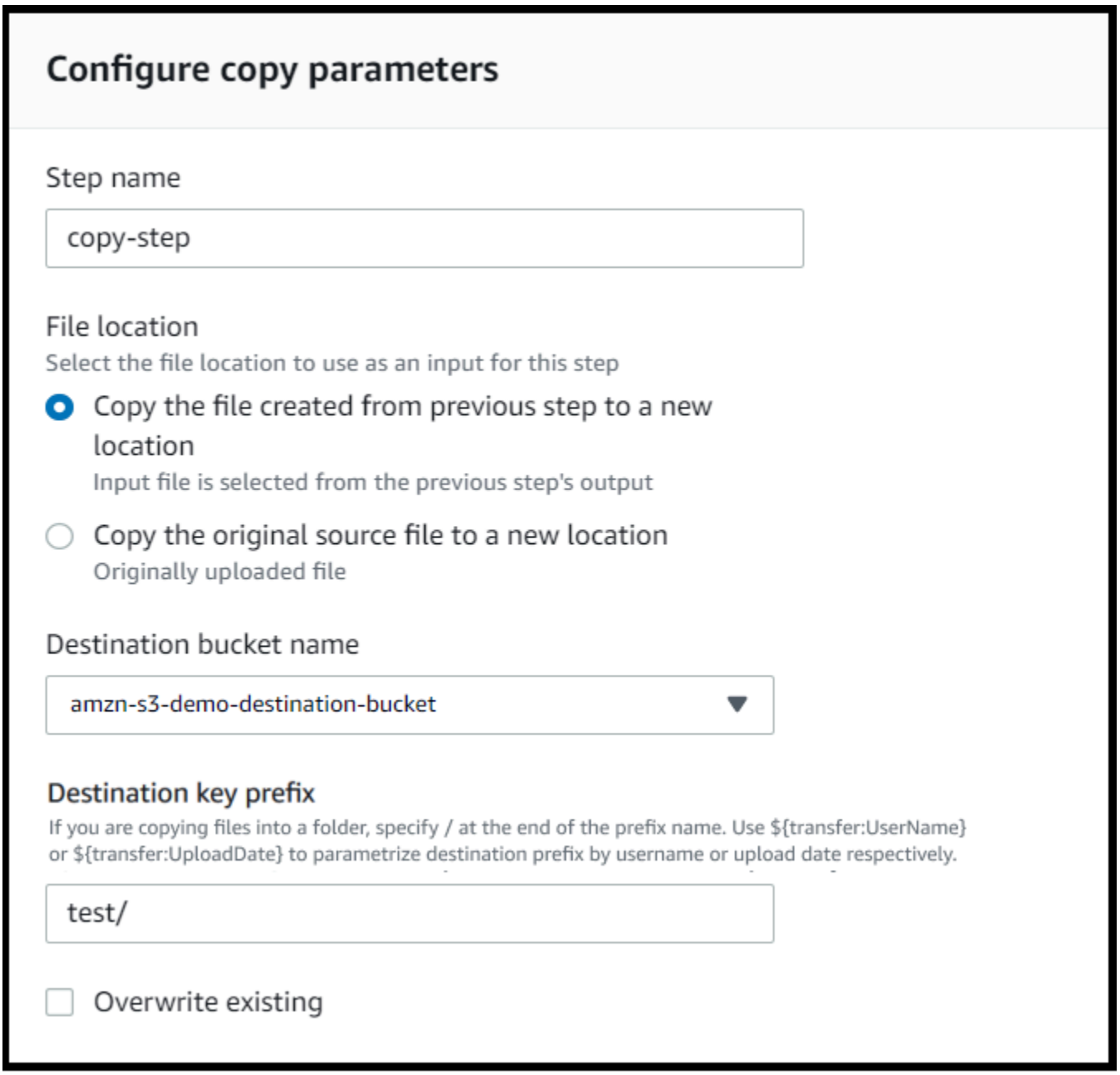
- 复制文件
- 解密文件
- 标记文件
- delete-file
- 工作流程的命名变量
- 标记和删除工作流程示例

复制文件

复制文件步骤会在新的 Amazon S3 位置创建已上传文件的副本。目前，您只能在 Amazon S3 上使用复制文件步骤。

以下复制文件步骤将文件复制到中的`test`文件夹*`amzn-s3-demo-destination-bucket`*。

如果复制文件步骤不是工作流程的第一步，则可以指定文件位置。通过指定文件位置，您可以复制上一步中使用的文件或上传的原始文件。您可以使用此功能制作原始文件的多个副本，同时保持源文件完好无损，便于文件存档和记录保留。有关示例，请参阅标记和删除工作流程示例。



提供存储桶和密钥的详细信息

您必须提供存储桶名称和复制文件步骤的目标密钥。密钥可以是路径名或文件名。将密钥视为路径名还是文件名取决于密钥是否以正斜杠 (/) 字符结尾。

如果最后一个字符是 /，则您的文件将被复制到此文件夹，并且其名称不会更改。如果最后一个字符是字母数字，则您上传的文件将被重命名为键值。在这种情况下，如果已存在具有该名称的文件，则相关行为将取决于“覆盖现有文件”字段的设置。

- 如果选择“覆盖现有文件”，则现有文件会被正在处理的文件替换。

- 如果未选择“覆盖现有文件”，则不会发生任何事情，并且工作流将会停止处理。

> **Tip**
>
> 如果在同一文件路径上执行并发写入，则在覆盖文件时可能会导致意外行为。

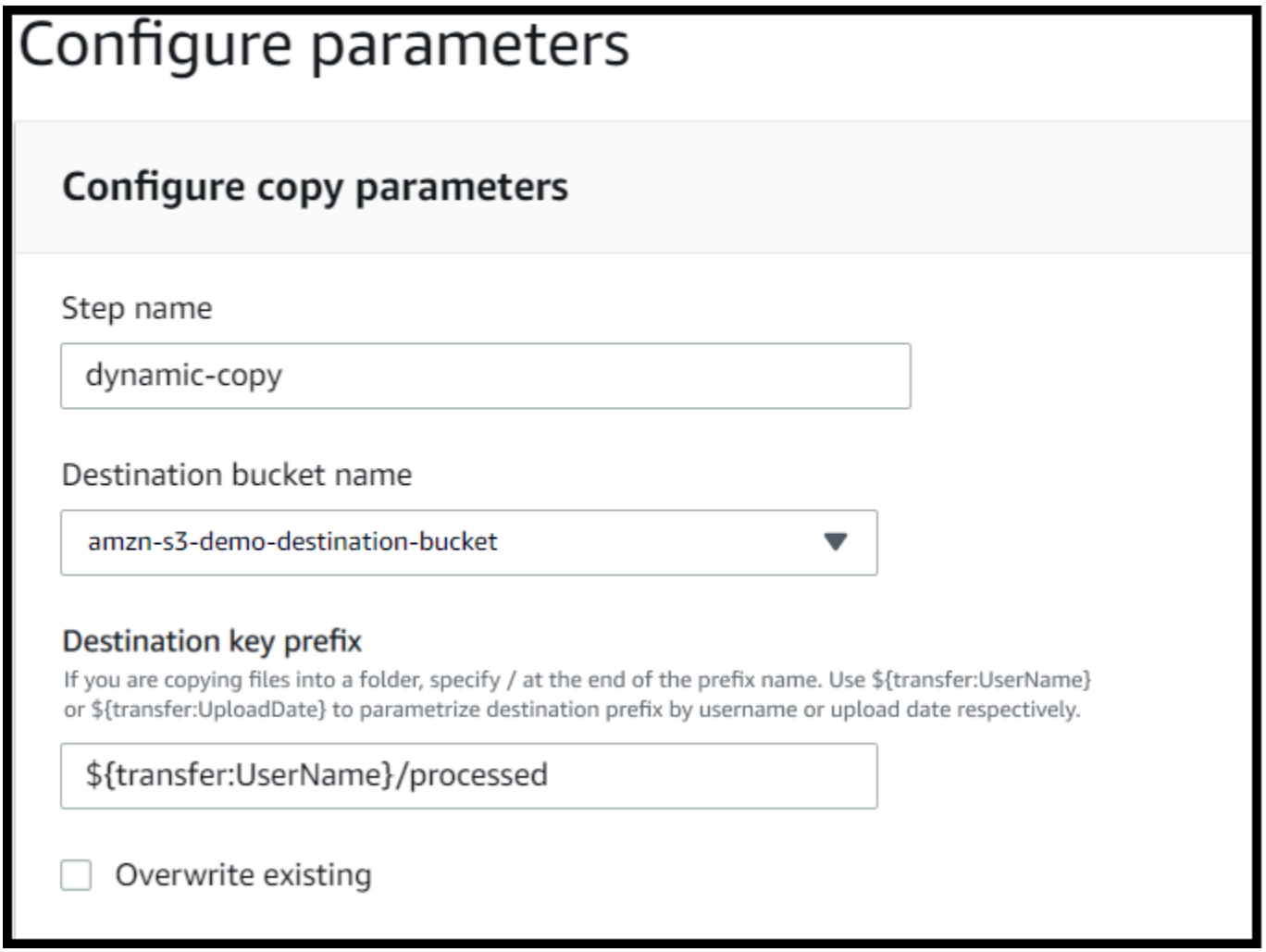
例如，如果您的键值是 `test/`，则您上传的文件将被复制到 `test` 文件夹。如果您的密钥值为 `test/today`，（并且选择了覆盖现有文件），则您上传的每个文件都将复制到该 `test` 文件夹中名为 `today` 的文件中，并且每个后续文件都会覆盖前一个文件。

> **Note**
>
> Amazon S3 支持存储桶和对象且没有层次结构。但是，您可以在对象键名称中使用前缀和分隔符来暗示层次结构，并以类似于文件夹的方式组织数据。

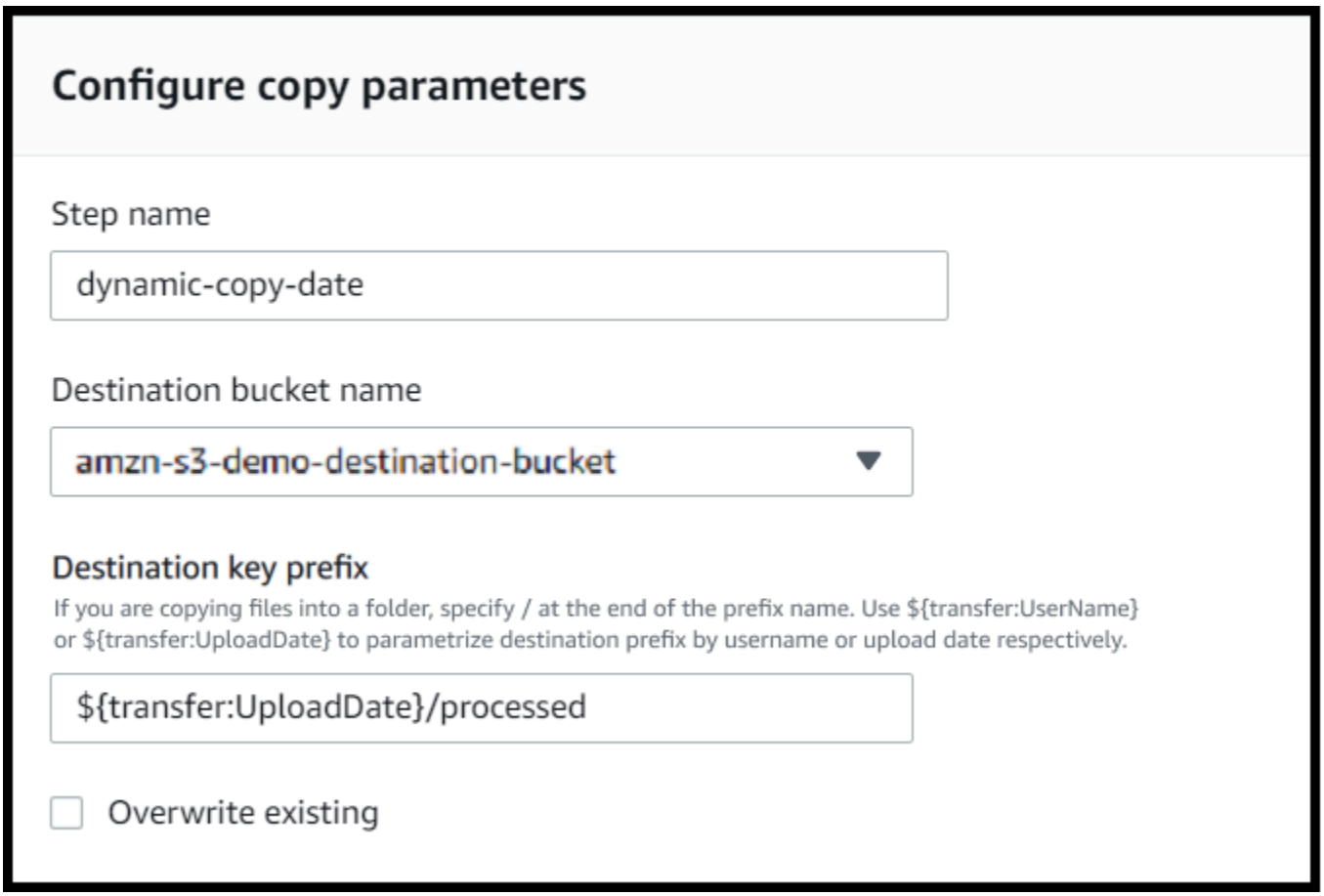
在复制文件步骤中使用命名变量

在复制文件步骤中，您可以使用变量将文件动态复制到用户特定的文件夹中。目前，您可以使用 `${transfer:UserName}` 或 `${transfer:UploadDate}` 作为变量，将文件复制到正在上传文件的给定用户的目标位置，或者根据当前日期将文件复制到目标位置。

在以下示例中，如果用户 `richard-roe` 上传文件，则该文件将被复制到 `amzn-s3-demo-destination-bucket/richard-roe/processed/` 文件夹。如果用户 `mary-major` 上传文件，则该文件将被复制到 `amzn-s3-demo-destination-bucket/mary-major/processed/` 文件夹。



同样，您可以使用 `${transfer:UploadDate}` 作为变量，将文件复制到以当前日期命名的目标位置。在以下示例中，如果您将目标设置为 2022 年 2 月 1 日的 `${transfer:UploadDate}/processed`，则上传的文件将复制到 `amzn-s3-demo-destination-bucket/2022-02-01/processed/` 文件夹。



您也可以同时使用这两个变量，将它们的功能结合起来。例如，您可以将 Destinati on key prefix 设置为**`folder/${transfer:UserName}/${transfer:UploadDate}/`**，这样可以创建嵌套文件夹`folder/marymajor/2023-01-05/`。

复制步骤的 IAM 权限

要允许复制步骤成功，请确保您的工作流程的执行角色包含以下权限。

```
{
    "Sid": "ListBucket",
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket"
    ]
}, {
    "Sid": "HomeDirObjectAccess",
    "Effect": "Allow",
    "Action": [
```

```
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObjectVersion",
        "s3:DeleteObject",
        "s3:GetObjectVersion"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}
```

> **Note**
>
> 仅当您未选择“覆盖现有文件”时，才需要 `s3:ListBucket` 权限。此权限会检查您的存储桶，以查看是否已存在同名文件。如果您选择了“覆盖现有文件”，则工作流程无需检查文件，只需将其写入即可。
> 如果您的 Amazon S3 文件有标签，则需要在 IAM 策略中添加一两个权限。
>
> - 为未进行版本控制的 Amazon S3 文件添加 `s3:GetObjectTagging`。
> - 为进行版本控制的 Amazon S3 文件添加 `s3:GetObjectVersionTagging`。

解密文件

Amazon 存储博客上有一篇文章描述了如何使用 Transfer Family Managed 工作流程、使用 PGP 加密和解密文件以及，无需编写任何代码即可简单地解密文件。 Amazon Transfer Family

支持的对称加密算法

对于 PGP 解密，Transfer Family 支持对称加密算法，这些算法用于加密 PGP 文件中的实际文件数据。

- 有关支持的对称加密算法的详细信息，请参见PGP 对称加密算法。
- 有关与这些对称算法一起使用的 PGP key pair 算法的信息，请参阅。PGP key pair 算法

在工作流程中使用 PGP 解密

Transfer Family 内置了对 Prety Good Privacy (PGP) 解密的支持。您可以对通过 SFTP、FTPS 或 FTP 上传到 Amazon Simple Storage Service (Amazon S3) 或 Amazon Elastic File System (Amazon EFS) 的文件使用 PGP 解密。

要使用 PGP 解密，必须创建并存储用于解密文件的 PGP 私钥。然后，您的用户可以使用相应的 PGP 加密密钥对文件进行加密，然后再将文件上传到您的 Transfer Family 服务器。收到加密文件后，可以在工作流程中解密这些文件。有关详细教程，请参阅 设置用于解密文件的托管工作流程。

有关支持的 PGP 算法和建议的信息，请参阅PGP 加密和解密算法。

若要在工作流程中使用 PGP 解密

1. 确定 Transfer Family 服务器来托管您的工作流，或创建新工作流。您需要先获得服务器 ID，然后才能使用正确的密钥名称在 Amazon Secrets Manager 中存储 PGP 密钥。
2. 将您的 PGP 密钥存储在所需的密钥名称 Amazon Secrets Manager 下。有关更多信息，请参阅管理 PGP 密钥。工作流程可以根据 Secrets Manager 中的密钥名称自动找到用于解密的正确 PGP 密钥。

   > **Note**
   >
   > 当你在 Secret Amazon Web Services 账户 s Manager 中存储密钥时，会产生费用。有关定价的信息，请参阅Amazon Secrets Manager 定价。

3. 使用您的 PGP 密钥对加密文件。（有关受支持的事件的列表，请参阅 支持的 PGP 客户端。）如果您使用命令行，请使用以下命令。要使用此命令，请将 *username@example.com* 替换为用于创建 PGP 密钥对的电子邮件地址。将 *testfile.txt* 替换为您要加密的文件名称。

   ```
   gpg -e -r username@example.com testfile.txt
   ```

   > **Important**
   >
   > 加密用于 Amazon Transfer Family 工作流程的文件时，请务必使用参数指定非匿名收件人。`-r`匿名加密（不指定收件人）可能会导致工作流程中的解密失败，因为系统无法识别要使用哪个密钥进行解密。有关此问题的调试信息，请访问解决匿名收件人加密问题。

4. 将加密文件上传至您的 Transfer Family 服务器。
5. 在工作流程中配置解密步骤。有关更多信息，请参阅 添加解密步骤。

添加解密步骤

解密步骤对作为工作流程一部分上传到 Amazon S3 或 Amazon EFS 的加密文件进行解密。有关配置解密的详细信息，请参阅 在工作流程中使用 PGP 解密。

在为工作流程创建解密步骤时，必须指定解密文件的目的地。如果目标位置已存在文件，则还必须选择是否覆盖现有文件。您可以使用 Ama CloudWatch zon Logs 监控解密工作流程结果并实时获取每个文件的审核日志。

为步骤选择解密文件类型后，将出现“配置参数”页面。填写“配置 PGP 解密参数”部分的值。

可用选项如下：

- 步骤名称 - 输入步骤的描述性名称。
- 文件位置 - 通过指定文件位置，您可以解密上一步中使用的文件或上传的原始文件。

> **Note**
>
> 如果此步骤是工作流的第一步，则此参数不可用。

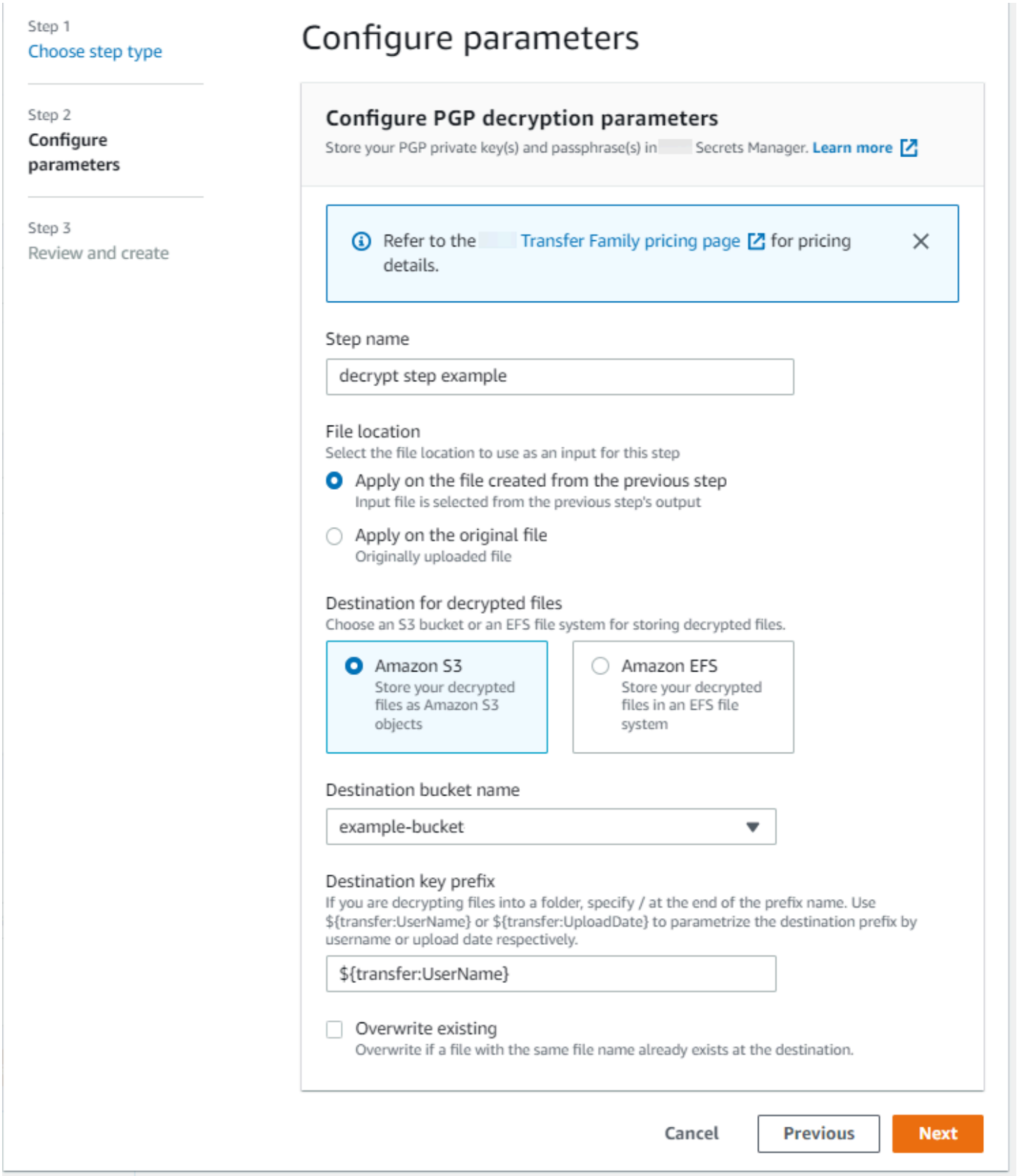
- 解密文件的目标 - 选择 Amazon S3 存储桶或 Amazon EFS 文件系统作为解密文件的目的地。
  - 如果您选择 Amazon S3，则必须提供目标存储桶名称和目标密钥前缀。要按用户名参数化目标密钥前缀，请为“**`${transfer:UserName}`**目标密钥前缀”输入 。同样，要按上传日期参数化目标密钥前缀，请为“目标密钥前缀”输入 **`${Transfer:UploadDate}`**。
  - 如果您选择 Amazon EFS，则必须提供目标文件系统和路径。

> **Note**
>
> 您在此处选择的存储选项必须与与此工作流程关联的 Transfer Family 服务器使用的存储系统相匹配。否则，当您尝试运行此工作流程时会收到错误。

- 覆盖现有文件 - 如果您上传了一个文件，并且目标位置上已经存在具有相同文件名的文件，则相关行为取决于此参数的设置：
  - 如果选择“覆盖现有文件”，则现有文件会被正在处理的文件替换。
  - 如果未选择“覆盖现有文件”，则不会发生任何事情，并且工作流将会停止处理。

> **Tip**
>
> 如果在同一文件路径上执行并发写入，则在覆盖文件时可能会导致意外行为。

以下屏幕截图显示了您可以为解密文件步骤选择的选项示例。


Step 1
Choose step type
Step 2
Configure parameters
Step 3
Review and create
Configure parameters
Configure PGP decryption parameters
Store your PGP private key(s) and passphrase(s) in Secrets Manager. Learn more
Refer to the Transfer Family pricing page for pricing details.
Step name
decrypt step example
File location
Select the file location to use as an input for this step
Apply on the file created from the previous step
Input file is selected from the previous step's output
Apply on the original file
Originally uploaded file
Destination for decrypted files
Choose an S3 bucket or an EFS file system for storing decrypted files.
Amazon S3
Store your decrypted files as Amazon S3 objects
Amazon EFS
Store your decrypted files in an EFS file system
Destination bucket name
example-bucket
Destination key prefix
If you are decrypting files into a folder, specify / at the end of the prefix name. Use ${transfer:UserName} or ${transfer:UploadDate} to parametrize the destination prefix by username or upload date respectively.
${transfer:UserName}
Overwrite existing
Overwrite if a file with the same file name already exists at the destination.
Cancel
Previous
Next

解密步骤的 IAM 权限

若要使解密步骤成功，请确保您的工作流程的执行角色包含以下权限。

```
{
    "Sid": "ListBucket",
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket"
    ]
}, {
    "Sid": "HomeDirObjectAccess",
    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObjectVersion",
        "s3:DeleteObject",
        "s3:GetObjectVersion"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}, {
    "Sid": "Decrypt",
    "Effect": "Allow",
    "Action": [
        "secretsmanager:GetSecretValue",
    ],
    "Resource": "arn:aws:secretsmanager:region:account-id:secret:aws/transfer/*"
}
```

Note

仅当您未选择“覆盖现有文件”时，才需要 `s3:ListBucket` 权限。此权限会检查您的存储桶，以查看是否已存在同名文件。如果您选择了“覆盖现有文件”，则工作流程无需检查文件，只需将其写入即可。

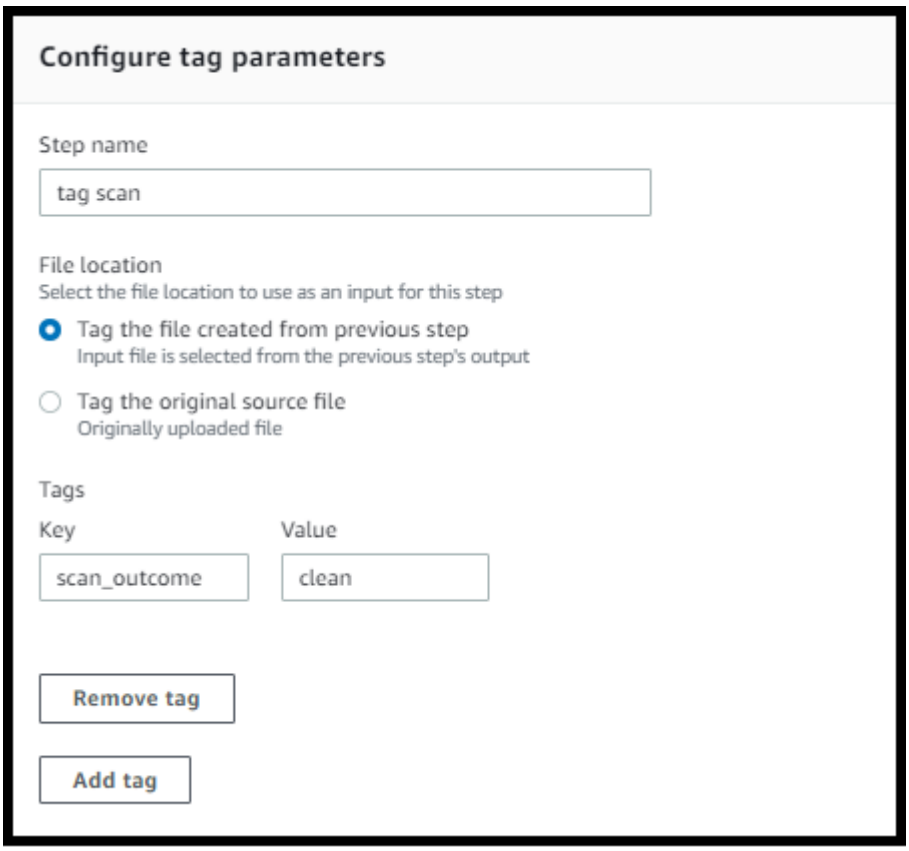
如果您的 Amazon S3 文件有标签，则需要在 IAM 策略中添加一两个权限。

- 为未进行版本控制的 Amazon S3 文件添加 `s3:GetObjectTagging`。
- 为进行版本控制的 Amazon S3 文件添加 `s3:GetObjectVersionTagging`。

标记文件

要标记传入文件以进行进一步的下游处理，请使用标记步骤。输入要分配给传入文件的标签值。当前，只有当您使用 Amazon S3 作为 Transfer Family 服务器存储时，才支持标签操作。

以下示例标签步骤将 `scan_outcome` 和 `clean` 分别指定为标签键和值。



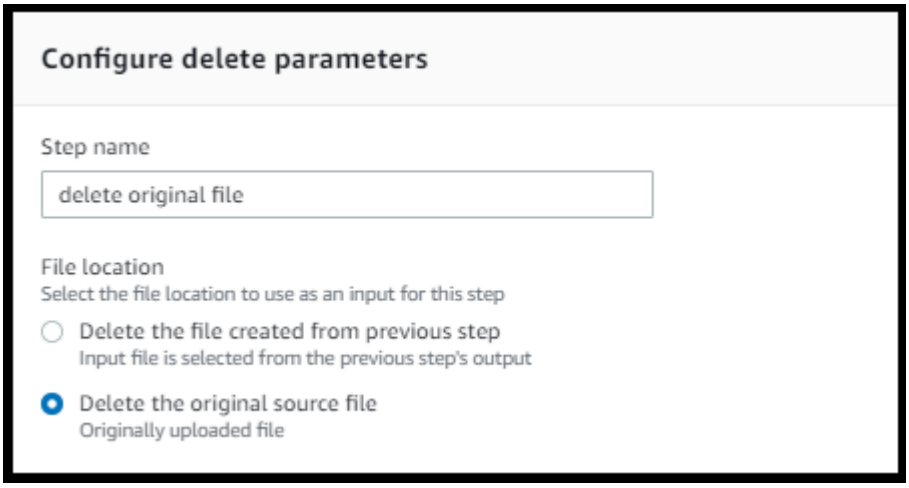
若要使标记步骤成功，请确保您的工作流程的执行角色包含以下权限。

```
{
            "Sid": "Tag",
            "Effect": "Allow",
            "Action": [
                "s3:PutObjectTagging",
                "s3:PutObjectVersionTagging"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
}
```

> **Note**
>
> 如果您的工作流程包含在复制或解密步骤之前运行的标签步骤，则需要向 IAM 策略添加一两个权限。
>
> - 为未进行版本控制的 Amazon S3 文件添加 `s3:GetObjectTagging`。
> - 为进行版本控制的 Amazon S3 文件添加 `s3:GetObjectVersionTagging`。

delete-file

要从上一个工作流程步骤中删除已处理的文件或删除最初上传的文件，请使用删除文件步骤。



若要使删除步骤成功，请确保您的工作流程的执行角色包含以下权限。

```
{
            "Sid": "Delete",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteObjectVersion",
                "s3:DeleteObject"
            ],
            "Resource": "arn:aws:secretsmanager:region:account-ID:secret:aws/transfer/
*"
        }
```

工作流程的命名变量

对于复制和解密步骤，您可以使用变量来动态执行操作。目前， Amazon Transfer Family 支持以下命名变量。

- 使用 `${transfer:UserName}` 根据上传文件的用户将文件复制或解密到目标位置。
- 使用 `${transfer:UploadDate}` 根据当前日期将文件复制或解密到目标位置。

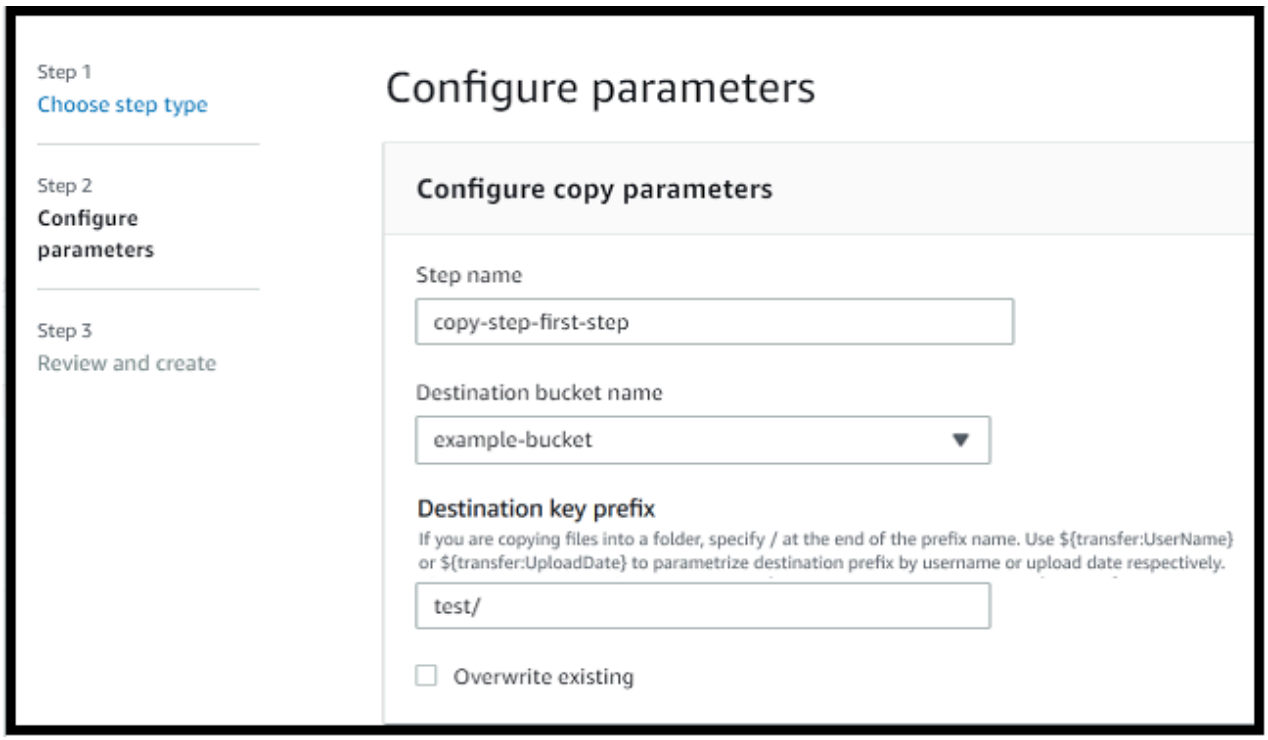
标记和删除工作流程示例

以下示例说明了一个工作流程，该工作流程用于标记需要由下游应用程序（例如数据分析平台）处理的传入文件。标记传入文件后，工作流程会删除最初上传的文件以节省存储成本。

Console

标记和移动工作流程示例

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在左侧导航窗格中，选择工作流。
3. 在 工作流页面，选择 创建工作流。
4. 在创建工作流页面，输入描述。此描述显示在“工作流程”页面上。
5. 添加第一步（复制）。
   a. 在标称步骤部分中，选择添加步骤。
   b. 选择复制文件，然后选择 下一步。
   c. 输入步骤名称，然后选择目标存储桶和密钥前缀。



d. 选择“下一步”，然后查看该步骤的详细信息。

e. 选择“创建步骤”以添加该步骤并继续。

6. 添加第二步（标记）。

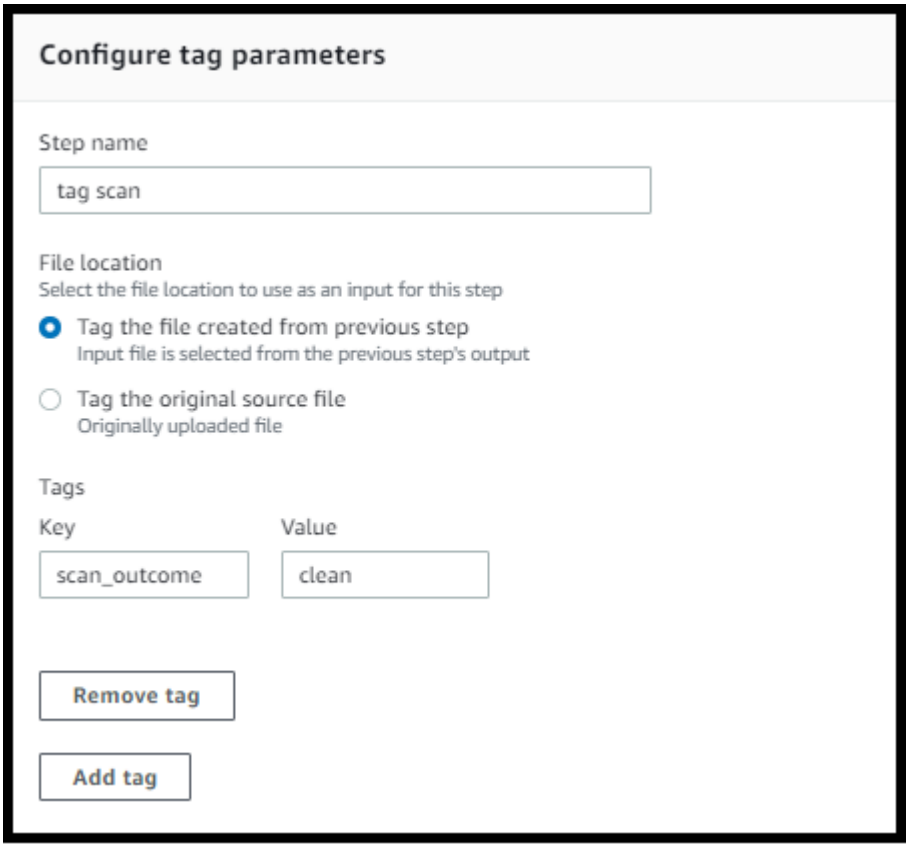
a. 在标称步骤部分中，选择添加步骤。

b. 选择您的标签文件，然后选择 下一步。

c. 输入步骤名称。

d. 在“文件位置”中，选择“标记上一步创建的文件”。

e. 输入键和值。



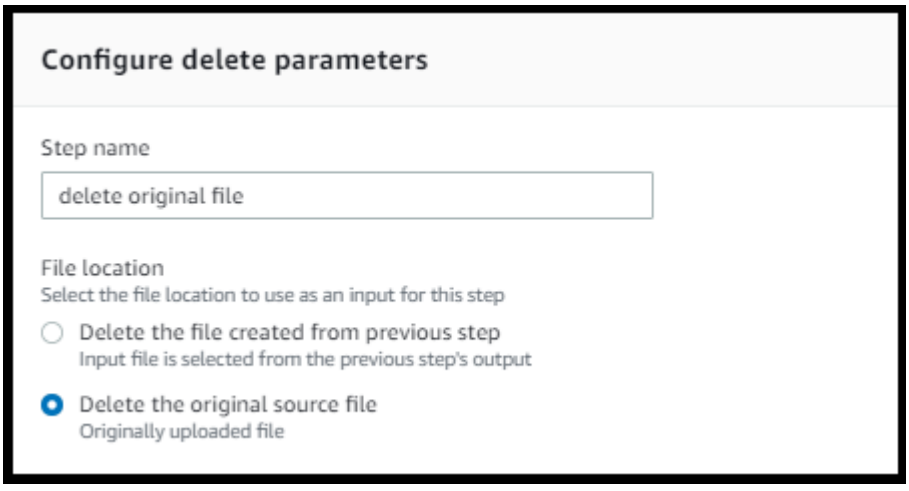
f. 选择“下一步”，然后查看该步骤的详细信息。

g. 选择“创建步骤”以添加该步骤并继续。

7. 添加第三步（删除）。

a. 在标称步骤部分中，选择添加步骤。

b. 选择 删除文件，然后选择 下一步。



c. 输入步骤名称。

d. 在“文件位置”中，选择“删除原始源文件”。

e. 选择“下一步”，然后查看该步骤的详细信息。

f. 选择“创建步骤”以添加该步骤并继续。

8. 查看工作流程配置，然后选择创建工作流程。

CLI

标记和移动工作流程示例

1. 将以下代码保存到文件中；例如，tagAndMoveWorkflow.json。将每个 *user input placeholder* 替换为您自己的信息。

```
[
   {
       "Type": "COPY",
       "CopyStepDetails": {
          "Name": "CopyStep",
          "DestinationFileLocation": {
             "S3FileLocation": {
                "Bucket": "amzn-s3-demo-bucket",
                "Key": "test/"
             }
          }
       }
   },
   {
       "Type": "TAG",
       "TagStepDetails": {
          "Name": "TagStep",
          "Tags": [
             {
                "Key": "name",
                "Value": "demo"
             }
          ],
          "SourceFileLocation": "${previous.file}"
       }
   },
   {
      "Type": "DELETE",
      "DeleteStepDetails":{
```

```
        "Name":"DeleteStep",
        "SourceFileLocation": "${original.file}"
      }
  }
]
```

第一步是将上传的文件复制到新的 Amazon S3 位置。第二步将标签（键值对）添加到复制到新位置的文件 (`previous.file`)。最后，第三步删除原始文件 (`original.file`)。

2. 使用保存的文件创建工作流程。将每个 *`user input placeholder`* 替换为您自己的信息。

```
aws transfer create-workflow --description "short-description" --steps
 file://path-to-file --region region-ID
```

例如：

```
aws transfer create-workflow --description "copy-tag-delete workflow" --steps
 file://tagAndMoveWorkflow.json --region us-east-1
```

> **Note**
>
> 有关使用文件加载参数的更多详细信息，请参阅如何从文件加载参数。

3. 更新现有服务器。

> **Note**
>
> 此步骤假设您已经有一台 Transfer Family 服务器，并且想要将工作流程与之关联。如果不是，请参阅 配置 SFTP、FTPS 或 FTP 服务器端点。将每个 *`user input placeholder`* 替换为您自己的信息。

```
aws transfer update-server --server-id server-ID --region region-ID
  --workflow-details '{"OnUpload":[{ "WorkflowId": "workflow-
ID","ExecutionRole": "execution-role-ARN"}]}'
```

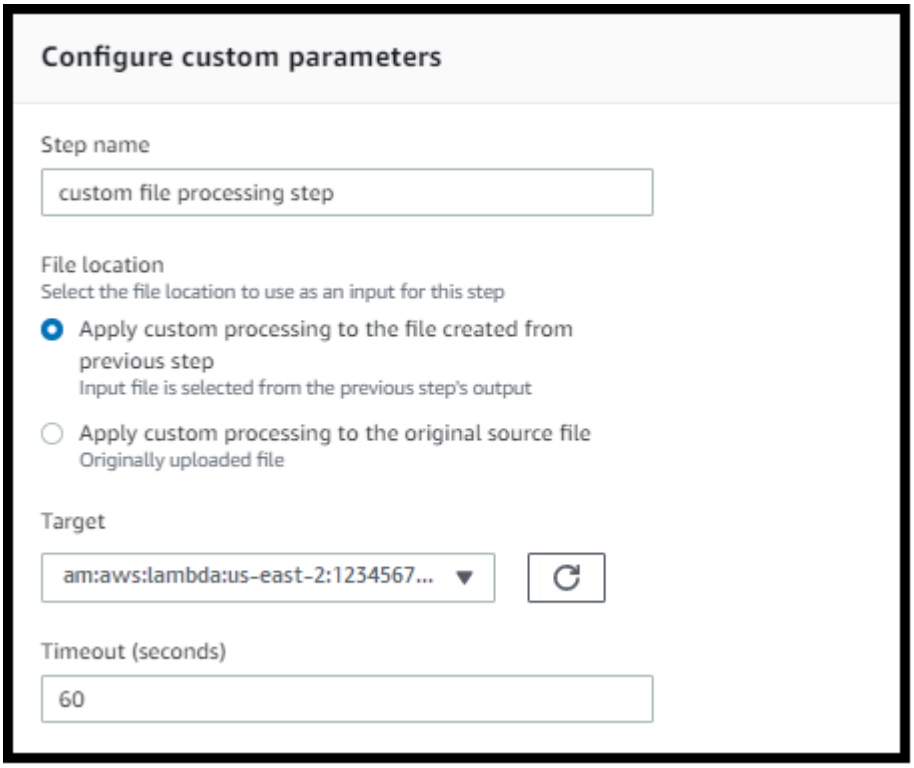
例如：

```
aws transfer update-server --server-id s-1234567890abcdef0 --region us-east-2
```

```
  --workflow-details '{"OnUpload":[{ "WorkflowId": "w-
abcdef01234567890","ExecutionRole": "arn:aws:iam::111111111111:role/nikki-wolf-
execution-role"}]}'
```

使用自定义文件处理步骤

通过使用自定义文件处理步骤，您可以使用 Amazon Lambda自带文件处理逻辑。文件到达后，Transfer Family 服务器会调用包含自定义文件处理逻辑的 Lambda 函数，例如加密文件、扫描恶意软件或检查文件类型是否不正确。在以下示例中，目标 Amazon Lambda 函数用于处理上一步的输出文件。



> **Note**
>
> 有关示例 Lambda 函数，请参阅 自定义工作流程步骤的 Lambda 函数示例。有关事件示例（包括传递到 Lambda 的文件的位置），请参阅 文件上传 Amazon Lambda 时发送到的事件示例。

使用自定义工作流程步骤，您必须配置 Lambda 函数以调用 SendWorkflowStepStateAPI 操作。 SendWorkflowStepState通知工作流程执行该步骤已完成，状态为成功或失

败。SendWorkflowStepState API 操作的状态根据 Lambda 函数的结果调用异常处理程序步骤或线性序列中的标称步骤。

如果 Lambda 函数失败或超时，则该步骤将失败，您将在日志StepErrored中看到。 CloudWatch 如果 Lambda 函数是标称步骤的一部分，并且函数响应 SendWorkflowStepState 为 Status="FAILURE" 或超时，则流程会继续执行异常处理程序步骤。在这种情况下，工作流不会继续执行剩余的（如果有）标称步骤。有关更多详细信息，请参阅工作流程的异常处理。

在调用 SendWorkflowStepState API 操作时，必须发送以下参数：

```
{
    "ExecutionId": "string",
    "Status": "string",
    "Token": "string",
    "WorkflowId": "string"
}
```

您可以从 Lambda 函数执行时传递的输入事件中提取 ExecutionId、Token 和 WorkflowId（以下各节显示了示例）。该Status值可以是 SUCCESS 或FAILURE。

为了能够从 Lambda 函数调用 SendWorkflowStepState API 操作，您必须使用在引入托管工作流程之后发布的 Amazon SDK 版本。

连续使用多个 Lambda 函数

当您依次使用多个自定义步骤时，“文件位置”选项的工作方式与仅使用单个自定义步骤时不同。Transfer Family 不支持传回 Lambda 处理过的文件以用作下一步的输入。因此，如果您将多个自定义步骤全部配置为使用 previous.file 选项，则它们都使用相同的文件位置（第一个自定义步骤的输入文件位置）。

> **Note**
>
> 如果您在自定义步骤之后有预定义的步骤（标记、复制、解密或删除），则 previous.file 设置的工作方式也会有所不同。如果将预定义步骤配置为使用 previous.file 设置，则预定义步骤将使用与自定义步骤相同的输入文件。来自自定义步骤的已处理文件不会传递到预定义的步骤。

在自定义处理后访问文件

如果您使用 Amazon S3 作为存储，并且您的工作流程包括对最初上传的文件执行操作的自定义步骤，则后续步骤将无法访问该已处理的文件。也就是说，自定义步骤之后的任何步骤都不能从自定义步骤输出中引用更新的文件。

例如，假设您的工作流程中有以下三个步骤。

- 步骤 1 - 上传名为 `example-file.txt` 的文件。
- 步骤 2 - 调用以某种方式更改`example-file.txt`的 Lambda 函数。
- 步骤 3 - 尝试对 `example-file.txt` 的更新版本执行进一步处理。

如果将步骤 3 的 `sourceFileLocation` 配置为 `${original.file}`，则步骤 3 将使用步骤 1 中服务器将文件上传到存储器时的原始文件位置。如果您在步骤 3 使用 `${previous.file}`，则步骤 3 会重复使用步骤 2 用作输入的文件位置。

因此，步骤 3 会导致错误。例如，如果步骤 3 尝试复制更新的 `example-file.txt`，则会收到以下错误：

```
{
    "type": "StepErrored",
    "details": {
        "errorType": "NOT_FOUND",
        "errorMessage": "ETag constraint not met (Service: null; Status Code: 412;
 Error Code: null; Request ID: null; S3 Extended Request ID: null; Proxy: null)",
        "stepType": "COPY",
        "stepName": "CopyFile"
    },
```

之所以出现此错误，是因为自定义步骤修改了的实体标签 (ETag)，`example-file.txt`使其与原始文件不匹配。

> **Note**
>
> 如果您使用的是 Amazon EFS，则不会发生这种情况，因为 Amazon EFS 不使用实体标签来识别文件。

文件上传 Amazon Lambda 时发送到的事件示例

以下示例显示了文件上传完成 Amazon Lambda 时发送到的事件。一个示例使用 Transfer Family 服务器，其中域名配置了 Amazon S3。另一个示例使用 Transfer Family 服务器，其中域名使用 Amazon EFS。

Custom step that uses an Amazon S3 domain

```
{
    "token": "MzI0Nzc4ZDktMGRmMi00MjFhLTgxMjUtYWZmZmRmODNkYjc0",
    "serviceMetadata": {
        "executionDetails": {
            "workflowId": "w-1234567890example",
            "executionId": "abcd1234-aa11-bb22-cc33-abcdef123456"
        },
        "transferDetails": {
            "sessionId": "36688ff5d2deda8c",
            "userName": "myuser",
            "serverId": "s-example1234567890"
        }
    },
    "fileLocation": {
        "domain": "S3",
        "bucket": "amzn-s3-demo-bucket",
        "key": "path/to/mykey",
        "eTag": "d8e8fca2dc0f896fd7cb4cb0031ba249",
        "versionId": null
    }
}
```

Custom step that uses an Amazon EFS domain

```
{
    "token": "MTg0N2Y3N2UtNWI5Ny00ZmZlLTk5YTgtZTU3YzViYjllNmZm",
    "serviceMetadata": {
        "executionDetails": {
            "workflowId": "w-1234567890example",
            "executionId": "abcd1234-aa11-bb22-cc33-abcdef123456"
        },
        "transferDetails": {
            "sessionId": "36688ff5d2deda8c",
            "userName": "myuser",
```

```
            "serverId": "s-example1234567890"
        }
    },
    "fileLocation": {
        "domain": "EFS",
        "fileSystemId": "fs-1234567",
        "path": "/path/to/myfile"
    }
}
```

自定义工作流程步骤的 Lambda 函数示例

以下 Lambda 函数提取有关执行状态的信息，然后调用 SendWorkflowStepStateAPI 操作将该步骤SUCCESS的状态返回到工作流程，可以是或。FAILURE在您的函数调用 SendWorkflowStepState API 操作之前，您可以将 Lambda 配置为根据您的工作流程逻辑执行操作。

```
import json
import boto3

transfer = boto3.client('transfer')

def lambda_handler(event, context):
    print(json.dumps(event))

    # call the SendWorkflowStepState API to notify the workflow about the step's
 SUCCESS or FAILURE status
    response = transfer.send_workflow_step_state(
        WorkflowId=event['serviceMetadata']['executionDetails']['workflowId'],
        ExecutionId=event['serviceMetadata']['executionDetails']['executionId'],
        Token=event['token'],
        Status='SUCCESS|FAILURE'
    )

    print(json.dumps(response))

    return {
      'statusCode': 200,
      'body': json.dumps(response)
    }
```

自定义步骤的 IAM 权限

若要使调用 Lambda 的步骤成功，请确保您的工作流程的执行角色包含以下权限。

```
{
    "Sid": "Custom",
    "Effect": "Allow",
    "Action": [
        "lambda:InvokeFunction"
    ],
    "Resource": [
        "arn:aws:lambda:region:account-id:function:function-name"
    ]
}
```

适用于工作流程的 IAM 策略

向服务器添加工作流程时，必须选择执行角色。服务器在执行工作流程时使用此角色。如果该角色没有适当的权限，则 Amazon Transfer Family 无法运行工作流程。

本节介绍一组可能的 Amazon Identity and Access Management (IAM) 权限，您可以使用这些权限来执行工作流程。本主题的后续部分中描述了其他示例。

> **Note**
>
> 如果您的 Amazon S3 文件有标签，则需要在 IAM 策略中添加一两个权限。
>
> - 为未进行版本控制的 Amazon S3 文件添加 `s3:GetObjectTagging`。
> - 为进行版本控制的 Amazon S3 文件添加 `s3:GetObjectVersionTagging`。

为您的工作流程创建执行角色

1. 创建新的 IAM 角色，并将 Amazon 托管策略`AWSTransferFullAccess`添加到该角色中。有关创建 IAM 角色的更多信息，请参见 the section called “创建 IAM 角色和策略”。
2. 按以下策略创建其他策略，然后将其内联至您的角色。将每个 *user input placeholder* 替换为您自己的信息。

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ConsoleAccess",
            "Effect": "Allow",
            "Action": "s3:GetBucketLocation",
            "Resource": "*"
        },
        {
            "Sid": "ListObjectsInBucket",
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket"
            ]
        },
        {
            "Sid": "AllObjectActions",
            "Effect": "Allow",
            "Action": "s3:*Object",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        },
        {
            "Sid": "GetObjectVersion",
            "Effect": "Allow",
            "Action": "s3:GetObjectVersion",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        },
        {
            "Sid": "Custom",
            "Effect": "Allow",
            "Action": [
                "lambda:InvokeFunction"
            ],
            "Resource": [
                "arn:aws:lambda:us-east-1:123456789012:function:function-name"
            ]
        },
        {
            "Sid": "Tag",
```

```
            "Effect": "Allow",
            "Action": [
                "s3:PutObjectTagging",
                "s3:PutObjectVersionTagging"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        }
    ]
}
```

3. 保存此角色并在向服务器添加工作流程时将其指定为执行角色。

> **Note**
>
> 在构建 IAM 角色时， Amazon 建议您尽可能限制工作流程对资源的访问权限。

工作流程信任关系

工作流程执行角色还需要与 `transfer.amazonaws.com` 建立信任关系。若要为 Amazon Transfer Family建立信任关系，请参见 建立信任关系。

在建立信任关系的同时，您也可以采取措施避免混淆代理问题。有关此问题的描述以及如何避免该问题的示例，请参见 the section called “防止跨服务混淆代理”。

执行角色示例：解密、复制和标记

如果您的工作流程包括标记、复制和解密步骤，则可以使用以下 IAM 策略。将每个 *user input placeholder* 替换为您自己的信息。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CopyRead",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectTagging",
```

```
            "s3:GetObjectVersionTagging"
        ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
    },
    {
        "Sid": "CopyWrite",
        "Effect": "Allow",
        "Action": [
            "s3:PutObject",
            "s3:PutObjectTagging"
        ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    },
    {
        "Sid": "CopyList",
        "Effect": "Allow",
        "Action": "s3:ListBucket",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-source-bucket",
            "arn:aws:s3:::amzn-s3-demo-destination-bucket"
        ]
    },
    {
        "Sid": "Tag",
        "Effect": "Allow",
        "Action": [
            "s3:PutObjectTagging",
            "s3:PutObjectVersionTagging"
        ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*",
        "Condition": {
            "StringEquals": {
                "s3:RequestObjectTag/Archive": "yes"
            }
        }
    },
    {
        "Sid": "ListBucket",
        "Effect": "Allow",
        "Action": "s3:ListBucket",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-destination-bucket"
        ]
    },
```

```
        {
            "Sid": "HomeDirObjectAccess",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObjectVersion",
                "s3:DeleteObject",
                "s3:GetObjectVersion"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
        },
        {
            "Sid": "Decrypt",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": "arn:aws:secretsmanager:us-east-1:123456789012:secret:aws/
transfer/*"
        }
    ]
}
```

执行角色示例：运行函数并删除

在此示例中，您有一个 Amazon Lambda 调用函数的工作流程。如果工作流程删除了上传的文件，并且有异常处理程序步骤可以对上一步中失败的工作流程执行采取行动，请使用以下 IAM 策略。将每个 *user input placeholder* 替换为您自己的信息。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "Delete",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteObject",
                "s3:DeleteObjectVersion"
            ],
            "Resource": "arn:aws:s3:::bucket-name"
```

```
        },
        {
            "Sid": "Custom",
            "Effect": "Allow",
            "Action": [
                "lambda:InvokeFunction"
            ],
            "Resource": [
                "arn:aws:lambda:us-east-1:123456789012:function:function-name"
            ]
        }
    ]
}
```

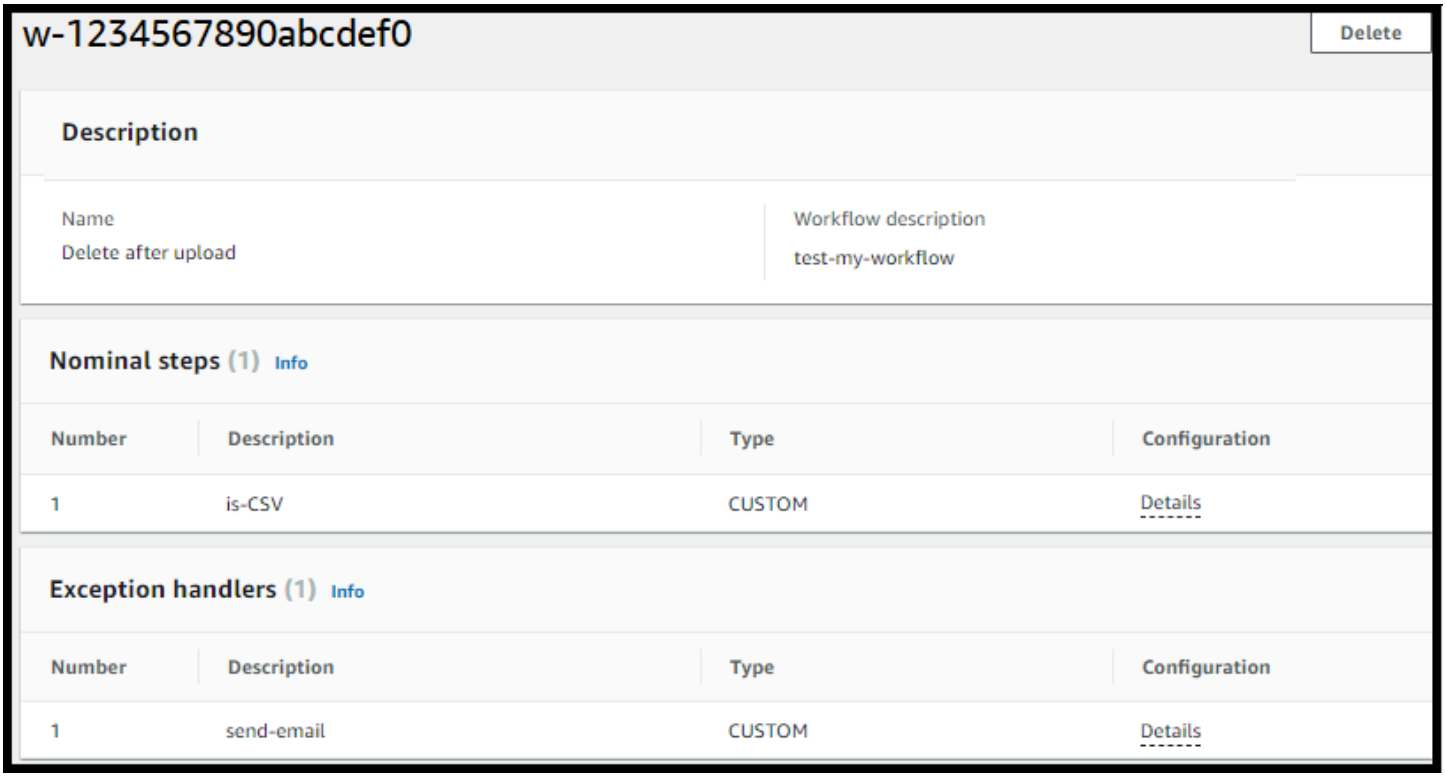
工作流程的异常处理

如果在工作流程执行过程中出现任何错误，则会执行您指定的异常处理步骤。为工作流指定错误处理步骤的方式与为工作流指定标称步骤的方式相同。例如，假设您已按名义步骤配置了自定义处理来验证传入的文件。如果文件验证失败，则异常处理步骤可以向管理员发送电子邮件。

以下示例工作流程包含两个步骤：

- 检查上传文件是否为 CSV 格式的标称步骤
- 一个异常处理步骤，用于在上传的文件不是 CSV 格式且标称步骤失败时发送电子邮件

要启动异常处理步骤，名义步骤中的 Amazon Lambda 函数必须使用响应。`Status="FAILURE"`有关工作流错误处理的更多信息，请参阅 the section called “使用自定义文件处理步骤”。



监控工作流程执行情况

Amazon 会实时 CloudWatch 监控您的 Amazon 资源和您运行 Amazon Web Services 云 的应用程序。您可以使用 Amazon CloudWatch 来收集和跟踪指标，这些指标是您可以衡量工作流程的变量。您可以使用 Amazon 查看工作流程指标和整合日志 CloudWatch。

CloudWatch 记录工作流程

CloudWatch 为工作流程进度和结果提供统一的审计和日志记录。

查看 Amazon 工作流程 CloudWatch 日志

1. 打开 Amazon CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
2. 在左侧导航窗格中选择日志，然后选择日志组。
3. 在日志组页面的导航栏上，为您的 Amazon Transfer Family 服务器选择正确的区域。
4. 选择与您的服务器相对应的日志组。

   例如，如果您的服务器 ID 是 `s-1234567890abcdef0`，则您的日志组是 `/aws/transfer/s-1234567890abcdef0`。
5. 在服务器的日志组详细信息页面上，将显示最新的日志流。您正在探索的用户有两个日志流：

- 每个 Secure Shell (SSH) 文件传输协议 (SFTP) 会话一个。
- 一个用于正在为您的服务器执行的工作流程。工作流程的日志流格式为 *username*.*workflowID*.*uniqueStreamSuffix*。

例如，如果您的用户是 mary-major，您具有以下日志流：

```
mary-major-east.1234567890abcdef0
mary.w-abcdef01234567890.021345abcdef6789
```

> **Note**
>
> 此示例中列出的 16 位字母数字标识符是虚构的。您在 Amazon 上看到 CloudWatch 的值不同。

mary-major-usa-east.1234567890abcdef0 的“日志事件”页面显示每个用户会话的详细信息，mary.w-abcdef01234567890.021345abcdef6789 日志流包含工作流程的详细信息。

以下是基于包含复制步骤的工作流程 (w-abcdef01234567890) 的 mary.w-abcdef01234567890.021345abcdef6789 日志流示例。

```
{
    "type": "ExecutionStarted",
    "details": {
        "input": {
            "initialFileLocation": {
                "bucket": "amzn-s3-demo-bucket",
                "key": "mary/workflowSteps2.json",
                "versionId": "version-id",
                "etag": "etag-id"
            }
        }
    },
    "workflowId":"w-abcdef01234567890",
    "executionId":"execution-id",
    "transferDetails": {
        "serverId":"s-server-id",
        "username":"mary",
        "sessionId":"session-id"
```

```
    }
},
{
    "type":"StepStarted",
    "details": {
        "input": {
            "fileLocation": {
                "backingStore":"S3",
                "bucket":"amzn-s3-demo-bucket",
                "key":"mary/workflowSteps2.json",
                "versionId":"version-id",
                "etag":"etag-id"
            }
        },
        "stepType":"COPY",
        "stepName":"copyToShared"
    },
    "workflowId":"w-abcdef01234567890",
    "executionId":"execution-id",
    "transferDetails": {
        "serverId":"s-server-id",
        "username":"mary",
        "sessionId":"session-id"
    }
},
{
    "type":"StepCompleted",
    "details":{
        "output":{},
        "stepType":"COPY",
        "stepName":"copyToShared"
    },
    "workflowId":"w-abcdef01234567890",
    "executionId":"execution-id",
    "transferDetails":{
        "serverId":"server-id",
        "username":"mary",
        "sessionId":"session-id"
    }
},
{
    "type":"ExecutionCompleted",
    "details": {},
    "workflowId":"w-abcdef01234567890",
```

```
    "executionId":"execution-id",
    "transferDetails":{
        "serverId":"s-server-id",
        "username":"mary",
        "sessionId":"session-id"
    }
}
```

CloudWatch 工作流程指标

Amazon Transfer Family 为工作流程提供了多个指标。您可以查看前一分钟有多少工作流程执行启动、成功完成和失败的指标。中描述了 Transfer Family 的所有 CloudWatch 指标使用 T CloudWatch ransfer Family 服务器的指标。

通过模板创建工作流

您可以部署用于创建工作流的 Amazon CloudFormation 堆栈和基于模板的服务器。此过程包含一个示例，您可以使用该示例来快速部署工作流程。

创建用于创建 Amazon Transfer Family 工作流程和服务器的 Amazon CloudFormation 堆栈

1. 在 https://console.aws.amazon.com/cloudformat ion 上打开 Amazon CloudFormation 控制台。
2. 将以下代码保存到文件中。

   YAML

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  SFTPServer:
    Type: 'AWS::Transfer::Server'
    Properties:
      WorkflowDetails:
        OnUpload:
          - ExecutionRole: workflow-execution-role-arn
            WorkflowId: !GetAtt
              - TransferWorkflow
              - WorkflowId
  TransferWorkflow:
    Type: AWS::Transfer::Workflow
    Properties:
      Description: Transfer Family Workflows Blog
```

```
      Steps:
        - Type: COPY
          CopyStepDetails:
            Name: copyToUserKey
            DestinationFileLocation:
              S3FileLocation:
                Bucket: archived-records
                Key: ${transfer:UserName}/
            OverwriteExisting: 'TRUE'
        - Type: TAG
          TagStepDetails:
            Name: tagFileForArchive
            Tags:
              - Key: Archive
                Value: yes
        - Type: CUSTOM
          CustomStepDetails:
            Name: transferExtract
            Target: arn:aws:lambda:region:account-id:function:function-name
            TimeoutSeconds: 60
        - Type: DELETE
          DeleteStepDetails:
            Name: DeleteInputFile
            SourceFileLocation: '${original.file}'
      Tags:
        - Key: Name
          Value: TransferFamilyWorkflows
```

JSON

```
{
    "AWSTemplateFormatVersion": "2010-09-09",
    "Resources": {
        "SFTPServer": {
            "Type": "AWS::Transfer::Server",
            "Properties": {
                "WorkflowDetails": {
                    "OnUpload": [
                        {
                            "ExecutionRole": "workflow-execution-role-arn",
                            "WorkflowId": {
                                "Fn::GetAtt": [
                                    "TransferWorkflow",
```

```
                                    "WorkflowId"
                                ]
                            }
                        }
                    ]
                }
            }
        },
        "TransferWorkflow": {
            "Type": "Amazon::Transfer::Workflow",
            "Properties": {
                "Description": "Transfer Family Workflows Blog",
                "Steps": [
                    {
                        "Type": "COPY",
                        "CopyStepDetails": {
                            "Name": "copyToUserKey",
                            "DestinationFileLocation": {
                                "S3FileLocation": {
                                    "Bucket": "archived-records",
                                    "Key": "${transfer:UserName}/"
                                }
                            },
                            "OverwriteExisting": "TRUE"
                        }
                    },
                    {
                        "Type": "TAG",
                        "TagStepDetails": {
                            "Name": "tagFileForArchive",
                            "Tags": [
                                {
                                    "Key": "Archive",
                                    "Value": "yes"
                                }
                            ]
                        }
                    },
                    {
                        "Type": "CUSTOM",
                        "CustomStepDetails": {
                            "Name": "transferExtract",
                            "Target": "arn:aws:lambda:region:account-
id:function:function-name",
```

```
                            "TimeoutSeconds": 60
                        }
                    },
                    {
                        "Type": "DELETE",
                        "DeleteStepDetails": {
                            "Name": "DeleteInputFile",
                            "SourceFileLocation": "${original.file}"
                        }
                    }
                ],
                "Tags": [
                    {
                        "Key": "Name",
                        "Value": "TransferFamilyWorkflows"
                    }
                ]
            }
        }
    }
}
```

3. 将以下值替换为您的实际值。

   - 将 *workflow-execution-role-arn* 替换为实际工作流执行角色的 ARN。例如，arn:aws:transfer:us-east-2:111122223333:workflow/w-1234567890abcdef0
   - 将 arn:aws:lambda:*region*:*account-id*:function:*function-name* 替换为 Lambda 函数的 ARN。例如 arn:aws:lambda:us-east-2:123456789012:function:example-lambda-idp。

4. 按照《Amazon CloudFormation 用户指南》的 “选择 Amazon CloudFormation 堆栈模板” 中有关从现有模板部署堆栈的说明进行操作。

部署堆栈后，您可以在 CloudFormation 控制台的 Outputs 选项卡中查看有关堆栈的详细信息。该模板创建了一个使用服务管理用户的新 Amazon Transfer Family SFTP 服务器和一个新的工作流程，并将该工作流与新服务器关联起来。

从 Transfer Family 服务器中移除工作流

如果您已将工作流程与 Transfer Family 服务器关联，而现在想要移除该关联，则可以使用控制台或以编程方式执行此操作。

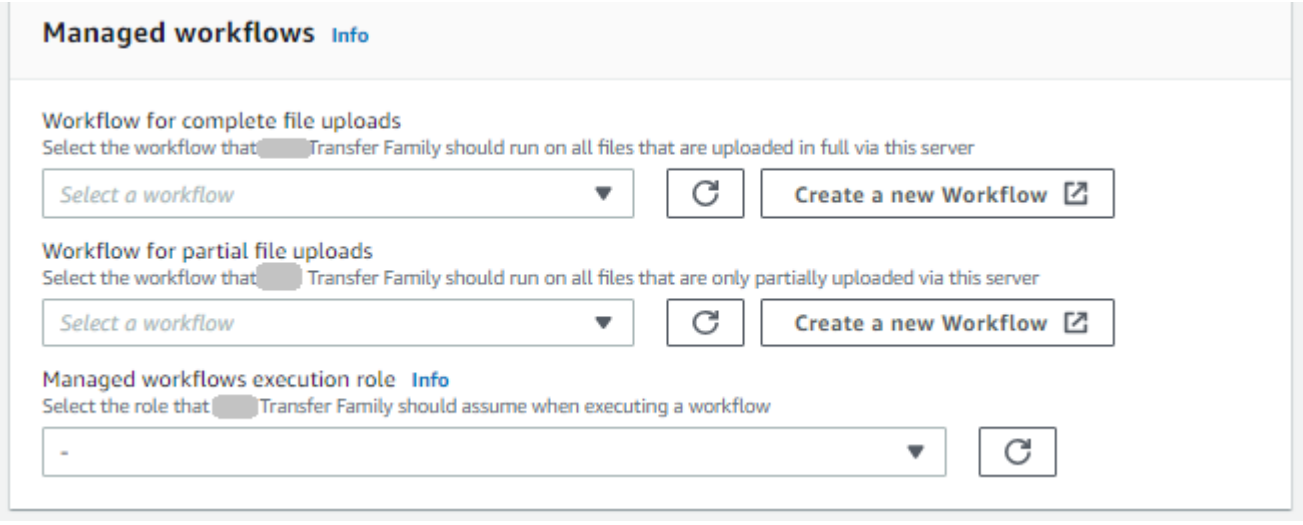
Console

若要从 Transfer Family 服务器中移除工作流

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在左侧导航窗格中选择服务器。
3. 在“服务器 ID”列中选择服务器的标识符。
4. 在服务器的详细信息页面上，向下滚动到其他详细信息部分，然后选择编辑。
5. 在编辑其他详细信息页面中的托管工作流程部分，清除所有设置的信息：
   - 从用于完整文件上载的工作流的工作流列表中选择短划线 (-)。
   - 如果尚未清除，从用于部分文件上载的工作流的工作流列表中选择短划线 (-)。
   - 从托管工作流程执行角色的角色列表中选择短划线 (-)。

   如果看不到破折号，请向上滚动直到看到它，因为它是每个菜单中的第一个值。

   该部分应该类似以下内容。



6. 要保存更改，请向下滚动并选择保存。

CLI

您可以使用 `update-server`（或 `UpdateServer` for API）调用，并为 `OnUpload` 和 `OnPartialUpload` 参数提供空参数。

从中 Amazon CLI，运行以下命令：

```
aws transfer update-server --server-id your-server-id --workflow-details
 '{"OnPartialUpload":[],"OnUpload":[]}'
```

将 *`your-server-id`* 替换为服务器的 ID。例如，如果您的服务器 ID 是 `s-01234567890abcdef`，则命令如下所示：

```
aws transfer update-server --server-id s-01234567890abcdef --workflow-details
 '{"OnPartialUpload":[],"OnUpload":[]}'
```

托管工作流限制和局限性

限制

以下限制目前适用于 Amazon Transfer Family的上传后处理工作流程。

- 不支持跨账户和跨区域 Amazon Lambda 功能。但是，您可以跨账户复制，前提是您的 Amazon Identity and Access Management (IAM) 策略配置正确。
- 对于所有工作流程步骤，工作流程访问的任何 Amazon S3 存储桶都必须与工作流程本身位于同一区域。
- 对于解密步骤，解密目标必须与区域和后备存储的来源相匹配（例如，如果要解密的文件存储在 Amazon S3 中，则指定的目标也必须在 Amazon S3 中）。
- 仅支持异步自定义步骤。
- 自定义步骤超时值是近似值。也就是说，超时所需的时间可能比指定时间稍长。此外，工作流程依赖于 Lambda 函数。因此，如果函数在执行过程中出现延迟，则工作流程不会意识到延迟。
- 如果您超过了限制限制，Transfer Family 不会将工作流程操作添加到队列中。
- 不会为大小为 0 的文件启动工作流程。大小大于 0 的文件会启动关联的工作流程。
- 您可以将文件处理工作流程附加到使用该 AS2 协议的 Transfer Family 服务器：但是， AS2 消息不会执行附加到服务器的工作流程。

限制

此外，以下功能限制适用于 Transfer Family 的工作流程：

- 每个区域、每个账户的工作流程数量限制为 10。
- 自定义步骤的最大超时时间为 30 分钟。
- 工作流中的最大步骤数为 8。
- 每个工作组的最大标签数是 50。
- 每个工作流程中包含解密步骤的最大并发执行数为 250 个。
- 在每台 Transfer Family 服务器上，每位用户最多可存储 3 个 PGP 私钥。
- 数据文件的最大大小为 10 GB。
- 我们使用容量暴增为 100、再填充率为 1 的令牌桶系统来限制新的执行率。
- 无论何时从服务器上移除工作流程并用新的工作流程替换它，或者更新服务器配置（这会影响工作流程的执行角色），都必须等待大约 10 分钟才能执行新的工作流程。Transfer Family 服务器会缓存工作流程细节，服务器需要 10 分钟才能刷新其缓存。

  此外，您必须注销所有活动的 SFTP 会话，然后等待 10 分钟重新登录才能看到更改。

管理服务器

在本部分中，您可以找到有关如何查看服务器列表、如何查看服务器详细信息、如何编辑服务器详细信息以及如何更改启用 SFTP 的服务器的主机密钥的信息。

主题

- 查看服务器列表
- 删除服务器
- 查看 SFTP、FTPS 和 FTP 服务器的详细信息
- 查看 AS2 服务器详细信息
- IPv6 支持 Transfer Family 服务器
- 编辑服务器详细信息
- 编辑身份提供商配置
- 管理启用 SFTP 的服务器的主机密钥
- 在控制台中监控使用情况

查看服务器列表

在 Amazon Transfer Family 控制台上，您可以找到位于所选 Amazon 区域内的所有服务器的列表。

要查找某个 Amazon 地区中存在的服务器的列表

- 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。

  如果您在当前 Amazon 区域有一台或多台服务器，则控制台会打开并显示您的服务器列表。如果未看到服务器列表，请确保您已进入正确的区域。也可以从导航窗格中选择服务器。

  有关查看您服务器详情的更多信息，请参阅 查看 SFTP、FTPS 和 FTP 服务器的详细信息。

删除服务器

此过程说明如何使用 Amazon Transfer Family 控制台或删除 Transfer Family 服务器 Amazon CLI。

> **Important**
>
> 在您删除服务器之前，您需要为允许访问您的端点的每项协议付费。

> **Warning**
>
> 删除服务器会导致其所有用户都被删除。使用服务器访问的存储桶中的数据不会被删除，拥有这些 Amazon S3 存储桶权限的 Amazon 用户仍可以访问这些数据。

Console

使用控制台删除服务器

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在左侧导航窗格中，选择服务器。
3. 选中您要删除的服务器的复选框。
4. 对于操作，选择删除。
5. 在显示的确认对话框中，输入单词 **delete**，然后选择删除以确认您要删除该用户。

服务器已从服务器页面中删除，您无需再为此付费。

Amazon CLI

使用 CLI 删除服务器

1. （可选）运行以下命令查看要永久删除的服务器的详细信息。

```
aws transfer describe-server --server-id your-server-id
```

此describe-server命令会返回您的服务器的所有详细信息。

2. 运行以下命令删除服务器。

```
aws transfer delete-server --server-id your-server-id
```

如果成功，该命令将删除服务器并且不返回任何信息。

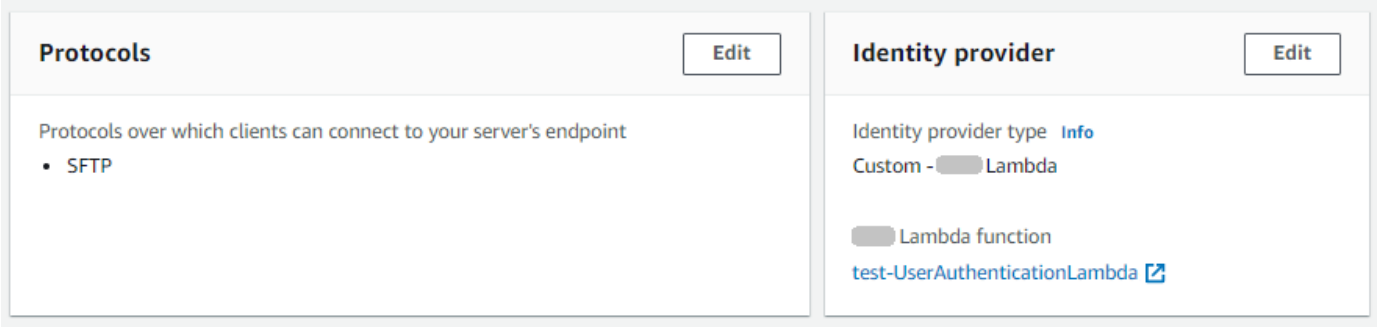
查看 SFTP、FTPS 和 FTP 服务器的详细信息

您可以找到单个 Amazon Transfer Family 服务器的详细信息和属性的列表。服务器属性包括协议、身份提供商、状态、端点类型、自定义主机名、端点、用户、日志记录角色、服务器主机密钥和标签。

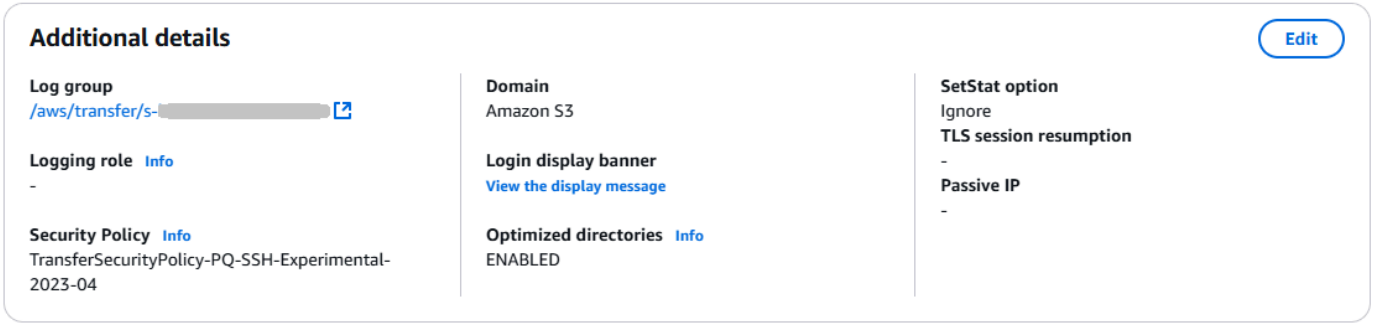
查看服务器详细信息

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在导航窗格中，选择服务器。
3. 选择服务器 ID 列中的标识符以查看服务器详细信息页面，如下所示。

   您可以通过选择编辑来更改服务器的属性。有关编辑服务器详情的更多信息，请参阅 编辑服务器详细信息。 AS2 服务器的详细信息页面略有不同。有关 AS2 服务器的信息，请参阅查看 AS2 服务器详细信息。

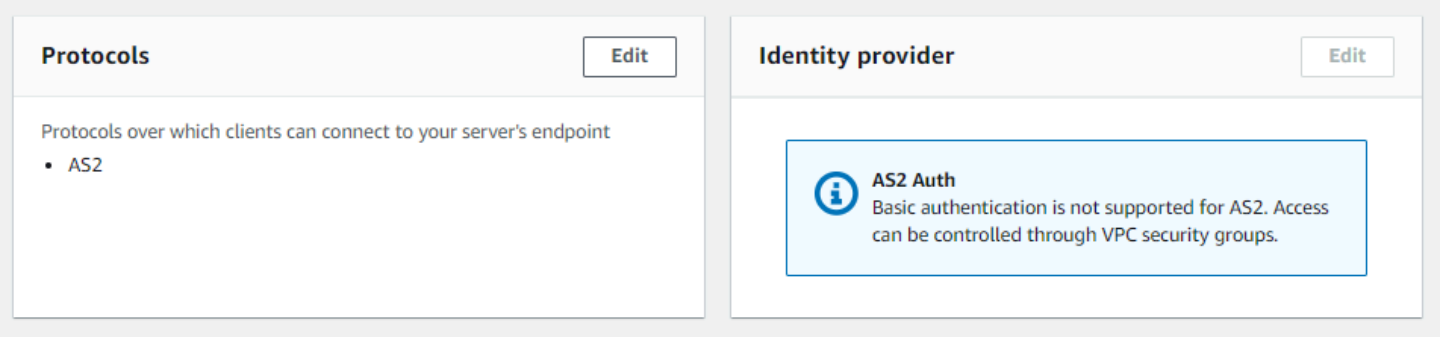


> **Note**
>
> 自 2022 年 9 月起，服务器主机密钥的描述和导入日期值是新的。引入这些值是为了支持多主机密钥功能。此功能需要迁移在引入多个主机密钥之前使用的所有单个主机密钥。
> 已迁移服务器主机密钥的导入日期值设置为服务器的上次修改日期。也就是说，您看到的迁移主机密钥的日期与服务器主机密钥迁移之前上次以任何方式修改服务器的日期相对应。
> 迁移的唯一密钥是您最旧的或唯一的服务器主机密钥。任何其他密钥的实际日期均从您导入时算起。此外，迁移后的密钥具有描述，便于将其识别为已迁移。
> 迁移发生在 9 月 2 日至 9 月 13 日之间。此范围内的实际迁移日期取决于服务器所在的地区。

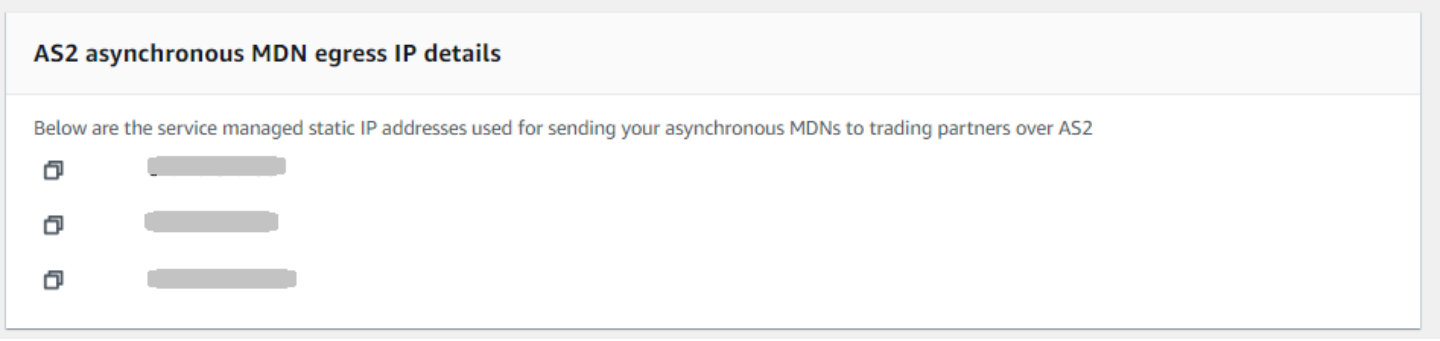


查看 AS2 服务器详细信息

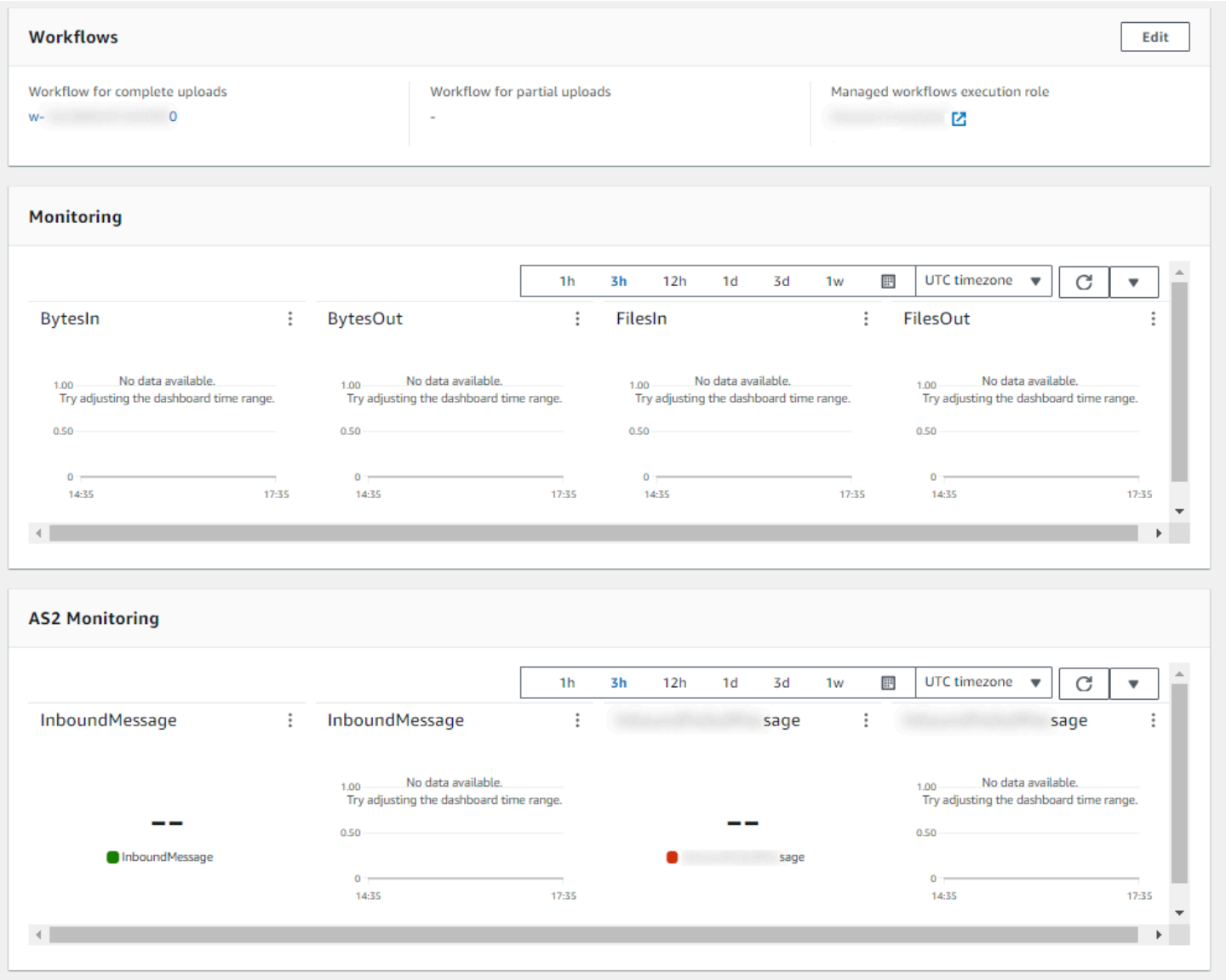
您可以找到单个 Amazon Transfer Family 服务器的详细信息和属性的列表。服务器属性包括协议、状态等。对于 AS2 服务器，您还可以查看 AS2 异步 MDN 出口 IP 地址。



为每 AS2 台服务器分配了三个静态 IP 地址。使用这些 IP 地址 MDNs 向您的贸易伙伴发送异步信息 AS2。



AS2 服务器详细信息页面的底部包含任何附加工作流程的详细信息以及监控和标记信息。



IPv6 支持 Transfer Family 服务器

Amazon Transfer Family 支持以下资源的双栈（IPv4 和 IPv6）端点：

- SFTP 公共终端节点
- 所有协议的 VPC 内部终端节点（SFTP/FTPS/FTP和 AS2）
- 使用中提供的步骤，为 AS2启用了 Transfer Family 服务器的公共终端节点 使用 Application Load Balancer 实现双栈 AS2服务器连接
- API 终端节点

借助双栈支持，您的 Transfer Family 端点可以与两个客户端 IPv4 和 IPv6已启用的客户端通信。这使您无需一次性切换所有系统 IPv4 即可逐步从 IPv6 基于系统的过渡，满足 IPv6 合规性要求，并且无需使用昂贵的网络设备来处理 IPv4 和之间的地址转换 IPv6。有关详细信息，请参阅 Amazon Transfer Family API 参考中的 DNS 和终端节点。有关可用终端节点的完整列表，请参阅中的Amazon Transfer Family 终端节点和配额Amazon Web Services 一般参考。

IPv6 局限性

以下 Transfer Family 资源目前不支持 IPv6：

- VPC 互联网终端节点
- 网络应用程序
- VPC_ENDPOINT 端点类型（已弃用）

FTPS 协议支持 PASV 和 EPSV 命令，用于请求开放数据端口以进行文件列表、获取和放置操作。但是，PASV 不起作用， IPv6因为它需要 IPv4特定的响应。EPSV 之所以能继续工作，是因为它只返回端口信息。

要使用 FTPS，我们建议使用以下方法之一：

- 将您的 FTPS 客户端配置为使用 EPSV
- 使用 IPv4 代替 IPv6

SFTP 同时支持 IPv4 和。 IPv6在使用双栈端点时，我们建议使用 SFTP 而不是 FTPS。

IPv6 为服务器配置

创建新服务器或更新现有服务器时，可以选择 IP 地址类型：

- IPv4（默认）：为了向后兼容，服务器将只接受 IPv4 连接。
- 双栈：服务器将同时接受 IPv4 和 IPv6连接。

要更新现有服务器的 IP 地址，请键入：

1. 停止服务器。
2. 编辑终端节点详细信息。
3. 将 IP 地址类型更改为双栈。

4. 启动 服务器。

> **Note**
>
> 对于 VPC-Internet 端点，目前不支持双栈模式。

使用 Application Load Balancer 实现双栈 AS2服务器连接

您可以使用具有面向公众的终端节点的 Application Load Balanc AS2 er 来启用与服务器的双栈（IPv4 和 IPv6）连接。这允许贸易伙伴使用 IPv4 或连接到您的 AS2 服务器 IPv6。

为您的服务器设置双栈 Application Load Balancer AS2

1. 使用以下设置创建 VPC：
   - 仅限 VPC
   - 手动 IPv4 CIDR 输入
   - 亚马逊提供 IPv6 的 CIDR 块
2. 在不同的可用区中创建至少两个子网：
   - IPv6 CIDRs 添加到子网
   - 创建子网时，仅分配 VPC IPv4/IPv6地址的子集，以便为其他子网留出可用的地址
3. 为 VPC 创建互联网网关。
4. 编辑路由表并添加两条路由：
   - 一条包含目的地的路线 `0.0.0.0/0`
   - 一条包含目的地的路线 `::/0`
   - 将两个路由目标都设置为您创建的互联网网关
5. 在步骤 1 AS2 中创建的 VPC 中创建启用了该功能的服务器。请务必指定`IpAddressType`为`DUALSTACK`。

   有关如何创建使用该 AS2 协议的 Transfer Family 服务器的详细信息，请参阅创建 AS2 服务器。
6. 创建目标组：
   - 对于 “指定群组详细信息”，请配置：

- 目标类型：IP 地址
- 姓名：输入姓名
- Protocol：HTTP
- 端口：5080
- VPC：选择您创建的 VPC
- 协议版本： HTTP1
- Health 检查：使用默认值

- 对于注册目标：
  - 输入 AS2 服务器的私有 IPv4 地址
  - 在下面选择 “包含为待处理”

7. 创建 Application Load Balancer：

- 输入一个名字
- 对于方案，请选择面向互联网
- 对于 IP 地址类型，请选择 Du alstack
- 对于网络映射：
  - 选择您创建的 VPC
  - 选择您在其中创建子网的可用区
- 对于安全组，请选择允许来自端口 80 上任何 IP 地址的入站 IPv6 流量 IPv4 和流量的安全组
- 对于监听器和路由：
  - Protocol：HTTP
  - Port：80
  - 默认操作：转发到您创建的目标群组
- 选择创建负载均衡器

在您创建 Application Load Balancer 之后，贸易伙伴可以使用其 DNS 名称向您的 AS2 服务器发送流量。此配置使您的 AS2 服务器能够通过双堆栈 Application Load Balancer 接受来自双方 IPv4 和 IPv6 客户端的连接。

编辑服务器详细信息

创建 Amazon Transfer Family 服务器后，可以编辑服务器配置。

主题

- 编辑文件传输协议
- 编辑服务器端点
- 编辑日志记录配置
- 编辑安全策略
- 更改服务器的托管工作流程
- 更改服务器的显示横幅
- 将服务器联机或脱机

编辑服务器的配置

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在左侧导航窗格中，选择服务器。
3. 选择服务器 ID 列中的标识符以查看服务器详细信息页面，如下所示。

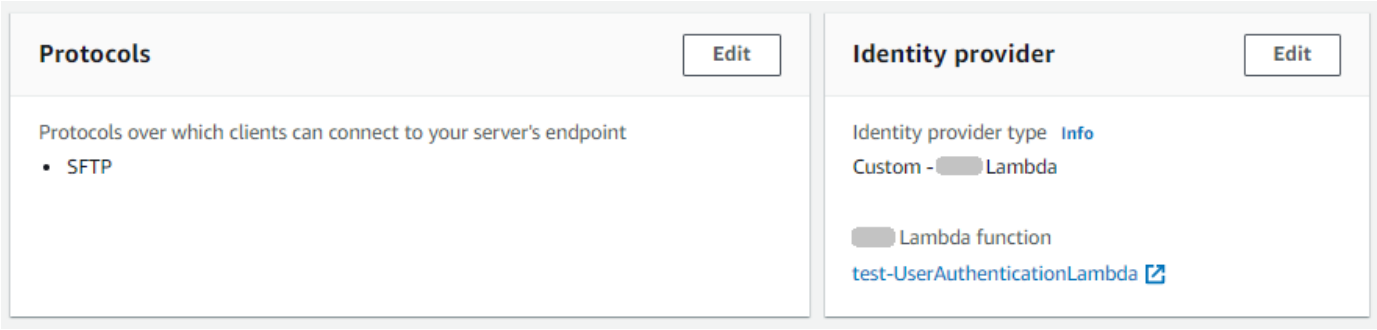
   您可以通过选择编辑来更改服务器的属性：

   - 要更改协议，请参阅 编辑文件传输协议。
   - 对于身份提供商，您现在可以在任何身份提供者类型（服务管理、 Amazon Directory Service 或自定义身份提供商）之间进行切换。有关更改身份提供者类型以及每次过渡所需的信息的详细信息，请参阅编辑身份提供商配置。
   - 要更改端点类型或自定义主机名，请参阅 编辑服务器端点。
   - 要添加协议，您需要先将协议 AS2 作为协议添加到您的服务器。有关更多信息，请参阅 编辑文件传输协议。
   - 要管理服务器的主机密钥，请参阅 管理启用 SFTP 的服务器的主机密钥。
   - 在其他详细信息下，您可以编辑以下信息：
     - 要更改日志记录角色，请参阅 编辑日志记录配置。
     - 要更改安全策略，请参阅 编辑安全策略。
     - 要更改服务器主机密钥，请参阅 管理启用 SFTP 的服务器的主机密钥。
     - 要更改服务器的托管工作流程，请参阅 更改服务器的托管工作流程。
     - 要编辑服务器的显示横幅，请参阅 更改服务器的显示横幅。
   - 在其他配置下，您可以编辑以下信息：

- SetStat 选项：启用此选项可忽略客户端尝试对您上传到 Amazon S3 存储桶的文件使用SETSTAT时生成的错误。有关其他详细信息，请参阅ProtocolDetails主题中的SetStatOption文档。
- TLS 会话恢复：提供一种机制来恢复或共享 FTPS 会话的控制和数据连接之间协商的私有密钥。有关其他详细信息，请参阅ProtocolDetails主题中的TlsSessionResumptionMode文档。
- 被动 IP：表示 FTP 和 FTPS 协议的被动模式。输入单个 IPv4 地址，例如防火墙、路由器或负载均衡器的公有 IP 地址。有关其他详细信息，请参阅ProtocolDetails主题中的PassiveIp文档。

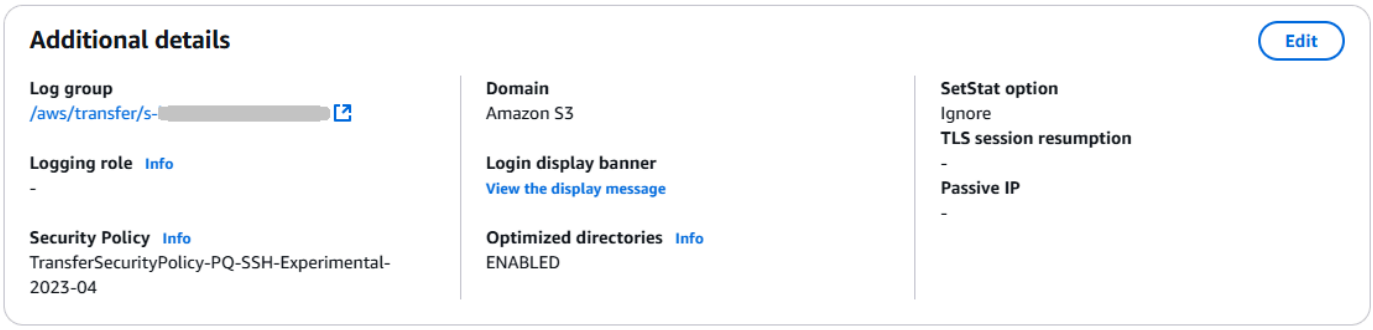
> **Note**
>
> 避免将网络负载均衡器 (NLBs) 或 NAT 网关放在 Amazon Transfer Family 服务器前面。这种配置会增加成本，并可能导致性能问题。有关更多详细信息，请参阅 避免将服务器放在 NLBs Amazon Transfer Family 服务器前面 NATs

- 要启动或停止服务器，请参阅 将服务器联机或脱机。
- 要删除服务器，请参阅 删除服务器。
- 要编辑用户的属性，请参阅 管理访问控制。



> **Note**
>
> 自 2022 年 9 月起，服务器主机密钥的描述和导入日期值是新的。引入这些值是为了支持多主机密钥功能。此功能需要迁移在引入多个主机密钥之前使用的所有单个主机密钥。已迁移服务器主机密钥的导入日期值设置为服务器的上次修改日期。也就是说，您看到的迁移主机密钥的日期与服务器主机密钥迁移之前上次以任何方式修改服务器的日期相对应。

迁移的唯一密钥是您最旧的或唯一的服务器主机密钥。任何其他密钥的实际日期均从您导入时算起。此外，迁移后的密钥具有描述，便于将其识别为已迁移。
迁移发生在 9 月 2 日至 9 月 13 日之间。此范围内的实际迁移日期取决于服务器所在的地区。



编辑文件传输协议

在 Amazon Transfer Family 控制台上，您可以编辑文件传输协议。文件传输协议将客户端连接到服务器的端点。

编辑协议

1. 在服务器详细信息页面上，选择协议旁边的编辑。
2. 在编辑协议页面，选中或清除协议复选框或复选框以添加或删除以下文件传输协议：

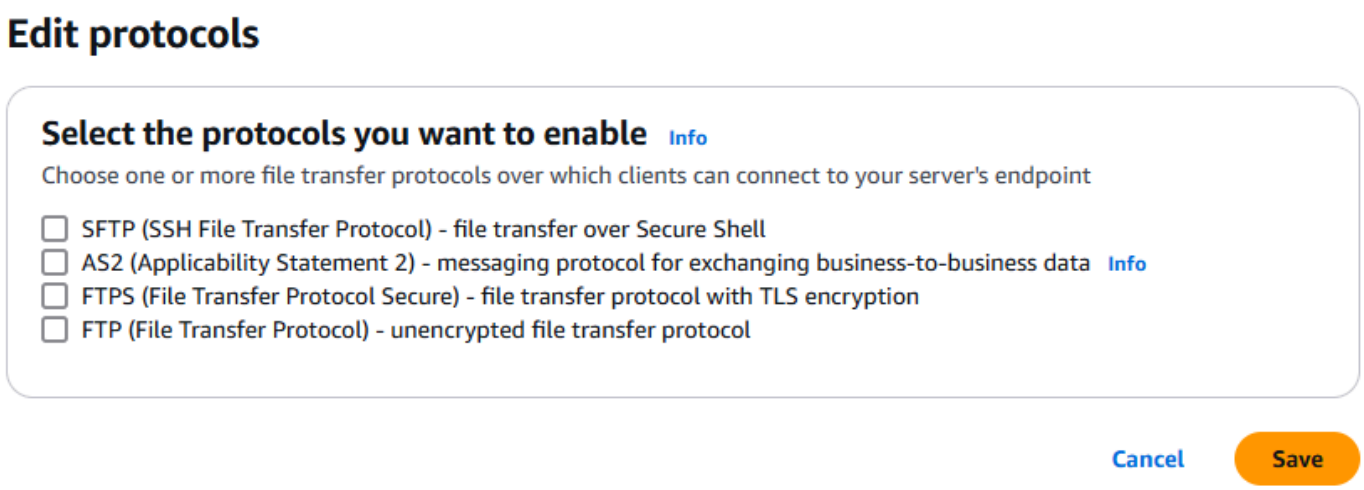
   - Secure Shell (SSH) 文件传输协议 (SFTP) — 通过 SSH 的文件传输

     有关 SFTP 的更多信息，请参阅 创建启用 SFTP 的服务器。
   - 文件传输协议安全 (FTPS) — 使用 TLS 加密的文件传输功能

     有关 FTP 的更多信息，请参阅 创建启用 FTPS 的服务器。
   - 文件传输协议 (FTP) — 未加密的文件传输功能

     有关 FTPS 的更多信息，请参阅 创建启用 FTP 的服务器。

> **Note**
>
> 如果现有服务器仅为 SFTP 启用，并且要添加 FTPS 和 FTP，则必须确保具有与 FTPS 和 FTP 兼容的正确身份提供商和端点类型设置。



如果选择 FTPS，则必须选择存储在 Amazon Certificate Manager (ACM) 中的证书，当客户端通过 FTPS 连接到服务器时，该证书将用于识别您的服务器。

要请求新的公有证书，请参阅 Amazon Certificate Manager 用户指南中的请求公有证书。

要将现有证书导入到 ACM 中，请参阅 Amazon Certificate Manager 用户指南中的将证书导入到 ACM。

要请求私有证书以通过私有 IP 地址使用 FTPS，请参阅 Amazon Certificate Manager 用户指南中的请求私有证书。

支持具有以下加密算法和密钥大小的证书：

- 2048 位 RSA (RSA_2048)
- 4096 位 RSA (RSA_4096)
- Elliptic Prime Curve 256 位 (EC_prime256v1)
- Elliptic Prime Curve 384 位 (EC_secp384r1)
- Elliptic Prime Curve 521 位 (EC_secp521r1)

> **Note**
>
> 该证书必须是指定了 FQDN 或 IP 地址的有效 SSL/TLS X.509 版本 3 证书，并包含有关颁发者的信息。

3. 选择保存。您将返回到服务器详细信息页面。

编辑服务器端点

在 Amazon Transfer Family 控制台上，您可以修改服务器端点类型和自定义主机名。此外，对于 VPC 终端节点，您可以编辑可用区信息。

要编辑服务器端点详细信息

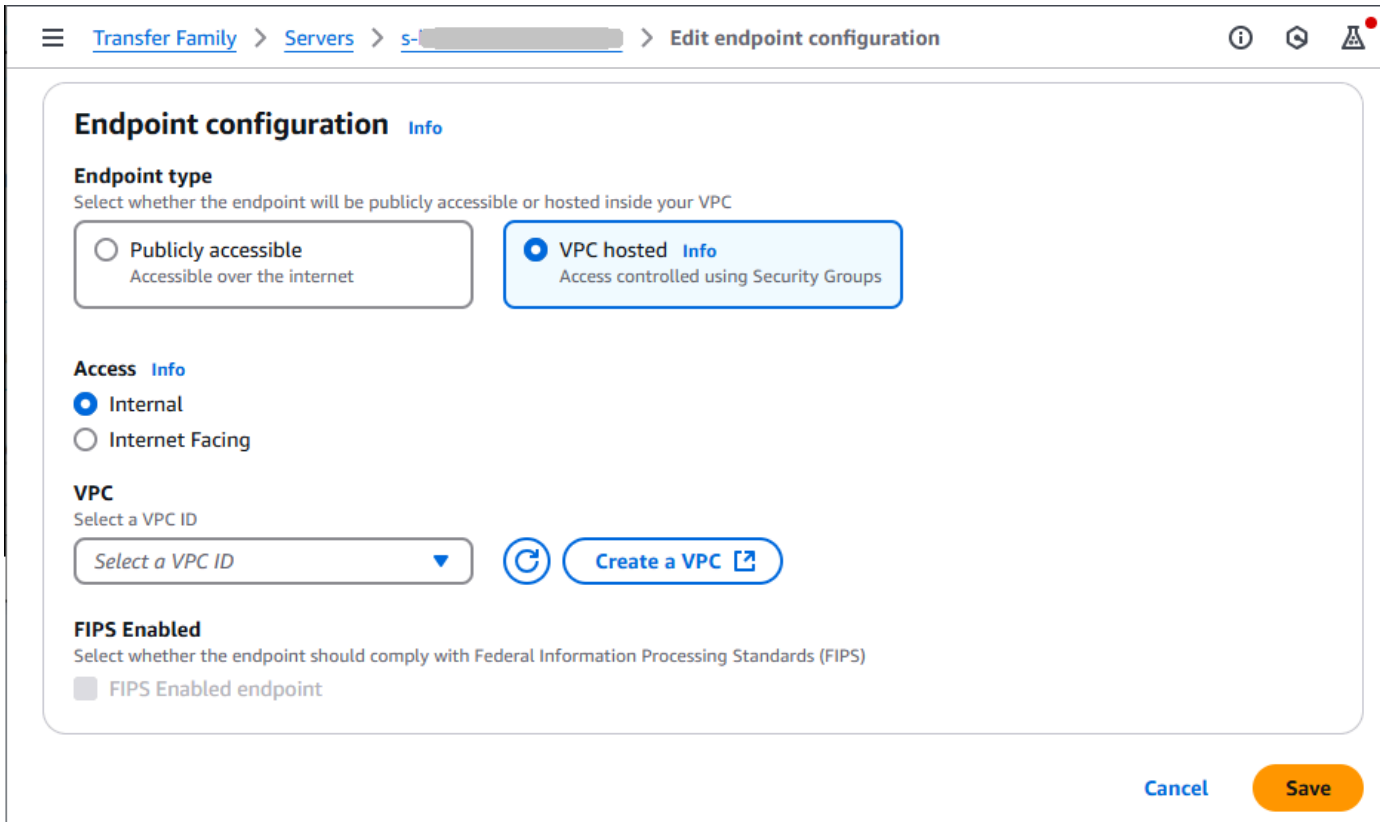
1. 在服务器详细信息页面上，选择端点详细信息旁边的编辑。
2. 在编辑端点类型之前，必须先停止服务器。然后，在编辑终端节点配置页面上，对于端点类型，您可以选择以下任一值：
   - 公有 — 通过此选项，您可以通过互联网访问服务器。
   - VPC — 通过此选项，您可以访问虚拟私有云 (VPC) 中的服务器。有关 VPC 的信息，请参阅 在虚拟私有云中创建服务器。
3. 对于自定义主机名，请选择以下选项之一：
   - 无 — 如果您不想使用自定义域，请选择无。

     您将获得由提供的服务器主机名 Amazon Transfer Family。服务器主机名使用格式 *serverId*.server.transfer.*regionId*.amazonaws.com。
   - Amazon Route 53 DNS 别名 — 要使用在 Route 53 中自动为您创建的 DNS 别名，请选择此选项。
   - 其他 DNS — 要使用您在外部 DNS 服务中已经拥有的主机名，请选择其他 DNS。

   选择 Amazon Route 53 DNS 别名或其他 DNS 可指定与服务器端点关联的名称解析方法。

   例如，您的自定义域可能是 `sftp.inbox.example.com`。自定义主机名使用由您提供并且 DNS 服务可以解析的 DNS 名称。您可以使用 Route 53 作为您 DNS 的解析程序，或者使用您自己的

DNS 服务提供商。要了解 Amazon Transfer Family 如何使用 Route 53 从自定义域将流量路由到服务器端点，请参阅 使用自定义主机名。



4. 对于 VPC 终端节点，您可以在可用区窗格中更改信息。
5. 选择保存。您将返回到服务器详细信息页面。

编辑日志记录配置

在 Amazon Transfer Family 控制台上，您可以更改日志配置。

> **Note**
>
> 如果 Transfer Family 在你创建服务器时为你创建了 CloudWatch 日志 IAM 角色，则会调用该 IAM 角色`AWSTransferLoggingAccess`。您可以将其用于所有的 Transfer Family 服务器。

要编辑日志记录配置

1. 在服务器详细信息页面上，选择其他详细信息旁边的编辑。

2. 根据您的配置，在日志记录角色、结构化 JSON 日志记录或两者之间进行选择。有关更多信息，请参阅 更新服务器的日志记录。

编辑安全策略

此过程说明如何使用 Amazon Transfer Family 控制台或更改 Transfer Family 服务器的安全策略 Amazon CLI。

> **Note**
>
> 如果您的终端节点已启用 FIPS，则无法将 FIPS 安全策略更改为非 FIPS 安全策略。

Console

使用控制台编辑安全策略

1. 在服务器详细信息页面上，选择其他详细信息旁边的编辑。
2. 在加密算法选项部分中，请选择包含允许服务器使用的加密算法的安全策略。

   有关安全策略的更多信息，请参阅 Amazon Transfer Family 服务器的安全策略。
3. 选择保存。

   您将返回到服务器详细信息页面，您可以在其中查看更新的安全策略。

Amazon CLI

使用 CLI 编辑安全策略

1. 运行以下命令以查看附加到您的服务器的当前安全策略。

   ```
   aws transfer describe-server --server-id your-server-id
   ```

   此`describe-server`命令返回服务器的所有详细信息，包括以下行：

   ```
   "SecurityPolicyName": "TransferSecurityPolicy-2018-11"
   ```

   在本例中，服务器的安全策略是`TransferSecurityPolicy-2018-11`。

2. 确保为命令提供安全策略的确切名称。例如，运行以下命令将服务器更新为TransferSecurityPolicy-2023-05。

```
aws transfer update-server --server-id your-server-id --security-policy-name
 "TransferSecurityPolicy-2023-05"
```

> **Note**
>
> 中列出了可用安全策略的名称Amazon Transfer Family 服务器的安全策略。

如果成功，该命令将返回以下代码，并更新服务器的安全策略。

```
{
    "ServerId": "your-server-id"
}
```

更改服务器的托管工作流程

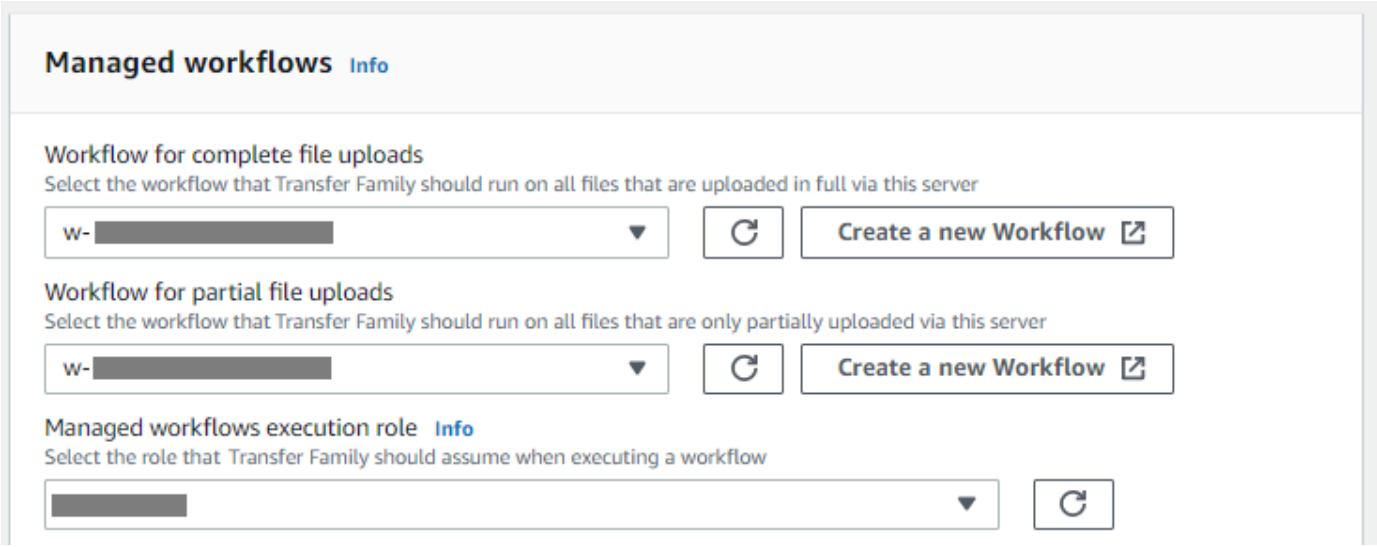
在 Amazon Transfer Family 控制台上，您可以更改与服务器关联的托管工作流程。

要更改托管工作流程

1. 在服务器详细信息页面上，选择其他详细信息旁边的编辑。
2. 在编辑其他详细信息页面的托管工作流程部分，选择要在所有上传中运行的工作流程。

> **Note**
>
> 如果您还没有工作流程，请选择创建新的工作流程来创建工作流程。

   a. 选择要使用的工作流程 ID。
   b. 选择执行角色。这是 Transfer Family 在执行工作流程步骤时所扮演的角色。有关更多信息，请参阅 适用于工作流程的 IAM 策略。选择 Save。



3. 选择保存。您将返回到服务器详细信息页面。

更改服务器的显示横幅

在 Amazon Transfer Family 控制台上，您可以更改与服务器关联的显示横幅。

要更改显示横幅

1. 在服务器详细信息页面上，选择其他详细信息旁边的编辑。
2. 在编辑其他详细信息页面的显示横幅部分，输入可用显示横幅的文本。
3. 选择保存。您将返回到服务器详细信息页面。

将服务器联机或脱机

在 Amazon Transfer Family 主机上，您可以将服务器置于联机状态或使其离线。

让您的服务器联机

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在导航窗格中，选择服务器。
3. 选中离线服务器的复选框。
4. 对于操作，选择启动。

服务器可能需要几分钟的时间才能从脱机状态切换到联机状态。

> **Note**
>
> 当您停止服务器以使其脱机时，目前仍在为该服务器累积服务费用。要消除基于服务器的附加费用，请删除该服务器。

让服务器离线

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在导航窗格中，选择服务器。
3. 选中在线服务器的复选框。
4. 对于操作，选择停止。

如果服务器正在启动或关闭，则该服务器无法用于文件操作。控制台不显示正在启动和正在停止状态。

如果您发现错误情况`START_FAILED`或`STOP_FAILED`，请联系 Amazon Web Services 支持 以帮助解决您的问题。

编辑身份提供商配置

您可以将服务器的身份提供者类型从任何类型更改为任何其他类型。可用的身份提供者类型有：

- 服务托管-将用户凭据存储在服务中
- Amazon Directory Ser vice — 使用 Amazon 托管的 Microsoft AD 或 Amazon 目录服务获取 Entra ID 域服务
- 自定义 — 使用 Lambda 函数或 Amazon API Gateway 与您现有的身份提供商集成

更改身份提供者类型时，您需要根据正在进行的过渡提供特定信息。以下各节描述了每种更改类型所需的信息。

> **Important**
>
> 更改身份提供者时的注意事项：
>
> - 用户迁移-更改身份提供者类型时，不会自动迁移现有用户配置。您需要在新的身份提供商系统中设置用户。

- 测试-在生产环境中进行更改之前，请彻底测试新的身份提供商配置。
- 权限 — 在进行更改之前，请确保新的身份提供商已配置必要的 IAM 权限和角色。

更改为服务托管身份提供商

从任何其他身份提供商类型更改为服务管理类型时，您需要：

- 选择 “服务托管” 作为身份提供者类型
- 更改完成 Amazon Transfer Family 后直接在中创建新用户，因为不会转移来自其他身份提供商的现有用户配置

示例：如果您要从自定义身份提供商更改为服务托管，则需要在服务中重新创建所有用户帐户及其关联权限。 Amazon Transfer Family

更改为 “ Amazon 目录服务”

从任何其他身份提供者类型更改为 Amazon Directory Service 时，您需要提供：

- 目录 — 为 Entra ID 域服务 Amazon 目录选择现有的 Amazon 托管 Microsoft AD 或目录服务
- 访问权限-选择是限制对特定群组的访问还是允许目录中的所有用户进行访问
- 访问角色 — 允许 Amazon Transfer Family 访问您的目录的 IAM 角色

示例：如果您要从服务管理更改为 Amazon Directory Service，则需要选择现有`d-1234567890`目录，选择限制对`TransferUsers`群组的访问权限，然后指定 `TransferDirectoryAccessRole` IAM 角色。

更改为自定义身份提供商

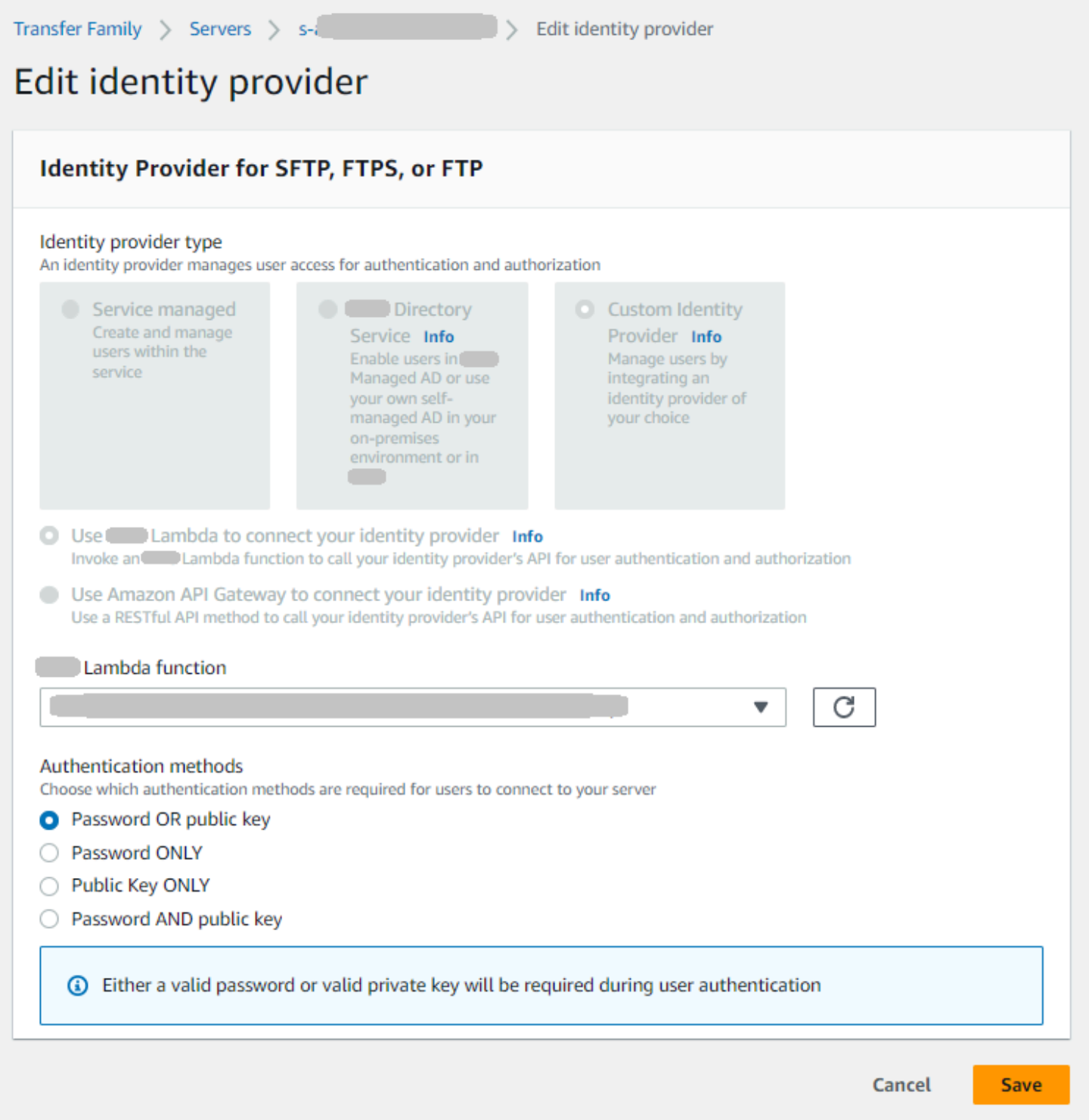
从任何其他身份提供商类型更改为自定义身份提供商时，您需要在 Lambda 函数或 Amazon API Gateway 之间进行选择，并提供所需的配置：

使用 Lambda 函数

对于 Lambda 函数集成，请提供：

- 函数-选择处理身份验证的现有 Lambda 函数
- 身份验证方法（对于 SFTP 协议）-选择密码、公钥或两者兼而有之

示例：如果您要从 D Amazon irectory Service 更改为自定义 Lambda 身份提供商，则需要选择自己的`TransferCustomAuth`函数并选择密码作为身份验证方法。

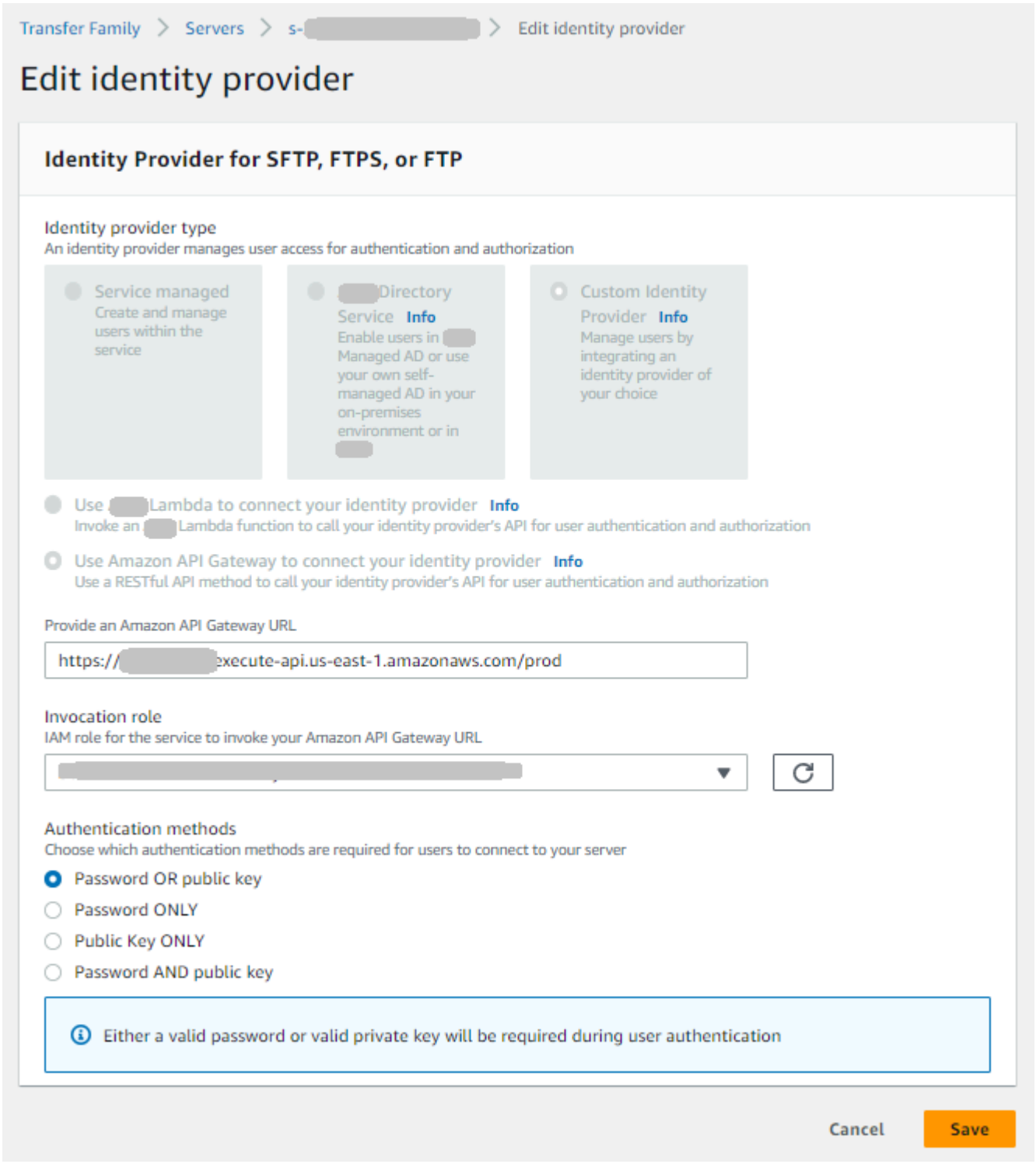


使用亚马逊 API Gateway

要集成 Amazon API Gateway，请提供：

- API Gateway 网址 — 您的 API 网关终端节点的调用网址
- 调用角色 — 允许调用您的 API Gatewa Amazon Transfer Family y 的 IAM 角色
- 身份验证方法（对于 SFTP 协议）-选择密码、公钥或两者兼而有之

示例：如果您要从服务管理更改为 API Gateway，则需要提供 URL`https://abcdef123.execute-api.us-east-1.amazonaws.com/prod`，指定 `TransferApiGatewayInvocationRole` IAM 角色，然后选择公钥作为身份验证方法。



从 Amazon API Gateway 更改为 Lambda 函数

常见的过渡是从 Amazon API Gateway 更改为 Lambda 函数以实现自定义身份提供商集成。此更改使您可以简化架构，同时保持相同的身份验证逻辑。

此过渡的关键注意事项：

- 相同的功能，不同的权限 — 您可以对 API Gateway 和直接 Lambda 集成使用相同的 Lambda 函数，但必须更新资源策略。
- 资源策略要求 — 更改为直接 Lambda 集成时，函数的资源策略除此之外还必须授予调用该函数的`transfer.amazonaws.com`权限。`apigateway.amazonaws.com`

要进行此更改

1. 更新您的 Lambda 函数的资源策略`transfer.amazonaws.com`以允许调用该函数。
2. 在 Amazon Transfer Family 控制台中，将身份提供商从 API Gateway 更改为 Lambda 函数。
3. 选择您的现有 Lambda 函数。
4. 测试配置以确保身份验证工作正常。

直接 Lambda 集成的资源策略示例：

```
{
   "Version":"2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Principal": {
         "Service": [
            "transfer.amazonaws.com",
            "apigateway.amazonaws.com"
         ]
      },
      "Action": "lambda:InvokeFunction",
      "Resource": "arn:aws:lambda:us-east-1:123456789012:function:function-name"
   }]
}
```

身份提供商过渡期间的用户保存

在身份提供商类型之间进行切换时，将在特定场景中保留现有用户配置，以便在出现问题时实现高效的回滚：

- 服务管理到自定义身份提供商然后返回 — 如果您从服务管理更改为自定义身份提供商，然后又更改为服务管理，则所有用户都将保留在他们上次已知的配置中。
- Amazon Directory Service 到自定义身份提供商然后返回 — 如果您从自定义身份提供商更改 Amazon Directory Service 为自定义身份提供商，然后又更改为 Amazon Directory Service，则委派访问组的所有定义都将保留在其上次已知的配置中。

这种保留行为允许您安全地测试自定义身份提供商配置并回滚到之前的设置，而不会丢失用户访问配置。

更改身份提供者时的重要注意事项

- 用户迁移-更改身份提供者类型时，不会自动迁移现有用户配置。您需要在新的身份提供商系统中设置用户。
- 测试-在生产环境中进行更改之前，请彻底测试新的身份提供商配置。
- 权限 — 在进行更改之前，请确保新的身份提供商已配置必要的 IAM 权限和角色。

管理启用 SFTP 的服务器的主机密钥

服务器主机密钥是 Transfer Family 服务器使用的私钥，用于向呼叫者提供唯一身份，并保证它是正确的服务器。这种保证是通过调用者的`known_hosts`文件中存在正确的公钥来强制执行的。（该`known_hosts`文件是大多数 SSH 客户端使用的一项标准功能，用于存储您所连接的服务器的公钥。）您可以通过为服务器运行`ssh-keyscan`来检索与您的服务器主机密钥相对应的公钥。

> **Important**
>
> 意外更改服务器的主机密钥会导致中断。根据您的 SFTP 客户端的配置方式，它可能会立即失败，并显示不存在可信主机密钥的消息，或者出现威胁性提示。如果有用于自动连接的脚本，它们很可能也会失败。

默认情况下，Amazon Transfer Family 会为启用 SFTP 的服务器生成主机密钥。您可以导入服务器主机密钥以保留主机身份并避免更新客户端信任存储库。 何时导入主机密钥列出了您可能想要这样做的几个原因。如果您不提供主机密钥，则会为您生成新的密钥。

Amazon Transfer Family 支持多个不同类型的主机密钥（RSA、ECDSA 和 ED25519），以提供与更广泛的客户端主机签名算法的兼容性。不同的密钥类型支持特定的算法：RSA 密钥启用 rsa-* 算

法，ECD SA 密钥启用 ecdsa-* 算法，密钥启用 ed 25519 算法。 ED25519 在创建服务器时规划密钥类型，因为在客户端开始与服务器交互之后引入其他密钥类型可能会对某些客户端造成干扰，并且可能与替换现有的主机密钥一样成问题。

为避免用户再次被提示验证启用了 SFTP 的服务器的真实性，请将本地服务器的主机密钥导入到启用了 SFTP 的服务器。这样做还可以防止您的用户收到有关潜在 man-in-the-middle攻击的警告。

作为一项额外的安全措施，您也可以定期轮换主机密钥。有关更多信息，请参阅 轮换服务器主机密钥。

> **Note**
>
> 服务器主机密钥由支持 SFTP 协议的服务器使用。

何时导入主机密钥

虽然 Amazon Transfer Family 可以自动生成主机密钥，但在以下几种情况下，导入自己的主机密钥会带来操作上的好处：

- 服务器迁移-您正在从现有服务器迁移到 Amazon Transfer Family 并希望避免更新现有客户端的客户端信任存储库（`known_hosts`文件）。
- 灾难恢复和故障转移-您有多 Amazon Transfer Family 台服务器（例如，一台位于美国东部（俄亥俄州），一台位于美国西部（俄勒冈）），它们共享相同的公有 DNS 名称。在两台服务器上使用相同的主机密钥可确保无缝故障转移，而不会出现客户端身份验证故障。
- 操作连续性-您希望主机密钥材料将来可用于其他服务器（Amazon Transfer Family 或其他服务器），以便在整个基础架构中保持一致的服务器身份。
- 算法控制-您希望通过提供更多主机密钥算法来提高客户端兼容性，或者您想通过仅提供与特定算法兼容的密钥来控制客户端可以使用的算法。

以下主题提供了管理服务器主机密钥的详细过程：

- 添加其他的服务器主机密钥-向服务器添加其他主机密钥
- 删除服务器主机密钥-从服务器上移除主机密钥
- 轮换服务器主机密钥-轮换主机密钥以增强安全性
- 其他服务器主机密钥信息-查看和管理主机密钥详细信息

添加其他的服务器主机密钥

在 Amazon Transfer Family 控制台上，您可以添加其他服务器主机密钥。添加其他不同格式的主机密钥对于在客户端连接到服务器时识别服务器以及改善您的安全配置文件非常适用。例如，如果您的原始密钥是 RSA 密钥，则可以添加其他 ECDSA 密钥。

> **Note**
>
> SFTP 客户端将使用配置中与密钥算法相匹配的最旧密钥进行连接。每种密钥类型（RSA、ECDSA 或 ED25519）的最旧密钥是该类型服务器的活动密钥。

Transfer Family 服务器有多种类型的主机密钥时的安全注意事项

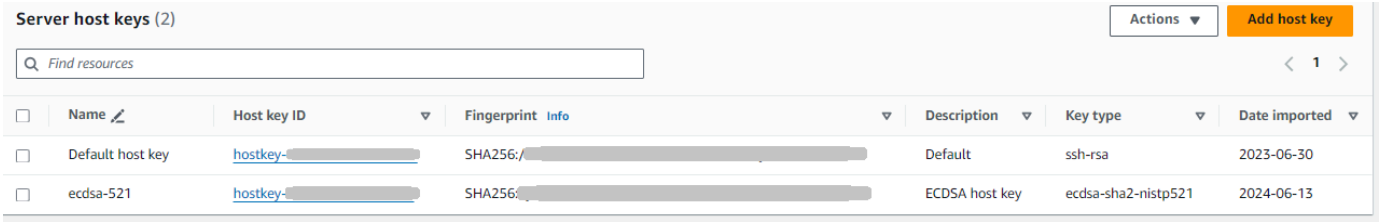
如果服务器有多种类型的主机密钥，则 SFTP 客户端可以按类型分配首选项。因此，当服务器有 RSA、ECDSA 和 ED25519 主机密钥时，选择将由类型的首选项决定。

现代 SFTP 客户端更喜欢使用 ECDSA 和 ED25519 主机密钥（如果它们存在）。如果要在服务器以前只有 RSA ED25519 密钥的情况下添加 ECDSA 或密钥，这一点就变得很重要。添加新的 ECDSA 或 ED25519 密钥可能会显示为对客户端的安全警告。

对于客户来说，密钥将显示为已更改，而实际上它并未更改：新密钥是在现有的 RSA 密钥之外添加的。如果您决定添加新类型的服务器主机密钥，请记住这一点。

要添加其他的服务器主机密钥

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在左侧导航窗格中，选择服务器，然后选择使用 SFTP 协议的服务器。
3. 在服务器详细信息页面上，向下滚动到服务器主机密钥部分。



4. 选择添加主机密钥。

   将显示添加服务器主机密钥页面。
5. 在“服务器主机密钥”部分，输入 RSA、ECDSA 或 ED25519 私钥，当客户端通过支持 SFTP 的服务器连接到服务器时，该密钥用于识别您的服务器。

> **Note**
>
> 创建服务器主机密钥时，请务必指定 `-N ""`（无密码）。有关如何生成密钥对的详细信息，请参阅 在 macOS、Linux 或 Unix 系统创建 SSH 密钥。

6. （可选）添加描述以区分多个服务器主机密钥。您可以为密钥添加标签。
7. 选择添加密钥。您将返回到服务器详细信息页面。

要使用 Amazon Command Line Interface (Amazon CLI) 添加主机密钥，请使用 ImportHostKeyAPI 操作并提供新的主机密钥。如果创建新的启用 SFTP 的服务器，则在 CreateServer API 操作中提供主机密钥作为参数。您也可以 Amazon CLI 使用更新现有主机密钥的描述。

以下示例`import-host-key` Amazon CLI 命令导入指定启用 SFTP 的服务器的主机密钥。

```
aws transfer import-host-key --description key-description --server-id your-server-id
 --host-key-body file://my-host-key
```

删除服务器主机密钥

在 Amazon Transfer Family 控制台上，您可以删除服务器主机密钥。

要删除服务器主机密钥

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 在左侧导航窗格中，选择服务器，然后选择使用 SFTP 协议的服务器。
3. 在服务器详细信息页面上，向下滚动到服务器主机密钥部分。

4. 在服务器主机密钥部分中，选择一个密钥，然后在操作下选择删除。
5. 在出现的确认对话框中，输入单词 **`delete`**，然后选择删除以确认要删除主机密钥。

主机密钥已从服务器页面中删除。

要使用删除主机密钥 Amazon CLI，请使用 DeleteHostKeyAPI 操作并提供服务器 ID 和主机密钥 ID。

以下示例delete-host-key Amazon CLI 命令删除指定启用 SFTP 的服务器的主机密钥。

```
aws transfer delete-host-key --server-id your-server-id --host-key-id your-host-key-id
```

轮换服务器主机密钥

您可以定期轮换服务器主机密钥。本主题介绍服务器如何选择要应用的密钥，以及轮换这些密钥的过程。

客户端如何选择服务器主机密钥

Transfer Family 选择应用哪个服务器密钥的方式取决于 SFTP 客户端的条件，如下所述。假设有一个较旧的密钥和一个较新的密钥。

- SFTP 客户端之前没有服务器的公用主机密钥。客户端首次连接到服务器时，会发生以下任一情况：
  - 如果配置为连接失败，则客户端会导致连接失败。
  - 或者，客户端选择与可能的可用算法相匹配的第一个密钥，并询问用户该密钥是否可信。如果是，则客户端会自动更新known_hosts文件（或客户端用来记录信任决策的任何本地配置文件或资源）并输入该密钥。
- SFTP 客户端known_hosts的文件中有一个较旧的密钥。即使存在较新的密钥，客户端也倾向于将此密钥用于此密钥的算法或其他算法。这是因为客户端对其known_hosts文件中的密钥具有更高的信任度。
- SFTP 客户端的密钥文件中包含新密known_hosts钥（采用任何可用的算法）。客户端会忽略旧密钥，因为它们不受信任，而是使用新密钥。
- SFTP 客户端known_hosts的文件中包含两个密钥。客户端通过索引选择与服务器提供的可用密钥列表相匹配的第一个密钥。

Transfer Family 更喜欢 SFTP 客户端在其known_hosts文件中包含所有密钥，因为这样在连接到 Transfer Family 服务器时可以获得最大的灵活性。密钥轮换基于这样一个事实，即同一个 Transfer Family 服务器known_hosts的文件中可能存在多个条目。

轮换服务器主机密钥程序

例如，假设您已将以下一组服务器主机密钥添加到 Transfer Family 服务器中。

服务器主机密钥

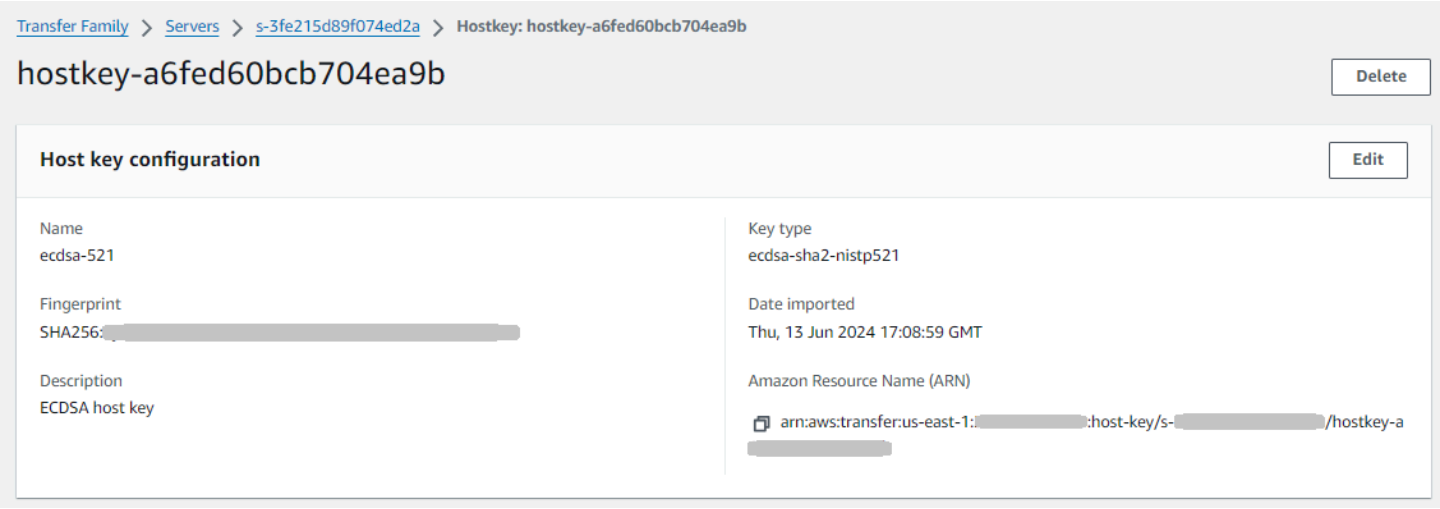
主机密钥类型	添加到服务器的日期
RSA	2020 年 4 月 1 日
ECDSA	2020 年 2 月 1 日
ED25519	2019 年 12 月 1 日
RSA	2019 年 10 月 1 日
ECDSA	2019 年 6 月 1 日
ED25519	2019 年 3 月 1 日

要轮换服务器主机密钥

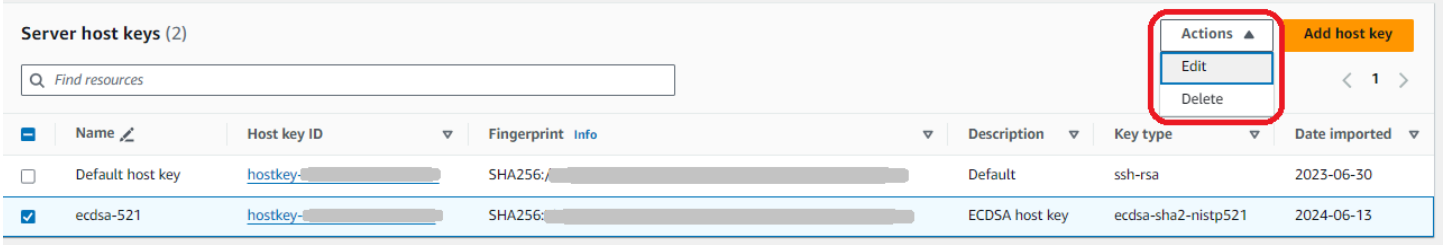
1. 添加新的服务器主机密钥。有关此过程的说明，请参阅 添加其他的服务器主机密钥。
2. 删除您之前添加的一个或多个相同类型的主机密钥。有关此过程的说明，请参阅 删除服务器主机密钥。
3. 所有按键均可见，并且可以处于活动状态，具体取决于前面中描述的行为客户端如何选择服务器主机密钥。

其他服务器主机密钥信息

您可以选择主机密钥以显示该密钥的详细信息。



您可以删除主机密钥，也可以从服务器详细信息屏幕上的操作菜单中编辑其描述。选择主机密钥，然后从菜单中选择相应的操作。



在控制台中监控使用情况

您可以在服务器详细信息页面上获取有关服务器指标的信息。这为您提供了一处位置以监控文件传输工作负载。您可以使用集中式控制面板跟踪与合作伙伴交换文件的数量，并密切跟踪其使用情况。有关更多信息，请参阅 查看 SFTP、FTPS 和 FTP 服务器的详细信息。下表描述了可用于 Transfer Family 的指标。

命名空间	指标	说明
AWS/Transfer	BytesIn	传输至服务器的字节总数。 报告标准： • Fo SFTP/FTP/FTPS r：在与 Transfer Family 服务器建立连接时每 5 分钟发出一次。如果在此期间没有传输任何文件或字节，则发出 “0”。 • 用于 AS2：当客户在其 AS2 服务器上收到一条消息并在入站消息处理完成后立即发出时 单位：计数 时长：5 分钟
	BytesOut	从服务器传出来的字节总数。 报告标准： • Fo SFTP/FTP/FTPS r：在与 Transfer Family 服务器建立连接时每 5 分钟发出一次。如果在此期间没有传输任何文件或字节，则发出 “0”。

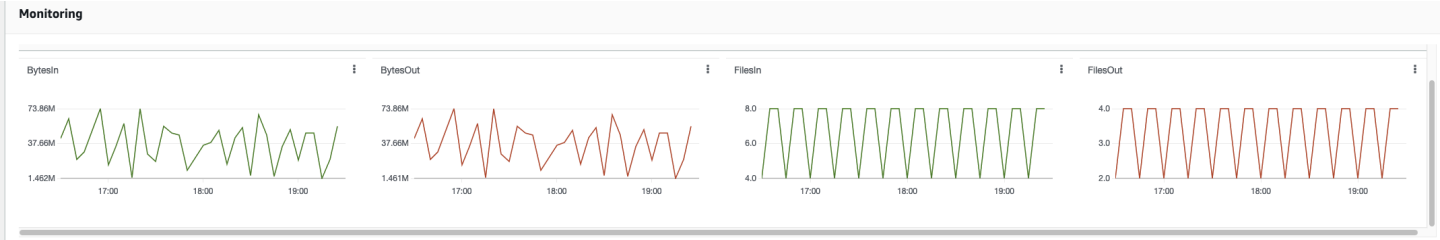
命名空间	指标	说明
		• 用于 AS2：当客户StartFileTransfer 从其 AS2 连接器呼叫并在出站消息处理完成后立即发出时。 单位：计数 时长：5 分钟
	FilesIn	传输至服务器的字节总数。 对于使用该 AS2 协议的服务器，此指标表示收到的消息数量。 报告标准： • Fo SFTP/FTP/FTPS r：在与 Transfer Family 服务器建立连接时每 5 分钟发出一次。如果在此期间没有传输任何文件或字节，则发出 “0”。 • 用于 AS2：当客户在其 AS2 服务器上收到一条消息，并在入站消息处理完毕后立即发出。 单位：计数 时长：5 分钟

命名空间	指标	说明
	FilesOut	从服务器传出来的字节总数。 报告标准： • Fo SFTP/FTP/FTPS r：在与 Transfer Family 服务器建立连接时每 5 分钟发出一次。如果在此期间没有传输任何文件或字节，则发出 “0”。 • 用于 AS2：当客户StartFileTransfer 从其 AS2 连接器呼叫并在出站消息处理完成后立即发出时。 单位：计数 时长：5 分钟
	InboundMessage	成功从交易伙伴处收到的 AS2 消息总数。 报告标准：当客户在其 AS2 服务器上收到一条消息并在成功处理入站消息后立即发出时 单位：计数 时长：5 分钟
	InboundFailedMessage	未成功从贸易伙伴处收到的 AS2 消息总数。也就是说，交易伙伴发送了一条消息，但是 Transfer Family 服务器无法成功处理该消息。 报告标准：当客户在其 AS2 服务器上收到一条消息并在入站消息处理失败后立即发出时 单位：计数 时长：5 分钟

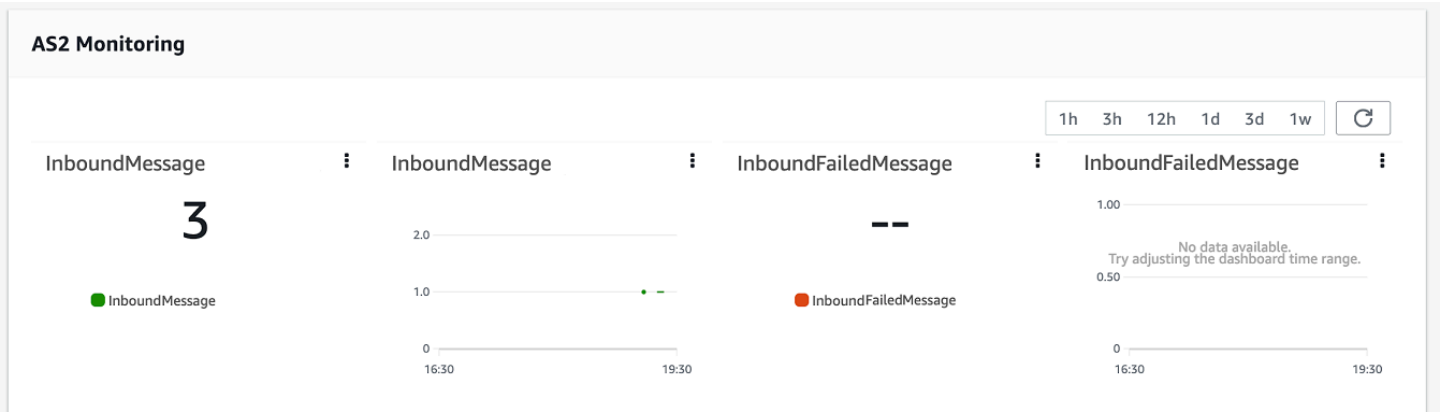
命名空间	指标	说明
	OnUploadExecutionsStarted	服务器上启动的工作流程执行总数。 报告标准：每次执行开始时触发 单位：计数 时间段：1 分钟
	OnUploadExecutionsSuccess	服务器上执行成功的工作流程总数。 报告标准：每次执行成功完成时触发 单位：计数 时间段：1 分钟
	OnUploadExecutionsFailed	在服务器上启动的失败工作流程执行总数。 报告标准：每次执行未成功完成时触发 单位：计数 时间段：1 分钟
	OutboundMessage	成功发送给交易伙伴的 AS2 消息总数。 报告标准：当客户StartFileTransfer 从其 AS2 连接器呼叫并在成功处理出站消息后立即发出时 单位：计数 时长：5 分钟

命名空间	指标	说明
	OutboundFailedMessage	未成功发送给贸易伙伴的 AS2 消息总数。 报告标准：当客户StartFileTransfer 从其 AS2 连接器呼叫并在出站消息处理失败后立即发出时 单位：计数 时长：5 分钟

监控部分包含四个单独的图表。这些图表显示了字节输入、字节输出、文件输入和文件输出。



对于启用了 AS2 协议的服务器，“AS2监控” 信息下方有一个 “监控” 部分。本节包含成功和失败的入站消息数的详细信息。



要在自己的窗口中打开所选图表，请选择展开图标
()。
您也可以单击图表的垂直省略号图标
()
以打开包含以下项目的下拉菜单：

- 放大 — 在自己的窗口中打开所选图表。

- 刷新 — 使用最新数据重新加载图表。
- 在指标中查看-在 Amazon 中打开相应的指标详情 CloudWatch。
- 查看日志-在中打开相应的日志组 CloudWatch。

管理访问控制

您可以使用 Amazon Identity and Access Management (IAM) 策略控制用户对 Amazon Transfer Family 资源的访问权限。IAM 策略是一个语句（通常采用 JSON 格式），它允许对资源进行特定级别的访问。您可以使用 IAM 策略来定义希望允许用户执行和不执行哪些文件操作。您还可以使用 IAM 策略来定义希望允许用户访问哪些 Amazon S3 存储桶。要为用户指定这些策略，您需要为其创建一个 IAM 策略和与之关联的信任关系的 IAM 角色。 Amazon Transfer Family

为每个用户分配一个 IAM 角色。 Amazon Transfer Family 使用的 IAM 角色类型称为服务角色。当用户登录到您的服务器时， Amazon Transfer Family 将使用映射到该用户的 IAM 角色。要了解如何创建向用户提供对 Amazon S3 存储桶的访问权限的 IAM 角色，请参阅 IAM 用户指南中的创建向 Amazon 服务委派权限的角色。

您可以使用 IAM 策略中的特定权限授予对 Amazon S3 对象的只写访问权限。有关更多信息，请参阅授予仅写入和列出文件的权限。

Amazon 存储博客包含一篇详细介绍如何设置最低权限访问权限的文章。有关详细信息，请参阅在Amazon Transfer Family 工作流程中实现最低权限访问权限。

> **Note**
>
> 如果您的 Amazon S3 存储桶使用 Amazon Key Management Service (Amazon KMS) 进行加密，则必须在策略中指定其他权限。有关更多信息，请参阅 数据保护和加密。此外，您可以在 IAM 用户指南中查看有关会话策略的更多信息。

主题

- 允许对 Amazon S3 存储桶的读取和写入访问权限
- 为 Amazon S3 存储桶创建会话策略
- 动态权限管理方法

允许对 Amazon S3 存储桶的读取和写入访问权限

此部分说明了如何创建 IAM 策略，以允许对特定 Amazon S3 存储桶进行读写访问。向您的用户分配具有此 IAM 策略的 IAM 角色后，该用户 read/write 便可以访问指定的 Amazon S3 存储桶。

以下策略允许通过编程方式对 Amazon S3 存储桶进行读写访问。只有当您需要启用跨账户存取时，才需要 GetObjectACL 和 PutObjectACL 语句。也就是说，您的 Transfer Family 服务器需要访问其他账户中的存储桶。

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid":"ReadWriteS3",
      "Action": [
            "s3:ListBucket"
                ],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectACL",
        "s3:PutObjectACL"
      ],
      "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket/*"]
    }
  ]
}
```

ListBucket 操作需要对存储桶本身的权限。PUT、GET 和 DELETE 操作需要对象权限。由于这些资源不同，因此使用不同的 Amazon 资源名称 (ARNs) 来指定。

要进一步限制用户，使其只能访问具有指定 home 前缀的 Amazon S3 存储桶，请参阅 为 Amazon S3 存储桶创建会话策略。

为 Amazon S3 存储桶创建会话策略

会话策略是一项 Amazon Identity and Access Management (IAM) 策略，它限制用户访问 Amazon S3 存储桶的某些部分。它通过实时评估访问来做到这一点。

> **Note**
>
> 会话策略仅适用于 Amazon S3。对于 Amazon EFS，您可以使用 POSIX 文件权限限制访问权限。

当您需要向一组用户授予对 Amazon S3 存储桶的特定部分的相同访问权限时，可以使用会话策略。例如，一组用户可能仅需访问 home 目录。该组用户共享相同的 IAM 角色。

> **Note**
>
> 路径的长度上限是 2048 个字符。有关更多详细信息，请参阅 API 参考中 `CreateUser` 操作的策略请求参数。

要创建会话策略，请在 IAM 策略中使用以下策略变量：

- `${transfer:HomeBucket}`
- `${transfer:HomeDirectory}`
- `${transfer:HomeFolder}`
- `${transfer:UserName}`

> **Important**
>
> 您不能在托管策略中使用前述变量。也不能在 IAM 角色定义中将其用作策略变量。您可以在 IAM 策略中创建这些变量，并在设置用户时直接提供这些变量。另外，您不能在此会话策略中使用 `${aws:Username}` 变量。此变量引用了 IAM 用户名而不是 Amazon Transfer Family所需的用户名。

会话策略示例

以下代码所示为会话策略示例。

```
{
  "Version":"2012-10-17",
  "Statement": [
      {
          "Sid": "AllowListingOfUserFolder",
          "Action": [
              "s3:ListBucket"
          ],
          "Effect": "Allow",
          "Resource": [
              "arn:aws:s3:::${transfer:HomeBucket}"
          ],
          "Condition": {
              "StringLike": {
                  "s3:prefix": [
                      "${transfer:HomeFolder}/*",
                      "${transfer:HomeFolder}"
                  ]
              }
          }
      },
      {
          "Sid": "HomeDirObjectAccess",
          "Effect": "Allow",
          "Action": [
              "s3:PutObject",
              "s3:GetObject",
              "s3:DeleteObjectVersion",
              "s3:DeleteObject",
              "s3:GetObjectVersion",
              "s3:GetObjectACL",
              "s3:PutObjectACL"
          ],
          "Resource": "arn:aws:s3:::${transfer:HomeDirectory}/*"
       }
  ]
}
```

> **Note**
>
> 前面的策略示例假设用户的主目录设置为包含尾部斜杠，以表示它是一个目录。另一方面，如果您设置的用户 HomeDirectory 不带尾部的斜杠，则应将其作为策略的一部分。

在前面的示例策略中，请注意使用transfer:HomeFolder、transfer:HomeBucket和transfer:HomeDirectory策略参数。这些参数是为用户配置的设置的，如HomeDirectory和中所述实施您的 API Gateway 方法。HomeDirectory这些参数具有以下定义：

- transfer:HomeBucket参数将替换为的HomeDirectory第一个组件。
- transfer:HomeFolder 参数将替换为 HomeDirectory 参数的其余部分。
- transfer:HomeDirectory参数删除了前导正斜杠 (/)，因此可以在Resource语句中将其用作 S3 Amazon 资源名称 (ARN) 的一部分。

> **Note**
>
> 如果您使用的是逻辑目录（即用户的homeDirectoryType是LOGICAL），则不支持这些策略参数（HomeBucket、HomeDirectory和HomeFolder）。

例如，假设为 Transfer Family 用户配置的 HomeDirectory 参数是 /home/bob/amazon/stuff/。

- transfer:HomeBucket 设置为 /home。
- transfer:HomeFolder 设置为 /bob/amazon/stuff/。
- transfer:HomeDirectory 变为 home/bob/amazon/stuff/。

第一个"Sid"允许用户列出从/home/bob/amazon/stuff/开始的所有目录。

第二个 "Sid" 限制用户对同一路径 /home/bob/amazon/stuff/ 的 put 和 get 访问权限。

借助上述策略，当用户登录时，他们只能访问其主目录中的对象。在连接时， Amazon Transfer Family 将这些变量替换为适合用户的值。这样做可以更轻松地将相同的策略文档应用于多个用户。此方法减少了用于管理用户对 Amazon S3 存储桶的访问的 IAM 角色和策略管理的开销。

您还可以使用会话策略以根据业务需求自定义每个用户的访问权限。有关更多信息，请参阅 IAM 用户指南 AssumeRoleWithWebIdentity中的权限 AssumeRole、 AssumeRoleWith SAM L 和。

> **Note**
>
> Amazon Transfer Family 存储策略 JSON，而不是策略的亚马逊资源名称 (ARN)。因此，当您在 IAM 控制台中更改策略时，您需要返回 Amazon Transfer Family 控制台并向用户更新最新的策略内容。您可以在用户配置部分的策略信息选项卡上更新用户。
> 如果您使用的是 Amazon CLI，则可以使用以下命令来更新策略。
>
> ```
> aws transfer update-user --server-id server --user-name user --policy \
>    "$(aws iam get-policy-version --policy-arn policy --version-id version --
> output json)"
> ```

会话策略的嵌套替换

Transfer Family 会话策略中不执行嵌套替换。会话策略可以使用嵌套变量，例如${transfer:HomeDirectory}。处理策略时，外部变量（例如，${transfer:HomeDirectory}）可能会被包含另一个变量的值（例如 {amzn-s3-demo-bucket:/$(transfer:UserName}）替换。但是，嵌套变量不会被实际用户名（例如 johndoe）进一步替换。

这意味着，在为 Transfer Family 创建会话策略时，您需要考虑这种行为，并确保相应地设计策略结构和变量用法。嵌套变量可能无法按预期解析，并且策略可能无法授予预期权限。必须彻底测试和验证会话策略，以确保它们按预期运行。在为您的 Transfer Family 环境实施访问控制和权限时，此行为是一个关键考虑因素。

解决此问题的一种方法是在会话策略中使用实际的 Amazon S3 存储桶名称。因此，例如，与其在会话策略${transfer:HomeDirectory}中指定，不如使用以下内容，其中 amzn-s3-demo-bucket 是您的实际存储桶：。${amzn-s3-demo-bucket/transfer:UserName}

动态权限管理方法

了解 Transfer Family 权限架构

Amazon Transfer Family 支持通过会话策略进行动态权限管理，允许您在运行时限制 IAM 角色的有效权限。这种方法适用于服务托管用户和自定义身份提供商用户，但仅在向 Amazon S3（不是 Amazon EFS）传输文件或从中传输文件时才受支持。

每个 Amazon Transfer Family 用户都使用权限模型进行操作，该模型包括：

1. 基本 IAM 角色-定义用户的基础权限
2. 可选会话策略-在运行时限制（范围缩小）基本权限

有效权限是基本角色权限和会话策略权限的交集。会话策略只能限制权限；它们不能授予超出基本角色允许范围的其他权限。

此架构适用于两种用户类型：

- 服务管理的用户-可以直接在用户设置中配置会话策略
- 自定义身份提供商用户-会话策略可以作为身份验证响应的一部分返回，也可以存储在 Amazon Secrets Manager

两种权限管理方法

在为需要独特访问模式的 Transfer Family 用户设计权限时，您可以选择两种主要方法：

每个用户一个角色

为每个 Transfer Family 用户创建一个单独的 IAM 角色，该角色具有针对该用户需求量身定制的特定权限。在以下情况下使用此方法：

- 每个用户需要的权限截然不同
- 权限管理由组织中的不同人员处理
- 您需要对个人用户访问权限进行精细控制

与会话策略共享角色

使用具有广泛权限的单个 IAM 角色（例如访问包含多个用户主目录的整个 Amazon S3 存储桶），并应用会话策略将每个用户限制在其特定区域内。与为每个用户管理单独的角色相比，这种方法可以显著减少管理开销。在以下情况下使用此方法：

- 用户需要类似类型的访问权限，但需要不同的资源（例如，所有用户都需要 read/write 访问权限，但每个用户只能访问自己的文件夹）
- 你想简化角色管理，避免创建数十或数百个个人角色
- 用户只能在共享存储桶中访问其指定的主目录
- 权限管理集中在您的组织内

例如，与其为用户 “alice”、“bob” 和 “charlie” 创建单独的角色，不如创建一个可以访问整个`s3://company-transfers/`存储桶的角色，然后使用会话策略将 alice 限制为`s3://company-transfers/alice/`、bob 限制为`s3://company-transfers/bob/`，依此类推。

实施会话策略

会话策略的工作原理是限制分配给用户的基本 IAM 角色的有效权限。最终权限是角色权限和会话策略权限的交集。

您可以通过两种方式实现动态会话策略：

变量替换

`${transfer:HomeBucket}`在会话策略中使用 Transfer `${transfer:Username}` Family 策略变量，例如`${transfer:HomeDirectory}`、和。这些变量在运行时会自动替换为实际值。有关这些变量的更多信息，请参阅为 Amazon S3 存储桶创建会话策略。

动态生成

对于自定义身份提供商，生成会话策略 on-the-fly作为您的 Lambda 函数或 API Gateway 方法的身份验证响应的一部分。这种方法允许您在身份验证时根据用户属性、群组成员资格或外部数据源创建高度自定义的策略。

您还可以 Amazon Secrets Manager 通过添加以会话策略 JSON 作为值命名的`Policy`密钥来存储预生成的会话策略。这使您可以跨多个用户使用相同的广泛的 IAM 角色，同时保持特定于用户的访问控制。

> **Note**
>
> 仅支持进出 Amazon S3 的文件传输和传出会话策略。它们不适用于 Amazon EFS 文件系统。对于 Amazon EFS，权限由 UID/GID 文件系统本身管理，权限位应用于文件系统本身。

按用户类型实现情况

服务托管用户

对于服务管理的用户，您可以通过 Amazon Transfer Family 控制台、API 或 CLI 直接在用户配置中指定会话策略。有关更多信息，请参阅 与服务托管用户合作。

自定义身份提供程序用户

对于自定义身份提供商用户，您可以通过两种方式提供会话策略：

- Amazon Secrets Manager 通过包括一个`Policy`以会话策略作为值命名的密钥
- 直接在 Lambda 函数响应或 API Gateway 响应中作为身份验证结果的一部分

有关更多信息，请参阅 自定义身份提供商解决方案。

示例：使用会话策略简化角色管理

此示例演示了动态权限管理如何在维护安全的同时显著减少管理开销。

场景

您的组织有 50 个用户需要 SFTP 访问权限才能传输文件。每个用户只能在名为的共享 Amazon S3 存储桶中访问自己的文件夹`company-transfers`。如果没有会话策略，则需要创建 50 个单独的 IAM 角色。

传统方法（无会话策略）

- 创建 50 个 IAM 角色：`TransferRole-Alice`、`TransferRole-Bob`、`TransferRole-Charlie`、、等
- 每个角色仅具有访问该用户文件夹的特定权限
- 管理权限需要更新各个角色
- 添加新用户需要创建新角色

动态方法（使用会话策略）

- 创建 1 个 IAM 角色：`TransferRole-Shared`拥有对整个存储桶的广泛权限
- 使用会话策略将每个用户限制在运行时访问其特定文件夹
- 管理权限需要更新一个角色或会话策略模板

- 添加新用户不需要新角色，只需配置用户即可

实施

以下是您将如何实现动态方法（以company-transfers存储桶为例，将其替换为实际的 Amazon S3 存储桶）：

实现动态权限管理

1. 创建一个具有广泛的 Amazon S3 权限的共享 IAM 角色：

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject"
      ],
      "Resource": "arn:aws:s3:::company-transfers/*"
    },
    {
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::company-transfers"
    }
  ]
}
```

2. 创建限制用户文件夹访问权限的会话策略模板：

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
```

```
        "s3:DeleteObject"
      ],
      "Resource": "arn:aws:s3:::company-transfers/${transfer:Username}/*"
    },
    {
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::company-transfers",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${transfer:Username}*"
        }
      }
    }
  ]
}
```

3. 为每位用户配置以下内容：

   - 共享的 IAM 角色
   - 会话策略的应用方式如下：
     - 服务管理的用户：在创建或修改用户时，使用 API 或 CLI 通过策略参数应用 JSON（控制台仅提供预定义的策略选项）
     - 自定义身份提供商用户：要么在身份验证期间将其作为 Lambda 函数响应的一部分返回，要么将其 Amazon Secrets Manager 作为名为 “Policy” 的密钥与用户的证书一起存储
   - 主目录：`/company-transfers/${transfer:Username}/`

Amazon CloudTrail 正在登录 Amazon Transfer Family

Amazon Transfer Family 与两者 Amazon CloudTrail 和 Amazon 集成 CloudWatch。 CloudTrail 并 CloudWatch 用于不同但互补的目的。

- 本主题介绍与的集成 CloudTrail ，该 Amazon 服务可记录在您的内部执行的操作 Amazon Web Services 账户。它持续监控和记录控制台登录、 Amazon Command Line Interface 命令和操作等活动的 API 操作。 SDK/API 这使您可以记录谁在何时何地采取了什么行动。 CloudTrail 通过提供 Amazon 环境中所有活动的历史记录，帮助审计、访问管理和监管合规性。有关详细信息，请参阅《Amazon CloudTrail 用户指南》。
- Amazon Amazon Transfer Family 服务器 CloudWatch 登录涵盖与 CloudWatch Amazon 资源和应用程序监控服务的集成。它收集指标和日志，以提供对资源利用率、应用程序性能和整体系统运行状况的可见性。 CloudWatch 帮助完成操作任务，例如故障排除、设置警报和自动缩放。有关详情，请参阅 Amazon CloudWatch 用户指南。

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 Amazon 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 操作的有序堆栈跟踪，因此它们不会按任何特定的顺序出现。

要持续记录您 Amazon 账户中的事件，包括的事件 Amazon Transfer Family，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。预设情况下，在控制台中创建跟踪时，此跟踪应用于所有 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 Amazon 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，请参阅下列内容：

- 创建跟踪记录概述
- CloudTrail 支持的服务和集成
- 配置 Amazon SNS 通知 CloudTrail
- 接收来自多个区域的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail 日志文件

所有 Amazon Transfer Family 操作都由记录 CloudTrail 并记录在中ActionsAPI reference。例如，调用`ListUsers`和`StopServer`操作会在 CloudTrail 日志文件中生成条目。`CreateServer`

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：

- 请求是使用根凭证还是 Amazon Identity and Access Management 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 userIdentity 元素。

如果您创建了跟踪，则可以允许将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括的事件 Amazon Transfer Family。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” 中查看最新的事件。

使用收集的信息 CloudTrail，您可以确定向哪个请求发出 Amazon Transfer Family、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。

要了解更多信息 CloudTrail，请参阅《Amazon CloudTrail 用户指南》。

主题

- 启用 Amazon CloudTrail 日志记录
- 创建服务器的日志条目示例
- 数据访问日志示例

启用 Amazon CloudTrail 日志记录

您可以使用监控 Amazon Transfer Family API 操作 Amazon CloudTrail。通过监控 API 操作，您可以获得有用的安全和操作信息。如果您启用了 Amazon S3 对象级日志记录，则 `RoleSessionName` 以 `[AWS:Role Unique Identifier]/username.sessionid@server-id` 形式包含在“请求者”字段。有关 Amazon Identity and Access Management (IAM) 角色唯一标识符的更多信息，请参阅Amazon Identity and Access Management 用户指南中的唯一标识符。

> **Important**
>
> `RoleSessionName` 名称的长度上限是 64 个字符。如果 `RoleSessionName` 较长，则 `server-id` 会被截断。

启用 Amazon S3 数据事件

要跟踪 Amazon Transfer Family 在 Amazon S3 存储桶上执行的文件操作，您需要为这些存储桶启用数据事件。数据事件提供对象级 API 活动，对于跟踪文件上传、下载和用户执行的其他操作特别有用。 Amazon Transfer Family

要为您的 Amazon Transfer Family 服务器启用 Amazon S3 数据事件，请执行以下操作：

1. 打开 CloudTrail 控制台，网址为https://console.aws.amazon.com/cloudtrail/。
2. 在导航窗格中，选择 T ra ils，然后选择现有跟踪或创建新跟踪。
3. 在数据事件下，选择编辑。
4. 对于数据事件类型，请选择 S3。
5. 选择要为其记录数据事件的 Amazon S3 存储桶。您可以记录所有存储桶的数据事件或指定单个存储桶。
6. 选择是记录读取事件、写入事件，还是同时记录两者。
7. 选择保存更改。

启用数据事件后，您可以在为您的 CloudTrail 跟踪配置的 Amazon S3 存储桶中访问这些日志。日志包括诸如执行操作的用户、操作时间戳、受影响的特定对象以及帮助跟踪所执行操作的`onBehalfOfuserId`字段等详细信息。 Amazon Transfer Family

创建服务器的日志条目示例

以下示例显示了演示`CreateServer`操作的 CloudTrail 日志条目（JSON 格式）。

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AAAA4FFF5HHHHH6NNWWWW:user1",
        "arn": "arn:aws:sts::123456789102:assumed-role/Admin/user1",
        "accountId": "123456789102",
        "accessKeyId": "AAAA52C2WWWWW3BB4Z",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-12-18T20:03:57Z"
            },
```

```
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AAAA4FFF5HHHHH6NNWWWW",
                "arn": "arn:aws:iam::123456789102:role/Admin",
                "accountId": "123456789102",
                "userName": "Admin"
            }
        }
    },
    "eventTime": "2024-02-05T19:18:53Z",
    "eventSource": "transfer.amazonaws.com",
    "eventName": "CreateServer",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "11.22.1.2",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/121.0.0.0 Safari/537.36",
    "requestParameters": {
        "domain": "S3",
        "hostKey": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "protocols": [
            "SFTP"
        ],
        "protocolDetails": {
            "passiveIp": "AUTO",
            "tlsSessionResumptionMode": "ENFORCED",
            "setStatOption": "DEFAULT"
        },
        "securityPolicyName": "TransferSecurityPolicy-2020-06",
        "s3StorageOptions": {
            "directoryListingOptimization": "ENABLED"
        }
    },
    "responseElements": {
        "serverId": "s-1234abcd5678efghi"
    },
    "requestID": "6fe7e9b1-72fc-45b0-a7f9-5840268aeadf",
    "eventID": "4781364f-7c1e-464e-9598-52d06aa9e63a",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789102",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
```

```
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "transfer.us-east-1.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}
```

数据访问日志示例

当您为跟踪启用 Amazon S3 数据事件时，您可以跟踪通过执行的文件操作 Amazon Transfer Family。CloudTrail 这些日志可帮助您监控谁访问了哪些数据、何时以及如何访问了哪些数据。

成功访问数据的日志条目示例

以下示例显示了通过成功执行文件下载操作的 CloudTrail 日志条目 Amazon Transfer Family。

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEID:TransferSessionUser",
        "arn": "arn:aws:sts::123456789012:assumed-role/TransferS3AccessRole/
TransferSessionUser",
        "accountId": "123456789012",
        "accessKeyId": "ASIAEXAMPLEKEY",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEID",
                "arn": "arn:aws:iam::123456789012:role/TransferS3AccessRole",
                "accountId": "123456789012",
                "userName": "TransferS3AccessRole"
            },
            "attributes": {
                "creationDate": "2025-07-15T16:12:05Z",
                "mfaAuthenticated": "true"
            }
        },
        "invokedBy": "transfer.amazonaws.com"
    },
    "eventTime": "2025-07-15T16:15:22Z",
    "eventSource": "s3.amazonaws.com",
    "eventName": "GetObject",
```

```
    "awsRegion": "us-east-1",
    "sourceIPAddress": "transfer.amazonaws.com",
    "userAgent": "transfer.amazonaws.com",
    "requestParameters": {
        "bucketName": "my-transfer-bucket",
        "key": "users/john.doe/reports/quarterly-report-2025-Q2.pdf",
        "Host": "my-transfer-bucket.s3.amazonaws.com",
        "x-amz-request-payer": "requester"
    },
    "responseElements": null,
    "additionalEventData": {
        "SignatureVersion": "SigV4",
        "CipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "bytesTransferredIn": 0,
        "bytesTransferredOut": 2458732,
        "x-amz-id-2":
 "EXAMPLE123456789+abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ="
    },
    "requestID": "EXAMPLE123456789",
    "eventID": "example12-3456-7890-abcd-ef1234567890",
    "readOnly": true,
    "resources": [
        {
            "type": "AWS::S3::Object",
            "ARN": "arn:aws:s3:::my-transfer-bucket/users/john.doe/reports/quarterly-
report-2025-Q2.pdf"
        },
        {
            "accountId": "123456789012",
            "type": "AWS::S3::Bucket",
            "ARN": "arn:aws:s3:::my-transfer-bucket"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "requestParameters": {
        "x-amz-onBehalfOf": "john.doe.sessionid@s-abcd1234efgh5678"
    }
}
```


在此示例中，请注意以下重要字段：

- `eventName`：表示已执行的 S3 API 操作（GetObject 用于文件下载）。
- `requestParameters.bucketName`和`requestParameters.key`：显示访问了哪个 S3 对象。
- `additionalEventData.bytesTransferredOut`：以字节为单位显示已下载文件的大小。
- `requestParameters.x-amz-onBehalfOf`：包含 Amazon Transfer Family 用户名和会话 ID，允许您跟踪执行操作的 Amazon Transfer Family 用户。

该`x-amz-onBehalfOf`字段特别重要，因为它将 S3 API 调用链接回发起操作的特定 Amazon Transfer Family 用户。此字段遵循以下格式`username.sessionid@server-id`，其中：

- `username`是 Amazon Transfer Family 用户名。
- `sessionid`是用户会话的唯一标识符。
- `server-id`是 Amazon Transfer Family 服务器的 ID。

常见的数据访问操作

通过监控数据访问时 Amazon Transfer Family，您通常会在 CloudTrail 日志中看到以下 S3 API 操作：

Amazon Transfer Family 日志中的常见 S3 操作

S3 API 操作	Amazon Transfer Family 操作	描述
GetObject	文件下载	用户从服务器下载了一个文件
PutObject	文件上传	用户已将文件上传到服务器
DeleteObject	文件删除	用户从服务器中删除了一个文件
ListObjects 或者 ListObjectsV2	目录清单	用户列出了目录中的文件
CopyObject	文件副本	用户在服务器内复制了一个文件

通过监控 CloudTrail 日志中的这些操作，您可以跟踪通过 Amazon Transfer Family 服务器执行的所有文件活动，从而帮助您满足合规性要求并检测未经授权的访问。

Amazon Amazon Transfer Family 服务器 CloudWatch 登录

Amazon CloudWatch 是一项强大的监控和可观察性服务，可让您全面了解您的 Amazon 资源，包括 Amazon Transfer Family。

- 实时监控：实时 CloudWatch 监控 Transfer Family 资源和应用程序，允许您跟踪和分析其性能。
- 指标收集： CloudWatch 收集和跟踪您的资源和应用程序的各种指标，这些指标是您可以衡量和用于分析的变量。
- CloudWatch 主页：主页会自动显示有关您使用的Transfer Family和其他 Amazon 服务的指标，从而集中查看您的监控数据。 CloudWatch
- 自定义仪表板：您可以在中创建自定义仪表板， CloudWatch 以显示特定于您的自定义应用程序和您选择监控的资源的指标。
- 警报和通知： CloudWatch 允许您创建警报，以监控您的指标，并在突破特定阈值时触发通知或自动操作。这对于监控 Transfer Family 服务器中的文件传输活动并相应地扩展资源非常有用。
- 成本优化：您可以使用收集的数据 CloudWatch 来识别未充分利用的资源，并采取措施（例如停止或删除实例）来优化成本。

总体而言，其中的全面监控功能 CloudWatch 使其成为管理和优化 Transfer Family 基础架构及其上运行的应用程序的宝贵工具。

有关 CloudWatch 登录 Transfer Family 网络应用程序的详细信息，请参阅CloudTrail 登录 Transfer Family 网络应用程序。

Transfer Family 的 CloudWatch 登录类型

Transfer Family 提供了两种记录事件的方法 CloudWatch：

- JSON 结构化日志记录
- 通过日志记录角色进行登录

对于 Transfer Family 服务器，你可以选择自己喜欢的日志机制。对于连接器和工作流程，仅支持日志记录角色。

JSON 结构化记录

要记录服务器事件，我们建议使用 JSON 结构化日志记录。这提供了一种更全面的日志格式，可以进行 CloudWatch 日志查询。对于此类日志记录，创建服务器（或编辑服务器的日志配置）的用户的 IAM 策略必须包含以下权限：

- logs:CreateLogDelivery
- logs:DeleteLogDelivery
- logs:DescribeLogGroups
- logs:DescribeResourcePolicies
- logs:GetLogDelivery
- logs:ListLogDeliveries
- logs:PutResourcePolicy
- logs:UpdateLogDelivery

以下是示例策略。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:GetLogDelivery",
                "logs:UpdateLogDelivery",
                "logs:DeleteLogDelivery",
                "logs:ListLogDeliveries",
                "logs:PutResourcePolicy",
                "logs:DescribeResourcePolicies",
                "logs:DescribeLogGroups"
            ],
            "Resource": "*"
        }
    ]
}
```

有关设置 JSON 结构化日志记录的详细信息，请参阅创建、更新和查看服务器的日志记录。

日志角色

要记录连接到服务器的托管工作流程以及连接器的事件，您需要指定日志记录角色。要设置访问权限，您需要创建一个基于资源的 IAM 策略和一个提供该访问信息的 IAM 角色。以下是可以记录服务器事件 Amazon Web Services 账户 的策略示例。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:DescribeLogStreams",
                "logs:CreateLogGroup",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/transfer/*"
        }
    ]
}
```

有关配置日志记录角色以记录工作流程事件的详细信息，请参阅管理工作流程的日志记录。

创建、更新和查看服务器的日志记录

对于所有 Amazon Transfer Family 服务器，我们都提供结构化日志记录。我们建议您对所有新的和现有的 Transfer Family 服务器使用结构化日志记录。使用结构化日志的好处包括以下几点：

- 接收结构化 JSON 格式的日志。
- 使用 Amazon Logs Insights 查询您的 CloudWatch 日志，它会自动发现 JSON 格式的字段。
- 跨 Amazon Transfer Family 资源共享日志组允许您将来自多个服务器的日志流合并到一个日志组中，从而更轻松地管理监控配置和日志保留设置。
- 创建可添加到 CloudWatch仪表板的聚合指标和可视化效果。
- 使用日志组创建整合的日志指标、可视化效果和控制面板，从而跟踪使用情况和性能数据。

要为连接到服务器的工作流程启用日志记录，必须使用日志记录角色。

> **Note**
>
> 添加日志记录角色时，日志组始终处于状态/aws/transfer/*your-serverID*，并且无法更改。这意味着，除非您将结构化服务器日志发送到同一个组，否则您将登录到两个不同的日志组。
> 如果您知道要将工作流程与服务器关联，因此需要添加日志记录角色，则可以设置结构化日志记录以记录到默认日志组/aws/transfer/*your-serverID*。
> 要修改您的日志组，请参阅 Amazon Transfer Family API 参考StructuredLogDestinations中的。

如果使用 Transfer Family 控制台创建新的服务器，将默认启用日志记录。创建服务器后，您可以使用 UpdateServer API 操作来更改日志配置。有关更多信息，请参阅 StructuredLogDestinations。

目前，对于工作流程，如果要启用日志记录，则必须指定日志记录角色：

- 如果您使用CreateServer或 UpdateServer API 操作将工作流与服务器关联，则系统不会自动创建日志记录角色。如果要记录工作流程事件，则需要将日志记录角色显式附加到服务器。
- 如果您使用 Transfer Family 控制台创建服务器并附加工作流程，则日志将发送到名称中包含服务器 ID 的日志组。格式为 /aws/transfer/*server-id*，例如 /aws/transfer/s-1111aaaa2222bbbb3。服务器日志可以发送到同一个日志组或另一个日志组。

在控制台中创建和编辑服务器的日志记录注意事项

- 除非将工作流程附加到服务器，否则通过控制台创建的新服务器仅支持结构化 JSON 日志记录。
- 无日志记录不是您在控制台中创建的新服务器的选项。
- 现有服务器可以随时通过控制台启用结构化 JSON 日志记录。
- 通过控制台启用结构化 JSON 日志记录会禁用现有的日志记录方法，以免向客户重复收费。如果将工作流程附加到服务器，则例外。
- 如果启用结构化 JSON 日志记录，则以后无法通过控制台将其禁用。
- 如果启用结构化 JSON 日志记录，则可以随时通过控制台更改日志组目标。
- 如果启用结构化 JSON 日志记录，则如果通过 API 启用了两种日志记录类型，则无法通过控制台编辑日志记录角色。如果服务器已附加工作流程，则例外。但是，日志记录角色会继续出现在其他详细信息中。

使用 API 或 SDK 创建和编辑服务器的日志记录注意事项

- 如果您通过 API 创建新服务器，则可以配置其中一种或两种类型的日志记录，或者选择不记录日志。
- 对于现有服务器，可以随时启用和禁用结构化 JSON 日志记录。
- 您可以随时通过 API 更改日志组。
- 您可以随时通过 API 更改日志记录角色。

若要启用结构化日志记录，您必须登录到具有以下权限的账户

- `logs:CreateLogDelivery`
- `logs:DeleteLogDelivery`
- `logs:DescribeLogGroups`
- `logs:DescribeResourcePolicies`
- `logs:GetLogDelivery`
- `logs:ListLogDeliveries`
- `logs:PutResourcePolicy`
- `logs:UpdateLogDelivery`

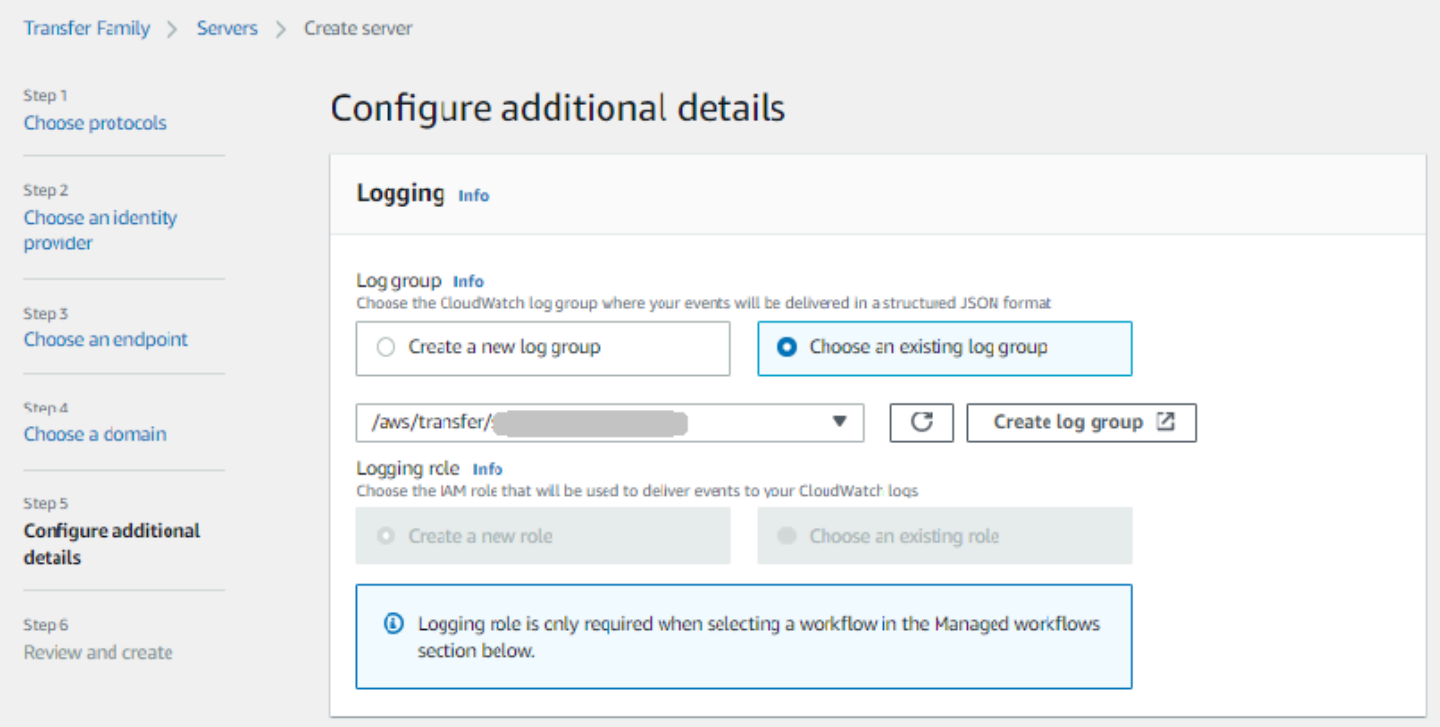
该部分提供了策略示例配置 CloudWatch 日志记录角色。

主题

- 为服务器创建日志
- 更新服务器的日志记录
- 查看服务器配置

为服务器创建日志

创建新服务器时，可以在配置其他详细信息页面上指定现有日志组或创建新日志组。



如果选择创建日志组，则 CloudWatch 控制台 (https://console.aws.amazon.com/cloudwatch/) 将打开创建日志组页面。有关详细信息，请参阅在 Log CloudWatch s 中创建日志组。

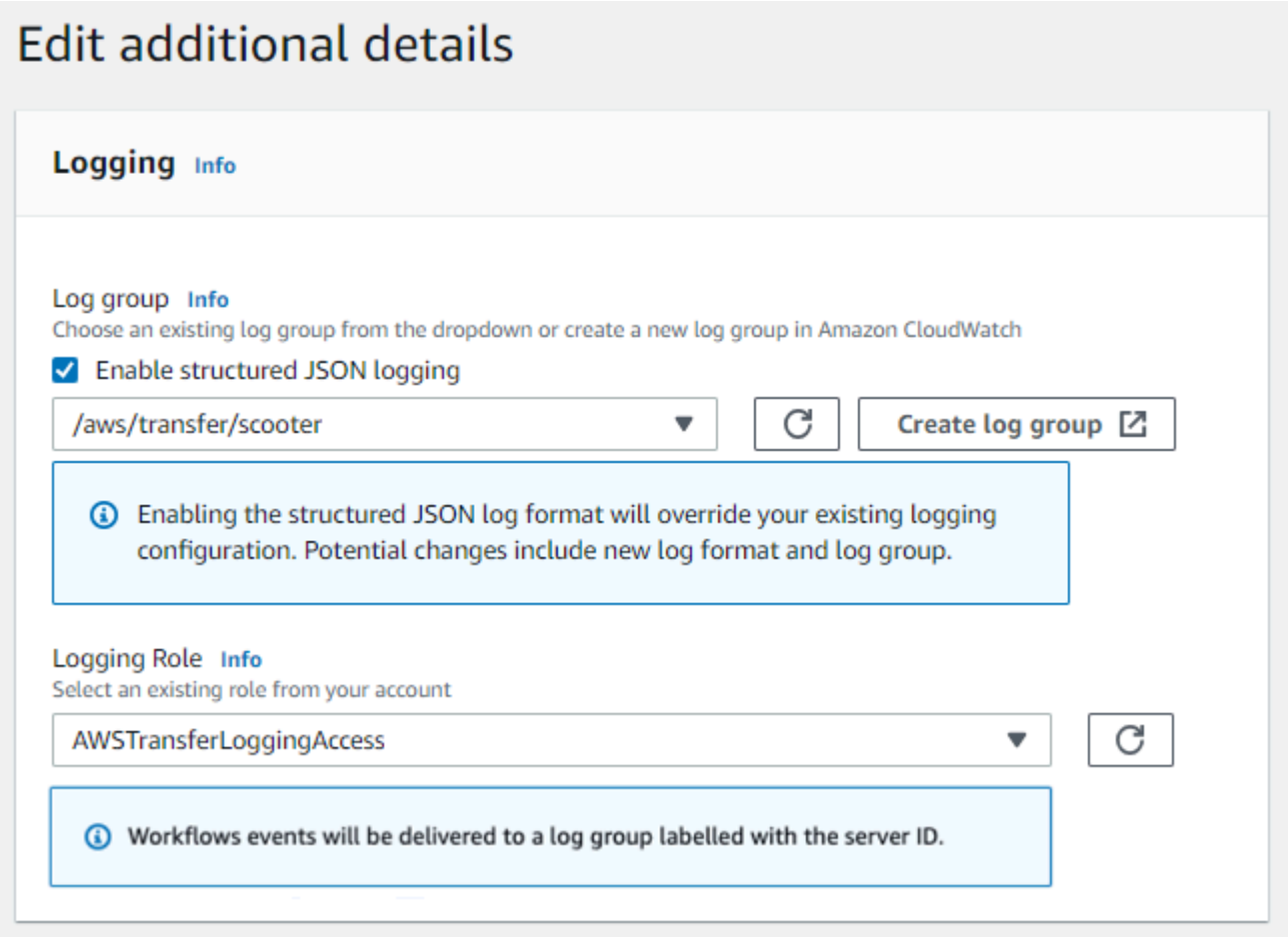
更新服务器的日志记录

日志记录的详细信息取决于您的更新场景。

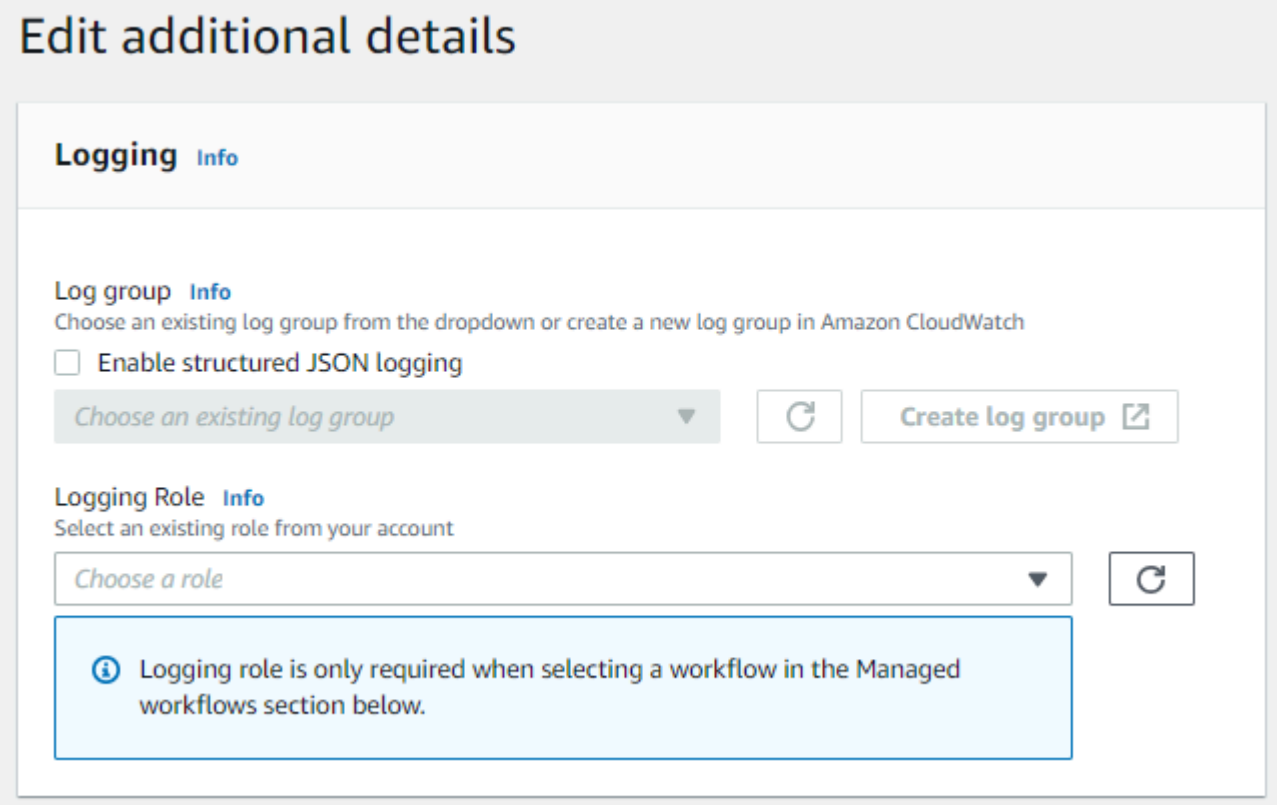
> **Note**
>
> 当您选择使用结构化 JSON 日志记录时，在极少数情况下，Transfer Family 会停止使用旧格式进行日志记录，但需要一些时间才能开始使用新的 JSON 格式进行日志记录。这可能会导致事件不被记录。不会出现任何服务中断，但是在更改日志记录方法后的第一个小时内，您应该谨慎传输文件，因为日志可能会被丢弃。

如果您正在编辑现有服务器，则选项取决于服务器的状态。

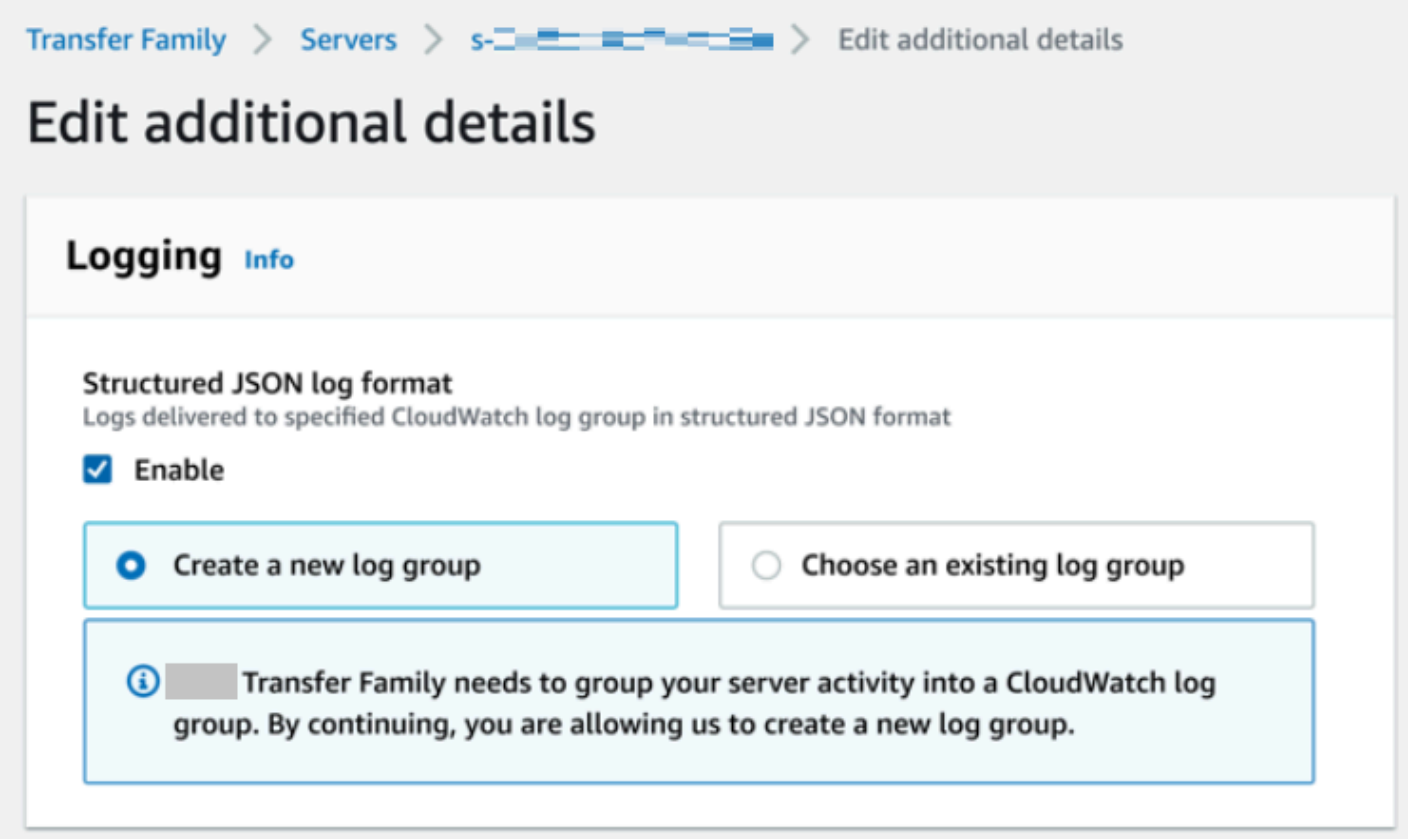
- 服务器已启用日志记录角色，但未启用结构化 JSON 日志记录。



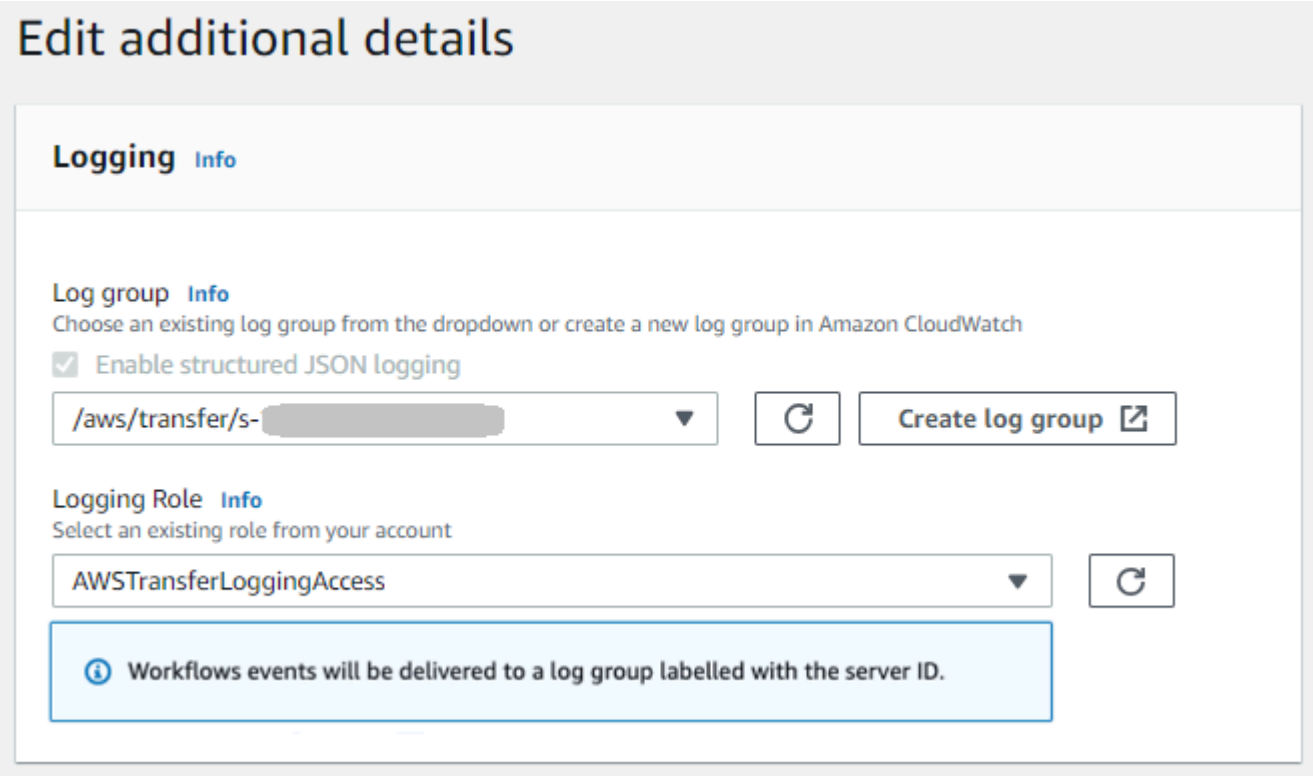
- 服务器未启用任何日志记录。



- 服务器已启用结构化 JSON 日志记录，但未指定日志记录角色。



- 服务器已启用结构化 JSON 日志记录，且已指定日志记录角色。

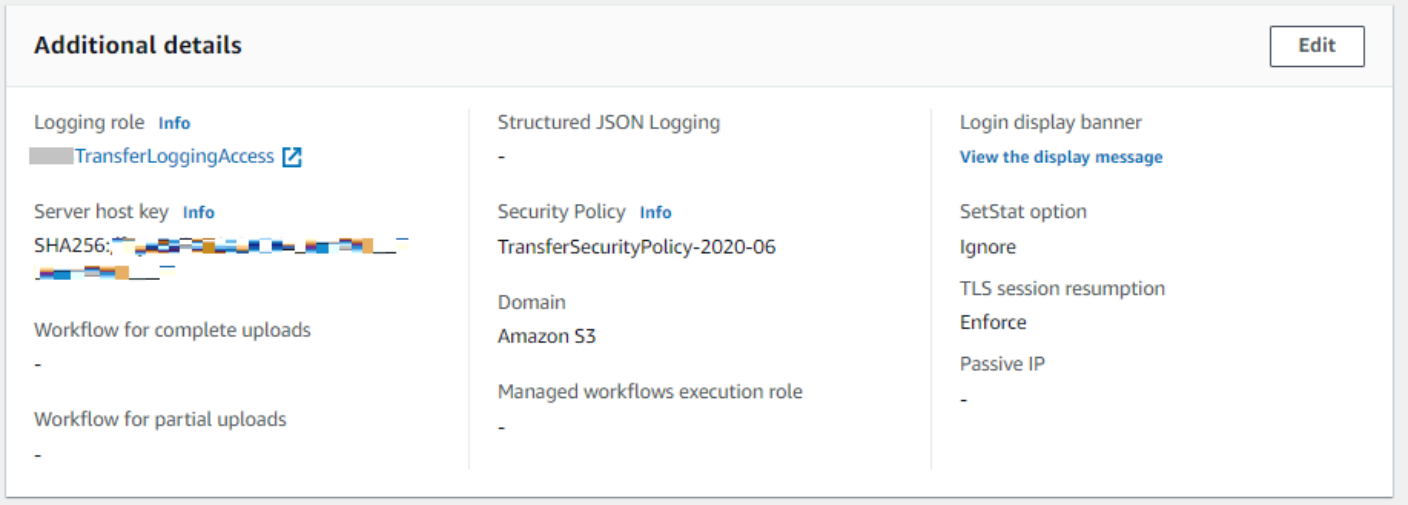


查看服务器配置

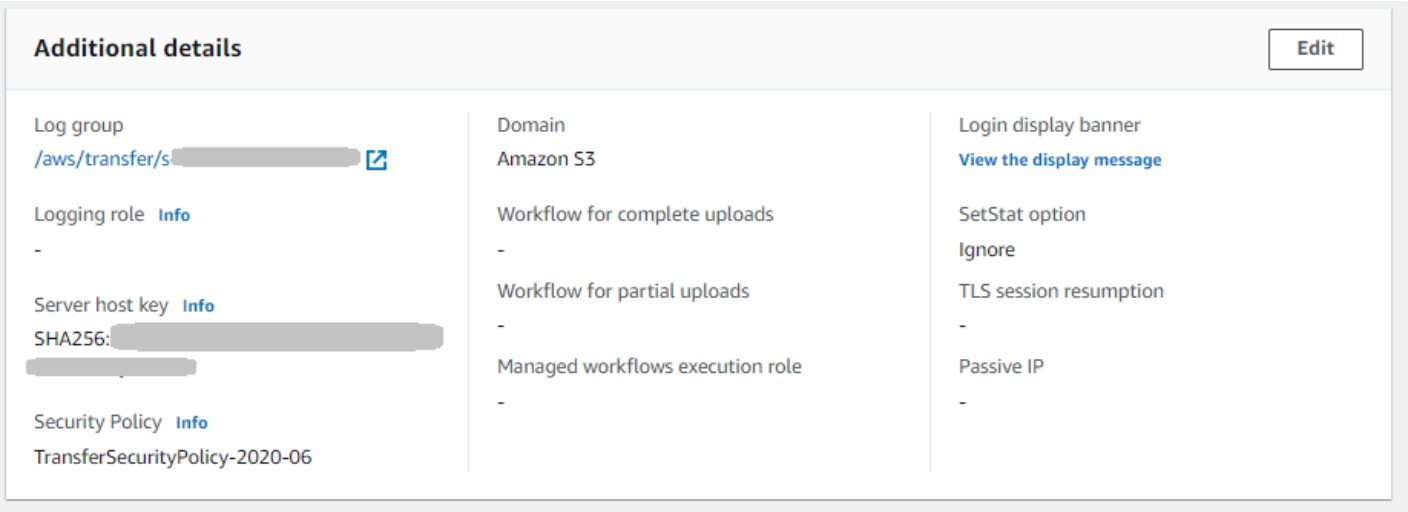
服务器配置页面的详细信息取决于您的场景：

根据您的场景，服务器配置页面可能类似于以下示例之一：

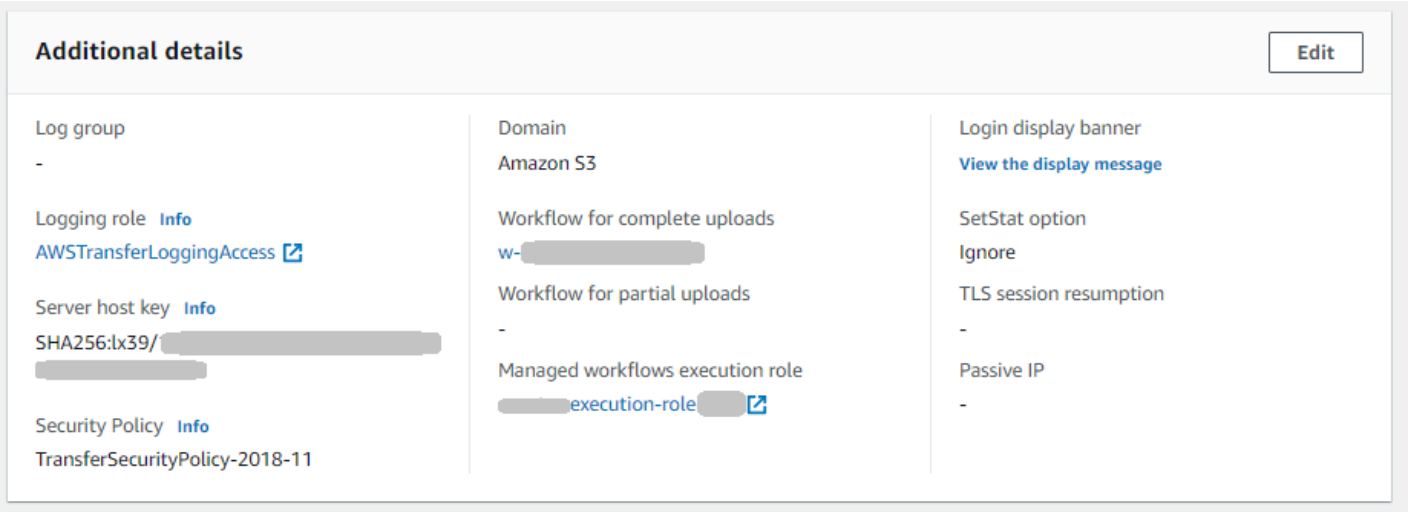
- 无日志记录已启用。



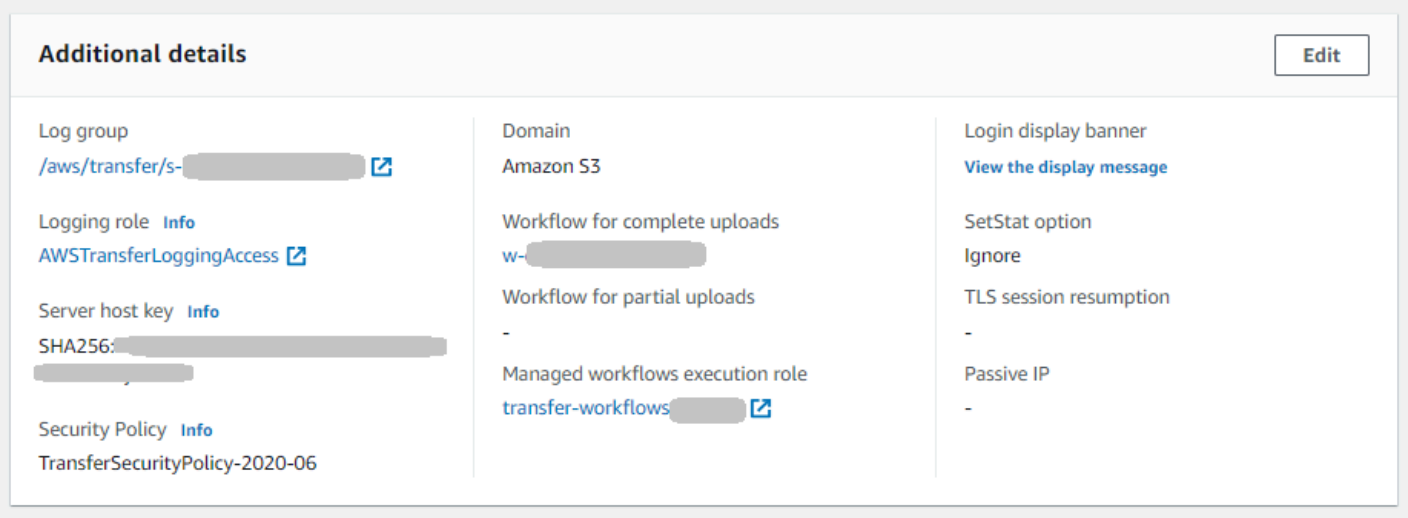
- 已启用结构化 JSON 日志记录。



- 日志记录角色已启用，但未启用结构化 JSON 日志记录。



- 两种类型的日志记录（日志记录角色和结构化 JSON 日志记录）均已启用。



管理工作流程的日志记录

CloudWatch 为工作流程进度和结果提供统一的审计和日志记录。此外，还为工作流程 Amazon Transfer Family 提供了多个指标。您可以查看前一分钟有多少工作流程执行启动、成功完成和失败的指标。中描述了 Transfer Family 的所有 CloudWatch 指标使用 T CloudWatch ransfer Family 服务器的指标。

查看 Amazon 工作流程 CloudWatch 日志

1. 打开 Amazon CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
2. 在左侧导航窗格中选择日志，然后选择日志组。
3. 在日志组页面的导航栏上，为您的 Amazon Transfer Family 服务器选择正确的区域。
4. 选择与您的服务器相对应的日志组。

   例如，如果您的服务器 ID 是 `s-1234567890abcdef0`，则您的日志组是 `/aws/transfer/s-1234567890abcdef0`。
5. 在服务器的日志组详细信息页面上，将显示最新的日志流。您正在探索的用户有两个日志流：

   - 每个 Secure Shell (SSH) 文件传输协议 (SFTP) 会话一个。
   - 一个用于正在为您的服务器执行的工作流程。工作流程的日志流格式为 *`username`*`.`*`workflowID`*`.`*`uniqueStreamSuffix`*。

   例如，如果您的用户是 `mary-major`，您具有以下日志流：

```
mary-major-east.1234567890abcdef0
mary.w-abcdef01234567890.021345abcdef6789
```

> **Note**
>
> 此示例中列出的 16 位字母数字标识符是虚构的。您在 Amazon 上看到 CloudWatch 的值不同。

mary-major-usa-east.1234567890abcdef0 的“日志事件”页面显示每个用户会话的详细信息，mary.w-abcdef01234567890.021345abcdef6789 日志流包含工作流程的详细信息。

以下是基于包含复制步骤的工作流程 (w-abcdef01234567890) 的 mary.w-abcdef01234567890.021345abcdef6789 日志流示例。

```
{
    "type": "ExecutionStarted",
    "details": {
        "input": {
            "initialFileLocation": {
                "bucket": "amzn-s3-demo-bucket",
                "key": "mary/workflowSteps2.json",
                "versionId": "version-id",
                "etag": "etag-id"
            }
        }
    },
    "workflowId":"w-abcdef01234567890",
    "executionId":"execution-id",
    "transferDetails": {
        "serverId":"s-server-id",
        "username":"mary",
        "sessionId":"session-id"
    }
},
{
    "type":"StepStarted",
    "details": {
        "input": {
            "fileLocation": {
                "backingStore":"S3",
```

```
                "bucket":"amzn-s3-demo-bucket",
                "key":"mary/workflowSteps2.json",
                "versionId":"version-id",
                "etag":"etag-id"
            }
        },
        "stepType":"COPY",
        "stepName":"copyToShared"
    },
    "workflowId":"w-abcdef01234567890",
    "executionId":"execution-id",
    "transferDetails": {
        "serverId":"s-server-id",
        "username":"mary",
        "sessionId":"session-id"
    }
},
{
    "type":"StepCompleted",
    "details":{
        "output":{},
        "stepType":"COPY",
        "stepName":"copyToShared"
    },
    "workflowId":"w-abcdef01234567890",
    "executionId":"execution-id",
    "transferDetails":{
        "serverId":"server-id",
        "username":"mary",
        "sessionId":"session-id"
    }
},
{
    "type":"ExecutionCompleted",
    "details": {},
    "workflowId":"w-abcdef01234567890",
    "executionId":"execution-id",
    "transferDetails":{
        "serverId":"s-server-id",
        "username":"mary",
        "sessionId":"session-id"
    }
}
```

配置 CloudWatch 日志记录角色

要设置访问权限，您需要创建一个基于资源的 IAM 策略和一个提供该访问信息的 IAM 角色。

要启用 Amazon CloudWatch 日志记录，首先要创建启用 CloudWatch日志记录的 IAM 策略。然后，您需要创建一个 IAM 角色并将策略附加到该角色。您可在创建服务器或编辑现有服务器时执行此操作。有关的更多信息 CloudWatch，请参阅 Amazon 是什么 CloudWatch？ 以及什么是 Amazon CloudWatch 日志？ 在《亚马逊 CloudWatch 用户指南》中。

使用以下 IAM 策略示例来允许 CloudWatch 日志记录。

Use a logging role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:DescribeLogStreams",
                "logs:CreateLogGroup",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/transfer/*"
        }
    ]
}
```

Use structured logging

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:GetLogDelivery",
                "logs:UpdateLogDelivery",
```

```
                "logs:DeleteLogDelivery",
                "logs:ListLogDeliveries",
                "logs:PutResourcePolicy",
                "logs:DescribeResourcePolicies",
                "logs:DescribeLogGroups"
            ],
            "Resource": "*"
        }
    ]
}
```

在前面的示例策略中，对于**Resource**，将*region-id*和*Amazon Web Services ##*替换为您的值。例如，**"Resource": "arn:aws::logs:us-east-1:111122223333:log-group:/aws/transfer/*"**

然后，您可以创建一个角色并附加您创建的 CloudWatch 日志策略。

创建 IAM 角色并附加策略

1. 在导航窗格中，选择角色，然后选择创建角色。

   在创建角色页面上，确保已选择Amazon 服务。

2. 从服务列表中选择转移，然后选择下一步：权限。这将在和 IAM 角色 Amazon Transfer Family 之间建立信任关系。此外，建议使用 `aws:SourceAccount` 和 `aws:SourceArn` 条件键来防止出现混淆代理问题。有关详细信息，请参阅以下文档：

   - 与以下机构建立信任关系的程序 Amazon Transfer Family：建立信任关系
   - 混淆代理问题描述：混淆代理问题

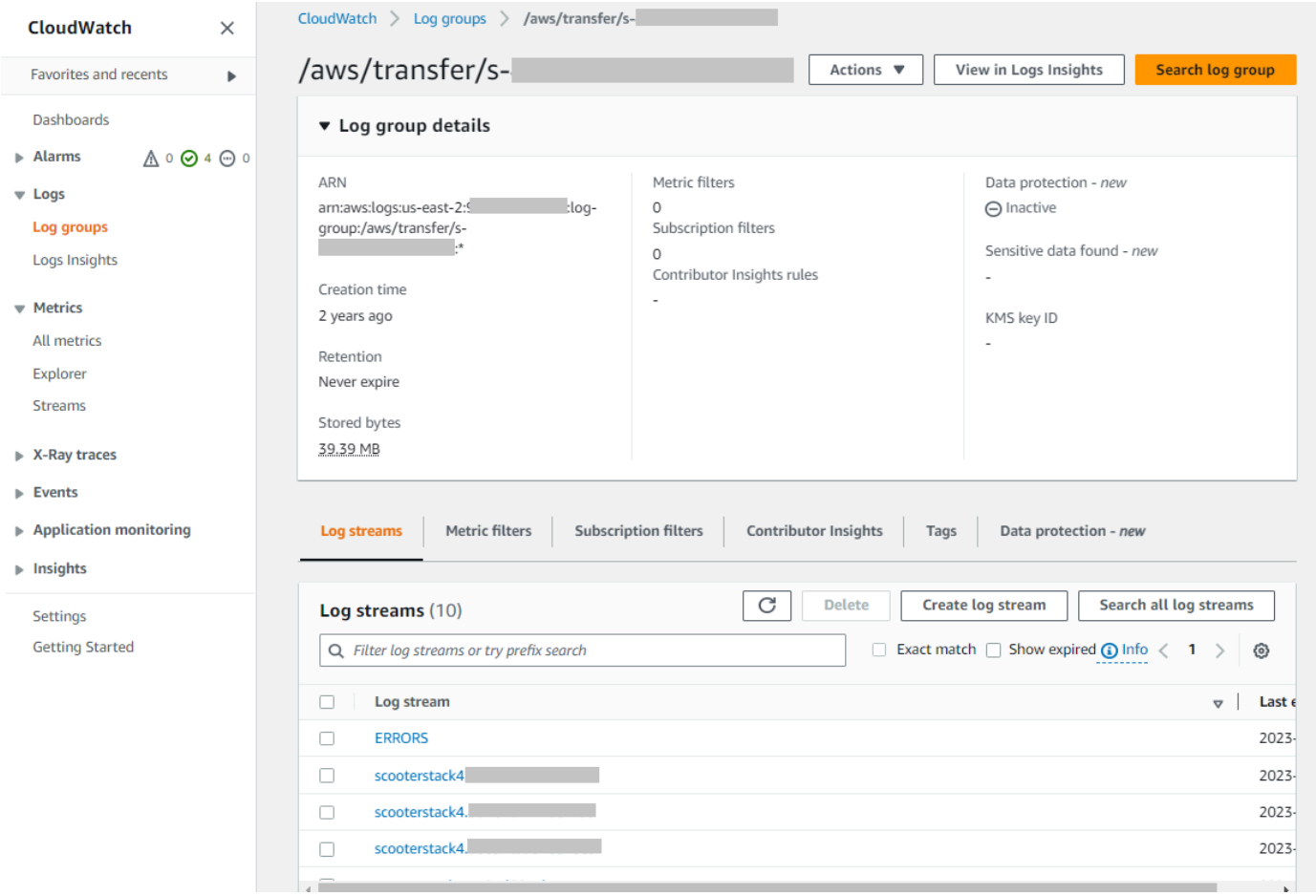
3. 在附加权限策略部分，找到并选择您刚刚创建的 CloudWatch 日志策略，然后选择下一步：标签。
4. （可选）输入标签的键和值，然后选择下一步：审核。
5. 在审核页面上，输入新角色的名称和描述，然后选择创建角色。
6. 要查看日志，请选择服务器 ID 以打开服务器配置页面，然后选择查看日志。您将被重定向到 CloudWatch 控制台，您可以在其中查看日志流。

在服务器 CloudWatch 页面上，您可以看到用户身份验证（成功和失败）、数据上传（PUT操作）和数据下载（GET操作）的记录。

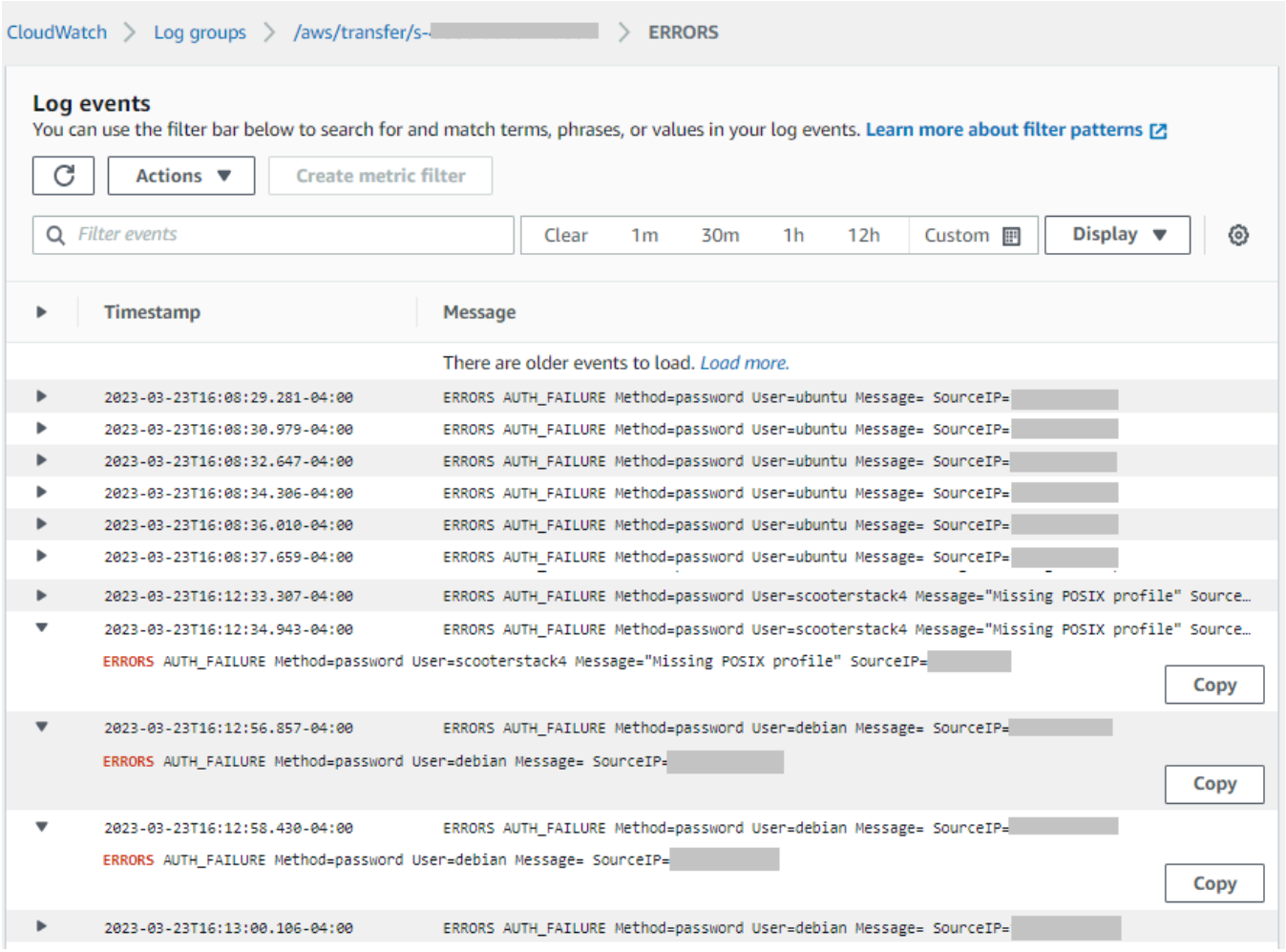
查看 Transfer Family 日志流

若要查看您的 Transfer Family 服务器日志

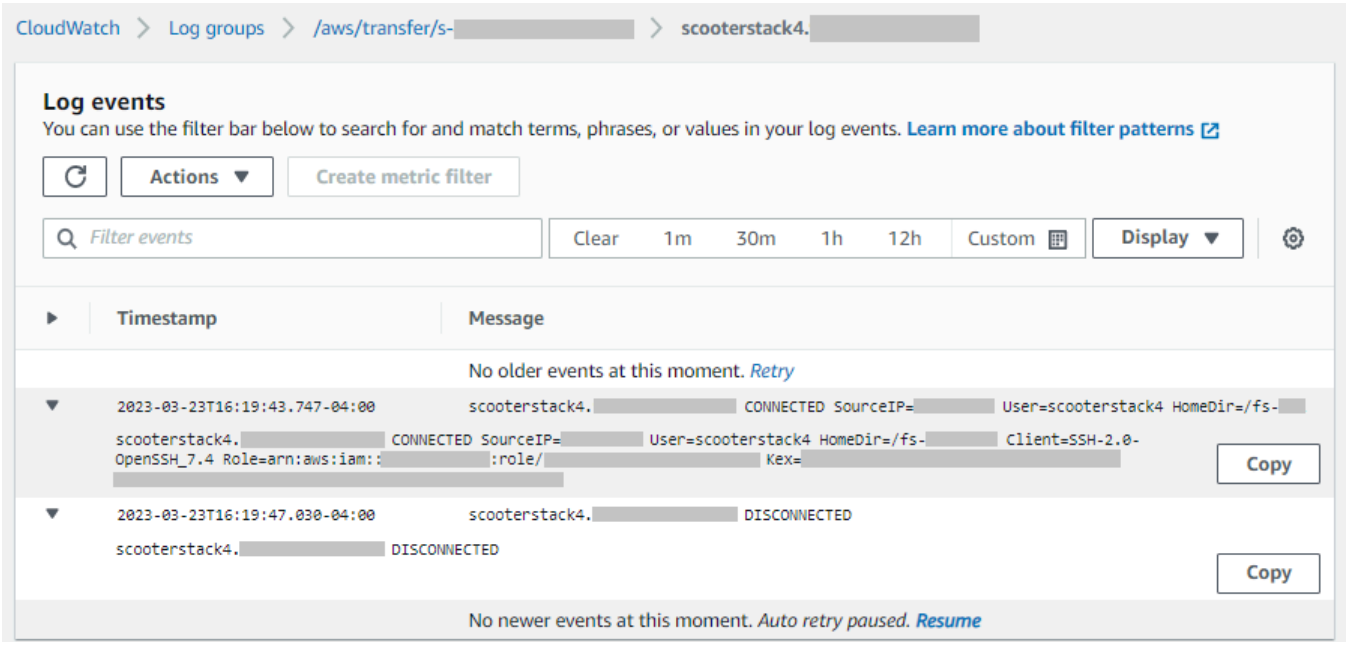
1. 导航到您的服务器详细信息页面。
2. 选择查看日志。这将打开 Amazon CloudWatch。
3. 将显示选定服务器的日志组。



4. 您可以选择一项日志流，显示该流数据的详细信息和单个条目。
   - 如果列出了错误，则可以选择它，以查看服务器最新错误的详细信息。

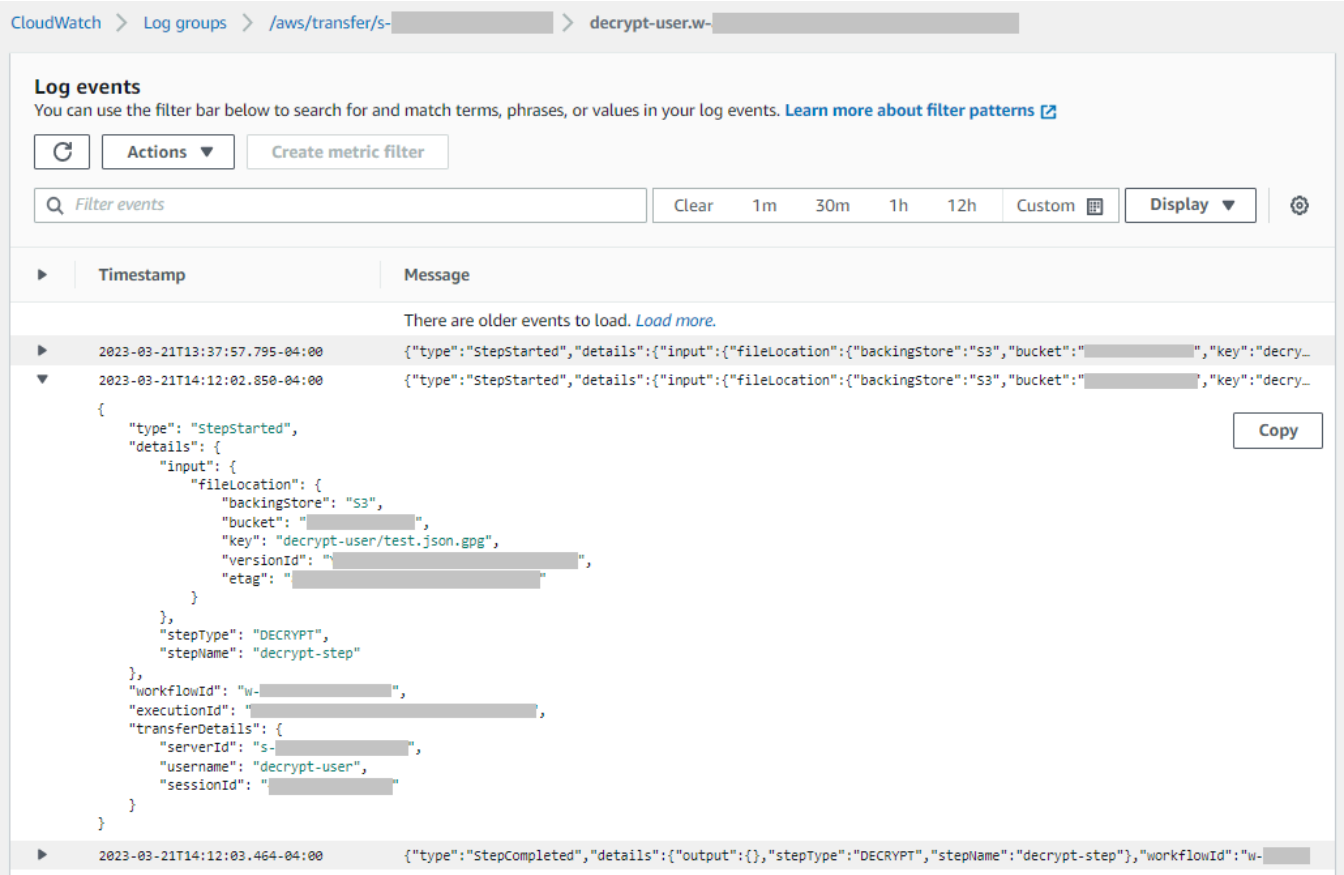


- 选择任何其他条目，以查看日志流示例。



- 如果您的服务器配备与之关联的托管工作流程，则可以查看工作流程运行日志。

> **Note**
>
> 工作流程的日志流格式为 *username*.*workflowId*.*uniqueStreamSuffix*。例如：对于日志流名称 decrypt-user.w-a1111222233334444.aaaa1111bbbb2222，其用户为 **decrypt-user**，工作流程为 **w-a1111222233334444**。



> **Note**
>
> 对于任何展开的日志条目，您可以通过选择复制将该条目复制到剪贴板。有关 CloudWatch 日志的更多详细信息，请参阅查看日志数据。

创建亚马逊 CloudWatch 警报

以下示例展示了如何使用 Amazon Transfer Family 指标创建 Amazon CloudWatch 警报`FilesIn`。

CDK

```
new cloudwatch.Metric({
  namespace: "AWS/Transfer",
  metricName: "FilesIn",
  dimensionsMap: { ServerId: "s-00000000000000000" },
  statistic: "Average",
  period: cdk.Duration.minutes(1),
}).createAlarm(this, "AWS/Transfer FilesIn", {
  threshold: 1000,
  evaluationPeriods: 10,
  datapointsToAlarm: 5,
  comparisonOperator:
 cloudwatch.ComparisonOperator.GREATER_THAN_OR_EQUAL_TO_THRESHOLD,
});
```

Amazon CloudFormation

```
Type: AWS::CloudWatch::Alarm
Properties:
  Namespace: AWS/Transfer
  MetricName: FilesIn
  Dimensions:
    - Name: ServerId
      Value: s-00000000000000000
  Statistic: Average
  Period: 60
  Threshold: 1000
  EvaluationPeriods: 10
  DatapointsToAlarm: 5
  ComparisonOperator: GreaterThanOrEqualToThreshold
```

将 Amazon S3 API 操作记录到 S3 访问日志中

> **Note**
>
> 本节不适用于 Transfer Family 网络应用程序。

如果您使用 Amazon S3 访问日志识别代表文件传输用户提出的 S3 请求，则使用 `RoleSessionName` 显示被假定为提供文件传输提供服务的 IAM 角色。它还显示其他信息，例如用于传输的用户名、会话 ID 以及服务器 ID。格式为 `[AWS:Role Unique Identifier]/username.sessionid@server-id`，且包含在 “请求者” 字段中。例如，以下是来自 S3 访问日志的、用于复制到 S3 存储桶中的“请求者”字段示例内容。

```
arn:aws:sts::AWS-Account-ID:assumed-role/IamRoleName/
username.sessionid@server-id
```

在上述中“请求者”字段中，它显示了名为 `IamRoleName` 的 IAM 角色。有关唯一标识符的更多信息，请参阅 Amazon Identity and Access Management 用户指南中的 IAM 标识符。

混淆代理问题限制示例

混淆代理问题是一个安全性问题，即不具有某操作执行权限的实体可能会迫使具有更高权限的实体执行该操作。在中 Amazon，跨服务模仿可能会导致混乱的副手问题。有关更多详细信息，请参阅防止跨服务混淆代理。

> **Note**
>
> 在以下示例中，用您自己的信息替换每个*user input placeholder*示例。
> 在这些示例中，如果您的服务器未附加任何工作流程，则可以删除工作流程的 ARN 详细信息。

以下示例 logging/invocation 策略允许账户中的任何服务器（和工作流程）代入该角色。

```
{
    "Version":"2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "AllowAllServersWithWorkflowAttached",
            "Effect": "Allow",
            "Principal": {
                "Service": "transfer.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                   "aws:SourceArn": [
                     "arn:aws:transfer:us-west-2:111122223333:server/*",
                     "arn:aws:transfer:us-west-2:111122223333:workflow/*"
                   ]
                }
            }
        }
    ]
}
```

以下示例 logging/invocation 策略允许特定的服务器（和工作流程）担任该角色。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSpecificServerWithWorkflowAttached",
            "Effect": "Allow",
            "Principal": {
                "Service": "transfer.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnEquals": {
                   "aws:SourceArn": [
                      "arn:aws:transfer:us-west-2:111122223333:server/server-id",
```

```
                    "arn:aws:transfer:us-west-2:111122223333:workflow/workflow-
id"
                ]
            }
        }
    ]
}
```

CloudWatch Transfer Family 的日志结构

本主题介绍了 Transfer Family 日志中填充的字段：包括 JSON 结构化日志条目和旧日志条目。

主题

- Transfer Family 的 JSON 结构化
- Transfer Family 的旧日志

Transfer Family 的 JSON 结构化

下表以新的 JSON 结构化日志格式包含 Transfer Family SFTP/FTP/FTPS 操作的日志条目字段的详细信息。

字段	描述	示例条目
活动类型	用户的操作	可用的活动类型如下：AUTH_FAILURE 、、、、CONNECTED 、DISCONNECTED 、、ERROR、EXIT_REASON 、CLOSE、CREATE_SYMLINK 、DELETE、MKDIR、OPEN、PCLOSE 、、RENAME、RMDIR、SETSTATE_FAILURE 。
bytes-in	用户上传的字节数	29238420042
bytes-out	用户下载的字节数	23094032490328

字段	描述	示例条目
ciphers	指定为连接协商的 SSH 密码（中列出了可用密码）加密算法	aes256-gcm@openssh.com
客户端	用户的客户端软件	ssh-2.0-openssh_7.4
主页目录	如果最终用户的主目录类型为：如果他们的主目录类型为PATH：如果他们有逻辑主目录，则此值始终为 /	/user-home-bucket/test
kex	为连接指定协商的 SSH 密钥交换 (KEX)（中列出了可用的KEX加密算法）	diffie-hellman-group14-sha256
message	提供与错误相关的更多信息	*<string>*
method	身份验证方法	publickey
mode	指定客户端如何打开文件	创建 | 截断 | 写入
operation	客户机对文件的操作	打开 | 关闭
path	实际文件路径受到影响	/amzn-s3-demo-bucket/test-file-1.pdf
ssh-public-key	正在连接的用户的公钥正文	AAAAC3nzac1L oy0qv6 Oi ZDI1 NTE5 AAAAIA9 XYVHaa WAcj2sp DJVbgjrq DPY4pxd6 GnHl

字段	描述	示例条目
ssh-public-key-fingerprint	公钥指纹，如服务托管用户列出用户密钥时的控制台中所示。 **Note** 在控制台中，显示的指纹末尾带有填充字符（如果有）：从 0 到 3 个等号 (=)。在日志条目中，此填充已从输出中去除。	SHA256: BY3g NMHw tfjd4n2vut4pty /0 LOk82z WZj4 KEYEu7y4r
ssh-public-key-type	公钥类型：Transfer Family 支持 RSA、ECDSA 和-格式的密钥 ED25519	ssh-ed25519
resource-arn	系统为特定资源（例如服务器）分配的唯一标识符	arn: aws: transfer: ap-northeast-1:12346789012: server/s-1234567890akeu2js2
角色	用户的 IAM 角色	arn: aws: iam:: 0293883675: 角色/测试用户角色
session-id	系统为单个会话分配的唯一标识符	9ca9a0e1cec6ad9d
来源 IP	客户端 IP 地址	18.323.0.129
用户	最终用户的用户名	myname192
用户政策	为最终用户指定的权限：如果用户的策略是会话策略，则填充此字段。	正在使用的会话策略的 JSON 代码

Transfer Family 的旧日志

下表包含各种 Transfer Family 操作的日志条目的详细信息。

> **Note**
>
> 这些条目不是采用新的 JSON 结构化日志格式。

下表以新的 JSON 结构化日志格式包含各种 Transfer Family 操作的日志条目的详细信息。

操作	Amazon 日志中的相应 CloudWatch 日志
身份验证失败次数	错误 auth_FAILURE method=publickey user=lhr message= “rsa: lfz3r2nm k+b7rb1rs v ae+a+hxg0c7l1jiz0" sourceip=3.8.172.211 SHA256 LY4ra UIb
COPY/TAG/DELETE/DECRYPT 工作流	{“type”:” “ , ” details” : {“input” : {StepStar ted“fileLocation” : {“backingStore”: “EFS”、“Fi lesystemid”: “fs-12345678”、“path”:” /lhr/rege x.py “}”}、“stepType”: “TAG”、“stepName”: “successful_tag_step”}、“workflowID”: “workflowID”: “workflowID”: “workflowID”: “workflowID”: “workflowID”: “workF11aaaa2222bbb3"、“exec utionID”: “81234abcd-1234-efgh-5678-i jklmnopqr90"、“TransferDetails”: {“serverID”: “s-1234abcdef5678efghi”、“用户名”: “lhr”、“se ssionID”: “1234567890abcdef0"}}
自定义步骤工作流程	{“type”:” “ , ” details” : {“输出” : {“token”: CustomStepInvoked “mzm4mjg5 M YWUt YTEz y00 yzu YjIz LWI3 OGMt 4 E5"}、“ste pType”: “自定义”、“stepName”: “efs-s3_c opy_2"}、“workflowID”: “w-9283e49d33297c3 f7”、“executionID”: “OGI2ZjQyMz12bacti onID”: “w-9283e49d33297c3f7”: “executio

操作	Amazon 日志中的相应 CloudWatch 日志
	nId”: “121234abcd-1234-efgh-5678-ijklmnopq r90" , “TransferDetails” : {“serverID”: “s-zzzz11 aaaa222223"、“用户名”: “lhr”、“sessionID”: “1234567890abcdef0"}}
删除	lhr.33a8fb495ffb383b 删除 /123.jpg Path=/buc ket/user
Downloads	lhr.33a8fb495ffb383b OPEN /123.jpg mode=Read Path=/bucket/user llhr.33a8fb495ffb383b 关闭 /123.jpg =3618546 Path=/bucket/user BytesOut
登录/登出	user.914984e553bcddb6 CONNECTED SourceIP=1.22.111.222 user=LOGICAL client=ssh-2.0-openssh_7.4 role=arn: aws:: iam:: 123456789012: role/sftp-s3-access HomeDir user.914984e553bcddb6 DISCONNECTED
重命名	lhr.33a8fb495ffb383b 重命名.png Path=/bucket/ user/lambo.png NewPath=/bucket/user/ferrari
工作流程错误日志示例	{“type”:” “ , ” details” : {“errorType” : StepE rrored“BAD_REQUEST” , “ErrorMessage” : “无法标记 Efs 文件” , “stepType” : “TAG” , “stepN ame” : “successful_tag_step”} , “w-1234a bcd5678efghi” , “executionID” : “81234ab cd5678efghi” : “81234abcd5678efghi” : “8 1234abcd5678efghi” : “8cd-1234-efgh-5678- ijklmnopqr90" , “TransferDetails” : {“serverID ”: “s-1234abcd5678efghi”、“用户名”: “lhr”、“se ssionID”: “1234567890abcdef0"}}

操作	Amazon 日志中的相应 CloudWatch 日志
symlinks	lhr.eb49cf7b8651e6d5 CREATE_SYMLINK =/fs-12345678/lhr/pqr.jpg =abc.jpg =abc.jpg LinkPath TargetPath
Uploads	lhr.33a8fb495ffb383b OPEN /123.jpg mode=create|truncate|Write Path=/bucket/user lhr.33a8fb495ffb383b 关闭 /123.jpg =3618546 Path=/bucket/user BytesIn
工作流	{“type”:” “ , ” details” : {“input” : {Executio nStarted“backingStore”: “EFS”、“Filesystemi d”: “fs-12345678”、“path”:” /lhr/regex.py “}}}、initialFileLocation “workflowID”: “w-1111aa aa2222bbbb3”、“executionID”: “1234abcd -1234-efbbid”: “w-11aaaa2222bbbb3”、“execut ionID”: “1234abcd-1234-efbbid”: “w-11aaaa 22gh-5678-ijklmnopqr90" , “TransferDetails” : {“serverID”: “s-zzzz1111aaaa222223"、“用户名 ”: “lhr”、“sessionID”: “1234567890abcdef0"}} {“type”:” “ , ” details” : {“input” : {StepStar ted“fileLocation” : {“backingStore”: “EFS”、“Fi lesystemid”: “fs-12345678”、“path”:” /lhr/rege x.py “}}、“stepType”: “CUSTOM”、“stepName ”: “efs-s3_copy_2"}、“workflowID”: “workflow ID”: “workflowID”: “workflowID”: “9283e49d 33297c3f7"、“executionID”: “1234abcd-1234- efgh-5678-ijklmnopqr90"、“TransferDetails”: {“serverID”: “s-18ca49dce5d842e0b”、“用户 名”: “lhr”、“sessionID”: “1234567890abb”、“用 户名”: “lhr”、“sessionID”: “1234567890aba” cdef0"}}

CloudWatch 日志条目示例

本主题介绍示例日志条目。

主题

- 传输会话日志条目示例
- SFTP 连接器的日志条目示例
- VPC Lattice 连接器的日志条目示例
- 密钥交换算法失败的日志条目示例

传输会话日志条目示例

在此示例中，SFTP 用户连接到 Transfer Family 服务器，上传文件，然后断开与会话的连接。

以下日志条目反映了连接到 Transfer Family 服务器的 SFTP 用户。

```
{
   "role": "arn:aws:iam::500655546075:role/transfer-s3",
   "activity-type": "CONNECTED",
   "ciphers": "chacha20-poly1305@openssh.com,chacha20-poly1305@openssh.com",
   "client": "SSH-2.0-OpenSSH_7.4",
   "source-ip": "52.94.133.133",
   "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/
s-3fe215d89f074ed2a",
   "home-dir": "/test/log-me",
   "ssh-public-key":
 "AAAAC3NzaC1lZDI1NTE5AAAAIA9OY0qV6XYVHaaOiWAcj2spDJVbgjrqDPY4pxd6GnHl",
   "ssh-public-key-fingerprint": "SHA256:BY3gNMHwTfjd4n2VuT4pTyLOk82zWZj4KEYEu7y4r/0",
   "ssh-public-key-type": "ssh-ed25519",
   "user": "log-me",
   "kex": "ecdh-sha2-nistp256",
   "session-id": "9ca9a0e1cec6ad9d"
}
```

以下日志条目反映了 SFTP 用户将文件上传到其 Amazon S3 存储桶的情况。

```
{
   "mode": "CREATE|TRUNCATE|WRITE",
   "path": "/test/log-me/config-file",
```

```
   "activity-type": "OPEN",
   "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/
s-3fe215d89f074ed2a",
   "session-id": "9ca9a0e1cec6ad9d"
}
```

以下日志条目反映了 SFTP 用户与 SFTP 会话断开连接的情况。首先，客户端关闭与存储桶的连接，然后断开 SFTP 会话。

```
{
   "path": "/test/log-me/config-file",
   "activity-type": "CLOSE",
   "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/
s-3fe215d89f074ed2a",
   "bytes-in": "121",
   "session-id": "9ca9a0e1cec6ad9d"
}

{
   "activity-type": "DISCONNECTED",
   "resource-arn": "arn:aws:transfer:us-east-1:500655546075:server/
s-3fe215d89f074ed2a",
   "session-id": "9ca9a0e1cec6ad9d"
}
```

> **Note**
>
> 可用的活动类型如下：AUTH_FAILURE、、、、CONNECTED、DISCONNECTED、ERROR、EXIT_REASON、CLOSE、CREA

SFTP 连接器的日志条目示例

本节包含成功和不成功传输的示例日志。日志生成到名为的日志组/aws/transfer/*connector-id*，其中*connector-id*是 SFTP 连接器的标识符。SFTP 连接器的日志条目是在运行StartFileTransfer或StartDirectoryListing命令时生成的。

此日志条目适用于成功完成的传输。

```
{
```

```
    "operation": "RETRIEVE",
    "timestamp": "2023-10-25T16:33:27.373720Z",
    "connector-id": "connector-id",
    "transfer-id": "transfer-id",
    "file-transfer-id": "transfer-id/file-transfer-id",
    "url": "sftp://192.0.2.0",
    "file-path": "/remotebucket/remotefilepath",
    "status-code": "COMPLETED",
    "start-time": "2023-10-25T16:33:26.945481Z",
    "end-time": "2023-10-25T16:33:27.159823Z",
    "account-id": "480351544584",
    "connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/connector-id",
    "local-directory-path": "/connectors-localbucket",
    "bytes": 514,
    "egress-type": "SERVICE_MANAGED"
}
```

此日志条目适用于超时但未成功完成的传输。

```
{
    "operation": "RETRIEVE",
    "timestamp": "2023-10-25T22:33:47.625703Z",
    "connector-id": "connector-id",
    "transfer-id": "transfer-id",
    "file-transfer-id": "transfer-id/file-transfer-id",
    "url": "sftp://192.0.2.0",
    "file-path": "/remotebucket/remotefilepath",
    "status-code": "FAILED",
    "failure-code": "TIMEOUT_ERROR",
    "failure-message": "Transfer request timeout.",
    "account-id": "480351544584",
    "connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/connector-id",
    "local-directory-path": "/connectors-localbucket",
    "egress-type": "SERVICE_MANAGED"
}
```

此日志条目用于成功执行的 SEND 操作。

```
{
    "operation": "SEND",
    "timestamp": "2024-04-24T18:16:12.513207284Z",
    "connector-id": "connector-id",
    "transfer-id": "transfer-id",
```

```
    "file-transfer-id": "transfer-id/file-transfer-id",
    "url": "sftp://server-id.server.transfer.us-east-1.amazonaws.com",
    "file-path": "/amzn-s3-demo-bucket/my-test-folder/connector-metrics-us-
east-1-2024-01-02.csv",
    "status-code": "COMPLETED",
    "start-time": "2024-04-24T18:16:12.295235884Z",
    "end-time": "2024-04-24T18:16:12.461840732Z",
    "account-id": "255443218509",
    "connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/connector-id",
    "bytes": 275,
    "egress-type": "SERVICE_MANAGED"
}
```

前面日志示例中一些关键字段的描述。

- timestamp表示何时将日志添加到 CloudWatch。 start-time并end-time对应于连接器实际开始和完成传输的时间。
- transfer-id是为每个start-file-transfer请求分配的唯一标识符。如果用户在单个 start-file-transfer API 操作中传递多个文件路径，则所有文件共享相同的路径transfer-id。
- file-transfer-id是为每个传输的文件生成的唯一值。请注意，的初始file-transfer-id部分与相同transfer-id。

VPC Lattice 连接器的日志条目示例

本节包含 VPC 莱迪思连接器的示例日志。对于 VPC Lattice 连接器，日志包括其他字段，这些字段提供有关连接器配置和网络设置的信息。

此日志条目适用于成功完成的 VPC Lattice 连接器发送操作。

```
{
  "operation": "SEND",
  "timestamp": "2025-09-05T14:20:19.577192454Z",
  "connector-id": "connector-id",
  "transfer-id": "transfer-id",
  "file-transfer-id": "transfer-id/file-transfer-id",
  "file-path": ""/amzn-s3-demo-bucket/my-test-folder/connector-vpc-lattice-us-
east-1-2025-03-22.csv"",
  "status-code": "COMPLETED",
  "start-time": "2025-09-05T14:20:19.434072509Z",
  "end-time": "2025-09-05T14:20:19.481453346Z",
  "account-id": "account-id",
```

```
  "connector-arn": "arn:aws:transfer:us-east-1:account-id:connector/connector-id",
  "remote-directory-path": "/test-bucket/test-folder/",
  "bytes": 262,
  "egress-type": "VPC_LATTICE",
  "vpc-lattice-resource-configuration-arn": "arn:aws:vpc-lattice:us-east-1:account-
id:resourceconfiguration/resource-configuration-arn-id",
  "vpc-lattice-port-number": 22
}
```

VPC Lattice 连接器日志包括以下其他字段：

- egress-type-连接器的出口配置类型
- vpc-lattice-resource-configuration-arn-定义目标 SFTP 服务器位置的 VPC 莱迪思资源配置的 ARN
- vpc-lattice-port-number-用于通过 VPC 莱迪思连接到 SFTP 服务器的端口号

密钥交换算法失败的日志条目示例

本节包含密钥交换算法 (KEX) 失败的示例日志。这些是结构化日志的 ER RO RS 日志流中的示例。

此日志条目是存在主机密钥类型错误的示例。

```
{
    "activity-type": "KEX_FAILURE",
    "source-ip": "999.999.999.999",
    "resource-arn": "arn:aws:transfer:us-east-1:999999999999:server/
s-999999999999999999",
    "message": "no matching host key type found",
    "kex": "ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ecdsa-sha2-
nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-
nistp521-cert-v01@openssh.com,ssh-ed25519,ssh-rsa,ssh-dss"
}
```

此日志条目是 KEX 不匹配的示例。

```
{
    "activity-type": "KEX_FAILURE",
    "source-ip": "999.999.999.999",
    "resource-arn": "arn:aws:transfer:us-east-1:999999999999:server/
s-999999999999999999",
```

```
    "message": "no matching key exchange method found",
    "kex": "diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,diffie-hellman-
group14-sha256"
}
```

使用 T CloudWatch ransfer Family 服务器的指标

> **Note**
>
> 您还可以从 Transfer Family 控制台获取 Transfer Family 指标。有关详细信息，请参阅 在控制台中监控使用情况

您可以使用 CloudWatch 指标获取有关服务器的信息。指标表示发布到的一组按时间顺序排列的数据点。 CloudWatch使用指标时，必须指定 Transfer Family 命名空间、指标名和维度。有关指标的更多信息，请参阅 Amazon CloudWatch 用户指南中的指标。

下表描述了 Transfer Family 的 CloudWatch 指标。

命名空间	指标	说明
AWS/Transfer	BytesIn	传输至服务器的字节总数。 报告标准： • Fo SFTP/FTP/FTPS r：在与 Transfer Family 服务器建立连接时每 5 分钟发出一次。如果在此期间没有传输任何文件或字节，则发出 “0”。 • 用于 AS2：当客户在其 AS2 服务器上收到一条消息并在入站消息处理完成后立即发出时 单位：计数 时长：5 分钟
	BytesOut	从服务器传出来的字节总数。 报告标准：

命名空间	指标	说明
		• Fo SFTP/FTP/FTPS r：在与 Transfer Family 服务器建立连接时每 5 分钟发出一次。如果在此期间没有传输任何文件或字节，则发出 “0”。 • 用于 AS2：当客户`StartFileTransfer` 从其 AS2 连接器呼叫并在出站消息处理完成后立即发出时。 单位：计数 时长：5 分钟
	`FilesIn`	传输至服务器的字节总数。 对于使用该 AS2 协议的服务器，此指标表示收到的消息数量。 报告标准： • Fo SFTP/FTP/FTPS r：在与 Transfer Family 服务器建立连接时每 5 分钟发出一次。如果在此期间没有传输任何文件或字节，则发出 “0”。 • 用于 AS2：当客户在其 AS2 服务器上收到一条消息，并在入站消息处理完成后立即发出。 单位：计数 时长：5 分钟

命名空间	指标	说明
	FilesOut	从服务器传出来的字节总数。 报告标准： • Fo SFTP/FTP/FTPS r：在与 Transfer Family 服务器建立连接时每 5 分钟发出一次。如果在此期间没有传输任何文件或字节，则发出 “0”。 • 用于 AS2：当客户StartFileTransfer 从其 AS2 连接器呼叫并在出站消息处理完成后立即发出时。 单位：计数 时长：5 分钟
	InboundMessage	成功从交易伙伴处收到的 AS2 消息总数。 报告标准：当客户在其 AS2 服务器上收到一条消息并在成功处理入站消息后立即发出时 单位：计数 时长：5 分钟
	InboundFailedMessage	未成功从贸易伙伴处收到的 AS2 消息总数。也就是说，交易伙伴发送了一条消息，但是 Transfer Family 服务器无法成功处理该消息。 报告标准：当客户在其 AS2 服务器上收到一条消息并在入站消息处理失败后立即发出时 单位：计数 时长：5 分钟

命名空间	指标	说明
	OnUploadExecutionsStarted	服务器上启动的工作流程执行总数。 报告标准：每次执行开始时触发 单位：计数 时间段：1 分钟
	OnUploadExecutionsSuccess	服务器上执行成功的工作流程总数。 报告标准：每次执行成功完成时触发 单位：计数 时间段：1 分钟
	OnUploadExecutionsFailed	在服务器上启动的失败工作流程执行总数。 报告标准：每次执行未成功完成时触发 单位：计数 时间段：1 分钟
	OutboundMessage	成功发送给交易伙伴的 AS2 消息总数。 报告标准：当客户StartFileTransfer 从其 AS2 连接器呼叫并在成功处理出站消息后立即发出时 单位：计数 时长：5 分钟

命名空间	指标	说明
	OutboundFailedMessage	未成功发送给贸易伙伴的 AS2 消息总数。 报告标准：当客户StartFileTransfer 从其 AS2 连接器呼叫并在出站消息处理失败后立即发出时 单位：计数 时长：5 分钟

Transfer Family 维度

维度是作为指标标识一部分的 name/value 配对。有关尺寸的更多信息，请参阅 Amazon CloudWatch 用户指南中的尺寸。

下表描述了 Transfer Family 的 CloudWatch 尺寸。

维度	说明
ServerId	服务器的唯一 ID。
ConnectorId	连接器的唯一 ID。用于 AS2、用于OutboundMessage 和 OutboundFailedMessage

Amazon 用户通知服务 与一起使用 Amazon Transfer Family

要获得有关 Amazon Transfer Family 事件的通知，您可以使用Amazon 用户通知服务设置各种交付渠道。当事件与您指定的规则匹配时，您会收到通知。

您可以通过多个渠道接收事件通知，包括电子邮件、聊天应用程序中的 Amazon Q 开发者版聊天通知或 Amazon Console Mobile Application 推送通知。您还可以在控制台通知中心查看通知。 用户通知服务 支持聚合，这可以减少您在特定事件期间收到的通知数量。

有关更多信息，请参阅使用 Amazon Transfer Family 托管工作流程自定义文件传送通知博客文章和什么是 Amazon 用户通知服务？ 在《Amazon 用户通知服务 用户指南》中。

使用查询筛选日志条目

您可以使用 CloudWatch 查询来筛选和识别 Transfer Family 的日志条目。本节包含一些示例。

1. 登录 Amazon Web Services 管理控制台 并打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
2. 您可以创建查询或规则。
   - 要创建 Logs Insight s 查询，请从左侧导航面板中选择 Lo gs Insights，然后输入查询的详细信息。
   - 要创建 “贡献者见解” 规则，请从左侧导航面板中选择 “见解” > “贡献者见解”，然后输入规则的详细信息。
3. 运行您创建的查询或规则。

查看身份验证失败的主要贡献者

在您的结构化日志中，身份验证失败日志条目类似于以下内容：

```
{
  "method":"password",
  "activity-type":"AUTH_FAILURE",
  "source-ip":"999.999.999.999",
  "resource-arn":"arn:aws:transfer:us-east-1:999999999999:server/s-0123456789abcdef",
  "message":"Invalid user name or password",
  "user":"exampleUser"
}
```

运行以下查询以查看导致身份验证失败的主要原因。

```
filter @logStream = 'ERRORS'
| filter `activity-type` = 'AUTH_FAILURE'
| stats count() as AuthFailures by user, method
| sort by AuthFailures desc
| limit 10
```

您可以创建 “CloudWatch 贡献者CloudWatch 见解” 规则来查看身份验证失败情况，而不是使用 Logs Insights。创建类似于以下内容的规则。

```
{
```

```
    "AggregateOn": "Count",
    "Contribution": {
        "Filters": [
            {
                "Match": "$.activity-type",
                "In": [
                    "AUTH_FAILURE"
                ]
            }
        ],
        "Keys": [
            "$.user"
        ]
    },
    "LogFormat": "JSON",
    "Schema": {
        "Name": "CloudWatchLogRule",
        "Version": 1
    },
    "LogGroupARNs": [
        "arn:aws:logs:us-east-1:999999999999:log-group:/customer/structured_logs"
    ]
}
```

查看文件打开位置的日志条目

在您的结构化日志中，文件读取日志条目类似于以下内容：

```
{
  "mode":"READ",
  "path":"/fs-0df669c89d9bf7f45/avtester/example",
  "activity-type":"OPEN",
  "resource-arn":"arn:aws:transfer:us-east-1:999999999999:server/s-0123456789abcdef",
  "session-id":"0049cd844c7536c06a89"
}
```

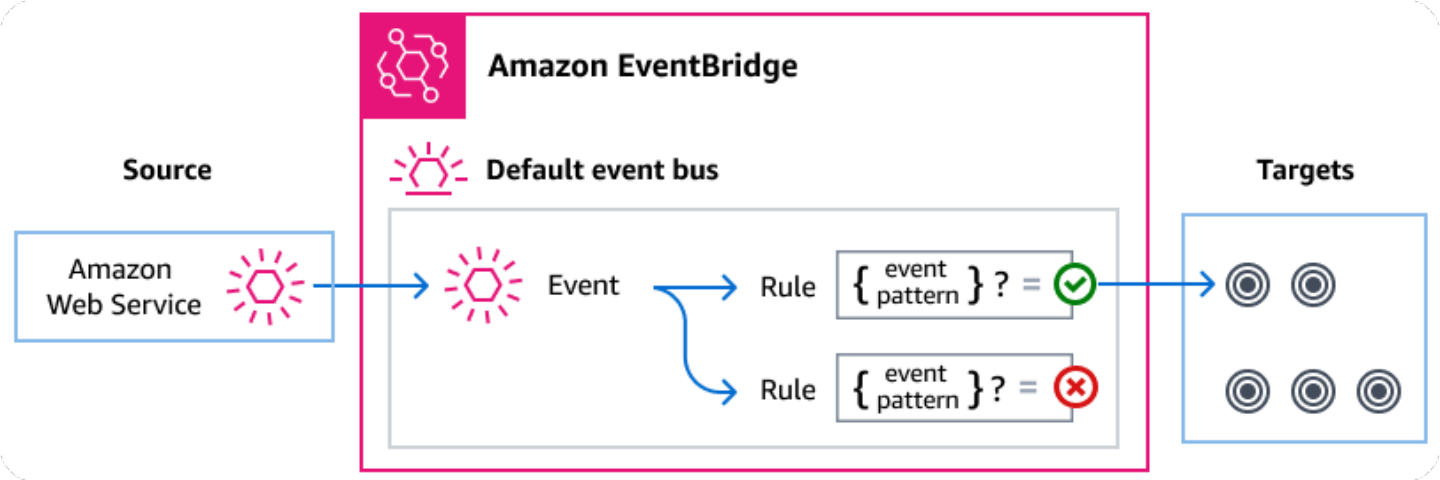
运行以下查询以查看表明文件已打开的日志条目。

```
filter `activity-type` = 'OPEN'
| display @timestamp, @logStream, `session-id`, mode, path
```

使用管理 Transfer Family 事件 Amazon EventBridge

Amazon EventBridge 是一项无服务器服务，它使用事件将应用程序组件连接在一起，这使您可以更轻松地构建可扩展的事件驱动应用程序。事件驱动架构是一种构建松散耦合的软件系统的风格，这些系统通过发射和响应事件来协同工作。事件代表资源或环境中的变化。

与许多 Amazon 服务一样， Transfer Family 生成事件并将其发送到 EventBridge 默认事件总线。请注意，默认事件总线会在每个 Amazon 账户中自动配置。事件总线是接收事件并将其传送到零个或多个目的地或目标的路由器。您可以为事件总线指定规则，该总线在事件到达时对其进行评估。每条规则都会检查事件是否与规则的事件模式相匹配。如果事件匹配，则事件总线会将事件发送到一个或多个指定的目标。



主题

- Transfer Family 事件
- 使用 EventBridge 规则发送 Transfer Family 事件
- Amazon EventBridge 权限
- 其他 EventBridge 资源
- Transfer Family 事件详情参考

Transfer Family 事件

Transfer Family 自动将事件发送到默认 EventBridge 事件总线。您可以在事件总线上创建规则，其中每条规则都包含一个事件模式和一个或多个目标。

与规则的事件模式相匹配的事件会尽力或持久地传送到指定目标（请注意，某些事件可能会乱序传送）。这些配送级别在《亚马逊 EventBridge 事件参考》中Amazon 服务事件的配送级别中进行了描述。

- SFTP、FTPS 和 FTP 服务器的服务器级事件是在尽力交付的基础上进行的。
- SFTP 连接器事件在持久的基础上交付。
- 这些 AS2 活动是在持久的基础上举办的。

以下事件由生成 Transfer Family。有关更多信息，请参阅《Amazon EventBridge 用户指南》中的EventBridge 事件。

SFTP、FTPS 和 FTP 服务器事件

下表列出了按事件类型组织的 SFTP、FTPS 和 FTP 服务器的事件。

文件上传和下载事件

事件详细信息类型	描述
FTP 服务器文件下载已完成	已成功下载适用于 FTP 协议的文件。
FTP 服务器文件下载失败	尝试下载 FTP 协议的文件失败。
FTP 服务器文件上传已完成	已成功上传适用于 FTP 协议的文件。
FTP 服务器文件上传失败	尝试上传 FTP 协议的文件失败。
FTPS 服务器文件下载已完成	已成功下载适用于 FTPS 协议的文件。
FTPS 服务器文件下载失败	尝试下载 FTPS 协议的文件失败。
FTPS 服务器文件上传已完成	已成功上传适用于 FTPS 协议的文件。
FTPS 服务器文件上传失败	尝试上传 FTPS 协议的文件失败。
SFTP 服务器文件下载已完成	已成功下载适用于 SFTP 协议的文件。
SFTP 服务器文件下载失败	尝试下载 SFTP 协议的文件失败。
SFTP 服务器文件上传已完成	已成功上传适用于 SFTP 协议的文件。

事件详细信息类型	描述
SFTP 服务器文件上传失败	尝试上传 SFTP 协议的文件失败。

其他文件操作事件

事件详细信息类型	描述
FTP 服务器目录创建已完成	已成功为 FTP 协议创建目录。
创建 FTP 服务器目录失败	尝试为 FTP 协议创建目录失败。
FTP 服务器目录删除已完成	已成功删除 FTP 协议的目录。
删除 FTP 服务器目录失败	尝试删除 FTP 协议的目录失败。
FTP 服务器文件删除已完成	已成功删除符合 FTP 协议的文件。
FTP 服务器文件删除失败	尝试删除 FTP 协议的文件失败。
FTP 服务器文件重命名已完成	文件已成功重命名为 FTP 协议。
FTP 服务器文件重命名失败	尝试重命名 FTP 协议的文件失败。
FTPS 服务器目录创建已完成	已成功为 FTPS 协议创建目录。
创建 FTPS 服务器目录失败	尝试为 FTPS 协议创建目录失败。
FTPS 服务器目录删除已完成	已成功删除 FTPS 协议的目录。
删除 FTPS 服务器目录失败	尝试删除 FTPS 协议的目录失败。
FTPS 服务器文件删除已完成	已成功删除 FTPS 协议的文件。
删除 FTPS 服务器文件失败	尝试删除 FTPS 协议的文件失败。
FTPS 服务器文件重命名已完成	已成功为 FTPS 协议重命名文件。
FTPS 服务器文件重命名失败	尝试重命名 FTPS 协议的文件失败。

事件详细信息类型	描述
SFTP 服务器目录创建已完成	已成功为 SFTP 协议创建目录。
创建 SFTP 服务器目录失败	尝试为 SFTP 协议创建目录失败。
SFTP 服务器目录删除已完成	已成功删除 SFTP 协议的目录。
删除 SFTP 服务器目录失败	尝试删除 SFTP 协议的目录失败。
SFTP 服务器文件删除已完成	已成功删除 SFTP 协议的文件。
删除 SFTP 服务器文件失败	尝试删除 SFTP 协议的文件失败。
SFTP 服务器文件重命名已完成	已成功重命名 SFTP 协议的文件。
SFTP 服务器文件重命名失败	尝试重命名 SFTP 协议的文件失败。

SFTP 连接器事件

> **Note**
>
> 这些事件按持久级别传送，如《Amazon EventBridge 事件参考》中Amazon 服务事件的交付级别中所述。 EventBridge

事件详细信息类型	描述
SFTP 连接器文件发送已完成	已成功完成从连接器到远程 SFTP 服务器的文件传输。
SFTP 连接器文件发送失败	从连接器向远程 SFTP 服务器传输文件失败。
SFTP 连接器文件检索已完成	已成功完成从远程 SFTP 服务器到连接器的文件传输。
检索 SFTP 连接器文件失败	从远程 SFTP 服务器向连接器传输文件失败。
SFTP 连接器目录列表已完成	已成功完成的启动文件目录列出调用。

事件详细信息类型	描述
SFTP 连接器目录列表失败	失败的起始文件目录列表。
SFTP 连接器远程移动已完成	已在远程服务器上成功移动或重命名文件或目录。
SFTP 连接器远程移动失败	无法在远程服务器上移动或重命名文件或目录。
SFTP 连接器远程删除已完成	已成功删除远程服务器上的文件或目录。
SFTP 连接器远程删除失败	无法删除远程服务器上的文件或目录。

AS2 事件

> **Note**
>
> 这些事件按持久级别传送，如《Amazon EventBridge 事件参考》中Amazon 服务事件的交付级别中所述。 EventBridge

事件详细信息类型	描述
AS2 有效载荷接收已完成	已收到 AS2 消息的有效负载。
AS2 有效载荷接收失败	尚未收到 AS2 消息的有效负载。
AS2 有效载荷发送已完成	AS2 消息的有效负载已成功发送。
AS2 有效载荷发送失败	AS2 消息的有效负载发送失败。
AS2 MDN 接收已完成	已收到一封 AS2 邮件的消息处置通知。
AS2 MDN 接收失败	尚未收到留言的 AS2 留言处置通知。
AS2 MDN 发送已完成	已成功发送 AS2 消息的消息处置通知。
AS2 MDN 发送失败	某封邮件的 AS2 邮件处理通知发送失败。

使用 EventBridge 规则发送 Transfer Family 事件

如果要 EventBridge 使用默认事件总线向目标发送 Transfer Family 事件，则必须创建一个规则，其中包含与所需事件中的数据匹配 Transfer Family 的事件模式。

在 Amazon 中捕捉 Amazon Transfer Family 事件 EventBridge

1. 登录 Amazon Web Services 管理控制台 并打开 Amazon EventBridge 控制台，网址为https://console.aws.amazon.com/events/。
2. 在导航窗格中，选择规则，然后选择创建规则。
3. 输入规则的描述性名称，也可以输入描述。
4. 对于 “规则类型”，选择 “带有事件模式的规则”，然后选择 “下一步”。
5. 在事件来源部分，选择Amazon 事件或 EventBridge 合作伙伴事件。
6. 在 “创建方法” 部分中，选择 “使用图案表单”。
7. 在事件模式部分，提供以下信息。

   a. 对于事件源，选择Amazon 服务。

   b. 要获得Amazon 服务，请选择传输。

   c. 对于事件类型，选择要触发规则的 Transfer Family 事件类型。

      根据您选择的事件类型，您可能会看到事件类型规范 1 部分。

   d. 如果您看到 “事件类型规范 1” 部分，请选择要捕获的特定事件（或选择 “任何事件” 以捕获所选事件类型的所有事件）。

   e. （可选）使用事件模式编辑器为事件详细信息指定过滤器。

   f. 选择下一步。
8. 从 “选择目标” 中的可用选项中选择一个目标。从以下可用目标中进行选择。

   - Amazon 服务。热门选项包括用于无服务器计算的 Lambda 函数、用于消息处理的 Amazon SQS 队列、用于通知和编排工作流程的 Amazon SNS 主题。 Amazon Step Functions
   - EventBridge API 目的地。如果您想将事件发送到外部的 HTTP 终端节点 Amazon，则可以使用 API 目标作为目标。
   - EventBridge 活动巴士。您可以将事件发送到另一个事件总线，可以是同一账户和区域中的另一条事件总线，也可以是不同的账户或区域。

     有关创建事件总线规则的全面说明，请参阅 Amazon EventBridge 用户指南中的创建对事件做出反应的规则。

有关选择目标的帮助，请参阅 Amazon EventBridge 用户指南中的选择目标。

9. 为您的目标配置任何其他选项，然后选择下一步。
10. （可选）向规则添加标签，然后选择下一步。
11. 在 “查看并创建” 屏幕中，如果一切正常，请选择 “创建规则”。

为事件创建 Transfer Family 事件模式

将事件 Transfer Family 传送到默认事件总线时， EventBridge 使用为每条规则定义的事件模式来确定是否应将事件传送到规则的目标。事件模式与所需 Transfer Family 事件中的数据相匹配。每个事件模式都是一个 JSON 对象，其中包含以下内容：

- 标识发送事件的服务的 `source` 属性。对于 Transfer Family 事件，来源是`aws.transfer`。
- （可选）包含要匹配的事件类型数组的`detail-type`属性。
- （可选）包含要匹配的任何其他事件数据的`detail`属性。

例如，以下事件模式与来自的所有事件匹配 Transfer Family：

```
{
  "source": ["aws.transfer"]
}
```

以下事件模式示例匹配所有 SFTP 连接器事件：

```
{
  "source": ["aws.transfer"],
  "detail-type": ["SFTP Connector File Send Completed", "SFTP Connector File Retrieve
 Completed",
                  "SFTP Connector File Retrieve Failed", "SFTP Connector File Send
 Failed"]
}
```

以下事件模式示例匹配所有 Transfer Family 失败事件：

```
{
  "source": ["aws.transfer"],
  "detail-type": [{"wildcard", "*Failed"}]
```

```
}
```

以下事件模式示例与用户*username*成功下载的 SFTP 相匹配：

```
{
  "source": ["aws.transfer"],
  "detail-type": ["SFTP Server File Download Completed"],
  "detail": {
    "username": [username]
  }
}
```

有关写入事件模式的更多信息，请参阅《EventBridge 用户指南》中的事件模式。

测试事件模式中的 Transfer Family 事件 EventBridge

您可以使用 EventBridge 沙盒快速定义和测试事件模式，而不必完成创建或编辑规则的更广泛过程。使用沙盒，您可以定义事件模式，并使用示例事件来确认该模式是否与所需事件匹配。 EventBridge 允许您选择通过直接从沙箱中使用该事件模式来创建新规则。

有关更多信息，请参阅《EventBridge 用户指南》中的使用 EventBridge 沙盒测试事件模式。

Amazon EventBridge 权限

Transfer Family 不需要任何其他权限即可向其发送事件 Amazon EventBridge。

您指定的目标可能需要特定的权限或配置。有关为目标使用特定服务的更多详细信息，请参阅《Amazon EventBridge 用户指南》中的 Amazon EventBridge 目标。

其他 EventBridge 资源

有关如何使用 EventBridge 处理和管理事件的更多信息，请参阅《Amazon EventBridge 用户指南》中的以下主题。

- 有关事件总线工作原理的详细信息，请参阅 Amazon EventBridge 事件总线。
- 有关事件结构的信息，请参阅事件。
- 有关构造事件模式 EventBridge 以便在将事件与规则进行匹配时使用的信息，请参阅事件模式。
- 有关创建规则以指定 EventBridge 所处理事件的信息，请参阅规则。
- 有关如何指定向哪些服务或其他目的地 EventBridge 发送匹配事件的信息，请参阅目标。

Transfer Family 事件详情参考

来自 Amazon 服务的所有事件都有一组公共字段，其中包含有关该事件的元数据。这些元数据可以包括作为事件来源的 Amazon 服务、事件的生成时间、事件发生的账户和区域等。有关这些常规字段的定义，请参阅《Amazon EventBridge 用户指南》中的事件结构参考。

此外，每个事件都有一个 `detail` 字段，其中包该特定事件专有的数据。以下参考定义了各种 Transfer Family 事件的详细信息字段。

使用 EventBridge 选择和管理 Transfer Family 事件时，请考虑以下几点：

- 来自的所有事件的`source`字段均设置 Transfer Family 为`aws.transfer`。
- `detail-type` 字段指定事件类型。

  例如 `FTP Server File Download Completed`。
- `detail` 字段包含该特定事件专有的数据。

有关如何构造使规则能够匹配 Transfer Family 事件的事件模式的信息，请参阅《Amazon EventBridge 用户指南》中的事件模式。

有关事件及其 EventBridge 处理方式的更多信息，请参阅《Amazon EventBridge 用户指南》中的Amazon EventBridge 事件。

主题

- SFTP、FTPS 和 FTP 服务器事件
- SFTP 连接器事件
- AS2 事件

SFTP、FTPS 和 FTP 服务器事件

以下是 SFTP、FTPS 和 FTP 服务器事件的详细信息字段：

- FTP 服务器目录创建已完成
- 创建 FTP 服务器目录失败
- FTP 服务器目录删除已完成
- 删除 FTP 服务器目录失败
- FTP 服务器文件删除已完成

- FTP 服务器文件删除失败
- FTP 服务器文件下载已完成
- FTP 服务器文件下载失败
- FTP 服务器文件重命名已完成
- FTP 服务器文件重命名失败
- FTP 服务器文件上传已完成
- FTP 服务器文件上传失败
- FTPS 服务器目录创建已完成
- 创建 FTPS 服务器目录失败
- FTPS 服务器目录删除已完成
- 删除 FTPS 服务器目录失败
- FTPS 服务器文件删除已完成
- 删除 FTPS 服务器文件失败
- FTPS 服务器文件下载已完成
- FTPS 服务器文件下载失败
- FTPS 服务器文件重命名已完成
- FTPS 服务器文件重命名失败
- FTPS 服务器文件上传已完成
- FTPS 服务器文件上传失败
- SFTP 服务器目录创建已完成
- 创建 SFTP 服务器目录失败
- SFTP 服务器目录删除已完成
- 删除 SFTP 服务器目录失败
- SFTP 服务器文件删除已完成
- 删除 SFTP 服务器文件失败
- SFTP 服务器文件下载已完成
- SFTP 服务器文件下载失败
- SFTP 服务器文件重命名已完成
- SFTP 服务器文件重命名失败
- SFTP 服务器文件上传已完成

- SFTP 服务器文件上传失败

下面包含source和detail-type字段，因为它们包含 Transfer Family 事件的特定值。有关所有事件中包含的其他元数据字段的定义，请参阅Amazon EventBridge 用户指南中的事件结构参考。

```
{
  . . .,
  "detail-type": "string",
  "source": "aws.transfer",
  . . .,
  "detail": {
    "failure-code" : "string",
    "status-code" : "string",
    "protocol" : "string",
    "bytes" : "number",
    "client-ip" : "string",
    "failure-message" : "string",
    "end-timestamp" : "string",
    "etag" : "string",
    "file-path" : "string",
    "original-file-path" : "string",
    "renamed-file-path" : "string",
    "directory-path" : "string",
    "server-id" : "string",
    "username" : "string",
    "session-id" : "string",
    "start-timestamp" : "string"
  }
}
```

`detail-type`

标识事件的类型。

对于此事件，该值是先前列出的 SFTP、FTPS 或 FTP 服务器事件名称之一。

`source`

标识生成事件的服务。对于 Transfer Family 事件，此值为`aws.transfer`。

`detail`

包含关于事件信息的 JSON 对象。生成事件的服务决定该字段的内容。

对于此事件，数据包括以下内容：

`failure-code`

传输失败原因的类别。值：PARTIAL_UPLOAD | PARTIAL_DOWNLOAD | UNKNOWN_ERROR

`status-code`

传输是否成功。价值观：COMPLETED | FAILED。

`protocol`

用于传输的协议。值：SFTP | FTPS | FTP

`bytes`

传输的字节数。

`client-ip`

参与传输的客户端 IP 地址

`failure-message`

对于失败的传输，提供传输失败原因的详细信息。

`end-timestamp`

对于成功传输，指文件处理完毕的时间戳。

`etag`

实体标签（仅用于 Amazon S3 文件）。

`file-path`

正在传输、删除或以其他方式操作的文件的路径。

`original-file-path`

对于文件重命名事件，指重命名前文件的原始路径。

`renamed-file-path`

对于文件重命名事件，指重命名后文件的新路径。

`directory-path`

对于目录创建和删除事件，指目录的路径。

`server-id`

Transfer Family 服务器的唯一 ID。

`username`

正在执行转移的用户。

`session-id`

传输会话的唯一标识符。

`start-timestamp`

对于成功传输，指文件处理开始时间的时间戳。

Example SFTP 服务器文件下载失败示例事件

以下示例显示了在 SFTP 服务器上下载失败的事件（Amazon EFS 是否正在使用存储空间）。

```
{
    "version": "0",
    "id": "event-ID",
    "detail-type": "SFTP Server File Download Failed",
    "source": "aws.transfer",
    "account": "958412138249",
    "time": "2024-01-29T17:20:27Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:transfer:us-east-1:958412138249:server/s-1234abcd5678efghi"
    ],
    "detail": {
        "failure-code": "PARTIAL_DOWNLOAD",
        "status-code": "FAILED",
        "protocol": "SFTP",
        "bytes": 4100,
        "client-ip": "IP-address",
        "failure-message": "File was partially downloaded.",
        "end-timestamp": "2024-01-29T17:20:27.749749117Z",
        "file-path": "/fs-1234abcd5678efghi/user0/test-file",
        "server-id": "s-1234abcd5678efghi",
        "username": "test",
        "session-id": "session-ID",
        "start-timestamp": "2024-01-29T17:20:16.706282454Z"
    }
```

```
}
```

Example FTP 服务器文件上传已完成示例事件

以下示例显示了在 FTP 服务器上成功完成上传的事件（Amazon S3 是否正在使用存储空间）。

```
{
    "version": "0",
    "id": "event-ID",
    "detail-type": "FTP Server File Upload Completed",
    "source": "aws.transfer",
    "account": "958412138249",
    "time": "2024-01-29T16:31:43Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:transfer:us-east-1:958412138249:server/s-1111aaaa2222bbbb3"
    ],
    "detail": {
        "status-code": "COMPLETED",
        "protocol": "FTP",
        "bytes": 1048576,
        "client-ip": "10.0.0.141",
        "end-timestamp": "2024-01-29T16:31:43.311866408Z",
        "etag": "b6d81b360a5672d80c27430f39153e2c",
        "file-path": "/amzn-s3-demo-bucket/test/1mb_file",
        "server-id": "s-1111aaaa2222bbbb3",
        "username": "test",
        "session-id": "event-ID",
        "start-timestamp": "2024-01-29T16:31:42.462088327Z"
    }
}
```

Example SFTP 服务器文件删除已完成示例事件

以下示例显示了在 SFTP 服务器上成功删除文件的事件。

```
{
    "version": "0",
    "id": "event-ID",
    "detail-type": "SFTP Server File Delete Completed",
    "source": "aws.transfer",
    "account": "958412138249",
    "time": "2025-05-15T14:30:27Z",
```

```
    "region": "us-east-1",
    "resources": [
        "arn:aws:transfer:us-east-1:958412138249:server/s-1234abcd5678efghi"
    ],
    "detail": {
        "status-code": "COMPLETED",
        "protocol": "SFTP",
        "client-ip": "IP-address",
        "end-timestamp": "2025-05-15T14:30:27.749749117Z",
        "file-path": "/fs-1234abcd5678efghi/user0/test-file-to-delete.txt",
        "server-id": "s-1234abcd5678efghi",
        "username": "test",
        "session-id": "session-ID",
        "start-timestamp": "2025-05-15T14:30:26.706282454Z"
    }
}
```

Example SFTP 服务器文件重命名已完成示例事件

以下示例显示了在 SFTP 服务器上成功重命名文件的事件。

```
{
    "version": "0",
    "id": "event-ID",
    "detail-type": "SFTP Server File Rename Completed",
    "source": "aws.transfer",
    "account": "958412138249",
    "time": "2025-05-15T15:45:12Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:transfer:us-east-1:958412138249:server/s-1234abcd5678efghi"
    ],
    "detail": {
        "status-code": "COMPLETED",
        "protocol": "SFTP",
        "client-ip": "IP-address",
        "end-timestamp": "2025-05-15T15:45:12.749749117Z",
        "original-file-path": "/fs-1234abcd5678efghi/user0/old-filename.txt",
        "renamed-file-path": "/fs-1234abcd5678efghi/user0/new-filename.txt",
        "server-id": "s-1234abcd5678efghi",
        "username": "test",
        "session-id": "session-ID",
        "start-timestamp": "2025-05-15T15:45:11.706282454Z"
    }
```

```
}
```

Example SFTP 服务器目录创建已完成示例事件

以下示例显示了在 SFTP 服务器上成功创建目录的事件。

```
{
    "version": "0",
    "id": "event-ID",
    "detail-type": "SFTP Server Directory Create Completed",
    "source": "aws.transfer",
    "account": "958412138249",
    "time": "2025-05-15T16:20:05Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:transfer:us-east-1:958412138249:server/s-1234abcd5678efghi"
    ],
    "detail": {
        "status-code": "COMPLETED",
        "protocol": "SFTP",
        "client-ip": "IP-address",
        "end-timestamp": "2025-05-15T16:20:05.749749117Z",
        "directory-path": "/fs-1234abcd5678efghi/user0/new-directory",
        "server-id": "s-1234abcd5678efghi",
        "username": "test",
        "session-id": "session-ID",
        "start-timestamp": "2025-05-15T16:20:04.706282454Z"
    }
}
```

SFTP 连接器事件

> **Note**
>
> 这些事件按持久级别传送，如《Amazon EventBridge 事件参考》中Amazon 服务事件的交付级别中所述。 EventBridge

以下是 SFTP 连接器事件的详细信息字段：

- SFTP 连接器文件发送已完成

- SFTP 连接器文件发送失败
- SFTP 连接器文件检索已完成
- 检索 SFTP 连接器文件失败
- SFTP 连接器目录列表已完成
- SFTP 连接器目录列表失败
- SFTP 连接器远程移动已完成
- SFTP 连接器远程移动失败
- SFTP 连接器远程删除已完成
- SFTP 连接器远程删除失败

下面包含source和detail-type字段，因为它们包含 Transfer Family 事件的特定值。有关所有事件中包含的其他元数据字段的定义，请参阅Amazon EventBridge 用户指南中的事件结构参考。

```
{
  . . .,
  "detail-type": "string",
  "source": "aws.transfer",
  . . .,
  "detail": {
    "operation" : "string",
    "max-items" : "number",
    "connector-id" : "string",
    "output-directory-path" : "string",
    "listing-id" : "string",
    "transfer-id" : "string",
    "file-transfer-id" : "string",
    "url" : "string",
    "file-path" : "string",
    "status-code" : "string",
    "failure-code" : "string",
    "failure-message" : "string",
    "start-timestamp" : "string",
    "end-timestamp" : "string",
    "local-directory-path" : "string",
    "remote-directory-path" : "string"
    "item-count" : "number"
    "truncated" : "boolean"
    "bytes" : "number",
    "egress-type" : "string",
```

```
    "vpc-lattice-resource-configuration-arn" : "string",
    "vpc-lattice-port-number" : "number",
    "local-file-location" : {
      "domain" : "string",
      "bucket" : "string",
      "key" : "string"
    },
    "output-file-location" : {
      "domain" : "string",
      "bucket" : "string",
      "key" : "string"
    }
  }
}
```

`detail-type`

标识事件的类型。

对于此事件，该值是先前列出的 SFTP 连接器事件名称之一。

`source`

标识生成事件的服务。对于 Transfer Family 事件，此值为`aws.transfer`。

`detail`

包含关于事件信息的 JSON 对象。生成事件的服务决定了该字段的内容。

对于此事件，数据包括以下内容：

`max-items`

要返回的最大 directory/file 名字数。

`operation`

`StartFileTransfer`请求是发送文件还是检索文件。价值观：`SEND|RETRIEVE`。

`connector-id`

正在使用的 SFTP 连接器的唯一标识符。

`output-directory-path`

Amazon S3 中存储 file/directory 列表结果的路径（存储桶和前缀）。

`listing-id`

StartDirectoryListingAPI 操作的唯一标识符。此标识符可用于检查 CloudWatch 日志，以查看上市请求的状态。

`transfer-id`

传输事件（StartFileTransfer请求）的唯一标识符。

`file-transfer-id`

正在传输的文件的唯一标识符。

`url`

合作伙伴 AS2 或 SFTP 终端节点的网址。

`file-path`

正在发送或检索的位置和文件。

`status-code`

传输是否成功。价值观：FAILED | COMPLETED。

`failure-code`

对于失败的传输，则为转移失败的原因代码。

`failure-message`

对于失败的传输，提供传输失败原因的详细信息。

`start-timestamp`

对于成功传输，指文件处理开始时间的时间戳。

`end-timestamp`

对于成功传输，指文件处理完成的时间戳。

`local-directory-path`

对于RETRIEVE请求，指存放检索到文件的位置。

`remote-directory-path`

对于SEND请求，指将文件放在合作伙伴的 SFTP 服务器上的文件目录。这是用户传递给StartFileTransfer请求RemoteDirectoryPath的的值。您可以在合作伙伴的 SFTP 服务器上指定默认目录。如果是，则此字段为空。

`item-count`

列表请求返回的项目（目录和文件）数量。

`truncated`

列表输出是否包含远程目录中包含的所有项目。

`bytes`

正在传输的字节数。对于失败的传输，该值为 0。

`egress-type`

连接器的出口配置类型。值：SERVICE_MANAGED或VPC_LATTICE。

`vpc-lattice-resource-configuration-arn`

定义目标 SFTP 服务器位置的 VPC_LATTICE 资源配置的 ARN。对于服务管理的连接器，此字段为空。

`vpc-lattice-port-number`

通过 VPC_LATTICE 连接到 SFTP 服务器的端口号。

`local-file-location`

此参数包含 Amazon 存储文件位置的详细信息。

`domain`

正在使用的存储空间。目前，唯一的值是S3。

`bucket`

Amazon S3 中对象的容器。

`key`

在 Amazon S3 中为对象分配的名称。

`output-file-location`

此参数包含存储目录列表结果的 Amazon 存储位置的详细信息。

`domain`

正在使用的存储空间。目前，唯一的值是S3。

`bucket`

Amazon S3 中对象的容器。

`key`

在 Amazon S3 中为对象分配的名称。

Example SFTP 连接器文件发送失败示例事件

以下示例显示了尝试向远程 SFTP 服务器发送文件时 SFTP 连接器出现故障的事件。

```
{
    "version": "0",
    "id": "event-ID",
    "detail-type": "SFTP Connector File Send Failed",
    "source": "aws.transfer",
    "account": "123456789012",
    "time": "2024-01-24T19:30:45Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:transfer:us-east-1:123456789012:connector/c-f1111aaaa2222bbbb3"
    ],
    "detail": {
        "operation": "SEND",
        "connector-id": "c-f1111aaaa2222bbbb3",
        "transfer-id": "transfer-ID",
        "file-transfer-id": "file-transfer-ID",
        "url": "sftp://s-21a23456789012a.server.transfer.us-east-1.amazonaws.com",
        "file-path": "/amzn-s3-demo-bucket/testfile.txt",
        "status-code": "FAILED",
        "failure-code": "CONNECTION_ERROR",
        "failure-message": "Unknown Host",
        "remote-directory-path": "",
        "bytes": 0,
        "start-timestamp": "2024-01-24T18:29:33.658729Z",
        "end-timestamp": "2024-01-24T18:29:33.993196Z",
        "local-file-location": {
            "domain": "S3",
            "bucket": "amzn-s3-demo-bucket",
            "key": "testfile.txt"
        }
    }
```

```
}
```

Example SFTP 连接器文件检索已完成示例事件

以下示例显示了一个事件，其中 SFTP 连接器成功检索了从远程 SFTP 服务器发送的文件。

```
{
    "version": "0",
    "id": "event-ID",
    "detail-type": "SFTP Connector File Retrieve Completed",
    "source": "aws.transfer",
    "account": "123456789012",
    "time": "2024-01-24T18:28:08Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:transfer:us-east-1:123456789012:connector/c-f1111aaaa2222bbbb3"
    ],
    "detail": {
        "operation": "RETRIEVE",
        "connector-id": "c-fc68000012345aa18",
        "transfer-id": "file-transfer-ID",
        "file-transfer-id": "file-transfer-ID",
        "url": "sftp://s-21a23456789012a.server.transfer.us-east-1.amazonaws.com",
        "file-path": "testfile.txt",
        "status-code": "COMPLETED",
        "local-directory-path": "/amzn-s3-demo-bucket",
        "bytes": 63533,
        "start-timestamp": "2024-01-24T18:28:07.632388Z",
        "end-timestamp": "2024-01-24T18:28:07.774898Z",
        "local-file-location": {
            "domain": "S3",
            "bucket": "amzn-s3-demo-bucket",
            "key": "testfile.txt"
        }
    }
}
```

Example SFTP 连接器目录列表已完成示例事件

以下示例显示了一个事件，在该事件中，启动目录列表调用从远程 SFTP 服务器检索到列表文件。

```
{
    "version": "0",
```

```
    "id": "event-ID",
    "detail-type": "SFTP Connector Directory Listing Completed",
    "source": "aws.transfer",
    "account": "123456789012",
    "time": "2024-01-24T18:28:08Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:transfer:us-east-1:123456789012:connector/c-f1111aaaa2222bbbb3"
    ],
    "detail": {
        "max-items": 10000,
        "connector-id": "c-fc68000012345aa18",
        "output-directory-path": "/amzn-s3-demo-bucket/example/file-listing-output",
        "listing-id": "123456-23aa-7980-abc1-1a2b3c4d5e",
        "url": "sftp://s-21a23456789012a.server.transfer.us-east-1.amazonaws.com",

        "status-code": "COMPLETED",
        "remote-directory-path": "/home",
        "item-count": 10000,
        "truncated": true,
        "start-timestamp": "2024-01-24T18:28:07.632388Z",
        "end-timestamp": "2024-01-24T18:28:07.774898Z",
        "output-file-location": {
            "domain": "S3",
            "bucket": "amzn-s3-demo-bucket",
            "key": "c-fc1ab90fd0d047e7a-70987273-49nn-4006-bab1-1a7290cc412ba.json"
        }
    }
}
```

AS2 事件

> **Note**
>
> 这些事件按持久级别传送，如《Amazon EventBridge 事件参考》中Amazon 服务事件的交付级别中所述。 EventBridge

以下是 AS2 事件的详细信息字段：

- AS2 有效载荷接收已完成
- AS2 有效载荷接收失败

- AS2 有效载荷发送已完成
- AS2 有效载荷发送失败
- AS2 MDN 接收已完成
- AS2 MDN 接收失败
- AS2 MDN 发送已完成
- AS2 MDN 发送失败

下面包含source和detail-type字段，因为它们包含 Transfer Family 事件的特定值。有关所有事件中包含的其他元数据字段的定义，请参阅Amazon EventBridge 用户指南中的事件结构参考。

```
{
   . . .,
  "detail-type": "string",
  "source": "aws.transfer",
  . . .,
  "detail": {
    "s3-attributes" : {
      "file-bucket" : "string",
      "file-key" : "string",
      "json-bucket" : "string",
      "json-key" : "string",
      "mdn-bucket" : "string",
      "mdn-key" : "string"
      }
    "mdn-subject" : "string",
    "mdn-message-id" : "string",
    "disposition" : "string",
    "bytes" : "number",
    "as2-from" : "string",
    "as2-message-id" : "string",
    "as2-to" : "string",
    "connector-id" : "string",
    "client-ip" : "string",
    "agreement-id" : "string",
    "server-id" : "string",
    "requester-file-name" : "string",
    "message-subject" : "string",
    "start-timestamp" : "string",
    "end-timestamp" : "string",
    "status-code" : "string",
```

```
    "failure-code" : "string",
    "failure-message" : "string",
    "transfer-id" : "string"
  }
}
```

`detail-type`

标识事件的类型。

对于此事件，该值是前面列出 AS2 的事件之一。

`source`

标识生成事件的服务。对于 Transfer Family 事件，此值为`aws.transfer`。

`detail`

包含关于事件信息的 JSON 对象。生成事件的服务决定该字段的内容。

`s3-attributes`

识别正在传输的文件的 Amazon S3 存储桶和密钥。对于 MDN 事件，它还会识别 MDN 文件的存储桶和密钥。

`file-bucket`

Amazon S3 中对象的容器。

`file-key`

在 Amazon S3 中为对象分配的名称。

`json-bucket`

对于已完成或失败的传输，为 JSON 文件的容器。

`json-key`

对于已完成或失败的传输，指在 Amazon S3 中分配给 JSON 文件的名称。

`mdn-bucket`

对于 MDN 事件，是 MDN 文件的容器。

`mdn-key`

对于 MDN 事件，指在 Amazon S3 中分配给 MDN 文件的名称。

`mdn-subject`

对于 MDN 事件，是消息处置的文本描述。

`mdn-message-id`

对于 MDN 事件，是 MDN 消息的唯一 ID。

`disposition`

对于 MDN 事件，指处置类别。

`bytes`

消息中的字节数。

`as2-from`

发送消息的 AS2 贸易伙伴。

`as2-message-id`

正在传输的 AS2 消息的唯一标识符。

`as2-to`

正在接收消息的 AS2 贸易伙伴。

`connector-id`

对于从 Transfer Family 服务器发送给贸易伙伴的 AS2 消息，使用 AS2 连接器的唯一标识符。

`client-ip`

对于服务器事件（从交易伙伴向 Transfer Family 服务器转账），是指参与转移的客户的 IP 地址。

`agreement-id`

对于服务器事件，是 AS2协议的唯一标识符。

`server-id`

对于服务器事件，仅适用于 Transfer Family 服务器的唯一 ID。

`requester-file-name`

对于负载事件，指传输期间收到的文件的原始名称。

`message-subject`

消息主题的文字描述。

`start-timestamp`

对于成功传输，指文件处理开始时间的时间戳。

`end-timestamp`

对于成功传输，指文件处理完成的时间戳。

`status-code`

与 AS2 消息传输过程状态相对应的代码。有效值：`COMPLETED | FAILED | PROCESSING`。

`failure-code`

对于失败的传输，指传输失败原因的类别。

`failure-message`

对于失败的传输，提供传输失败原因的详细信息。

`transfer-id`

转账事件的唯一标识符。

Example AS2 Payload 接收已完成示例事件

```
{
    "version": "0",
     "id": "event-ID",
    "detail-type": "AS2 Payload Receive Completed",
    "source": "aws.transfer",
    "account": "076722215406",
    "time": "2024-02-07T06:47:05Z",
    "region": "us-east-1",
    "resources": ["arn:aws:transfer:us-east-1:076722215406:connector/
c-1111aaaa2222bbbb3"],
    "detail": {
        "s3-attributes": {
            "file-key": "/inbound/processed/testAs2Message.dat",
            "file-bucket": "amzn-s3-demo-bucket"
        },
```

```
        "client-ip": "client-IP-address",
        "requester-file-name": "testAs2MessageVerifyFile.dat",
        "end-timestamp": "2024-02-07T06:47:06.040031Z",
        "as2-from": "as2-from-ID",
        "as2-message-id": "as2-message-ID",
        "message-subject": "Message from AS2 tests",
        "start-timestamp": "2024-02-07T06:47:05.410Z",
        "status-code": "PROCESSING",
        "bytes": 63,
        "as2-to": "as2-to-ID",
        "agreement-id": "a-1111aaaa2222bbbb3",
        "server-id": "s-1234abcd5678efghi"
    }
}
```

Example AS2 MDN 接收失败示例事件

```
{
  "version": "0",
  "id": "event-ID",
  "detail-type": "AS2 MDN Receive Failed",
  "source": "aws.transfer",
  "account": "889901007463",
  "time": "2024-02-06T22:05:09Z",
  "region": "us-east-1",
  "resources": ["arn:aws:transfer:us-east-1:076722215406:server/s-1111aaaa2222bbbb3"],
  "detail": {
      "mdn-subject": "Your Requested MDN Response re: Test run from Id 123456789abcde
 to partner ijklmnop987654",
      "s3-attributes": {
          "json-bucket": "amzn-s3-demo-bucket1",
          "file-key": "/as2Integ/TestOutboundWrongCert.dat",
          "file-bucket": "amzn-s3-demo-bucket2",
          "json-key": "/as2Integ/failed/TestOutboundWrongCert.dat.json"
      },
      "mdn-message-id": "MDN-message-ID",
      "end-timestamp": "2024-02-06T22:05:09.479878Z",
      "as2-from": "PartnerA",
      "as2-message-id": "as2-message-ID",
      "connector-id": "c-1234abcd5678efghj",
      "message-subject": "Test run from Id 123456789abcde to partner ijklmnop987654",
      "start-timestamp": "2024-02-06T22:05:03Z",
      "failure-code": "VERIFICATION_FAILED_NO_MATCHING_KEY_FOUND",
```

```
      "status-code": "FAILED",
      "as2-to": "MyCompany",
      "failure-message": "No public certificate matching message signature could be
 found in profile: p-1234abcd5678efghj",
      "transfer-id": "transfer-ID"
  }
}
```

安全性 Amazon Transfer Family

云安全 Amazon 是重中之重。作为 Amazon 客户，您可以受益于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。

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：

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。有关您在使用时的合规责任的更多信息 Amazon Web Services 服务，请参阅Amazon 安全文档。

本文档可帮助您了解在使用时如何应用分担责任模型 Amazon Transfer Family。以下主题向您介绍如何进行配置 Amazon Transfer Family 以满足您的安全和合规性目标。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 Transfer Family 资源。

我们提供一个研讨会，提供规范性指导和动手实验，介绍如何在无需修改现有应用程序或管理服务器基础架构 Amazon 的情况下构建可扩展且安全的文件传输架构。您可以在此处查看本次研讨会的详细信息。

主题

- VPC 连接安全优势
- Amazon Transfer Family 服务器的安全策略
- Amazon Transfer Family SFTP 连接器的安全策略
- 使用与 Amazon Transfer Family的混合后量子密钥交换
- 数据保护和加密
- 在 Transfer Family 中管理 SSH 和 PGP 密钥
- 的身份和访问管理 Amazon Transfer Family
- 合规性验证 Amazon Transfer Family
- 韧性在 Amazon Transfer Family

- 在 VPC 和之间创建私有连接 Amazon Transfer Family APIs
- 中的基础设施安全 Amazon Transfer Family
- 添加 Web 应用程序防火墙
- 防止跨服务混淆代理
- Amazon Transfer Famil Amazon y 的托管政策

VPC 连接安全优势

具有 VPC 出口类型的 SFTP 连接器通过跨虚拟私有网络资源访问提供增强的安全优势：

- 网络隔离：所有流量都保留在您的 VPC 环境中，从而为私有终端节点连接提供与公共互联网的完全网络隔离。
- 源 IP 控制：远程 SFTP 服务器只能看到您的 VPC CIDR 范围中的 IP 地址，因此您可以完全控制用于连接的源 IP 地址。
- 私有终端节点访问：使用私有 IP 地址直接连接到 VPC 中的 SFTP 服务器，从而消除了对公共互联网的暴露。
- 混合连接：通过已建立的 VPN 或 Direct Connect 连接安全地访问本地 SFTP 服务器，无需额外的互联网接入。
- VPC 安全控制：利用现有 VPC 安全组和路由策略来控制和监控 SFTP 连接器流量。 NACLs

VPC 莱迪思安全模型

SFTP 连接器的 VPC 连接使用 Amazon VPC 莱迪思和服务网络来提供安全的多租户访问：

- 混乱的副手预防：身份验证和授权检查可确保连接器只能访问其配置的特定资源，从而防止未经授权的跨租户访问。
- IPv6仅限服务网络：使用 IPv6寻址来避免潜在的 IP 地址冲突并增强安全隔离。
- 转发访问会话 (FAS)：临时凭证处理无需长期存储凭证或手动共享资源。
- 资源级访问控制：每个连接器都与特定的资源配置相关联，从而确保对各个 SFTP 服务器进行精细的访问控制。

VPC 连接的安全最佳实践

使用 VPC 出口类型连接器时，请遵循以下安全最佳实践：

- 安全组：将安全组配置为仅允许必要资源之间的 SFTP 流量（端口 22）。将源和目标 IP 范围限制在所需的最小范围内。
- 资源网关放置：尽可能在私有子网中部署资源网关，并确保它们跨越至少两个可用区以实现高可用性。
- 网络监控：使用 VPC 流日志和 Amazon CloudWatch 监控网络流量模式并检测异常活动。
- 访问日志：启用连接器日志记录以跟踪文件传输活动并维护合规性要求的审计跟踪。
- 资源配置管理：定期检查和更新资源配置，确保它们指向正确的 SFTP 服务器并使用适当的网络设置。

Amazon Transfer Family 服务器的安全策略

中的服务器安全策略 Amazon Transfer Family 允许您限制与服务器关联的一组加密算法（消息身份验证码 (MACs)、密钥交换 (KEXs)、密码套件、内容加密密码和哈希算法）。

Amazon Transfer Family 支持使用混合密钥交换算法的后量子安全策略，将传统加密方法与后量子算法相结合，以提供针对未来量子计算威胁的增强安全性。详情请参见使用与 Amazon Transfer Family 的混合后量子密钥交换。

有关支持的密钥算法的列表，请参阅 加密算法。有关支持的服务器主机秘钥和服务托管用户秘钥算法列表，请参见 在 Transfer Family 中管理 SSH 和 PGP 密钥。

> **Note**
>
> 我们强烈建议将您的服务器更新为我们的最新安全政策。
>
> - `TransferSecurityPolicy-2024-01`是使用控制台、API 或 CLI 创建服务器时附加到服务器的默认安全策略。
> - 如果您使用默认安全策略创建 Transfer Family 服务器 CloudFormation 并接受默认安全策略，则会分配该服务器`TransferSecurityPolicy-2018-11`。
>
> 如果您担心客户端兼容性，请明确说明在创建或更新服务器时您希望使用哪种安全策略，而不是使用默认策略，默认策略可能会发生变化。要更改服务器的安全策略，请参阅编辑安全策略。

有关 Transfer Family 安全性的更多信息，请参阅以下博客文章：

- 提高 Amazon Transfer Family 服务器安全性的六个技巧
- Transfer Family 如何帮助您构建安全、合规的托管文件传输解决方案

主题

- 加密算法
- TransferSecurityPolicy-2024-01
- TransferSecurityPolicy-SshAuditCompliant -2025-02
- TransferSecurityPolicy-2023-05
- TransferSecurityPolicy-2022-03
- TransferSecurityPolicy-2020-06 和-Restricted-2020-06 TransferSecurityPolicy
- TransferSecurityPolicy-2018-11 和-Restricted-2018-11 TransferSecurityPolicy
- TransferSecurityPolicy-FIPS-2024-01/-FIPS-2024-05 TransferSecurityPolicy
- TransferSecurityPolicy-FIPS-2023-05
- TransferSecurityPolicy-FIPS-2020-06
- TransferSecurityPolicy-AS2 限量版-2025-07
- 后量子安全策略

加密算法

对于主机密钥，我们支持以下算法：

- `rsa-sha2-256`
- `rsa-sha2-512`
- `ecdsa-sha2-nistp256`
- `ecdsa-sha2-nistp384`
- `ecdsa-sha2-nistp521`
- `ssh-ed25519`

此外，以下安全策略允许`ssh-rsa`：

- TransferSecurityPolicy-2018-11
- TransferSecurityPolicy-2020-06

- TransferSecurityPolicy-FIPS-2020-06
- TransferSecurityPolicy-FIPS-2023-05
- TransferSecurityPolicy-FIPS-2024-01
- TransferSecurityPolicy-pq-ssh-fips-Experimental-2023-04

> **Note**
>
> 了解 RSA 密钥类型（始终是）和 RSA 主机密钥算法（可以是任何支持的算法`ssh-rsa`）之间的区别非常重要。

以下是各种安全策略支持的加密算法列表。

> **Note**
>
> 在下表和策略中，请注意算法类型的以下用法。
>
> - SFTP 服务器仅使用SshCiphersSshKexs、和SshMacs部分中的算法。
> - FTPS 服务器仅使用该TlsCiphers部分中的算法。
> - 由于FTP服务器不使用加密，因此不使用任何这些算法。
> - AS2 服务器仅使用ContentEncryptionCiphers和HashAlgorithms部分中的算法。这些部分定义了用于加密和签名文件内容的算法。
> - FIPS-2024-05 和 FIPS-2024-01 的安全策略是相同的，只是 FIPS-2024-05 不支持该`ssh-rsa`算法。
> - Transfer Family推出了新的限制政策，这些政策与现有政策非常相似：
>   - TransferSecurityPolicy-Restricted-2018-11 和 TransferSecurityPolicy -2018-11 安全策略完全相同，唯一的不同是受限策略不支持密码。`chacha20-poly1305@openssh.com`
>   - TransferSecurityPolicy-Restricted-2020-06 和 TransferSecurityPolicy -2020-06 安全策略是相同的，唯一的不同是受限策略不支持密码。`chacha20-poly1305@openssh.com`
>
> * 在下表中，`chacha20-poly1305@openssh.com`密码仅包含在非限制策略中，

安全策略	2024-01	SshAuditCompliant-2025-02	2023-05	2022-03	2020-06 2020-06 受限制	FIPS-2024-05 FIPS-2024-01	FIPS-2023-05	FIPS-2022-06	2018-11 2018-11 受限制	TransferSecurityPolicy-AS2 限量版-2025-07
SshCiphers										
aes128-ctr	♦	♦			♦	♦		♦	♦	♦
aes128-gcm@openssh.com	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦
aes192-ctr	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦
aes256-ctr	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦
aes256-gcm@openssh.com	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦
chacha20-poly1305@openssh.com					♦*				♦*	
SshKexs										
mlkem768x25519-										♦

安全策略	2024-01	SshAuditCompliant-2025-02	2023-05	2022-03	2020-06 2020-06 受限制	FIPS-2024-05 FIPS-2024-01	FIPS-2023-05	FIPS-2022-06	2018-11 2018-11 受限制	TransferSecurityPolicy-AS2 限量版-2025-07
sha256										
mlkem768nistp256-sha256										♦
mlkem1024nistp384-sha384										♦
curve25519-sha256	♦	♦	♦	♦					♦	♦
curve25519-sha256@libssh.org	♦	♦	♦	♦					♦	♦
diffie-hellman-group14-sha1									♦	

安全策略	2024-01	SshAuditCompliant-2025-02	2023-05	2022-03	2020-06 2020-06 受限制	FIPS-2024-05 FIPS-2024-01	FIPS-2023-05	FIPS-2022-06	2018-11 2018-11 受限制	TransferSecurityPolicy-AS2 限量版-2025-07
diffie-hellman-group14-sha256					♦			♦	♦	
diffie-hellman-group16-sha512	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦
diffie-hellman-group18-sha512	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦

安全策略	2024-01	SshAuditCompliant-2025-02	2023-05	2022-03	2020-06 2020-06 受限制	FIPS-2024-05 FIPS-2024-01	FIPS-2023-05	FIPS-2022-06	2018-11 2018-11 受限制	TransferSecurityPolicy-AS2 限量版-2025-07
diffie-hellman-group-exchange-sha256	♦	♦	♦	♦	♦		♦	♦	♦	♦
ecdh-sha2-nistp256	♦				♦	♦		♦	♦	♦
ecdh-sha2-nistp384	♦				♦	♦		♦	♦	♦
ecdh-sha2-nistp521	♦				♦	♦		♦	♦	♦
SshMacs										
hmac-sha1									♦	
hmac-sha1-etm@openssh.com									♦	

安全策略	2024-01	SshAuditCompliant-2025-02	2023-05	2022-03	2020-06 2020-06 受限制	FIPS-2024-05 FIPS-2024-01	FIPS-2023-05	FIPS-2022-06	2018-11 2018-11 受限制	TransferSecurityPolicy-AS2 限量版-2025-07
hmac-sha2-256				♦	♦			♦	♦	
hmac-sha2-256-etm@openssh.com	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦
hmac-sha2-512				♦	♦			♦	♦	
hmac-sha2-512-etm@openssh.com	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦
umac-128-etm@openssh.com					♦				♦	
umac-128@openssh.com					♦				♦	

安全策略	2024-01	SshAuditCompliant-2025-02	2023-05	2022-03	2020-06 2020-06 受限制	FIPS-2024-05 FIPS-2024-01	FIPS-2023-05	FIPS-2022-06	2018-11 2018-11 受限制	TransferSecurityPolicy-AS2 限量版-2025-07
umac-64-etm@openssh.com									♦	
umac-64@openssh.com									♦	
ContentEncryptionCiphers										
aes256-cbc	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦
aes192-cbc	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦
aes128-cbc	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦
3des-cbc	♦	♦	♦	♦	♦	♦	♦	♦	♦	
HashAlgorithms										
sha256	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦
sha384	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦
sha512	♦	♦	♦	♦	♦	♦	♦	♦	♦	♦
sha1	♦	♦	♦	♦	♦	♦	♦	♦	♦	

安全策略	2024-01	SshAuditCompliant-2025-02	2023-05	2022-03	2020-06 2020-06 受限制	FIPS-2024-05 FIPS-2024-01	FIPS-2023-05	FIPS-2022-06	2018-11 2018-11 受限制	TransferSecurityPolicy-AS2 限量版-2025-07
TlsCiphers										
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	♦	♦	♦	♦	♦	♦	♦	♦	♦	
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	♦	♦	♦	♦	♦	♦	♦	♦	♦	
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	♦	♦	♦	♦	♦	♦	♦	♦	♦	
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	♦	♦	♦	♦	♦	♦	♦	♦	♦	

安全策略	2024-01	SshAuditCompliant-2025-02	2023-05	2022-03	2020-06 2020-06 受限制	FIPS-2024-05 FIPS-2024-01	FIPS-2023-05	FIPS-2022-06	2018-11 2018-11 受限制	TransferSecurityPolicy-AS2 限量版-2025-07
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256		♦	♦	♦	♦	♦	♦	♦	♦	♦
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256		♦	♦	♦	♦	♦	♦	♦	♦	♦
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384		♦	♦	♦	♦	♦	♦	♦	♦	♦
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384		♦	♦	♦	♦	♦	♦	♦	♦	♦
TLS_RSA_WITH_AES_128_CBC_SHA256									♦	

安全策略	2024-01	SshAuditCompliant-2025-02	2023-05	2022-03	2020-06 2020-06 受限制	FIPS-2024-05 FIPS-2024-01	FIPS-2023-05	FIPS-2022-06	2018-11 2018-11 受限制	TransferSecurityPolicy-AS2 限量版-2025-07
TLS_RSA_WITH_AES_256_CBC_SHA256									◆	

TransferSecurityPolicy-2024-01

以下显示了 TransferSecurityPolicy -2024-01 安全策略。

```
{
    "SecurityPolicy": {
        "Fips": false,
        "SecurityPolicyName": "TransferSecurityPolicy-2024-01",
        "SshCiphers": [
            "aes128-gcm@openssh.com",
            "aes256-gcm@openssh.com",
            "aes128-ctr",
            "aes256-ctr",
            "aes192-ctr"
        ],
        "SshKexs": [
            "ecdh-sha2-nistp256",
            "ecdh-sha2-nistp384",
            "ecdh-sha2-nistp521",
            "curve25519-sha256",
            "curve25519-sha256@libssh.org",
            "diffie-hellman-group18-sha512",
            "diffie-hellman-group16-sha512",
            "diffie-hellman-group-exchange-sha256"
        ],
        "SshMacs": [
            "hmac-sha2-256-etm@openssh.com",
```

```
            "hmac-sha2-512-etm@openssh.com"
        ],
        "ContentEncryptionCiphers": [
            "aes256-cbc",
            "aes192-cbc",
            "aes128-cbc",
            "3des-cbc"
        ],
        "HashAlgorithms": [
            "sha256",
            "sha384",
            "sha512",
            "sha1"
        ],
        "TlsCiphers": [
            "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
            "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
            "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
            "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
            "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
            "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
            "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
            "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
        ]
    }
}
```

TransferSecurityPolicy-SshAuditCompliant -2025-02

以下显示了 TransferSecurityPolicy-SshAuditCompliant -2025-02 安全策略。

> **Note**
>
> 此安全策略是围绕该工具提供的建议设计的，并且与该ssh-audit工具100%兼容。

```
{
  "SecurityPolicy": {
    "Fips": false,
    "Protocols": [
      "SFTP",
      "FTPS"
```

```
    ],
    "SecurityPolicyName": "TransferSecurityPolicy-SshAuditCompliant-2025-02",
    "SshCiphers": [
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com",
      "aes128-ctr",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "curve25519-sha256",
      "curve25519-sha256@libssh.org",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512-etm@openssh.com"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc",
      "3des-cbc"
    ],
    "HashAlgorithms": [
      "sha256",
      "sha384",
      "sha512",
      "sha1"
    ],
    "TlsCiphers": [
      "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ],
    "Type": "SERVER"
  }
```

```
}
```

TransferSecurityPolicy-2023-05

以下显示了 TransferSecurityPolicy -2023-05 安全策略。

```
{
    "SecurityPolicy": {
        "Fips": false,
        "SecurityPolicyName": "TransferSecurityPolicy-2023-05",
        "SshCiphers": [
            "aes256-gcm@openssh.com",
            "aes128-gcm@openssh.com",
            "aes256-ctr",
            "aes192-ctr"
        ],
        "SshKexs": [
            "curve25519-sha256",
            "curve25519-sha256@libssh.org",
            "diffie-hellman-group16-sha512",
            "diffie-hellman-group18-sha512",
            "diffie-hellman-group-exchange-sha256"
        ],
        "SshMacs": [
            "hmac-sha2-512-etm@openssh.com",
            "hmac-sha2-256-etm@openssh.com"
        ],
        "ContentEncryptionCiphers": [
            "aes256-cbc",
            "aes192-cbc",
            "aes128-cbc",
            "3des-cbc"
        ],
        "HashAlgorithms": [
            "sha256",
            "sha384",
            "sha512",
            "sha1"
        ],
        "TlsCiphers": [
            "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
            "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
            "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
```

```
            "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
            "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
            "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
            "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
            "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
        ]
    }
}
```

TransferSecurityPolicy-2022-03

以下显示了 TransferSecurityPolicy -2022-03 安全策略。

```
{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2022-03",
    "SshCiphers": [
      "aes256-gcm@openssh.com",
      "aes128-gcm@openssh.com",
      "aes256-ctr",
      "aes192-ctr"
    ],
    "SshKexs": [
      "curve25519-sha256",
      "curve25519-sha256@libssh.org",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group-exchange-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-512-etm@openssh.com",
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512",
      "hmac-sha2-256"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc"
      "3des-cbc",
    ],
    "HashAlgorithms": [
```

```
      "sha256",
      "sha384",
      "sha512"
      "sha1"
    ],
    "TlsCiphers": [
      "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
  }
}
```

TransferSecurityPolicy-2020-06 和-Restricted-2020-06 TransferSecurityPolicy

以下显示了 TransferSecurityPolicy -2020-06 安全策略。

> **Note**
>
> TransferSecurityPolicy-Restricted-2020-06 和 TransferSecurityPolicy -2020-06 安全策略是相同的，唯一的不同是受限策略不支持密码。chacha20-poly1305@openssh.com

```
{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2020-06",
    "SshCiphers": [
      "chacha20-poly1305@openssh.com", //Not included in TransferSecurityPolicy-
Restricted-2020-06
      "aes128-ctr",
      "aes192-ctr",
      "aes256-ctr",
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com"
```

```
    ],
    "SshKexs": [
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "diffie-hellman-group-exchange-sha256",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group14-sha256"
    ],
    "SshMacs": [
      "umac-128-etm@openssh.com",
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512-etm@openssh.com",
      "umac-128@openssh.com",
      "hmac-sha2-256",
      "hmac-sha2-512"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc"
            "3des-cbc",
    ],
    "HashAlgorithms": [
      "sha256",
      "sha384",
      "sha512"
      "sha1"
    ],
    "TlsCiphers": [
      "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
  }
}
```

TransferSecurityPolicy-2018-11 和-Restricted-2018-11 TransferSecurityPolicy

以下显示了 TransferSecurityPolicy -2018-11 的安全策略。

> **Note**
>
> TransferSecurityPolicy-Restricted-2018-11 和 TransferSecurityPolicy -2018-11 安全策略完全相同，唯一的不同是受限策略不支持密码。chacha20-poly1305@openssh.com

```
{
  "SecurityPolicy": {
    "Fips": false,
    "SecurityPolicyName": "TransferSecurityPolicy-2018-11",
    "SshCiphers": [
      "chacha20-poly1305@openssh.com", //Not included in TransferSecurityPolicy-
Restricted-2018-11
      "aes128-ctr",
      "aes192-ctr",
      "aes256-ctr",
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com"
    ],
    "SshKexs": [
      "curve25519-sha256",
      "curve25519-sha256@libssh.org",
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "diffie-hellman-group-exchange-sha256",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group14-sha256",
      "diffie-hellman-group14-sha1"
    ],
    "SshMacs": [
      "umac-64-etm@openssh.com",
      "umac-128-etm@openssh.com",
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512-etm@openssh.com",
      "hmac-sha1-etm@openssh.com",
```

```
      "umac-64@openssh.com",
      "umac-128@openssh.com",
      "hmac-sha2-256",
      "hmac-sha2-512",
      "hmac-sha1"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc"
            "3des-cbc",
    ],
    "HashAlgorithms": [
      "sha256",
      "sha384",
      "sha512",
      "sha1"
    ],
    "TlsCiphers": [
      "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384",
      "TLS_RSA_WITH_AES_128_CBC_SHA256",
      "TLS_RSA_WITH_AES_256_CBC_SHA256"
    ]
  }
}
```

TransferSecurityPolicy-FIPS-2024-01/-FIPS-2024-05 TransferSecurityPolicy

以下显示了-FIPS-2024-0 TransferSecurityPolicy 1 和-FIPS-2024-05 安全策略。TransferSecurityPolicy

> **Note**
>
> FIPS 服务终端节点以及 TransferSecurityPolicy-FIPS-2024-01 和-FIPS-2024-05 安全策略仅在 TransferSecurityPolicy某些地区可用。 Amazon 有关更多信息，请参阅 Amazon Web Services 一般参考 中的 Amazon Transfer Family 端点和配额。
> 这两种安全策略之间的唯一区别是-FIPS-2024-01支持该算法，而 TransferSecurityPolicy-FIPS-2024-05不支持该ssh-rsa算法。 TransferSecurityPolicy


```
{
    "SecurityPolicy": {
        "Fips": true,
        "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2024-01",
        "SshCiphers": [
            "aes128-gcm@openssh.com",
            "aes256-gcm@openssh.com",
            "aes128-ctr",
            "aes256-ctr",
            "aes192-ctr"
        ],
        "SshKexs": [
            "ecdh-sha2-nistp256",
            "ecdh-sha2-nistp384",
            "ecdh-sha2-nistp521",
            "diffie-hellman-group18-sha512",
            "diffie-hellman-group16-sha512",
            "diffie-hellman-group-exchange-sha256"
        ],
        "SshMacs": [
            "hmac-sha2-256-etm@openssh.com",
            "hmac-sha2-512-etm@openssh.com"
        ],
        "ContentEncryptionCiphers": [
            "aes256-cbc",
            "aes192-cbc",
            "aes128-cbc"
            "3des-cbc"
        ],
        "HashAlgorithms": [
            "sha256",
            "sha384",
            "sha512"
```

```
            "sha1"
        ],
        "TlsCiphers": [
            "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
            "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
            "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
            "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
            "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
            "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
            "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
            "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
        ]
    }
}
```

TransferSecurityPolicy-FIPS-2023-05

FIPS 认证详情 Amazon Transfer Family 可在以下网址找到 https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search/all

以下显示了 TransferSecurityPolicy-FIPS-2023-05 安全策略。

> **Note**
>
> FIPS 服务终端节点和 TransferSecurityPolicy-FIPS-2023-05 安全策略仅在某些地区可用。Amazon 有关更多信息，请参阅 Amazon Web Services 一般参考 中的 Amazon Transfer Family 端点和配额。

```
{
    "SecurityPolicy": {
        "Fips": true,
        "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2023-05",
        "SshCiphers": [
            "aes256-gcm@openssh.com",
            "aes128-gcm@openssh.com",
            "aes256-ctr",
            "aes192-ctr"
        ],
        "SshKexs": [
            "diffie-hellman-group16-sha512",
```

```
            "diffie-hellman-group18-sha512",
            "diffie-hellman-group-exchange-sha256"
        ],
        "SshMacs": [
            "hmac-sha2-256-etm@openssh.com",
            "hmac-sha2-512-etm@openssh.com"
        ],
        "ContentEncryptionCiphers": [
            "aes256-cbc",
            "aes192-cbc",
            "aes128-cbc"
            "3des-cbc"
        ],
        "HashAlgorithms": [
            "sha256",
            "sha384",
            "sha512"
            "sha1"
        ],
        "TlsCiphers": [
            "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
            "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
            "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
            "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
            "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
            "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
            "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
            "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
        ]
    }
}
```

TransferSecurityPolicy-FIPS-2020-06

FIPS 认证详情 Amazon Transfer Family 可在以下网址找到 https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search/all

以下显示了 TransferSecurityPolicy-FIPS-2020-06 安全策略。

> **Note**
>
> FIPS 服务终端节点和 TransferSecurityPolicy-FIPS-2020-06 安全策略仅在某些地区可用。Amazon 有关更多信息，请参阅 Amazon Web Services 一般参考 中的 Amazon Transfer Family 端点和配额。


```
{
  "SecurityPolicy": {
    "Fips": true,
    "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2020-06",
    "SshCiphers": [
      "aes128-ctr",
      "aes192-ctr",
      "aes256-ctr",
      "aes128-gcm@openssh.com",
      "aes256-gcm@openssh.com"
    ],
    "SshKexs": [
      "ecdh-sha2-nistp256",
      "ecdh-sha2-nistp384",
      "ecdh-sha2-nistp521",
      "diffie-hellman-group-exchange-sha256",
      "diffie-hellman-group16-sha512",
      "diffie-hellman-group18-sha512",
      "diffie-hellman-group14-sha256"
    ],
    "SshMacs": [
      "hmac-sha2-256-etm@openssh.com",
      "hmac-sha2-512-etm@openssh.com",
      "hmac-sha2-256",
      "hmac-sha2-512"
    ],
    "ContentEncryptionCiphers": [
      "aes256-cbc",
      "aes192-cbc",
      "aes128-cbc"
            "3des-cbc",
    ],
    "HashAlgorithms": [
      "sha256",
      "sha384",
```

```
      "sha512"
            "sha1",
    ],
    "TlsCiphers": [
      "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
      "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
      "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
      "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
    ]
  }
}
```

TransferSecurityPolicy-AS2 限量版-2025-07

此安全策略专为需要通过排除传统加密算法来增强安全性的 AS2 文件传输而设计。它支持现代 AES 加密和 SHA-2 哈希算法，同时取消了对 3DES 和 SHA-1 等较弱算法的支持。

```
{
    "SecurityPolicy": {
        "Fips": false,
        "SecurityPolicyName": "TransferSecurityPolicy-AS2Restricted-2025-07",
        "SshCiphers": [
            "aes256-gcm@openssh.com",
            "aes128-gcm@openssh.com",
            "aes128-ctr",
            "aes256-ctr",
            "aes192-ctr"
        ],
        "SshKexs": [
            "mlkem768x25519-sha256",
            "mlkem768nistp256-sha256",
            "mlkem1024nistp384-sha384",
            "ecdh-sha2-nistp256",
            "ecdh-sha2-nistp384",
            "ecdh-sha2-nistp521",
            "curve25519-sha256",
            "curve25519-sha256@libssh.org",
            "diffie-hellman-group16-sha512",
            "diffie-hellman-group18-sha512",
```

```
            "diffie-hellman-group-exchange-sha256"
        ],
        "SshMacs": [
            "hmac-sha2-256-etm@openssh.com",
            "hmac-sha2-512-etm@openssh.com"
        ],
        "ContentEncryptionCiphers": [
            "aes256-cbc",
            "aes192-cbc",
            "aes128-cbc"
        ],
        "HashAlgorithms": [
            "sha256",
            "sha384",
            "sha512"
        ],
        "TlsCiphers": [
            "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
            "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
            "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
            "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
            "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
            "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
            "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
            "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
        ],
        "Type": "SERVER",
        "Protocols": [
            "AS2"
        ]
    }
}
```

后量子安全策略

下表列出了 Transfer Family 后量子安全策略算法。有关此策略的详细描述，请参见使用与 Amazon Transfer Family的混合后量子密钥交换。

政策列表如下表所示。

> **Note**
>
> 较早的后量子政策（TransferSecurityPolicy-pq-ssh-experimental-2023-04 和-pq-ssh-fips-experimental-2023-04）已被弃用。TransferSecurityPolicy我们建议您改用新政策。

安全策略	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-FIPS-2025-03
SSH ciphers		
aes128-ctr	♦	♦
aes128-gcm@openssh.com	♦	♦
aes192-ctr	♦	♦
aes256-ctr	♦	♦
aes256-gcm@openssh.com	♦	♦
KEXs		
mlkem768x25519-sha256	♦	♦
mlkem768nistp256-sha256	♦	♦
mlkem1024nistp384-sha384	♦	♦
diffie-hellman-group14-sha256	♦	♦
diffie-hellman-group16-sha512	♦	♦
diffie-hellman-group18-sha512	♦	♦
ecdh-sha2-nistp384	♦	♦
ecdh-sha2-nistp521	♦	♦
ecdh-sha2-nistp256	♦	♦

安全策略	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-FIPS-2025-03
diffie-hellman-group-exchange-sha256	♦	♦
curve25519-sha256@libssh.org	♦	
curve25519-sha256	♦	
MACs		
hmac-sha2-256-etm@openssh.com	♦	♦
hmac-sha2-512-etm@openssh.com	♦	♦
ContentEncryptionCiphers		
aes256-cbc	♦	♦
aes192-cbc	♦	♦
aes128-cbc	♦	♦
3des-cbc	♦	♦
HashAlgorithms		
sha256	♦	♦
sha384	♦	♦
sha512	♦	♦
sha1	♦	♦
TLS ciphers		

安全策略	TransferSecurityPolicy-2025-03	TransferSecurityPolicy-FIPS-2025-03
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_ SHA256	♦	♦
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ SHA256	♦	♦
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_ SHA384	♦	♦
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ SHA384	♦	♦
TLS_ECDHE_RSA_WITH_AES_128_CBC_ SHA256	♦	♦
TLS_ECDHE_RSA_WITH_AES_128_GCM_ SHA256	♦	♦
TLS_ECDHE_RSA_WITH_AES_256_CBC_ SHA384	♦	♦
TLS_ECDHE_RSA_WITH_AES_256_GCM_ SHA384	♦	♦

TransferSecurityPolicy-2025-03

以下显示了 TransferSecurityPolicy -2025-03 安全策略。

```
{
    "SecurityPolicy": {
        "Fips": false,
        "SecurityPolicyName": "TransferSecurityPolicy-2025-03",
        "SshCiphers": [
            "aes256-gcm@openssh.com",
            "aes128-gcm@openssh.com",
            "aes128-ctr",
            "aes256-ctr",
```

```
            "aes192-ctr"
        ],
        "SshKexs": [
            "mlkem768x25519-sha256",
            "mlkem768nistp256-sha256",
            "mlkem1024nistp384-sha384",
            "ecdh-sha2-nistp256",
            "ecdh-sha2-nistp384",
            "ecdh-sha2-nistp521",
            "curve25519-sha256",
            "curve25519-sha256@libssh.org",
            "diffie-hellman-group16-sha512",
            "diffie-hellman-group18-sha512",
            "diffie-hellman-group-exchange-sha256"
        ],
        "SshMacs": [
            "hmac-sha2-256-etm@openssh.com",
            "hmac-sha2-512-etm@openssh.com"
        ],
        "ContentEncryptionCiphers": [
            "aes256-cbc",
            "aes192-cbc",
            "aes128-cbc"
            "3des-cbc"
        ],
        "HashAlgorithms": [
            "sha256",
            "sha384",
            "sha512"
            "sha1"
        ],
        "TlsCiphers": [
            "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
            "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
            "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
            "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
            "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
            "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
            "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
            "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
        ],
        "Type": "SERVER",
        "Protocols": [
           "SFTP",
```

```
            "FTPS"
        ]
    }
}
```

TransferSecurityPolicy-FIPS-2025-03

以下显示了 TransferSecurityPolicy-FIPS-2025-03 安全策略。

```
{
    "SecurityPolicy": {
        "Fips": true,
        "SecurityPolicyName": "TransferSecurityPolicy-FIPS-2025-03",
        "SshCiphers": [
            "aes256-gcm@openssh.com",
            "aes128-gcm@openssh.com",
            "aes256-ctr",
            "aes192-ctr",
            "aes128-ctr"
        ],
        "SshKexs": [
            "mlkem768x25519-sha256",
            "mlkem768nistp256-sha256",
            "mlkem1024nistp384-sha384",
            "ecdh-sha2-nistp256",
            "ecdh-sha2-nistp384",
            "ecdh-sha2-nistp521",
            "diffie-hellman-group-exchange-sha256",
            "diffie-hellman-group16-sha512",
            "diffie-hellman-group18-sha512"
        ],
        "SshMacs": [
            "hmac-sha2-512-etm@openssh.com",
            "hmac-sha2-256-etm@openssh.com"
        ],
        "ContentEncryptionCiphers": [
            "aes256-cbc",
            "aes192-cbc",
            "aes128-cbc"
            "3des-cbc"
        ],
        "HashAlgorithms": [
            "sha256",
```

```
            "sha384",
            "sha512"
            "sha1"
        ],
        "TlsCiphers": [
            "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
            "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
            "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
            "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
            "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
            "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
            "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
            "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
        ],
        "Type": "SERVER",
        "Protocols": [
           "SFTP",
           "FTPS"
        ]
    }
}
```

TransferSecurityPolicy-AS2 限量版-2025-07

以下显示了 TransferSecurityPolicy-AS2 限制型 2025-07 安全策略。

> **Note**
>
> 此安全策略与 TransferSecurityPolicy -2025-03 相同，不同之处在于它不支持 3DES（in ContentEncryptionCiphers），也不支持 SHA1 （in）。 HashAlgorithms它包括 2025-03 年的所有算法，包括后量子加密算法 (mlkem*)。 KEXs

```
{
    "SecurityPolicy": {
        "Fips": false,
        "SecurityPolicyName": "TransferSecurityPolicy-AS2Restricted-2025-07",
        "SshCiphers": [
            "aes256-gcm@openssh.com",
            "aes128-gcm@openssh.com",
            "aes128-ctr",
            "aes256-ctr",
```

```
            "aes192-ctr"
        ],
        "SshKexs": [
            "mlkem768x25519-sha256",
            "mlkem768nistp256-sha256",
            "mlkem1024nistp384-sha384",
            "ecdh-sha2-nistp256",
            "ecdh-sha2-nistp384",
            "ecdh-sha2-nistp521",
            "curve25519-sha256",
            "curve25519-sha256@libssh.org",
            "diffie-hellman-group16-sha512",
            "diffie-hellman-group18-sha512",
            "diffie-hellman-group-exchange-sha256"
        ],
        "SshMacs": [
            "hmac-sha2-256-etm@openssh.com",
            "hmac-sha2-512-etm@openssh.com"
        ],
        "ContentEncryptionCiphers": [
            "aes256-cbc",
            "aes192-cbc",
            "aes128-cbc"
        ],
        "HashAlgorithms": [
            "sha256",
            "sha384",
            "sha512"
        ],
        "TlsCiphers": [
            "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
            "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
            "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256",
            "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
            "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
            "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
            "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384",
            "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384"
        ],
        "Type": "SERVER",
        "Protocols": [
           "SFTP",
           "FTPS"
        ]
```

```
    }
}
```

Amazon Transfer Family SFTP 连接器的安全策略

中的 SFTP 连接器安全策略 Amazon Transfer Family 允许您限制与 SFTP 连接器关联的一组加密算法（消息身份验证码 (MACsKEXs)、密钥交换 () 和密码套件）。以下是每个 SFTP 连接器安全策略支持的加密算法列表。

> **Note**
>
> `TransferSFTPConnectorSecurityPolicy-2024-03`是应用于 SFTP 连接器的默认安全策略。

您可以更改连接器的安全策略。从 T r ansfer Family 左侧导航窗格中选择 “连接器”，然后选择您的连接器。然后在 Sftp 配置部分中选择编辑。在 “加密算法选项” 部分，从 “安全策略” 字段的下拉列表中选择任何可用的安全策略。

加密算法

对于主机密钥，SFTP 连接器支持 Transfer Family 服务器支持的所有算法，ed25519 除外：

- `rsa-sha2-256`
- `rsa-sha2-512`
- `ecdsa-sha2-nistp256`
- `ecdsa-sha2-nistp384`
- `ecdsa-sha2-nistp521`

此外，对于主机密钥，我们支持`ssh-rsa`，但仅支持`TransferSFTPConnectorSecurityPolicy-2023-07`。

对于身份验证，SFTP 连接器支持以下密钥类型：

- `ssh-rsa`
- `ecdsa`

SFTP 连接器安全策略详细信息

下表显示了每个 SFTP 连接器安全策略支持的特定加密算法。

安全策略	转账 SFTPConnector SecurityPolicy-FIPS-2024-10	转账 SFTPConnector SecurityPolicy-2024-03	转会 SFTPConnector SecurityPolicy-2023-07
Ciphers			
aes128-ctr			♦
aes128-gcm@openssh.com	♦	♦	♦
aes192-ctr		♦	♦
aes256-ctr		♦	♦
aes256-gcm@openssh.com	♦	♦	♦
Kexs			
curve25519-sha256		♦	♦
curve25519-sha256@libssh.org		♦	♦
diffie-hellman-group14-sha1			♦
diffie-hellman-group16-sha512		♦	♦
diffie-hellman-group18-sha512		♦	♦
diffie-hellman-group-exchange-sha256		♦	♦

安全策略	转账 SFTPConnector SecurityPolicy-FIPS-2024-10	转账 SFTPConnector SecurityPolicy-2024-03	转会 SFTPConnector SecurityPolicy-2023-07
ecdh-sha2-nistp256	♦		
ecdh-sha2-nistp384	♦		
ecdh-sha2-nistp521	♦		
Macs			
hmac-sha2-512-etm@openssh.com		♦	♦
hmac-sha2-256-etm@openssh.com		♦	♦
hmac-sha2-512	♦	♦	♦
hmac-sha2-256	♦	♦	♦
hmac-sha1			♦
hmac-sha1-96			♦
Host Key Algorithms			
rsa-sha2-256	♦	♦	♦
rsa-sha2-512	♦	♦	♦
ecdsa-sha2-nistp256	♦	♦	♦
ecdsa-sha2-nistp384		♦	♦
ecdsa-sha2-nistp521		♦	♦
ssh-rsa			♦

使用与 Amazon Transfer Family的混合后量子密钥交换

Transfer Family 支持安全外壳 (SSH) 协议的混合后量子密钥建立选项。之所以需要建立后量子密钥，是因为已经有可能记录网络流量并将其保存以备将来由量子计算机解密，这被称为攻击。store-now-harvest-later

当您连接至 Transfer Family，您可使用此选项，将在 Amazon Simple Storage Service (Amazon S3) 存储或 Amazon Elastic File System (Amazon EFS) 内外安全传输文件。SSH 中的后量子混合密钥创建引入了后量子密钥建立机制，该机制与经典的密钥交换算法结合使用。通过传统密码套件创建的 SSH 密钥可以免受当前技术的暴力攻击。但是，在未来大规模量子计算出现之后，预计传统加密依然无法保证安全。

如果您的组织需要使 Transfer Family 连接传输的数据保持长期机密性，在目前没有大规模后量子计算机的情况下，可考虑改用后量子密码技术。

为了保护当今加密的数据免受未来潜在的攻击， Amazon 正在与密码学界一起开发抗量子算法或后量子算法。我们在 Transfer Family 中实施了混合后量子密钥交换密码套件，通过将传统加密算法与后量子算法相结合。

这些混合密码套件可以在大多数 Amazon 区域中用于您的生产工作负载。不过，由于混合密码套件的性能特征及带宽要求与传统密钥交换机制的性能特征及带宽要求有所不同，我们建议您针对您的 Transfer Family 连接开展测试。

在后量子密码学安全博客文章中了解后量子密码的更多信息。

目录

- 关于 SSH 中的后量子混合密钥交换
- 后量子混合密钥创建如何在 Transfer Family 中运行
  - 为什么 ML-KEM？
  - 后量子混合 SSH 密钥交换和加密要求 (FIPS 140)
- 在 Transfer Family 中测试后量子混合密钥交换
  - 在 SFTP 端点启用后量子混合密钥交换
  - 设置支持后量子混合密钥交换的 SFTP 客户端
  - 确认 SFTP 中的后量子混合密钥交换

关于 SSH 中的后量子混合密钥交换

Transfer Family 支持后量子混合密钥交换密码套件，该套件同时使用经典的 El liptic Curve Diffie-Hellman (ECDH) 密钥交换算法和 ML- KEM。ML-KEM是一种后量子公钥加密和密钥建立算法，美国国家标准与技术研究所（NIST）已将其指定为其第一个标准的后量子密钥协议算法。

客户端和服务器仍进行 ECDH 密钥交换。此外，服务器将后量子共享密钥封装至客户端后量子 KEM 公钥，该公钥参见客户端的 SSH 密钥交换消息。该策略将经典密钥交换的高度保证与拟议的后量子密钥交换的安全性相结合，以帮助确保只要 ECDH 或后量子共享机密无法破解，握手就会受到保护。

后量子混合密钥创建如何在 Transfer Family 中运行

Amazon 最近宣布支持在 SFTP 文件传输中进行后量子密钥交换。 Amazon Transfer Family Transfer Family 使用 SFTP 和其他协议安全地将 business-to-business文件传输扩展到 Amazon 存储服务。SFTP 是 SSH 运行的文件传输协议 (FTP) 的更安全的版本。Transfer Family 的后量子密钥交换支持提高了 SFTP 传输数据的安全门槛。

Transfer Family 中对后量子混合密钥交换 SFTP 的支持包括将后量子算法 ML-KEM-768 和 ML-KEM-1024 与 P256、P384 或 Curve25519 曲线上的 ECDH 相结合。后量子混合 SSH 秘钥交换草稿中指定以下对应的 SSH 秘钥交换方法。

- `mlkem768nistp256-sha256`
- `mlkem1024nistp384-sha384`
- `mlkem768x25519-sha256`

为什么 ML-KEM？

Amazon 致力于支持标准化、可互操作的算法。ML-KEM 是 NIST 后量子密码学项目标准化和批准的唯一一种后量子密钥交换算法。标准机构已经在将 ML-KEM 整合到协议中。 Amazon 已在某些 Amazon API 端点中支持 TLS 中的 ML-KEM。

作为该承诺的一部分， Amazon 已向IETF提交了一份后量子加密提案草案，该提案将ML-KEM与NIST批准的曲线（例如用于SSH的P256）相结合。为了帮助增强客户的安全性，在 SFTP 和 SSH 中 Amazon 实施后量子密钥交换遵循了该草案。在我们的提案被 IETF 采纳并成为标准之前，我们计划支持未来更新。

随着草案向标准化发展，新的密钥交换方法（列于本节后量子混合密钥创建如何在 Transfer Family 中运行）可能会发生变化。

> **Note**
>
> 后量子算法支持在 TLS 中用于后量子混合密钥交换 Amazon KMS （参见使用混合后量子 TLS Amazon KMS ）和 Amazon Secrets Manager API Amazon Certificate Manager端点。

后量子混合 SSH 密钥交换和加密要求 (FIPS 140)

对于需要符合 FIPS 标准的客户，Transfer Family 使用 FIPS 140 认证的开源加密库-LC 在 SSH 中提供 Amazon FIPS 认可的加密。 Amazon根据NIST的SP 800-56Cr2（第2节），Tran TransferSecurityPolicy sfer Family中-FIPS-2025-03中支持的后量子混合密钥交换方法已获得FIPS的批准。德国联邦信息安全办公室 (BSI) 和法国国家信息系统安全局 (ANSSI) 也推荐了这种后量子混合密钥交换方法。

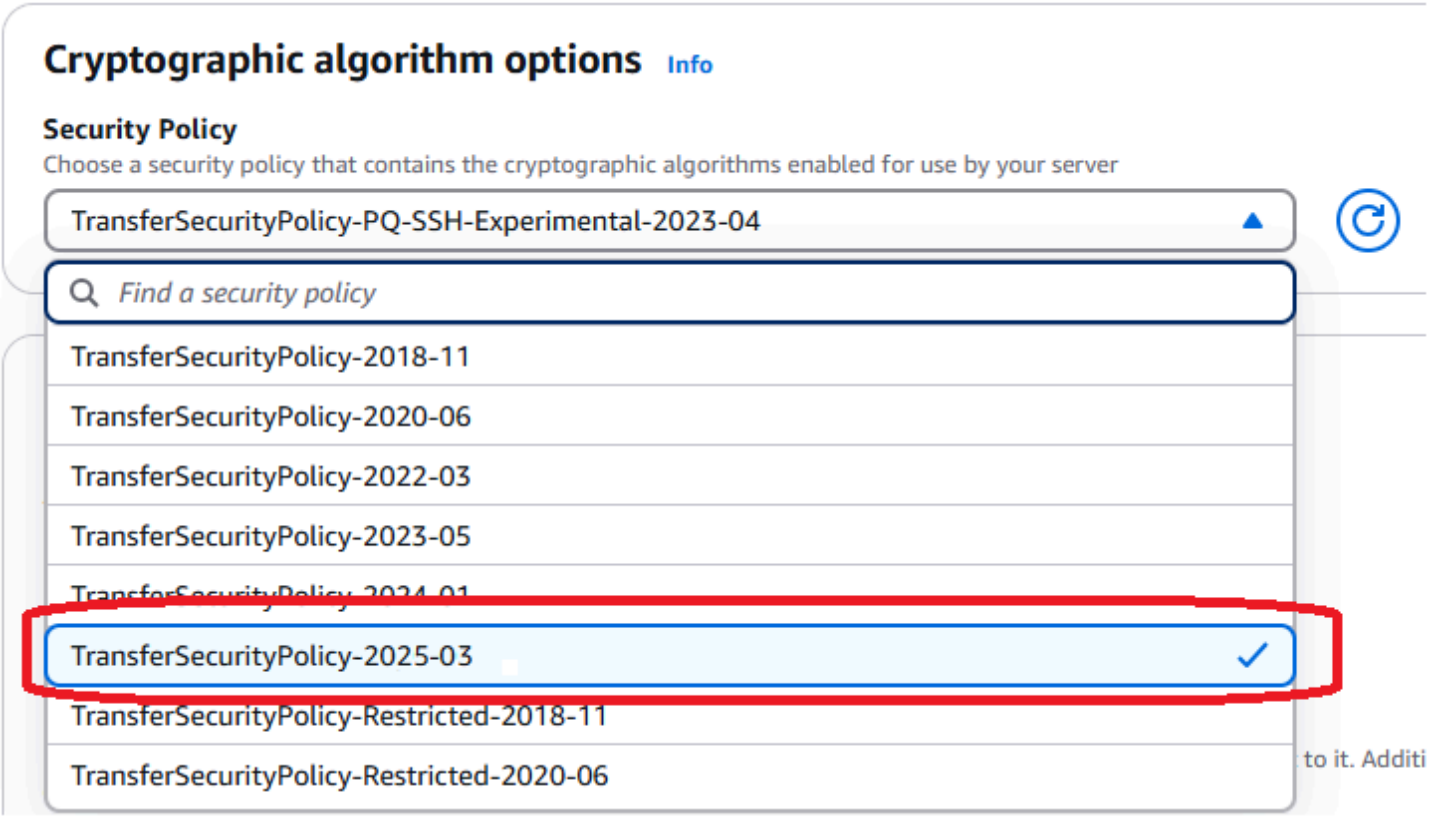
在 Transfer Family 中测试后量子混合密钥交换

本节介绍测试后量子混合密钥交换所需步骤。

1. 在 SFTP 端点启用后量子混合密钥交换.
2. 遵循上述规范草案中的指导，使用支持后量子混合密钥交换的 SFTP 客户端 (例如 设置支持后量子混合密钥交换的 SFTP 客户端)。
3. 通过 Transfer Family 服务器传输文件。
4. 确认 SFTP 中的后量子混合密钥交换.

在 SFTP 端点启用后量子混合密钥交换

当您在 Transfer Family 创建 SFTP 服务器端点时，您可选择 SSH 策略，或在现有 SFTP 端点编辑加密算法选项。以下快照显示了您在 Amazon Web Services 管理控制台 何处更新 SSH 策略的示例。



支持后量子密钥交换的 SSH 策略名称为 TransferSecurityPolicy-2025-03 和-FIPS-2025-03。TransferSecurityPolicy有关 Transfer Family 政策的更多详情，请参阅 Amazon Transfer Family 服务器的安全策略。

设置支持后量子混合密钥交换的 SFTP 客户端

在 SFTP Transfer Family 端点中选择正确的后量子 SSH 策略后，您可以在 Transfer Family 中尝试后量子 SFTP。在本地系统上安装最新的 OpenSSH 客户端（例如 9.9 版）进行测试。

> **Note**
>
> 确保您的客户端支持前面列出的一种或多种 ML-KEM 算法。您可以通过运行以下命令来查看您的OpenSSH版本支持的算法:. `ssh -Q kex`

您可以运行示例 SFTP 客户端，通过使用后量子混合密钥交换方法连接到 SFTP 端点（例如`s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com`），如以下命令所示。

```
sftp -v -o \
```

```
    KexAlgorithms=mlkem768x25519-sha256 \
    -i username_private_key_PEM_file \
    username@server-id.server.transfer.region-id.amazonaws.com
```

在上一个命令中，将以下项目替换为您自己的信息：

- *username_private_key_PEM_file*替换为 SFTP 用户的私钥 PEM 编码文件
- 替换*username*为 SFTP 用户名
- *server-id*替换为 Transfer Family 服务器 ID
- *region-id*替换为 Transfer Family 服务器所在的实际区域

确认 SFTP 中的后量子混合密钥交换

要确认 SFTP 至 Transfer Family 的 SSH 连接期间是否使用了后量子混合密钥交换，请查看客户端输出。或者您可以使用数据包捕获程序。如果您使用 OpenSSH 9.9 客户端，则输出应类似于以下内容（为了简洁起见，省略了不相关的信息）：

```
% sftp -o KexAlgorithms=mlkem768x25519-sha256 -v -o IdentitiesOnly=yes -
i username_private_key_PEM_file username@s-1111aaaa2222bbbb3.server.transfer.us-
west-2.amazonaws.com
OpenSSH_9.9p2, OpenSSL 3.4.1 11 Feb 2025
debug1: Reading configuration data /Users/username/.ssh/config
debug1: /Users/username/.ssh/config line 146: Applying options for *
debug1: Reading configuration data /Users/username/.ssh/bastions-config
debug1: Reading configuration data /opt/homebrew/etc/ssh/ssh_config
debug1: Connecting to s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com
 [xxx.yyy.zzz.nnn] port 22.
debug1: Connection established.
[...]
debug1: Local version string SSH-2.0-OpenSSH_9.9
debug1: Remote protocol version 2.0, remote software version AWS_SFTP_1.1
debug1: compat_banner: no match: AWS_SFTP_1.1
debug1: Authenticating to s-1111aaaa2222bbbb3.server.transfer.us-
west-2.amazonaws.com:22 as 'username'
debug1: load_hostkeys: fopen /Users/username/.ssh/known_hosts2: No such file or
 directory
[...]
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: kex: algorithm: mlkem768x25519-sha256
```

```
debug1: kex: host key algorithm: ssh-ed25519
debug1: kex: server->client cipher: aes128-ctr MAC: hmac-sha2-256-etm@openssh.com
 compression: none
debug1: kex: client->server cipher: aes128-ctr MAC: hmac-sha2-256-etm@openssh.com
 compression: none
debug1: expecting SSH2_MSG_KEX_ECDH_REPLY
debug1: SSH2_MSG_KEX_ECDH_REPLY received
debug1: Server host key: ssh-ed25519 SHA256:Ic1Ti0cdDmFdStj06rfU0cmmNccwAha/ASH2unr6zX0
[...]
debug1: rekey out after 4294967296 blocks
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug1: SSH2_MSG_NEWKEYS received
debug1: rekey in after 4294967296 blocks
[...]
Authenticated to s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com
 ([xxx.yyy.zzz.nnn]:22) using "publickey".
debug1: channel 0: new session [client-session] (inactive timeout: 0)
[...]
Connected to s-1111aaaa2222bbbb3.server.transfer.us-west-2.amazonaws.com.
sftp>
```

输出显示使用后量子混合 `mlkem768x25519-sha256` 方法执行的、以及成功创建 SFTP 会话的客户端协商。

数据保护和加密

Amazon 分适用于 Amazon Transfer Family（Transfer Family）中的数据保护。如本模型所述 Amazon ，负责保护运行所有 Amazon 云的全球基础架构。您负责维护对托管在此基础结构上的内容的控制。此内容包括您使用的 Amazon 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。有关欧洲数据保护的信息，请参阅 Amazon 安全性博客中的 Amazon 责任共担模式和 GDPR 博客文章。

出于数据保护目的，我们建议您保护 Amazon 账户凭据并使用设置个人用户帐户 Amazon IAM Identity Center。这仅向每个用户授予履行其工作职责所需的权限。我们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）。
- 用于 SSL/TLS 与 Amazon 资源通信。支持 TLS 1.2。
- 使用设置 API 和用户活动日志 Amazon CloudTrail。
- 使用 Amazon 加密解决方案以及 Amazon 服务中的所有默认安全控制。

- 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 中的个人数据。
- 如果在通过命令行界面或 API 访问 Amazon 时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅美国联邦信息处理标准 (FIPS) 第 140-2 版。

我们强烈建议您切勿将敏感的可识别信息（例如您客户的账号）放入自由格式字段（例如名称字段）。这包括您使用控制台、API 或使用 Tr Amazon ansfer Family Amazon CLI或其他服务时 Amazon SDKs。您输入至 Transfer Family 服务配置或其他服务配置中的数据可选择并纳入诊断日志。当您向外部服务器提供网址时，请勿在网址中包含凭证信息来验证您对该服务器的请求。

相比之下，来自 Transfer Family 服务器的上传和下载数据被视为完全私密，永远不会存在于SFTP 或 FTPS 连接等加密通道之外 。仅经过授权的人员才能访问这些数据。

Transfer Family 中的数据加密

Amazon Transfer Family 使用您为 Amazon S3 存储桶设置的默认加密选项来加密您的数据。如果对存储桶启用加密，则存储到该存储桶中的所有对象都会进行加密。这些对象使用服务器端加密，使用 Amazon S3 托管密钥 (SSE-S3) 或 () 托管密钥 Amazon Key Management Service (SSE-KMS Amazon KMS) 进行加密。有关服务器端加密的更多信息，请参阅 Amazon Simple Storage Service 用户指南中的使用服务器端加密保护数据。

以下步骤向您展示如何加密中的数据 Amazon Transfer Family。

允许加密 Amazon Transfer Family

1. 为 Amazon S3 存储桶启用默认加密。有关更多详细信息，请参阅 Amazon Simple Storage Service 用户指南中的适用于 S3 存储桶的 Amazon S3 默认加密。
2. 更新附加到用户的 Amazon Identity and Access Management (IAM) 角色策略以授予所需的 Amazon Key Management Service (Amazon KMS) 权限。
3. 如果您为用户使用会话策略，则会话策略必须授予所需的 Amazon KMS 权限。

以下示例显示了一个 IAM 策略，该策略授予与启用 Amazon KMS 加密的 Amazon S3 存储桶 Amazon Transfer Family 一起使用时所需的最低权限。如果您使用用户 IAM 角色策略和会话策略，请将此示例策略包含在其中。

```
{
   "Sid": "Stmt1544140969635",
```

```
    "Action": [
       "kms:Decrypt",
       "kms:Encrypt",
       "kms:GenerateDataKey",
       "kms:GetPublicKey",
       "kms:ListKeyPolicies"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:kms:region:account-id:key/kms-key-id"
}
```

> **Note**
>
> 您在此策略中指定的 KMS 密钥 ID 必须与步骤 1 中为默认加密指定的密钥 ID 相同。Amazon KMS 密钥策略中必须允许根角色或用户使用的 IAM 角色。有关 Amazon KMS 密钥策略的信息，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。

Amazon Transfer Family 静态加密

由于 Amazon Transfer Family 是一项文件传输服务，因此它不管理您的静态存储数据。 Amazon Transfer Family 支持的存储服务和系统负责保护处于该状态的数据。但是，有些与服务相关的数据是静态 Amazon Transfer Family 管理的。

什么是加密？

唯一 Amazon Transfer Family 可以处理的静态数据与操作文件传输服务器和处理传输所需的详细信息有关。 Amazon Transfer Family 在 Amazon DynamoDB 中使用完全静态加密存储以下数据：

- 服务器配置（例如，服务器设置、协议配置和端点详细信息）。
- 用户身份验证数据，包括 SSH 公钥和用户元数据。
- 工作流程执行详细信息和步骤配置。
- 第三方系统的连接器配置和身份验证凭证。这些凭证使用 Amazon Transfer Family 托管加密密钥进行加密。

密钥管理

您无法管理用于在 DynamoDB 中存储与运行服务器和处理传输相关的信息的加密密钥。 Amazon Transfer Family 这些信息包括您的服务器配置、用户身份验证数据、工作流程详细信息和连接器凭据。

哪些内容未加密？

尽管 Amazon Transfer Family 不能控制存储数据的静态加密方式，但我们仍然建议您配置存储位置所支持的最高安全级别。例如，您可以使用 Amazon S3 托管加密密钥 (SSE-S3) 或密 Amazon KMS 钥 (SSE-KMS) 加密对象。

详细了解 Amazon 存储服务如何加密静态数据：

- Amazon S3
- Amazon EFS

在 Transfer Family 中管理 SSH 和 PGP 密钥

在本节中，您可以找到有关 SSH 密钥的信息，包括如何生成密钥以及如何轮换的信息。有关使用 Transfer Family Amazon Lambda 来管理密钥的详细信息，请参阅博客文章 “使用Amazon Transfer Family 和启用用户自助服务密钥管理” Amazon Lambda。有关自动部署和管理拥有多个 SSH 密钥的用户，请参阅Transfer Family terraform 模块。

> **Note**
>
> Amazon Transfer Family 接受用于 SSH 身份验证的 RSA、ECDSA 和 ED25519 密钥。

本节还介绍如何生成与管理 Pretty Good Privacy (PGP) 密钥。

有关所有支持的加密和密钥算法的全面概述，包括针对不同用例的建议，请参阅加密和密钥算法概述。

加密和密钥算法概述

Amazon Transfer Family 支持用于不同目的的不同类型的算法。了解针对您的特定用例使用哪些算法有助于确保文件传输的安全性和兼容性。

算法快速参考

使用场景	推荐算法	符合 FIPS	注意
SSH/SFTP 身份验证	RSA (rsa-sha2-256/512)、ECDSA 或 ED25519	RSA：是的，ECDSA：是，：否 ED25519	与所有 SSH 客户端和服务器兼容
PGP 密钥生成	RSA 或 ECC (NIST)	是	用于工作流程解密
PGP 文件加密	AES-256	是	由 PGP 软件决定

SSH 身份验证算法

这些算法用于在客户端和 Amazon Transfer Family 服务器之间进行 SSH/SFTP 身份验证。在为用户身份验证或服务器主机密钥生成 SSH 密钥对时，请选择其中一个。

RSA（推荐）

与所有 SSH 客户端和服务器兼容，并且符合 FIPS。与 SHA-2 哈希一起使用可增强安全性：

- `rsa-sha2-256`-推荐用于大多数用例
- `rsa-sha2-512`-更高的安全性选项

ED25519

现代而高效。密钥大小更小，安全性强：

- `ssh-ed25519`-快速安全，但不符合 FIPS

ECDSA

椭圆曲线选项。安全性和性能的良好平衡：

- `ecdsa-sha2-nistp256`-标准曲线
- `ecdsa-sha2-nistp384`-更高的安全性曲线
- `ecdsa-sha2-nistp521`-最高安全性曲线

> **Note**
>
> 我们 SHA1 支持`ssh-rsa`较旧的安全策略。有关更多信息，请参阅 加密算法。

选择正确的 SSH 算法

- 对于大多数用户：将 RSA 与或一起`rsa-sha2-256`使用 `rsa-sha2-512`
- 为了符合 FIPS 标准：使用 RSA 或 ECDSA 算法
- 适用于现代环境： ED25519 提供卓越的安全性和性能

PGP 加密和解密算法

PGP（Pretty Good Privacy）使用两种类型的算法协同工作来加密和解密工作流程中的文件：

1. 密钥对算法-用于生成用于加密和数字签名的密 public/private 钥对
2. 对称算法-用于加密实际文件数据（key pair 算法加密对称密钥）

PGP key pair 算法

生成用于工作流解密的 PGP 密钥对时，请选择以下算法之一：

RSA（推荐）

建议大多数用户使用。得到广泛支持、成熟且符合 FIPS 标准。在安全性和兼容性之间取得了良好的平衡。

ECC（椭圆曲线密码学）

比 RSA 更高效，密钥大小更小，同时还能保持强大的安全性：

- NIST 曲线-广泛支持标准曲线，符合 FIPS 标准
- BrainPool 曲线-针对特定合规要求的替代曲线
- Curve25519-现代高性能曲线，提供强大的安全性和高效的计算

ElGamal

传统算法。支持与旧系统兼容。使用 RSA 或 ECC 进行新的实现。

有关生成 PGP 密钥的详细说明，请参阅生成 PGP 密钥。

PGP 对称加密算法

这些算法会加密您的实际文件数据。使用的算法取决于 PGP 软件创建 PGP 文件的方式：

符合 FIPS 的算法（建议在受监管的环境中使用）

- AES-128、AES-192、AES-256-高级加密标准（推荐）
- 3DES-三重数据加密标准（旧版，尽可能使用 AES）

其他支持的算法

- IDEA、 CAST5、Blowfish、DES TwoFish、、CAMELLIA-128、CAMELLIA-192、CAMELLIA-256

> **Note**
>
> 使用 Amazon Transfer Family 工作流程时，您不会直接选择对称算法，而是由用于创建加密文件的 PGP 软件决定的。但是，您可以将 PGP 软件配置为首选符合 FIPS 的算法，例如 AES-256。

有关支持的对称算法的更多信息，请参见支持的对称加密算法。

为服务托管用户生成 SSH 密钥

您可以设置服务器以使用服务管理的身份验证方法对用户进行身份验证，其中用户名和 SSH 密钥存储在服务中。用户的公有 SSH 密钥作为用户属性上传到服务器。服务器将此密钥用作密钥标准身份验证过程的一部分。每个用户均可使用单个服务器存档多个公有 SSH 密钥。有关每个用户可以存储的密钥数量限制，请参阅中的 Amazon Web Services 一般参考 中的 Amazon Transfer Family 端点和配额。

作为服务托管身份验证方法的替代方法，您可以使用自定义身份提供商对用户进行身份验证，或者 Amazon Directory Service for Microsoft Active Directory。有关更多信息，请参阅 使用自定义身份提供程序或 使用微软 Active Directory 的 Amazon 目录服务。

服务器只能使用一种方法（服务托管、目录服务或自定义身份提供程序）对用户进行身份验证，并且该方法在创建服务器后无法更改。

主题

- 在 macOS、Linux 或 Unix 系统创建 SSH 密钥

- 在 Microsoft Windows 上创建 SSH 密钥
- 将 SSH2 密钥转换为 SSH 公钥格式

在 macOS、Linux 或 Unix 系统创建 SSH 密钥

在 macOS、Linux 或 Unix 操作系统中，您可以使用 ssh-keygen 命令创建 SSH 公钥和 SSH 私钥（也称为密钥对）。

> **Note**
>
> 在以下示例中，我们未指定密码：在这种情况下，该工具会要求您输入密码，然后重复密码进行验证。创建密码可以更好地保护您的私钥，还可以提高系统整体安全性。您无法恢复密码：如果您忘记了密码，则必须创建新的密钥。
> 但是，如果要生成服务器主机密钥，则必须通过在命令中指定 -N "" 选项（或者在出现提示时按 **Enter** 两次）指定空密码，原因是 Transfer Family 服务器无法在启动时请求密码。

若要在 macOS、Linux 或 Unix 操作系统上创建 SSH 密钥

1. 在 macOS、Linux 或 Unix 操作系统，打开命令终端。
2. Amazon Transfer Family 接受 RSA-、ECDSA-和 ED25519-格式的密钥。根据您生成的密钥对类型选择相应的命令。

   提示：*key_name*替换为 SSH 密钥对文件的实际名称。

   - 生成 RSA 4096 位密钥对：

     ```
     ssh-keygen -t rsa -b 4096 -f key_name
     ```

   - 若要生成 ECDSA 521 位密钥对（ECDSA 大小为 256、384 和 521），请执行以下操作：

     ```
     ssh-keygen -t ecdsa -b 521 -f key_name
     ```

   - 要生成 ED25519 密钥对，请执行以下操作：

     ```
     ssh-keygen -t ed25519 -f key_name
     ```

   下面是 ssh-keygen 输出的示例。

```
ssh-keygen -t rsa -b 4096 -f key_name
Generating public/private rsa key pair.

Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in key_name.
Your public key has been saved in key_name.pub.
The key fingerprint is:
SHA256:8tDDwPmanTFcEzjTwPGETVWOGW1nVz+gtCCE8hL7PrQ bob.amazon.com
The key's randomart image is:
+---[RSA 4096]----+
|    . ....E      |
| .   = ...       |
|. . . = ..o      |
| . o +  oo =     |
|  + =  .S.= *    |
| . o o ..B + o   |
|     .o.+.* .    |
|     =o*+*.      |
|    ..*o*+.      |
+----[SHA256]-----+
```

提示：如上所示运行ssh-keygen命令时，它会将公钥和私钥创建为当前目录中的文件。

您的 SSH 密钥对现已准备就绪，可以使用。按照步骤 3 和 4 为服务托管用户存储 SSH 公钥。这些用户在 Transfer Family 服务器端点上传输文件时使用这些密钥。

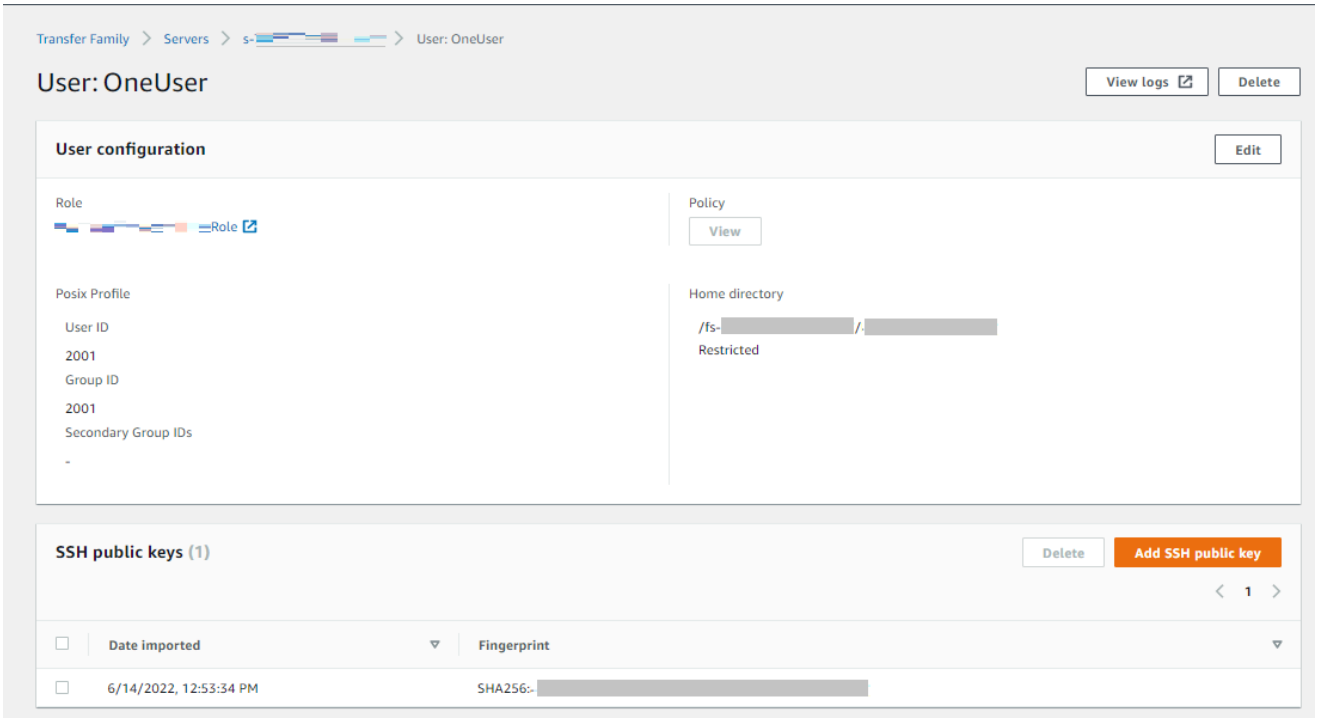
3. 导航到 *key_name*.pub 文件并打开它。
4. 复制文本并将其粘贴至服务托管用户的 SSH 公钥中。

   a. 打开 Amazon Transfer Family 控制台 https://console.aws.amazon.com/transfer/，然后从导航窗格中选择 “服务器”。

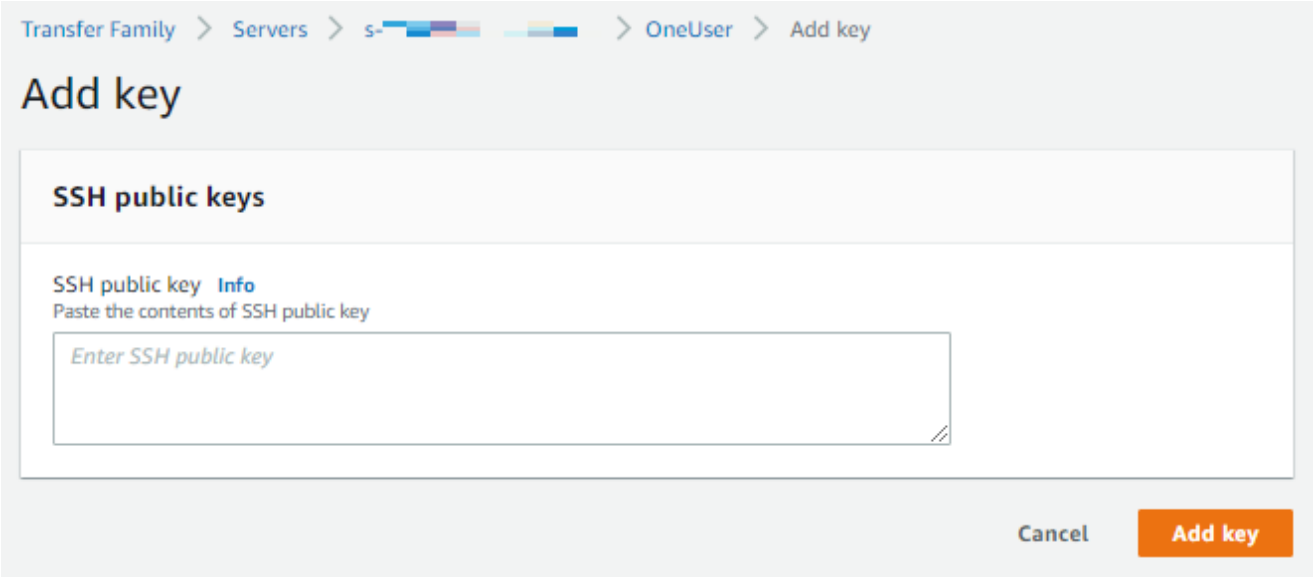
   b. 在服务器页面，选择包含要更新用户服务器的服务器 ID。

   c. 选择要为其添加公钥的目标用户。

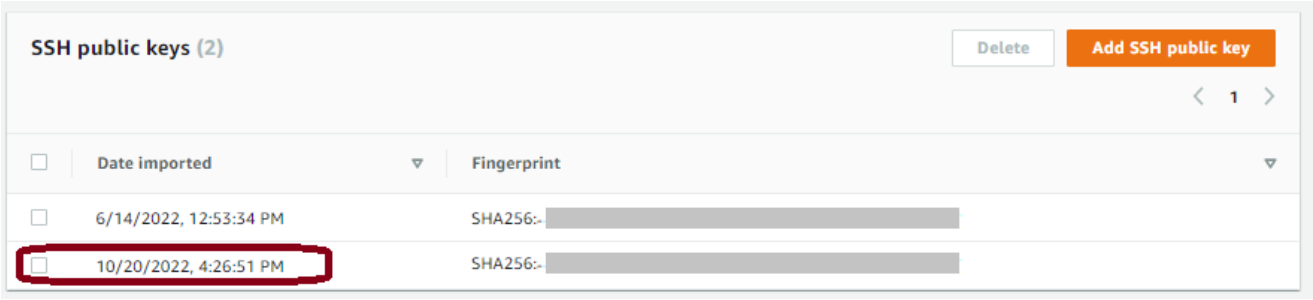
   d. 在 SSH 公钥窗格，选择添加 SSH 公钥。



e. 将您生成的公钥文本粘贴至 SSH 公钥文本框中，然后选择添加密钥。



新密钥列于 SSH 公钥窗格。



在 Microsoft Windows 上创建 SSH 密钥

Windows 将 OpenSSH 作为一项内置功能包括在内，你可以用它来生成与 Linux 或 macOS 相同格式的 SSH 密钥。或者，你可以使用第三方工具，比如 PuTTY 的密钥生成器 (PuTTYgen)。

使用 Windows 内置的 OpenSSH

Windows 的最新版本默认包含 OpenSSH。你可以使用与 macOS/Linux 一节中所述相同的`ssh-keygen`命令：

1. 打开 Windows PowerShell 或命令提示符。
2. 根据要生成的密钥类型运行以下命令之一：
   - 生成 RSA 4096 位密钥对：

     ```
     ssh-keygen -t rsa -b 4096 -f key_name
     ```
   - 要生成 ECDSA 521 位密钥对，请执行以下操作：

     ```
     ssh-keygen -t ecdsa -b 521 -f key_name
     ```
   - 要生成 ED25519 密钥对，请执行以下操作：

     ```
     ssh-keygen -t ed25519 -f key_name
     ```
3. 按照与该 macOS/Linux 部分相同的步骤将您的公钥上传到 Amazon Transfer Family。

使用 PuTTYgen （第三方工具）

某些适用于 Windows 的第三方 SSH 客户端（例如 PuTTY）使用不同的密钥格式。Putty 使用私PPK钥的格式。如果你使用的是 Putty 或 WinSCP 等相关工具，你可以使用 Pu TTYgen 来创建这种格式的密钥。

> **Note**
>
> 如果您向 WinSCP 提供的私有密钥文件不是 .ppk 格式，该客户端会为您将密钥转换为 .ppk 格式。

有关使用 Pu 创建 SSH 密钥的教程TTYgen，请访问 SSH.com 网站。

将 SSH2 密钥转换为 SSH 公钥格式

Amazon Transfer Family 仅接受 SSH 格式的公钥。如果您有 SSH2 公钥，则需要对其进行转换。SSH2 公钥的格式如下：

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20160402"
AAAAB3NzaC1yc2EAAAABJQAAAgEAiL0jjDdFqK/kYThqKt7THrjABTPWvXmB3URI
:
:
---- END SSH2 PUBLIC KEY ----
```

SSH 公钥的格式如下：

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAA...
```

运行以下命令将格式的公钥转换为 SSH SSH2 格式的公钥。*ssh2-key*替换为 SSH2 密钥的*ssh-key*名称和 SSH 密钥的名称。

```
ssh-keygen -i -f ssh2-key.pub > ssh-key.pub
```

轮换 SSH 密钥

出于安全原因，我们推荐轮换 SSH 密钥的最佳安全实践。通常，此轮换被指定为安全策略的一部分，并以某种自动化的方式实现。根据安全级别，对于高度敏感的通信，SSH 密钥对可能只使用一次。这样做可以消除因存储密钥而导致的任何风险。但是，更常见的做法是将 SSH 凭证存储一段时间，并设置一个不会给用户带来过多负担的间隔。通常，时间间隔为 3 个月。

> **Note**
>
> 有关使用基础设施即代码的自动 SSH 密钥轮换，请参阅Transfer Family terraform 模块。

有两种方法用于执行 SSH 密钥轮换：

- 在控制台上，您可以上传新的 SSH 公钥和删除现有 SSH 公钥。
- 使用 API，您可以使用 AP DeleteSshPublicKeyI 删除用户的安全外壳 (SSH) 公钥，使用 ImportSshPublicKeyAPI 向用户账户添加新的安全外壳 (SSH) 公钥，从而更新现有用户。

Console

若要控制台中执行密钥轮换

1. 打开 Amazon Transfer Family 控制台，网址为https://console.aws.amazon.com/transfer/。
2. 导航至服务器页面。
3. 选择服务器 ID 列中的标识符以查看服务器详细信息页面。
4. 在用户下，选中要轮换其 SSH 公钥用户的复选框，然后选择操作，然后选择添加密钥以查看添加密钥页面。

   或者

   选择用户名以查看用户详细信息页面，然后选择添加 SSH 公钥 以查看添加密钥页面。
5. 输入新的 SSH 公钥并选择添加密钥。

   > **Important**
   > SSH 公有密钥格式取决于您生成的密钥的类型。
   >
   > - RSA 密钥的格式为 `ssh-rsa` *`string`*。
   > - 对于 ED25519 密钥，格式为`ssh-ed25519` *`string`*。
   > - 对于 ECDSA 密钥，`ecdsa-sha2-nistp256` 字符串为 `ecdsa-sha2-nistp384` 或 `ecdsa-sha2-nistp521`，具体取决于您生成的密钥的大小。然后，先是 *`string`*，后跟开头字符串，这与其他秘钥类型类似。

   您将返回用户配置屏幕，您刚刚输入的新 SSH 公钥将出现在 SSH 公钥部分。
6. 选中要删除的旧密钥旁边的复选框，然后选择删除。
7. 输入单词 `delete` 以确认删除操作，然后选择删除。

API

若要使用 API 执行密钥轮换

1. 在 macOS、Linux 或 Unix 操作系统，打开命令终端。
2. 输入以下命令，以检索要删除的 SSH 密钥。若要使用此命令，请将 *serverID* 替换为您的 Transfer Family 服务器的服务器 ID，然后将 *username* 替换为您的用户名。

```
aws transfer describe-user --server-id='serverID' --user-name='username'
```

该命令返回有关此用户的详细信息。复制 "SshPublicKeyId": 字段的内容。您将需要稍后在此程序中输入此值。

```
"SshPublicKeys": [ { "SshPublicKeyBody": "public-key", "SshPublicKeyId":
 "keyID",
   "DateImported": 1621969331.072 } ],
```

3. 接下来，为您的用户导入新 SSH 密钥。在 提示符中，输入以下命令。若要使用此命令，请将 *serverID* 替换为您的 Transfer Family 服务器的服务器 ID，将 *public-key* 替换为您的用户名，并将 *username* 替换为新公钥的指纹。

```
aws transfer import-ssh-public-key --server-id='serverID' --user-name='username'
   --ssh-public-key-body='public-key'
```

如果命令成功，则不返回任何输出。

4. 最后通过运行以下命令删除旧密钥。若要使用此命令，将 *serverID* 替换为 Transfer Family 服务器的服务器 ID，将 *username* 替换为您的用户名，将 *keyID-from-step-2* 替换为您在此程序第 2 步中复制的秘钥 ID 值。

```
aws transfer delete-ssh-public-key --server-id='serverID' --user-name='username'
   --ssh-public-key-id='keyID-from-step-2'
```

5. （可选）要确认旧密钥是否存在，请重复第 2 步。

生成 PGP 密钥

您可以对 Transfer Family 通过工作流程处理的文件使用 Pretty Good Privacy (PGP) 解密。要在工作流程步骤中使用解密，请提供 PGP 密钥。有关 PGP 密钥算法的详细信息，包括建议和 FIPS 合规性，请参阅。PGP key pair 算法

Amazon 存储博客上有一篇文章描述了如何使用 Transfer Family Managed 工作流程、使用 PGP 加密和解密文件以及，无需编写任何代码即可简单地解密文件。 Amazon Transfer Family

用于生成 PGP 密钥的运算符取决于您的操作系统和所使用的密钥生成软件的版本。

如果您使用的是 Linux 或 Unix，请使用软件包安装程序安装 gpg。根据您的 Linux 发行版，在以下选择适用于您的命令。

```
sudo yum install gnupg
```

```
sudo apt-get install gnupg
```

对于 Windows 或 macOS，您可以从 https://gnupg.org/download/ 下载您需要的内容。

安装 PGP 密钥生成器软件后，运行 `gpg --full-gen-key` 或 `gpg --gen-key` 命令生成密钥对。

> **Note**
>
> 如果您使用的版本是 GnuPG 2.3.0 或以上，则必须运行 `gpg --full-gen-key`。当提示输入要创建的密钥类型时，请选择 RSA 或 ECC。如果选择 ECC，则可以选择BrainPool和Curve25519作为椭圆曲线。NIST

有用的 **gpg** 子命令

以下是一些有用的gpg子命令：

- `gpg --help` — 此命令列出了可用选项，可能还包括一些示例。
- `gpg --list-keys`— 此命令列出了您创建的所有密钥对的详细信息。
- `gpg --fingerprint`— 此命令列出了所有密钥对的详细信息，包括每个密钥的指纹。
- `gpg --export -a` *`user-name`* — 此命令导出生成密钥时 *`user-name`* 使用密钥的公钥部分。

管理 PGP 密钥

要管理您的 PGP 密钥，请使用 Amazon Secrets Manager。

> **Note**
>
> 您的秘钥名称包括 Transfer Family 服务器 ID。这意味着您应在 Amazon Secrets Manager中存储 PGP 秘钥信息之前识别或创建服务器。

如果您想为所有用户使用同一个密钥和密码，则可以将 PGP 密钥区块信息存储在机密名称 `aws/transfer/server-id/@pgp-default` 下，其中 *`server-id`* 是 Transfer Family 服务器的 ID。如果没有与正在执行工作流程的用户*`user-name`*匹配的密钥，Transfer Family 将使用此默认密钥。

您可以为特定用户创建密钥。在本例中，密钥名称的格式为`aws/transfer/`*`server-id`*`/`*`user-name`*，其中*`user-name`*匹配正在为 Transfer Family 服务器运行工作流程的用户。

> **Note**
>
> 在每台 Transfer Family 服务器上，每位用户最多可存储 3 个 PGP 私钥。

配置用户解密的 PGP 密钥

1. 根据您使用的 GPG 版本，运行以下命令之一来生成 PGP key pair。

   - 如果您使用的是 **GnuPG** 版本为 2.3.0 或以上，请运行以下命令：

     ```
     gpg --full-gen-key
     ```

     您可以选择**RSA**，或者，如果选择**ECC**，则可以选择椭圆曲线**BrainPool**或**Curve25519**。**NIST**如果`gpg --gen-key`改为运行，则创建使用 ECC Curve 25519 加密算法的密钥对。

   - 对于 2.3.0 之前版本的 **GnuPG**，您可以使用以下命令，原因是 RSA 是默认的加密类型。

     ```
     gpg --gen-key
     ```

> **Important**
>
> 密钥生成过程中，您必须提供密码和电子邮箱地址。请务必记下这些值。在本过程的 Amazon Secrets Manager 后面输入密钥详细信息时，必须提供密码。您必须提供相同的电子邮件地址才能在下一步中导出私钥。

2. 运行以下命令以导出私钥。要使用此命令，请将 *private.pgp* 替换为用于保存私钥块的文件名，并将 *marymajor@example.com* 替换为生成密钥对时使用的电子邮件地址。

```
gpg --output private.pgp --armor --export-secret-key marymajor@example.com
```

3. 用于存储 Amazon Secrets Manager 您的 PGP 密钥。

   a. 登录 Amazon Web Services 管理控制台 并打开 Amazon Secrets Manager 控制台，网址为https://console.aws.amazon.com/secretsmanager/。

   b. 在左侧导航窗格中，选择密钥。

   c. 在密钥页面，选择存储新密钥。

   d. 在选择密钥类型页面上，为密钥类型选择其他密钥类型。

   e. 在秘钥/值对部分，选择秘钥/值选项卡。

   - 密钥 - 输入 **PGPPrivateKey**。

     > **Note**
     >
     > 必须准确输入 **PGPPrivateKey** 字符串：切勿在字符前面或字符之间添加任何空格。

   - 值 — 将您的私钥文本粘贴至值字段。您可以在文件中找到私钥文本（例如 `private.pgp`），该文件是在您之前导出密钥时指定的文件。密钥开头为 `-----BEGIN PGP PRIVATE KEY BLOCK-----`，结尾为 `-----END PGP PRIVATE KEY BLOCK-----`。

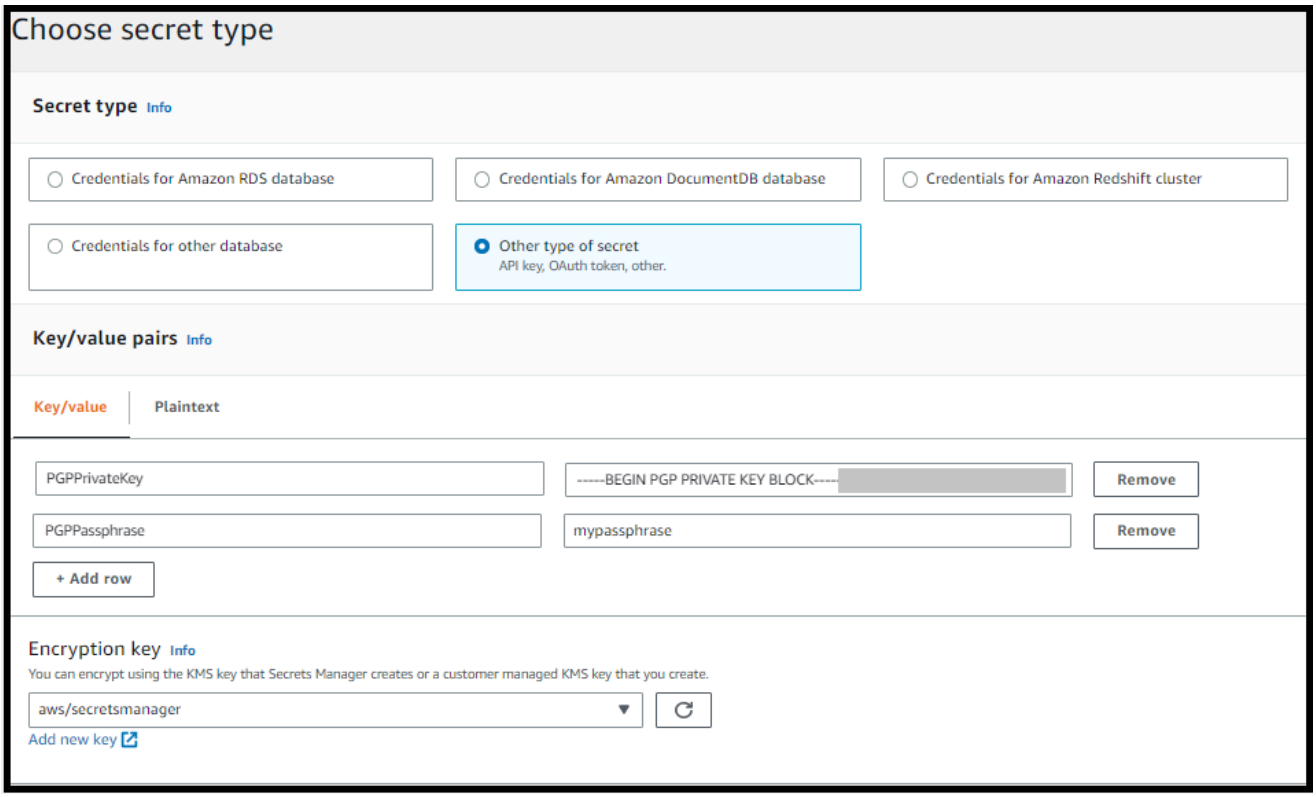
     > **Note**
     >
     > 确保文本块仅包含私钥，且不包含公钥。

   f. 选择添加行，然后在秘钥/值对部分选择秘钥/值选项卡。

- 键 — 输入 **PGPPassphrase**。

> **Note**
>
> 必须准确输入 **PGPPassphrase** 字符串：切勿在字符前面或字符之间添加任何空格。

- 值 – 输入您在生成 PGP 密钥对时使用的密码。



> **Note**
>
> 您最多可添加 3 组密钥和密码。若要添加第二组，请添加两行新行，为秘钥输入 **PGPPrivateKey2** 和 **PGPPassphrase2**，并粘贴至其他私钥和密码。若要添加第三组，秘钥值必须为 **PGPPrivateKey3** 和 **PGPPassphrase3**。

g. 选择下一步。

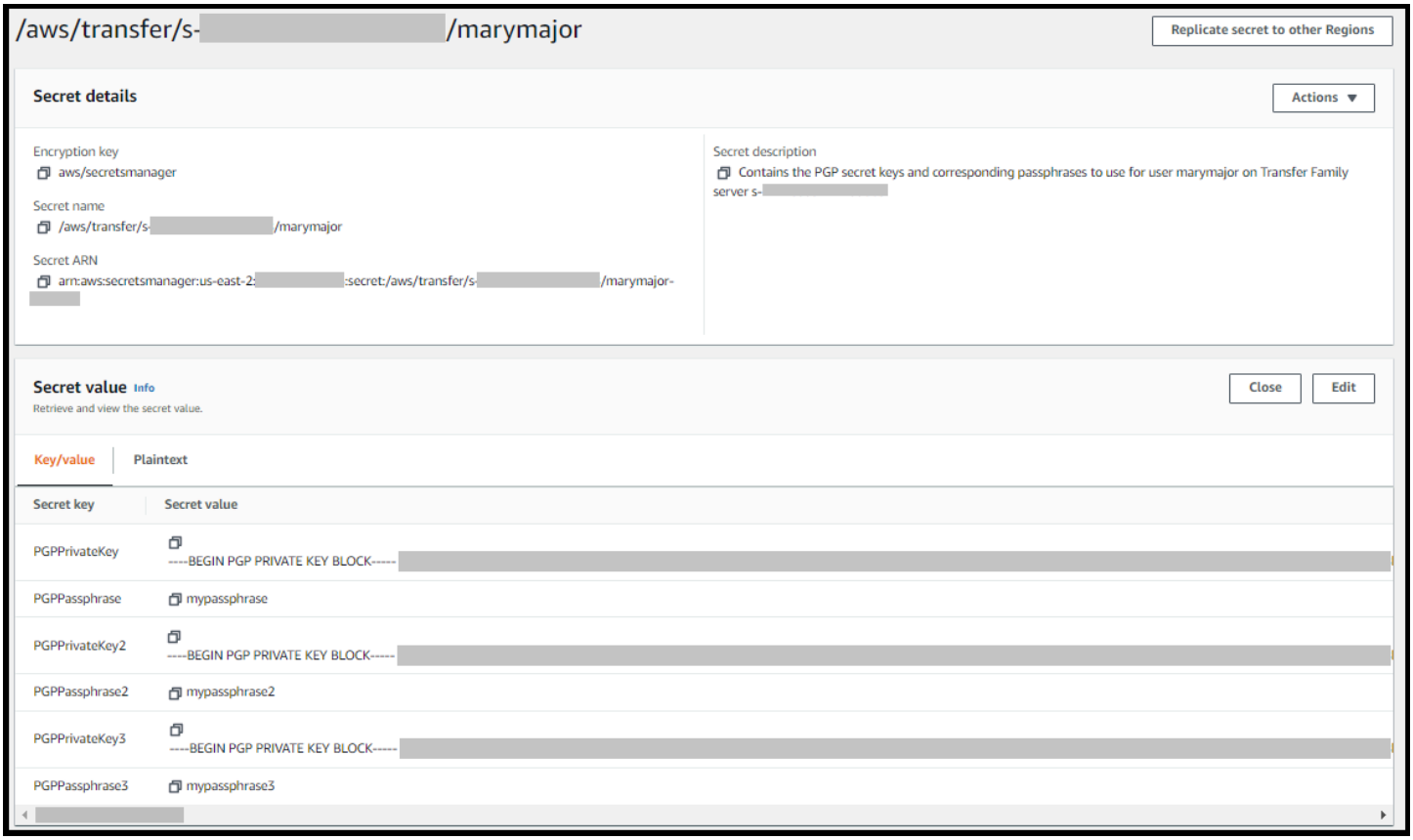
h. 在配置密钥页面，输入密钥的名称和描述。

- 如果您要创建默认密钥，即可供任何 Transfer Family 用户使用的密钥，请输入 **aws/transfer/*server-id*/@pgp-default**。将 *server-id* 替换为包含解密工作流程服务器的 ID。
- 如果您正在创建供特定 Transfer Family 用户使用的密钥，请输入 **aws/transfer/*server-id*/*user-name***。将 *server-id* 替换为包含解密工作流程服务器的 ID，将 *user-name* 更换为运行工作流程的用户名称。*user-name* 存储在 Transfer Family 服务器正在使用的身份提供程序。

i. 选择下一步，接受配置轮换页面的默认设置。然后选择下一步。

j. 在审核页面，选择存储以创建和存储密钥。

以下屏幕截图显示了指定 Transfer Family 服务器用户 **marymajor** 的详细信息。此示例显示三个密钥及其对应的密码。

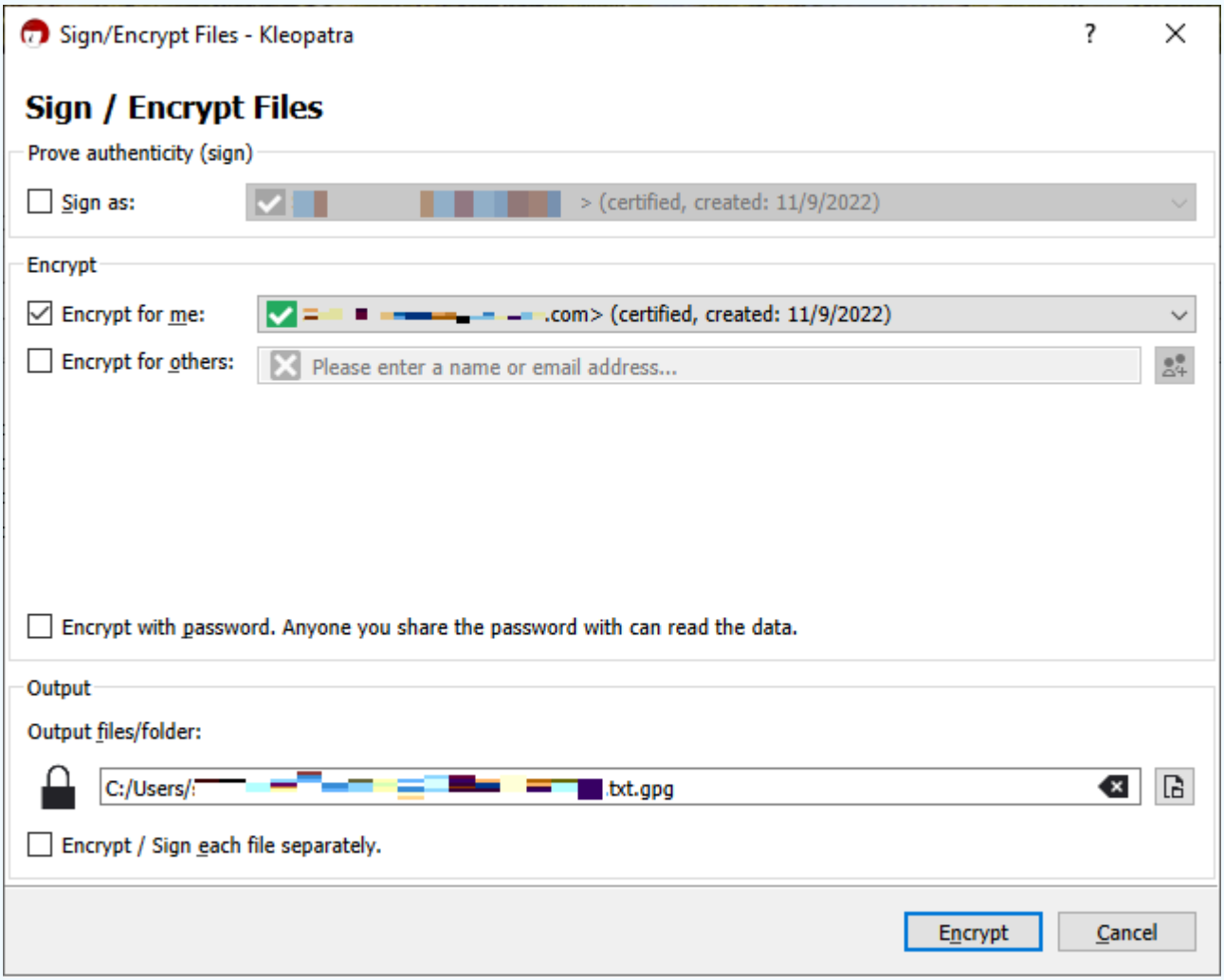


支持的 PGP 客户端

以下客户端已通过 Transfer Family 进行测试，可用于生成 PGP 密钥，以及加密您打算通过工作流程解密的文件。

- Gpg4win + Kleopatra。

> **Note**
>
> 当您选择签名/加密文件时，请务必取消选择签名身份：我们目前不支持对加密文件进行签名。



如果您对加密文件进行签名并尝试使用解密工作流程将其上传到 Transfer Family 服务器，则会收到以下错误：

```
Encrypted file with signed message unsupported
```

- GnuPG 主要版本：2.4、2.3、2.2、2.0 和 1.4。

请注意，其他 PGP 客户端也可运行，但只有此处提到的客户端通过 Transfer Family 进行了测试。

的身份和访问管理 Amazon Transfer Family

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 管理员控制谁可以进行身份验证（登录）和授权（有权限）使用 Amazon Transfer Family 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
- 如何 Amazon Transfer Family 与 IAM 配合使用
- Amazon Transfer Family 基于身份的策略示例
- Amazon Transfer Family 基于标签的策略示例
- 对 Amazon Transfer Family 身份和访问进行故障排除
- 用于组织治理的 IAM 条件密钥

受众

您的使用方式 Amazon Identity and Access Management (IAM) 因您的角色而异：

- 服务用户：如果您无法访问功能，请从管理员处请求权限（请参阅对 Amazon Transfer Family 身份和访问进行故障排除）
- 服务管理员：确定用户访问权限并提交权限请求（请参阅如何 Amazon Transfer Family 与 IAM 配合使用）
- IAM 管理员：编写用于管理访问权限的策略（请参阅Amazon Transfer Family 基于身份的策略示例）

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 用户身份进行身份验证 Amazon Web Services 账户根用户，或者通过担任 IAM 角色进行身份验证。

对于编程访问， Amazon 提供 SDK 和 CLI 来对请求进行加密签名。有关更多信息，请参阅《IAM 用户指南》中的适用于 API 请求的Amazon 签名版本 4。

Amazon Web Services 账户根用户

创建时 Amazon Web Services 账户，首先会有一个名为 Amazon Web Services 账户 root 用户的登录身份，该身份可以完全访问所有资源 Amazon Web Services 服务 和资源。我们强烈建议不要使用根用户进行日常任务。有关需要根用户凭证的任务，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，要求人类用户使用与身份提供商的联合身份验证才能 Amazon Web Services 服务 使用临时证书进行访问。

联合身份是指来自您的企业目录、Web 身份提供商的用户 Amazon Directory Service ，或者 Amazon Web Services 服务 使用来自身份源的凭据进行访问的用户。联合身份代入可提供临时凭证的角色。

IAM 用户和群组

IAM 用户是对某个人员或应用程序具有特定权限的一个身份。建议使用临时凭证，而非具有长期凭证的 IAM 用户。有关更多信息，请参阅 IAM 用户指南中的要求人类用户使用身份提供商的联合身份验证才能 Amazon 使用临时证书进行访问。

IAM 组指定一组 IAM 用户，便于更轻松地对大量用户进行权限管理。有关更多信息，请参阅《IAM 用户指南》中的 IAM 用户使用案例。

IAM 角色

IAM 角色是具有特定权限的身份，可提供临时凭证。您可以通过从用户切换到 IAM 角色（控制台）或调用 Amazon CLI 或 Amazon API 操作来代入角色。有关更多信息，请参阅《IAM 用户指南》中的担任角色的方法。

IAM 角色对于联合用户访问、临时 IAM 用户权限、跨账户访问、跨服务访问以及在 Amazon 上运行的应用程序非常有用。 EC2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。

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。策略定义了与身份或资源关联时的权限。 Amazon 在委托人提出请求时评估这些政策。大多数策略都以 JSON 文档的 Amazon 形式存储在中。有关 JSON 策略文档的更多信息，请参阅《IAM 用户指南》中的 JSON 策略概述。

管理员使用策略，通过定义哪个主体可以在什么条件下对哪些资源执行哪些操作来指定谁有权访问什么。

默认情况下，用户和角色没有权限。IAM 管理员创建 IAM 策略并将其添加到角色中，然后用户可以担任这些角色。IAM 策略定义权限，与执行操作所用的方法无关。

基于身份的策略

基于身份的策略是您附加到身份（用户、组或角色）的 JSON 权限策略文档。这些策略控制身份可以执行什么操作、对哪些资源执行以及在什么条件下执行。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。

基于身份的策略可以是内联策略（直接嵌入到单个身份中）或托管策略（附加到多个身份的独立策略）。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。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。您必须在基于资源的策略中指定主体。

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 支持其他策略类型，这些策略类型可以设置更常见的策略类型授予的最大权限：

- 权限边界 – 设置基于身份的策略可以授予 IAM 实体的最大权限。有关更多信息，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)-在中指定组织或组织单位的最大权限 Amazon Organizations。有关更多信息，请参阅《Amazon Organizations 用户指南》中的服务控制策略。

- 资源控制策略 (RCPs)-设置账户中资源的最大可用权限。有关更多信息，请参阅《Amazon Organizations 用户指南》中的资源控制策略 (RCPs)。
- 会话策略 – 在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。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。

如何 Amazon Transfer Family 与 IAM 配合使用

在使用 Amazon Identity and Access Management (IAM) 管理访问权限之前 Amazon Transfer Family，您应该了解哪些可用的 IAM 功能 Amazon Transfer Family。要全面了解如何 Amazon Transfer Family 和其他 Amazon 服务与 IAM 配合使用，请参阅 IAM 用户指南中的与 IAM 配合使用的 Amazon 服务。

主题

- Amazon Transfer Family 基于身份的策略
- Amazon Transfer Family 基于资源的策略
- 基于 Amazon Transfer Family 标签的授权
- Amazon Transfer Family IAM 角色

Amazon Transfer Family 基于身份的策略

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，以及指定在什么条件下允许或拒绝操作。 Amazon Transfer Family 支持特定操作、资源和条件键。要了解您在 JSON 策略中使用的所有元素，请参阅 Amazon Identity and Access Management 用户指南中的 IAM JSON 策略元素参考。

操作

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。在策略中包含操作以授予执行关联操作的权限。

正在执行的策略操作在操作前 Amazon Transfer Family 使用以下前缀:`transfer:`. 例如，要授予某人使用 Transfer Family `CreateServer` API 操作创建 VPC 的权限，您应将 `transfer:CreateServer` 操作纳入其策略中。策略语句必须包括 `Action` 或 `NotAction` 元素。Amazon Transfer Family 定义了自己的一组操作，这些操作描述了可使用该服务执行的任务。

要在单个语句中指定多项 操作，请使用逗号将它们隔开，如下所示。

```
"Action": [
      "transfer:action1",
      "transfer:action2"
```

您也可以使用通配符 (*) 指定多个操作。例如，要指定以单词 `Describe` 开头的所有操作，请包括以下操作。

```
"Action": "transfer:Describe*"
```

要查看 Amazon Transfer Family 操作列表，请参阅《服务授权参考》 Amazon Transfer Family中定义的操作。

资源

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。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于不支持资源级权限的操作，请使用通配符 (*) 指示语句应用于所有资源。

```
"Resource": "*"
```

Transfer Family 服务器资源具有以下 ARN。

```
arn:aws:transfer:${Region}:${Account}:server/${ServerId}
```

例如，要在语句中指定 `s-01234567890abcdef` Transfer Family 服务器，请使用以下 ARN。

```
"Resource": "arn:aws:transfer:us-east-1:123456789012:server/s-01234567890abcdef"
```

有关格式的更多信息 ARNs，请参阅《服务授权参考》中的 A mazon 资源名称 (ARNs) 或 IAM 用户指南 ARNs中的 IAM。

要指定属于特定账户的所有实例，请使用通配符 (*)。

```
"Resource": "arn:aws:transfer:us-east-1:123456789012:server/*"
```

有些 Amazon Transfer Family 操作是在多个资源上执行的，例如 IAM 策略中使用的资源。在这些情况下，您必须使用通配符 (*)。

```
"Resource": "arn:aws:transfer:*:123456789012:server/*"
```

在某些情况下，您需要指定多种类型的资源，例如，如果您创建了允许访问 Transfer Family 服务器与用户的策略。要在单个语句中指定多个资源，请 ARNs 用逗号分隔。

```
"Resource": [
      "resource1",
      "resource2"
            ]
```

要查看 Amazon Transfer Family 资源列表，请参阅《服务授权参考》 Amazon Transfer Family中定义的资源类型。

条件键

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。

Condition 元素根据定义的条件指定语句何时执行。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。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。

Amazon Transfer Family 定义自己的条件键集，还支持使用一些全局条件键。要查看 Amazon Transfer Family 条件键列表，请参阅《服务授权参考》 Amazon Transfer Family中的条件密钥。

示例

要查看 Amazon Transfer Family 基于身份的策略的示例，请参阅。Amazon Transfer Family 基于身份的策略示例有关特定于 VPC 终端节点的 IAM 策略，请参阅。限制 Transfer Family 服务器的 VPC 终端节点访问权限

Amazon Transfer Family 基于资源的策略

基于资源的策略是 JSON 策略文档，用于指定委托人可以在哪些条件下对 Amazon Transfer Family 资源执行哪些操作。Amazon S3 支持亚马逊 S3 *buckets* 的基于资源的权限策略。基于资源的策略允许您基于资源向其他账户授予使用权限。您也可以使用基于资源的策略来允许 Amazon 服务访问您的 Amazon S3 *buckets*。

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委托人。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。当委托人和资源位于不同的 Amazon 账户中时，您还必须向委托人实体授予访问资源的权限。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 Amazon Identity and Access Management 用户指南中的 IAM 角色与基于资源的策略有何不同。

Amazon S3 服务仅支持一种基于资源的策略，即*bucket*策略，该策略附加到。*bucket*这个策略定义哪些委托人实体（账户、用户、角色和联合身份用户）可以在对象上执行操作。

示例

要查看 Amazon Transfer Family 基于资源的策略的示例，请参阅Amazon Transfer Family 基于标签的策略示例。

基于 Amazon Transfer Family 标签的授权

您可以为 Amazon Transfer Family 资源附加标签或在请求中传递标签 Amazon Transfer Family。要基于标签控制访问，您需要使用 `transfer: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。有关如何使用标签控制对 Amazon Transfer Family 资源的访问的信息，请参阅Amazon Transfer Family 基于标签的策略示例。

Amazon Transfer Family IAM 角色

I AM 角色是您的 Amazon 账户中具有特定权限的实体。

将临时证书与 Amazon Transfer Family

可以使用临时凭证进行联合身份验证登录，分派 IAM 角色或分派跨账户角色。您可以通过调用AssumeRole或之类的 Amazon STS API 操作来获取临时安全证书GetFederationToken。

Amazon Transfer Family 支持使用临时证书。

Amazon Transfer Family 基于身份的策略示例

默认情况下，IAM 用户和角色没有创建或修改 Amazon Transfer Family 资源的权限。他们也无法使用 Amazon Web Services 管理控制台 Amazon CLI、或 Amazon API 执行任务。IAM 管理员必须创建 IAM 策略，以便为用户和角色授予权限以对所需的指定资源执行特定的 API 操作。然后，管理员必须将这些策略附加到需要这些权限的 IAM 用户或组。

要了解如何使用这些示例 JSON 策略文档创建 IAM 基于身份的策略，请参阅 Amazon Identity and Access Management 用户指南中的在 JSON 选项卡上创建策略。

主题

- 策略最佳实践
- 使用 Amazon Transfer Family 控制台
- 允许用户查看他们自己的权限

策略最佳实践

基于身份的策略决定了某人是否可以在您的账户中创建、访问或删除 Amazon Transfer Family 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 托管策略或工作职能的Amazon 托管策略。
- 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 中的安全最佳实操。

使用 Amazon Transfer Family 控制台

要访问 Amazon Transfer Family 控制台，您必须拥有一组最低权限。这些权限必须允许您列出和查看有关您 Amazon 账户中 Amazon Transfer Family 资源的详细信息。如果您创建的基于身份的策略比所需的最低权限更严格，则无法为具有该策略的实体（IAM 用户或角色）正常运行控制台。有关更多信息，请参阅 Amazon Identity and Access Management 用户指南中的为用户添加权限。

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，只允许访问与您尝试执行的 API 操作相匹配的操作。

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": "*"
        }
    ]
}
```

Amazon Transfer Family 基于标签的策略示例

以下是如何根据标签控制 Amazon Transfer Family 资源访问权限的示例。

使用标签控制对 Amazon Transfer Family 资源的访问

IAM 策略中的条件是所需语法的一部分，您可以使用它们指定对 Amazon Transfer Family 资源的权限。您可以根据这些 Amazon Transfer Family 资源的标签来控制对这些资源（例如用户、服务器、角色和其他实体）的访问权限。标签是键值对。有关为资源添加标签的更多信息，请参阅中的为Amazon 资源添加标签。Amazon Web Services 一般参考

在中 Amazon Transfer Family，资源可以有标签，有些操作可以包含标签。在创建 IAM 策略时，您可以使用标签条件键来控制：

- 根据 Amazon Transfer Family 资源所具有的标签，哪些用户可以对资源执行操作。
- 哪些标签可以在操作的请求中传递。
- 是否特定标签键可在请求中使用。

通过使用基于标签的访问控制，您可以应用比 API 级别更精细的控制。与使用基于资源的访问控制相比，您还可以应用更多动态控制。您可以创建 IAM 策略，以允许或拒绝按请求中提供的标签（请求标签）执行操作。您还可以根据正在操作资源的标签（资源标签）创建 IAM 策略。通常，资源标签用于资源上已有的标签，请求标签用于向资源添加标签或从资源中删除标签。

有关标签条件键的完整请求和语义，请参阅 IAM 用户指南中的使用资源标签控制 Amazon 资源的访问。有关使用 API Gateway 指定 IAM 策略的详细信息，请参阅 API Gateway 开发人员指南中的控制访问具有 IAM 权限的 API。

示例 1：基于资源标签拒绝操作

您可根据标签拒绝资源上执行的操作。如果用户或服务器资源通过秘钥 stage 和值 prod 标记，则以下示例策略拒绝
TagResource、UntagResource、StartServer、StopServer、DescribeServer 以及 DescribeUser 操作。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "transfer:TagResource",
                "transfer:UntagResource",
                "transfer:StartServer",
                "transfer:StopServer",
                "transfer:DescribeServer",
                "transfer:DescribeUser"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/stage": "prod"
                }
            }
        }
    ]
}
```

示例 2：基于资源标签允许操作

您可以允许根据标签对资源执行操作。如果用户或服务器资源通过秘钥 stage 和值 prod 标记，则以下示例策略拒绝
TagResource、UntagResource、StartServer、StopServer、DescribeServer 以及 DescribeUser 操作。

```
{
    "Version":"2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "transfer:TagResource",
                "transfer:UntagResource",
                "transfer:StartServer",
                "transfer:StopServer",
                "transfer:DescribeServer",
                "transfer:DescribeUser"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/stage": "prod"
                }
            }
        }
    ]
}
```

示例 3：拒绝根据请求标签创建用户或服务器

以下示例策略包含两个语句。如果标签的成本中心密钥无值，则第一条语句拒绝对所有资源执行 `CreateServer` 操作。

如果标签的成本中心密钥包含除 1、2 或 3 之外的任何其他值，则第二条语句将拒绝 `CreateServer` 操作。

> **Note**
>
> 此策略确实允许创建或删除包含 `costcenter` 秘钥和 1、2 或 3 值的资源。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
```

```
                "transfer:CreateServer"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "Null":  {
                    "aws:RequestTag/costcenter": "true"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": "transfer:CreateServer",
            "Resource": [
                "*"
            ],
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "aws:RequestTag/costcenter": [
                        "1",
                        "2",
                        "3"
                    ]
                }
            }
        }
    ]
}
```

对 Amazon Transfer Family 身份和访问进行故障排除

使用以下信息来帮助您诊断和修复在使用 Amazon Transfer Family 和 IAM 时可能遇到的常见问题。

主题

- 我无权在以下位置执行操作 Amazon Transfer Family
- 我无权执行 iam：PassRole
- 我想允许 Amazon 账户之外的人访问我的 Amazon Transfer Family 资源

我无权在以下位置执行操作 Amazon Transfer Family

如果 Amazon Web Services 管理控制台 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。

如果 `mateojackson` IAM 用户尝试使用控制台查看有关 *`widget`* 的详细信息，但没有 `transfer:`*`GetWidget`* 权限，则会出现以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 transfer:GetWidget on resource: my-example-widget
```

在这种情况下，Mateo 请求他的管理员更新其策略，以允许他使用 `transfer;:`*`GetWidget`* 操作访问 *`my-example-widget`* 资源。

我无权执行 iam：PassRole

如果您收到一个错误，表明您无权执行 `iam:PassRole` 操作，则必须更新策略以允许您将角色传递给。 Amazon Transfer Family

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 Transfer Family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。

以下示例策略包含将角色传递给 Amazon Transfer Family的权限。**`123456789012`**替换为您的 AWS 账户 ID 和**`MyTransferRole`**您的实际 IAM 角色名称。

```
{
   "Version":"2012-10-17",
   "Statement": [
      { "Action": "iam:PassRole",
        "Resource": "arn:aws:iam::123456789012:role/MyTransferRole",
```

```
        "Effect": "Allow"
      }
   ]
}
```

我想允许 Amazon 账户之外的人访问我的 Amazon Transfer Family 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：

- 要了解是否 Amazon Transfer Family 支持这些功能，请参阅如何 Amazon Transfer Family 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。

用于组织治理的 IAM 条件密钥

Amazon Transfer Family 提供了 IAM 条件密钥，允许您在任何 IAM 策略中限制资源配置。这些条件密钥可用于附加到用户或角色的基于身份的策略，或用于组织治理的服务控制策略 (SCPs)。

服务控制策略是适用于整个 Amazon 组织的 IAM 策略，为多个账户提供预防性护栏。在中使用这些条件密钥时 SCPs，有助于在整个组织范围内强制执行安全与合规性要求。

另请参阅

- Transfer Family 的操作、资源和条件密钥
- 服务控制策略 (SCPs)
-

可用的条件键

Amazon Transfer Family 支持在 IAM 策略中使用以下条件键：

`transfer:RequestServerEndpointType`

根据终端节点类型（公共、VPC、VPC_ENDPOINT）限制服务器的创建和更新。通常用于阻止面向公众的端点。

`transfer:RequestServerProtocols`

根据支持的协议（SFTP、FTPS、FTP 等）限制服务器的创建和更新。 AS2

`transfer:RequestServerDomain`

根据域类型（S3、EFS）限制服务器的创建。

`transfer:RequestConnectorProtocol`

根据协议（AS2、SFTP）限制连接器的创建。

支持的操作

条件键可以应用于以下 Amazon Transfer Family 操作：

- `CreateServer`: 支持`RequestServerEndpointType`、`RequestServerProtocols`、和`RequestServerDomain`条件键
- `UpdateServer`: 支撑键`RequestServerEndpointType`和`RequestServerProtocols`条件键
- `CreateConnector`: 支持`RequestConnectorProtocol`条件键

SCP 策略示例

以下示例 SCP 阻止在整个组织中创建公共 Amazon Transfer Family 服务器：

```
{
    "Version":"2012-10-17",
    "Statement": [{
        "Sid": "DenyPublicTransferServers",
        "Effect": "Deny",
        "Action": ["transfer:CreateServer", "transfer:UpdateServer"],
        "Resource": "*",
```

```
        "Condition": {
            "StringEquals": {
                "transfer:RequestServerEndpointType": "PUBLIC"
            }
        }
    }]
}
```

合规性验证 Amazon Transfer Family

Amazon Transfer Family 作为多个合规计划的一部分，第三方审计师对安全性和 Amazon 合规性进行评估。其中包括 SOC、PCI、HIPAA 等。有关完整列表，请参阅按合规计划划分的范围内的Amazon 服务。

有关特定合规计划范围内的 Amazon 服务列表，请参阅按合规计划划分的范围内的Amazon 服务。有关一般信息，请参阅 Amazon 合规性计划。

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 Transfer Family 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：

- 安全与合规性快速入门指南 — 这些部署指南讨论了架构注意事项，并提供了在上部署以安全性和合规性为重点的基准环境的步骤。 Amazon
- HIPAA 安全与合规架构白皮书 — 本白皮书描述了各公司如何使用它来 Amazon 创建符合 HIPAA 标准的应用程序。
- ：此业务手册和指南集合可能适用于您的行业和位置。
- Amazon Config— 该 Amazon 服务评估您的资源配置在多大程度上符合内部实践、行业指导方针和法规。
- Amazon Security Hub CSPM— 此 Amazon 服务可全面了解您的安全状态 Amazon ，帮助您检查是否符合安全行业标准和最佳实践。

韧性在 Amazon Transfer Family

Amazon 全球基础设施是围绕 Amazon 区域和可用区构建的。 Amazon 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相连。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架构相比，可用区具有更高的可用性、容错性和可扩展性。

Amazon Transfer Family 最多支持 3 个可用区，并由 auto Scaling 的冗余队列提供支持，用于处理您的连接和传输请求。

对于所有 Transfer Family 端点：

- 该服务内置了可用区域级别的冗余。
- 每个可用区都有冗余实例集。
- 这种冗余是自动提供的。

> **Note**
>
> 对于虚拟私有云 (VPC) Private Cloud 中的终端节点，可以提供单个子网。但是，我们建议您在您的 VPC 内的多个可用区中创建终端节点，以降低可用区中断期间服务中断的风险。

另请参阅

- 有关如何在 VPC 中创建 Transfer Family 服务器的详细信息，请参阅在虚拟私有云中创建服务器。
- 有关 Amazon Web Services 区域 和可用区的更多信息，请参阅Amazon 全球基础架构。
- 有关如何使用基于延迟的路由来构建更高的冗余并最大限度地减少网络延迟的示例，请参阅博客文章最大限度地减少服务器的网络延迟。 Amazon Transfer Family

在 VPC 和之间创建私有连接 Amazon Transfer Family APIs

您可以 Amazon Transfer Family APIs 通过创建由提供支持的接口 VPC 终端节点在您的 VPC 和之间建立私有连接Amazon PrivateLink。您可以像在 VPC 中 Amazon Transfer Family APIs 一样进行访问，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 Amazon Transfer Family APIs 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。在为设置接口 VPC 终端节点之前 Amazon Transfer Family APIs，请查看Amazon PrivateLink 指南中的注意事项。

使用 VPC 终端节点策略控制访问

默认情况下，允许通过终端节点进行完全访问。 Amazon Transfer Family APIs 您可以使用 VPC 端点策略控制对接口端点的访问。您可以为 VPC 端点附加控制对 Amazon Transfer Family APIs 的访问的端点策略。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 端点控制对服务的访问。

以下是的终端节点策略示例 Amazon Transfer Family APIs。当连接到终端节点时，此策略授予对所有资源 Amazon Transfer Family APIs 执行所有操作的访问权限，但标有密钥`Environment`和值的资源除外`Test`。

```
{
    "Statement": [{
        "Effect": "Deny",
        "Action": "transfer:StartFileTransfer",
        "Principal": "*",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/Environment": "Test"
            }
        }
    }, {
        "Effect": "Allow",
        "Action": "transfer:*",
        "Principal": "*",
        "Resource": "*"
    }]
}
```

为 Amazon Transfer Family APIs 创建接口 VPC 终端节点

您可以 Amazon Transfer Family APIs 使用 Amazon VPC 控制台或 Amazon 命令行界面 (Amazon CLI) 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 端点。

Amazon Transfer Family APIs 使用以下服务名称之一创建 VPC 终端节点：

- `com.amazonaws.region.transfer`
- `com.amazonaws.region.transfer-fips`— 创建符合联邦信息处理标准 (FIPS) 出版物 140-3 美国政府标准的接口 VPC 终端节点。

如果为端点启用私有 DNS，则可以使用其默认 DNS 名称作为区域，向 Amazon Transfer Family APIs 发送 API 请求，例如 `transfer.us-east-1.amazonaws.com`。

中的基础设施安全 Amazon Transfer Family

作为一项托管服务 Amazon Transfer Family ，受 Amazon 全球网络安全的保护。有关 Amazon 安全服务以及如何 Amazon 保护基础设施的信息，请参阅Amazon 云安全。要使用基础设施安全的最佳实践来设计您的 Amazon 环境，请参阅 S Amazon ecurity Pillar Well-Architected Fram ework 中的基础设施保护。

您可以使用 Amazon 已发布的 API 调用 Amazon Transfer Family 通过网络进行访问。客户端必须支持以下内容：

- 传输层安全性协议（TLS）。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密（PFS）的密码套件，例如 DHE（临时 Diffie-Hellman）或 ECDHE（临时椭圆曲线 Diffie-Hellman）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

避免将服务器放在 NLBs Amazon Transfer Family 服务器前面 NATs

> **Note**
>
> 配置有 FTP 和 FTPS 协议的服务器仅允许使用 VPC 进行配置：没有可用于 FTP/FTPS 的公共端点。

许多客户将 Network Load Balancer (NLB) 配置为将流量路由到其 Amazon Transfer Family 服务器。他们之所以这样做，要么是因为他们之前创建了服务器， Amazon 提供了一种从 VPC 内部和互联网访问服务器的方法，要么是为了支持 Internet 上的 FTP。这种配置不仅会增加客户的成本，还可能导致其他问题，我们在本节中对此进行了介绍。

当客户端从公司防火墙后面的客户专用网络进行连接时，NAT 网关是必备组件。但是，您应该注意，当许多客户端位于同一 NAT 网关后面时，这可能会影响性能和连接限制。如果从客户端到 FTP 或 FTPS 服务器的通信路径中有 NLB 或 NAT，则服务器无法准确识别客户端的 IP 地址，因为只能 Amazon Transfer Family 看到 NLB 或 NAT 的 IP 地址。

如果您在 NLB 后面使用 Transfer Family 服务器的配置，我们建议您移至 VPC 终端节点并使用弹性 IP 地址而不是 NLB。使用 NAT 网关时，请注意下述的连接限制。

如果您使用的是 FTPS 协议，则此配置不仅会降低您审核谁在访问您的服务器的能力，而且还会影响性能。 Amazon Transfer Family 使用源 IP 地址在我们的数据平面上对您的连接进行分片。对于 FTPS 来说，这意味着通信路由上带有 NLB 或 NAT 网关的 Transfer Family 服务器不会同时拥有 10,000 个连接，而是仅限于 300 个同步连接。

尽管我们建议避免在 Amazon Transfer Family 服务器前面使用网络负载均衡器，但如果您的 FTP 或 FTPS 实施需要在客户端的通信路由中使用 NLB 或 NAT，请遵循以下建议：

- 对于 NLB，请使用端口 21 而不是端口 8192-8200 进行运行状况检查。
- 对于 Amazon Transfer Family 服务器，通过设置启用 TLS 会话恢复`TlsSessionResumptionMode = ENFORCED`。

> **Note**
>
> 这是推荐的模式，因为它提供了增强的安全性：
>
> - 要求客户端在后续连接中使用 TLS 会话恢复。
> - 通过确保一致的加密参数来提供更强的安全保障。
> - 有助于防止潜在的降级攻击。
> - 在优化性能的同时保持对安全标准的合规性。

- 如果可能，请停止使用 NLB，以充分利用 Amazon Transfer Family 性能和连接限制。

有关 NLB 替代方案的更多指导，请通过 Amazon Support 联系 Amazon Transfer Family 产品管理团队。有关改善安全状况的更多信息，请参阅博客文章《提高 Amazon Transfer Family 服务器安全性的六个技巧》。

VPC 连接基础设施安全

具有 VPC 出口类型的 SFTP 连接器通过网络隔离和私有连接提供增强的基础设施安全性：

网络隔离的好处

- 私有网络流量：所有到私有 SFTP 服务器的连接器流量都保留在您的 VPC 内，从不通过公共互联网。
- 受控出口：对于通过 VPC 访问的公共终端节点，流量通过您的 NAT 网关路由，让您能够控制出口 IP 地址和网络策略。
- VPC 安全控制：利用现有 VPC 安全组 ACLs、网络和路由表来控制连接器网络访问。
- 混合连接：通过已建立的 VPN 或 Direct Connect 连接访问本地 SFTP 服务器，无需额外的互联网接入。

资源网关安全注意事项

资源网关为跨VPC资源访问提供安全的入口点：

- 多可用区部署：资源网关要求子网位于至少两个可用区中，以实现高可用性和容错能力。
- 安全组控制：将安全组配置为仅限授权来源访问 SFTP 端口（通常为端口 22）。
- 私有子网放置：连接到私有 SFTP 服务器时，在私有子网中部署资源网关以保持网络隔离。
- 连接限制：每个资源网关最多支持 350 个并发连接，TCP 连接的空闲超时时间为 350 秒。

添加 Web 应用程序防火墙

Amazon WAF 是一种 Web 应用程序防火墙，可帮助保护 Web 应用程序和 APIs 免受攻击。通过它，您可以配置一组规则（称为 Web 访问控制列表，即 Web ACL），基于可自定义的 Web 安全规则以及您定义的条件，允许、阻止或统计 Web 请求。有关更多信息，请参阅使用 Amazon WAF 保护您的 APIs。

要添加 Amazon WAF

1. 打开 API Gateway 控制台，网址为https://console.aws.amazon.com/apigateway/。
2. 在APIs导航窗格中，然后选择您的自定义身份提供商模板。
3. 选择 Stages (阶段)。
4. 在 Stages (阶段) 窗格中，选择该阶段的名称。
5. 在 Stage Editor (阶段编辑器) 窗格中，选择设置选项卡。
6. 请执行以下操作之一：

- 在 Web 应用程序防火墙 (WAF) 下，选择要与此阶段关联的 Web ACL。
- 如果您所需的 Web ACL 不存在，则通过以下方式创建：
  1. 选择创建 Web ACL。
  2. 在 Amazon WAF 服务主页上，选择创建 Web ACL。
  3. 在 Web ACL 详细信息，在 名称 中键入 Web ACL 的名称。
  4. 在规则，选择添加规则，然后选择添加自己的规则和规则组。
  5. 对于规则类型，选择 IP 集以标识特定 IP 地址列表。
  6. 对于规则，输入规则的名称。
  7. 对于 IP 集，请选择现有的 IP 集。要创建 IP 集，请参阅创建 IP 集。
  8. 对于用作初始地址的 IP 地址，请选择标头中的 IP 地址
  9. 在标头题字段名中，输入 `SourceIP`。
  10. 对于标头内位置，选择第一个 IP 地址。
  11. 对于缺少 IP 地址的回退，请根据标题中无效（或缺失）IP 地址的处理方式，选择匹配或不匹配。
  12. 在操作中，选择 IP 集的操作。
  13. 对于不符合任何规则请求的默认 Web ACL 操作，请选择允许或阻止，然后单击下一步。
  14. 对于步骤 4 和 5，选择下一步。
  15. 在审核和创建中，查看您的选择，然后选择创建 Web ACL。
7. 选择保存更改。
8. 选择资源。
9. 对于操作，选择部署 API。

有关使用 Amazon 网络应用程序防火墙的 Transfer Family 如何安全的信息，请参阅 Amazon 存储博客中的使用 Amazon 应用程序防火墙和 Amazon API Gateway 保护 Transfer Fam ily。

防止跨服务混淆代理

混淆代理问题是一个安全性问题，即不具有某操作执行权限的实体可能会迫使具有更高权限的实体执行该操作。在中 Amazon，跨服务模仿可能会导致混乱的副手问题。一个服务（呼叫服务）调用另一项服务（所谓的服务）时，可能会发生跨服务模拟。可以操纵调用服务以使用其权限对另一个客户的资源进行操作，否则该服务不应有访问权限。为防止这种情况， Amazon 提供可帮助您保护所有服务的数据

的工具，而这些服务中的服务主体有权限访问账户中的资源。有关此问题的详细描述，请参阅 IAM 用户指南中的混淆代理问题。

我们建议在资源策略中使用aws:SourceArn和aws:SourceAccount全局条件上下文密钥来限制 Transf Amazon er Family 对资源的权限。如果使用两个全局条件上下文键，在同一策略语句中使用时，aws:SourceAccount 值和 aws:SourceArn 值中的账户必须使用相同的账户 ID。

防止混淆代理问题的最有效方法是使用您想要允许的资源的准确 Amazon 资源名称 (ARN)。如果您要指定多个资源，请使用带有通配符 (*) 的 aws:SourceArn 全局上下文条件键来表示 ARN 的未知部分。例如 arn:aws:transfer::*region*::*account-id*:server/*。

Amazon Transfer Family 使用以下类型的角色：

- 用户角色-允许服务管理的用户访问必要的 Transfer Family 资源。 Amazon Transfer Family 在 Transfer Family 用户 ARN 的背景下担任此角色。
- 访问角色 - 仅提供对正在传输的 Amazon S3 文件的访问权限。对于入站 AS2 转移，访问角色使用协议的 Amazon 资源名称 (ARN)。对于出站 AS2 传输，访问角色使用连接器的 ARN。
- 调用角色 – 用于作为服务器自定义身份提供程序的 Amazon API Gateway。Transfer Family 在 Transfer Family 服务器 ARN 的背景下扮演这个角色。
- 日志角色-用于将条目登录到 Amazon CloudWatch。Transfer Family 使用此角色记录成功和失败的详细信息以及有关文件传输的信息。Transfer Family 在 Transfer Family 服务器 ARN 的背景下扮演这个角色。对于出站 AS2 传输，日志角色使用连接器 ARN。
- 执行角色 - 允许 Transfer Family 用户调用和启动工作流程。Transfer Family 在 Transfer Family 工作流程 ARN 的背景下担任此角色。

有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。

> **Note**
>
> 在以下示例中，用您自己的信息替换每个*user input placeholder*示例。

> **Note**
>
> 在我们的示例中，我们同时使用 ArnLike 和 ArnEquals。它们在功能上是相同的，因此您可以在制定策略时使用其中任何一个。Transfer Family 文档在条件包含通配符时使用 ArnLike，ArnEquals 用于表示完全匹配的条件。

Amazon Transfer Family 用户角色跨服务混淆副手预防

以下示例策略允许账户中的任何服务器担任该角色。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "transfer.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:transfer:us-east-1:123456789012:user/
*"
                }
            }
        }
    ]
}
```

以下示例策略允许任何特定服务器用户承担此角色。

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "transfer.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
```

```
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:transfer:us-east-1:123456789012:user/server-id/
*"
        }
      }
    }
  ]
}
```

以下示例策略允许特定服务器的特定用户担任该角色。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "transfer.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:transfer:us-
east-1:123456789012:user/server-id/user-name"
                }
            }
        }
    ]
}
```

Amazon Transfer Family 工作流程角色跨服务混乱副手预防

以下示例策略允许账户中的任何工作流程担任该角色。

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "transfer.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:transfer:us-
west-2:111122223333:workflow/*"
                }
            }
        }
    ]
}
```

以下示例策略允许特定工作流程承担此角色。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "transfer.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:transfer:us-
west-2:111122223333:workflow/workflow-id"
                }
            }
        }
    ]
```

```
}
```

Amazon Transfer Family 连接器角色跨服务混乱副手预防

以下示例策略允许账户中的任何连接器代入该角色。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "transfer.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:transfer:us-
east-1:123456789012:connector/*"
                }
            }
        }
    ]
}
```

以下示例策略允许特定的连接器担任该角色。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "transfer.amazonaws.com"
```

```
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:transfer:us-
east-1:123456789012:connector/connector-id"
                }
            }
        }
    ]
}
```

Amazon Transfer Family 日志和调用角色跨服务混淆了副手预防

> **Note**
>
> 以下示例可用于日志记录和调用角色。
> 在这些示例中，如果您的服务器未附加任何工作流程，则可以删除该工作流程的 ARN 详细信息。

以下示例 logging/invocation 策略允许账户中的任何服务器（和工作流程）代入该角色。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAllServersWithWorkflowAttached",
            "Effect": "Allow",
            "Principal": {
                "Service": "transfer.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnLike": {
                   "aws:SourceArn": [
                     "arn:aws:transfer:us-west-2:111122223333:server/*",
```

```
                    "arn:aws:transfer:us-west-2:111122223333:workflow/*"
                ]
            }
        }
    ]
}
```

以下示例 logging/invocation 策略允许特定的服务器（和工作流程）担任该角色。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSpecificServerWithWorkflowAttached",
            "Effect": "Allow",
            "Principal": {
                "Service": "transfer.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "ArnEquals": {
                   "aws:SourceArn": [
                       "arn:aws:transfer:us-west-2:111122223333:server/server-id",
                       "arn:aws:transfer:us-west-2:111122223333:workflow/workflow-
id"
                   ]
                }
            }
        }
    ]
}
```

Amazon Transfer Famil Amazon y 的托管政策

要向用户、群组和角色添加权限，使用 Amazon 托管策略比自己编写策略要容易得多。创建 Amazon Identity and Access Management (IAM) 客户托管策略仅向您的团队提供他们所需的权限需要时间和

专业知识。要快速入门，您可以使用我们的 Amazon 托管策略。这些策略涵盖常见使用案例，可在您的 Amazon Web Services 账户中使用。有关 Amazon 托管式策略的更多信息，请参阅《IAM 用户指南》中的 Amazon 托管式策略。有关所有 Amazon 托管策略的详细列表，请参阅Amazon 托管策略参考指南。

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 托管式策略添加额外权限以支持新特征。此类更新会影响附加策略的所有身份（用户、组和角色）。当启动新特征或新操作可用时，服务最有可能会更新 Amazon 托管式策略。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。

此外，还 Amazon 支持跨多个服务的工作职能的托管策略。例如，`ReadOnlyAccess` Amazon 托管策略提供对所有 Amazon 服务和资源的只读访问权限。当服务启动一项新功能时， Amazon 会为新操作和资源添加只读权限。有关工作职能策略的列表和说明，请参阅 IAM 用户指南中的适用于工作职能的 Amazon 托管式策略。

Amazon 托管策略： AWSTransferConsoleFullAccess

该`AWSTransferConsoleFullAccess`政策提供通过 Amazon 管理控制台对 Transfer Family 的完全访问权限。有关更多信息，请参阅 Transfer F amily 的 Amazon 服务相关角色。

Amazon 托管策略： AWSTransferFullAccess

此 `AWSTransferFullAccess` 策略提供对 Transfer Family 服务的完全访问权限。有关更多信息，请参阅 Transfer F amily 的 Amazon 服务相关角色。

Amazon 托管策略： AWSTransferLoggingAccessV3

该`AWSTransferLoggingAccessV3`策略授予管理权限，允许将您 Amazon 的 Transfer Family 服务器活动记录到 Amazon CloudWatch Logs 中。因此，您应该将此策略附加至日志记录角色。

权限详细信息

此策略包括以下权限 Amazon CloudWatch Logs。

- `CreateLogStream` — 授权主体创建日志流。
- `DescribeLogStreams`— 授权主体列出日志组的日志流。
- `CreateLogGroup` — 授权主体创建日志组。
- `PutLogEvents` – 授予权限以将一批日志事件上传到指定的日志流。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:DescribeLogStreams",
                "logs:CreateLogGroup",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws-cn:logs:*:*:log-group:/aws/transfer/*"
        }
    ]
}
```

Amazon 托管策略： AWSTransferReadOnlyAccess

此 AWSTransferReadOnlyAccess 策略提供对 Transfer Family 服务的只读访问权限。有关更多信息，请参阅 Transfer F amily 的 Amazon 服务相关角色。

Amazon 将 Family 更新转移到 Amazon 托管政策

查看 Transfer Family Amazon 托管政策自该服务开始跟踪这些变更以来这些更新的详细信息。Amazon 要获得有关此页面更改的自动提示，请订阅 的文档历史记录 Amazon Transfer Family 页面上的 RSS 源。

更改	描述	日期
文档更新	为每个 Transfer Family 托管策略添加章节。	2022 年 1 月 27 日
AWSTransferReadOnlyAccess：对现有策略的更新	Amazon Transfer Family 添加了允许读取策略的新权限 Amazon Managed Microsoft AD。	2021 年 9 月 30 日

更改	描述	日期
AWSTransferLogging AccessV3 — 更新现有政策	AWSTransferLogging AccessV3 与标记为服务角色策略的 AWSTransferLoggingAccessV2 不同。此标记表示它旨在向 Transfer Family Amazon 服务授予权限。无功能性变更。	2021 年 6 月 15 日
AWSTransferLogging AccessV2 — 已弃用	此策略已被 AWSTransferLoggingAccessV3 取代。	2021 年 6 月 15 日
Amazon Transfer Family 开始追踪变更	Amazon Transfer Family 开始跟踪其 Amazon 托管政策的变更。	2021 年 6 月 15 日

Transfer Family terraform 模块

HashiCorpTerraform 是使用 HashiCorp 配置语言 (HCL) 开发的开源基础设施即代码 (IaC) 引擎。Terraform 提供了一致的命令行界面 (CLI) 工作流程，该工作流程与 Amazon 用于后端基础架构的 Transfer Family 配合使用，可以管理数百种云服务，并将云编码 APIs 为声明性配置文件。

你可以使用 Terraform 安全地部署 Amazon Transfer Family SFTP 服务器和 SFTP 连接器以及相关的依赖项和自定义项。有关包含用于创建运行 Amazon Transfer Family 所需资源的 Terraform 代码的存储库，请参阅上的 Terraform Transfer Family 模块源代码。 GitHub

> **Note**
>
> Terra Amazon form 的 Transfer Family 模块是一项由社区支持的项目。它们不是 Amazon 服务的一部分。 Amazon 存储社区提供尽力支持。

SFTP 服务器

此自动化为您提供了可自定义的 Terraform 模块和 end-to-end示例，用于创建 SFTP 终端节点（PUBLIC或VPC终端节点类型）、与 Amazon 集成 CloudWatch 以进行日志记录和监控、管理终端节点访问的用户身份，以及配置 IAM 角色以访问存储文件的 Amazon S3 存储桶。该模块支持每个用户多个 SSH 公钥（最多 50 个密钥），以增强安全性和密钥轮换功能。

SFTP 连接器

Amazon Transfer Family Terraform 模块现在支持部署 SFTP 连接器，以便在亚马逊 S3 和远程 SFTP 服务器之间传输文件。SFTP 连接器提供完全托管的低代码功能，可以在 Amazon S3 和远程 SFTP 服务器之间复制文件。

现在，您可以使用 Terraform 在单个部署中以编程方式配置 SFTP 连接器、关联的依赖项和自定义项。该模块还提供了基于时间表或事件触发器自动执行文件传输工作流程的 end-to-end示例。使用 Terraform 进行部署，无需进行耗时且容易出错的手动配置，并为您提供可扩展的快速、可重复且安全的部署选项。

AS2

要显示对 AS2 Terraform 模板的支持，请在 Transfer Family Ter raf orm 模板功能请求中添加竖起大拇指的反应 (#)。您也可以添加评论来描述您的用例。

B2B 数据交换

Amazon B2B Data Interchange 自动将电子数据交换 (EDI) 文档与 JSON 和 XML 数据格式之间的转换、验证和生成。要显示对用于 B2B 数据交换的 Terraform 模板的支持，请在功能请求中添加竖起大拇指的反应 (#)。您也可以添加评论来描述您的用例。

故障排除 Amazon Transfer Family

本章提供您在使用时可能遇到的常见问题的疑难解答信息 Amazon Transfer Family。每个部分都侧重于一个特定的功能领域，以帮助您快速找到问题的解决方案。

- 有关 Transfer Family 中的 IAM 问题，请参阅 对 Amazon Transfer Family 身份和访问进行故障排除。
- 有关您的 Transfer Family 网络应用程序的问题，请参阅对 Web 应用程序进行故障排除。

主题

- 对身份认证问题进行故障排除
- 对 SFTP 连接器问题进行故障排除
- 对 SFTP 连接和传输问题进行故障排除
- 对自定义身份提供商问题进行故障排除
- 解决工作流程问题
- 对 EFS 问题进行故障排除
- 对存储和加密问题进行故障排除
- 对监控和警报问题进行故障排除
- 解决跨区域传输问题
- 对 Terraform 部署问题进行故障排除
- Web 应用程序防火墙集成问题疑难解答
- 解决服务托管用户问题
- AS2 问题疑难解答

对身份认证问题进行故障排除

本节介绍以下身份验证问题的可能解决方案。

主题

- 身份验证失败 — SSH/SFTP
- 托管 AD 领域不匹配问题

- 已超出活动目录组限制
- 其他身份验证问题
- 对 Amazon API Gateway 问题进行故障排除
- 对测试您的身份提供商进行故障排除
- 在网络应用程序中重复亚马逊 S3 存储桶

身份验证失败 — SSH/SFTP

描述

当您尝试使用 Secure Shell (SSH) 文件传输协议 (SFTP) 连接到服务器时，会收到类似于以下内容的消息：

```
Received disconnect from 3.130.115.105 port 22:2: Too many authentication failures
  Authentication failed.
```

> **Note**
>
> 如果您使用的是 API Gateway 并收到此错误，请参阅 身份验证失败次数过多。

原因

您尚未为用户添加 RSA 密钥对，因此必须改用密码进行身份验证。

解决方案

运行该 `sftp` 命令时，请指定 `-o PubkeyAuthentication=no` 选项。此选项会强制系统请求您的密码。例如：

```
sftp -o PubkeyAuthentication=no sftp-user@server-id.server.transfer.region-
id.amazonaws.com
```

托管 AD 领域不匹配问题

描述

用户的领域和他们的组领域必须匹配。它们必须都在默认领域中，或者它们都必须位于可信领域。

原因

如果用户及其组不匹配，则无法通过 Transfer Family 对该用户进行身份验证。如果您测试用户的身份提供商，则会收到错误找不到用户组的关联访问权限。

解决方案

引用用户领域中与组领域（默认或可信）相匹配的组。

已超出活动目录组限制

描述

尝试向 Amazon Transfer Family 服务器添加更多 Active Directory 群组时，您会收到一条错误消息，指出您已达到允许的最大群组数。

原因

Amazon Transfer Family 默认限制为每台服务器 100 个 Active Directory 组。

解决方案

以下是两种可能的解决方案：

- 整合您的 Active Directory 群组以减少所需的总数。
- 如果您的用例需要超过 100 个群组，请考虑使用自定义身份提供商解决方案，如使用自定义身份提供商简化 Active Directory 身份验证中所述 Amazon Transfer Family。

其他身份验证问题

描述

您收到身份验证错误，但其他故障排除均无效

原因

您可能已经为包含前导或尾部斜杠 (/) 的逻辑目录指定了目标。

解决方案

更新您的逻辑目录目标，确保它以斜杠开头，并且不包含尾部斜杠。例如，/amzn-s3-demo-bucket/images可以接受amzn-s3-demo-bucket/images，但不/amzn-s3-demo-bucket/images/是。

对 Amazon API Gateway 问题进行故障排除

本节介绍以下 API Gateway 问题的可能解决方案。

主题

- 身份验证失败次数过多
- 连接关闭

身份验证失败次数过多

描述

当您尝试使用 Secure Shell (SSH) 文件传输协议 (SFTP) 连接到服务器时，会出现以下错误：

```
Received disconnect from 3.15.127.197 port 22:2: Too many authentication failures
Authentication failed.
Couldn't read packet: Connection reset by peer
```

原因

您可能输入了错误的用户密码。请重试输入正确的密码。

如果密码正确，则问题可能是由角色 Amazon 资源名称 (ARN) 无效引起的。要确认这是问题所在，请测试服务器的身份提供商。如果您看到类似于以下内容的响应，则角色 ARN 仅为占位符，如全部为零的角色 ID 值所示：

```
{
    "Response": "{\"Role\": \"arn:aws:iam::000000000000:role/MyUserS3AccessRole\",
\"HomeDirectory\": \"/\"}",
    "StatusCode": 200,
    "Message": "",
    "Url": "https://api-gateway-ID.execute-api.us-east-1.amazonaws.com/prod/
servers/transfer-server-ID/users/myuser/config"
}
```

解决方案

将占位符角色 ARN 替换为有权访问服务器的实际角色。

更新角色

1. 在 https://console.aws.amazon.com/cloudformation 上打开 Amazon CloudFormation 控制台。
2. 在左侧导航窗格中，选择堆栈。
3. 在堆栈列表中，选择您的堆栈，然后选择参数选项卡。
4. 选择更新。在更新堆栈页面上，选择使用当前模板，然后选择下一步。
5. 替换为UserRoleArn具有足够权限访问您的 Transfer Family 服务器的角色 ARN。

> **Note**
>
> 要授予必要的权限，您也可以将 `AmazonAPIGatewayAdministrator` 和 `AmazonS3FullAccess` 托管策略添加到角色中。

6. 选择下一步，然后再次选择下一步。在 “查看 ***stack***” 页面上，选择 “我确认 Amazon CloudFormation 可能会创建 IAM 资源”，然后选择 “更新堆栈”。

连接关闭

描述

当您尝试使用 Secure Shell (SSH) 文件传输协议 (SFTP) 连接到服务器时，会出现以下错误：

```
Connection closed
```

原因

造成此问题的一个可能原因是，您的亚马逊 CloudWatch 日志角色与 Transfer Family 没有信任关系。

解决方案

确保服务器的日志记录角色与 Transfer Family 具有信任关系。有关更多信息，请参阅 建立信任关系。

对测试您的身份提供商进行故障排除

描述

如果您使用控制台或 TestIdentityProvider API 操作测试身份提供商，则该Response字段为空。例如：

```
{
    "Response": "{}",
    "StatusCode": 200,
    "Message": ""
}
```

原因

最可能的原因是用户名或密码不正确导致身份验证失败。

解决方案

确保您使用的是正确的用户凭证，并在必要时更新用户名或密码。

在网络应用程序中重复亚马逊 S3 存储桶

描述

同一个亚马逊 S3 存储桶在 Transfer Family 网络应用程序界面中多次出现。

原因

当用户属于对同一 Amazon S3 存储桶拥有权限的多个 Amazon S3 存储桶的活动目录组时，就会发生这种情况。Web 应用程序列出了与用户的 UID 或 GID 关联的所有顶级授权，包括对同一存储桶位置的重复授权。

解决方案

为防止重复上架商品，请合并授权，这样每位用户在每个 Amazon S3 地点只能获得一次授权。查看您的 Amazon S3 访问授权配置，删除不同活动目录组中对同一存储桶的冗余授权。

对 SFTP 连接器问题进行故障排除

本节介绍了 SFTP 连接器问题的可能解决方案。

主题

- 为您的 SFTP 连接器添加可信主机密钥进行故障排除
- 密钥协商失败

- SFTP 连接器限制
- 优化 SFTP 连接器性能
- 排除 VPC 连接问题
- 其他 SFTP 连接器问题

为您的 SFTP 连接器添加可信主机密钥进行故障排除

描述

创建或编辑 SFTP 连接器并添加可信主机密钥时，您会收到以下错误：`Failed to edit connector details (Invalid host key format.)`

原因

如果您粘贴了正确的公钥，则问题可能在于您包含了密钥的`comment`部分。 Amazon Transfer Family 目前不接受密钥的注释部分。

解决方案

将密钥的注释部分粘贴到文本字段中时，将其删除。例如，假设您的密钥可能如下所示：

```
ssh-rsa AAAA...== marymajor@dev-dsk-marymajor-1d-c1234567.us-east-1.amazon.com
```

删除 == 字符后面的文本，然后仅粘贴密钥中直至并包括 == 的部分。

```
ssh-rsa AAAA...==
```

密钥协商失败

描述

您会收到密钥交换协商失败的错误。例如：

```
Key exchange negotiation failed due to incompatible host key algorithms.
Client offered: [ecdsa-sha2-nistp256, ecdsa-sha2-nistp384,
ecdsa-sha2-nistp521, rsa-sha2-512, rsa-sha2-256] Server offered: [ssh-rsa]
```

原因

出现此错误是因为服务器支持的主机密钥算法与连接器支持的主机密钥算法之间没有重叠。

解决方案

确保远程服务器支持错误消息中列出的至少一种客户端主机密钥算法。有关支持的算法列表，请参阅 Amazon Transfer Family SFTP 连接器的安全策略。

SFTP 连接器限制

描述

使用 SFTP 连接器进行文件传输时，您会遇到以下错误：

```
{"type":"ExecutionThrottled","details":{},"connectorId":"c-1234567890abcdef0"}
```

或者，您会注意到在大容量操作期间，文件传输会间歇性延迟或失败。

原因

SFTP 连接器的服务配额限制了并发文件传输和 API 操作的数量。当超过这些限制时，会进行限流以保护服务并确保所有客户的公平使用。

解决方案

要解决 SFTP 连接器问题，请尝试以下解决方案：

1. 在应用程序中实现指数退避和重试逻辑。例如，创建一个函数，该函数会自动重试失败的操作，并且两次尝试之间的等待时间会增加。
2. 在您的应用程序中实现速率限制：
   - 限制并发传输的数量。
   - 添加传输批次之间的延迟。
3. 根据服务配额监控您的使用情况：
   - 使用 CloudWatch 指标来跟踪 API 使用情况。
   - 设置警报，以便在接近配额限制时通知您。
4. 有关扩展 SFTP 连接器的选项，请参阅扩展您的 SFTP 连接器。
5. 如果限制仍然存在并影响您的业务运营，请通过 Service Quotas 控制台申请增加配额。

优化 SFTP 连接器性能

描述

您的 SFTP 连接器传输速度比预期的要慢，或者性能不稳定。

原因

SFTP 连接器的性能可能会受到各种因素的影响，包括网络状况、文件大小、远程服务器配置和并发传输限制。

解决方案

优化 SFTP 连接器性能，请执行以下操作：

- 配置您的远程 SFTP 服务器以获得最佳性能：
  - 增加每个会话的最大会话数和传输次数
  - 为高延迟连接优化 TCP 窗口大小
  - 如果两端都支持，则使用压缩
- 考虑网络优化，将 Transfer Family 连接器放置在靠近远程 SFTP 服务器的区域。
- 实施监控策略以识别性能瓶颈：
  - 监控网络吞吐量和延迟
  - 分析日志以了解慢速传输中的模式

排除 VPC 连接问题

本节介绍启用了 vpc_Lattice 的 SFTP 连接器常见问题的解决方案。

连接器停留在 “待处理” 状态

描述

您的启用 vpc_lattice 的 SFTP 连接器会在很长一段时间（超过 10 分钟）内保持`PENDING`状态。

原因

这可能是由于 DNS 解析延迟、资源网关配置问题或 VPC Lattice 服务网络关联问题造成的。

解决方案

请通过 Amazon Web Services 支持 C Amazon ontact.contact. 联系以帮助分析问题的根本原因。您也可以尝试以下解决方法。

1. 验证您的资源网关是否处于`ACTIVE`状态：

```
aws vpc-lattice get-resource-gateway --resource-gateway-
identifier rgw-1234567890abcdef0
```

2. 检查您的资源配置是否正确配置且处于活动状态：

```
aws vpc-lattice get-resource-configuration --resource-configuration-
identifier rcfg-1234567890abcdef0
```

3. 确保您的资源网关在至少两个支持 VPC Lattice 的可用区中有子网。
4. 如果问题仍然存在，请删除并重新创建具有相同配置的连接器。

连接器处于 “错误” 状态

描述

您的启用 vpc_Lattice 的 SFTP 连接器会显示状态和错误详情。ERRORED

原因

常见原因包括资源配置 ARN 无效、VPC 子网中的 IP 地址不足或尝试跨区域资源共享。

解决方案

1. 使用`describe-connector`以下命令查看错误详情：

```
aws transfer describe-connector --connector-id c-1234567890abcdef0
```

2. 验证资源配置 ARN 是否正确且与您的连接器位于同一区域。
3. 确保您的 VPC 子网有足够的可用的 IP 地址用于资源网关。
4. 检查您的资源配置目标（IP 地址或 DNS 名称）是否可以从您的 VPC 访问。

不支持公有 IP 地址错误

描述

在尝试使用公有 IP 地址创建资源配置时，您会收到错误消息：`ValidationException: IP address x.x.x.x is not in allowed ranges.`

原因

公共终端节点的资源配置必须使用 DNS 名称，而不是 IP 地址。

解决方案

创建资源配置时，使用 SFTP 服务器的公有 DNS 名称而不是其 IP 地址：

```
aws vpc-lattice create-resource-configuration \
    --name my-public-server-config \
    --resource-gateway-identifier rgw-1234567890abcdef0 \
    --resource-configuration-definition dnsResource={domainName="my.sftp.server.com"} \
    --port-ranges 22
```

不支持可用区错误

描述

创建资源网关时收到错误消息：`Subnet subnet-xxx is not valid because it is not in a supported Availability Zone.`

原因

并非所有可用区都支持 VPC 莱迪思跨VPC资源访问。错误消息列出了您所在地区支持的 AZs 内容。

解决方案

1. 在错误消息中列出的支持的可用区中创建子网。
2. 更新您的资源网关，使其 AZs仅使用支持的子网。
3. 确保在不同的支持 AZs中至少有两个子网。

使用 VPC_LATTICE 连接器的连接超时

描述

通过 VPC 连接器传输文件会间歇性超时或失败。

原因

VPC Lattice 有连接限制（每个资源 350 个连接）和空闲超时（TCP 为 350 秒）。

解决方案

1. 监控并发连接，使其保持在每个资源的 350 个连接限制之内。
2. 在应用程序中实现连接池和重复使用。
3. 在 SFTP 客户端应用程序中配置适当的超时值（小于 350 秒）。
4. 考虑为同一个目标创建多个资源配置来分配负载。

其他 SFTP 连接器问题

描述

运行后您会收到错误`StartFileTransfer`，但不知道问题的原因，并且在 API 调用后只返回连接器 ID。

原因

此错误可能有多种原因。要排除故障，我们建议您测试连接器并搜索 CloudWatch 日志。

解决方案

- 测试您的连接器：请参阅测试 SFTP 连接器。如果测试失败，系统会根据测试失败的原因提供错误消息。该部分介绍如何通过控制台或使用 TestConnectionAPI 命令测试您的连接器。
- 查看您的连接器的 CloudWatch 日志：请参阅SFTP 连接器的日志条目示例。本主题提供了 SFTP 连接器日志条目的示例，以及命名惯例，以帮助您找到相应的日志。

对 SFTP 连接和传输问题进行故障排除

本节介绍了 SFTP 连接和文件传输问题的可能解决方案。

主题

- 对 SFTP 连接问题进行故障排除
- 对 SFTP 客户端问题进行故障排除
- 文件上传问题进行故障排除
- 排除 VPC 出口类型 SFTP 连接器问题

对 SFTP 连接问题进行故障排除

描述

您的 SFTP 客户端无法启动连接。此问题可能持续发生，也可能间歇性发生。例如，您可能会在 SFTP 客户端调试日志中看到以下事件序列：

```
sftp -vvv username@1.1.1.1
.................................
debug1: Local version string ...........
kex_exchange_identification: read: Connection reset by peer
Connection reset by 1.1.1.1 port 22
Connection closed.
```

原因

在极端情况下，零字节 TCP ACK（无数据的 ACK）（也称为三次握手）要么被丢弃，要么被延迟。

解决方案

作为一种解决方法，Transfer Family 提供了一种解决方案，该解决方案使用不同的配置来解决此问题，但可能会导致与旧客户端的兼容性问题。因此，此解决方案仅在端口 2223 上可用。

在 VPC 中创建 Transfer Family 服务器的过程中（在虚拟私有云中创建服务器），当您指定安全组时，请将 SSH 流量配置为使用端口 2223。

对 SFTP 客户端问题进行故障排除

中描述了 SFTP 客户端消息。SFTP 消息解决 SFTP 客户端问题的最佳方法是查看 SFTP 客户端日志，如有必要，请联系您的网络管理员。

文件上传问题进行故障排除

本节介绍以下文件上传问题的可能解决方案。

主题

- 对 Amazon S3 文件上传错误进行故障排除
- 对无法读取的文件名称进行故障排除

对 Amazon S3 文件上传错误进行故障排除

描述

当您尝试使用 Transfer Family 将文件上传到 Amazon S3 存储空间时，您会收到如下错误消息：Amazon Transfer 不支持对 S3 对象进行随机访问写入。

原因

当您使用 Amazon S3 作为服务器存储空间时，Transfer Family 不支持单次传输的多个连接。

解决方案

如果您的 Transfer Family 服务器使用 Amazon S3 进行存储，请禁用任何提及使用多个连接进行单次传输的客户端软件选项。

对无法读取的文件名称进行故障排除

描述

您会在上传的某些文件中看到文件名已损坏。用户有时会在 FTP 和 SFTP 传输中遇到问题，这些问题会破坏文件名中的某些字符，例如变音符号、重音字母或某些脚本，例如中文或阿拉伯语。

原因

尽管 FTP 和 SFTP 协议允许客户端协商文件名的字符编码，但 Amazon S3 和 Amazon EFS 却不允许。相反，它们需要 UTF-8 字符编码。因此，某些字符无法正确呈现。

解决方案

要解决此问题，请查看您的客户端应用程序中的文件名字符编码，并确保将其设置为 UTF-8。

排除 VPC 出口类型 SFTP 连接器问题

如果您在使用 VPC 出口类型 SFTP 连接器时遇到问题，请检查以下内容：

连接器状态为 “待定”

描述

您的 VPC 出口类型连接器在创建后的几分钟内仍处于待处理状态，并 TestConnection 返回 “连接器不可用”。

原因

VPC 连接器的 DNS 解析在创建后可能需要几分钟才能完成。

解决方案

在尝试传输文件之前，请等待连接器状态变为 “活动”。这是 VPC 出口类型连接器的正常行为。

连接超时

描述

尝试连接 SFTP 服务器时，您的 VPC 出口类型连接器超时。

原因

安全组可能不允许您的资源网关子网和目标 SFTP 服务器之间的端口 22 上的流量。

解决方案

确认安全组允许您的资源网关子网和目标 SFTP 服务器之间的端口 22 上的流量。

资源配置错误

描述

由于资源配置问题，您的 VPC 出口类型连接器无法连接。

原因

资源配置可能指向错误的 IP 地址或 DNS 名称，或者资源网关可能与您的 SFTP 服务器（用于私有终端节点）不在同一 VPC 中。

解决方案

确保您的资源配置指向正确的 IP 地址或 DNS 名称，并且资源网关与您的 SFTP 服务器（用于私有终端节点）位于同一个 VPC 中。有关更多信息，请参阅《Amazon VPC Lattice User Guide》中的 Resource configurations。

公共端点问题

描述

您的 VPC 出口类型连接器无法连接到公有 SFTP 终端节点。

原因

对于公共终端节点，您必须在资源配置中使用 DNS 名称（而不是 IP 地址），并且您的 VPC 必须具有用于出站互联网访问的 NAT 网关。

解决方案

确保您在资源配置中使用的是 DNS 名称，而不是 IP 地址。确认您的 VPC 具有用于出站互联网访问的 NAT 网关。

可用区问题

描述

由于可用区域限制，您无法创建资源网关。

原因

资源网关要求子网位于至少 2 个可用区，但并非所有可用区都 AZs 支持 VPC Lattice。

解决方案

查看您所在地区支持的 VPC Lattice 可用区，并确保至少有 2 个支持子网。 AZs

对自定义身份提供商问题进行故障排除

本节介绍了 Transfer Family 中与自定义身份提供者相关的问题的可能解决方案。

主题

- 对 API Gateway 集成错误进行故障排除
- 对 Lambda 函数超时进行故障排除
- 解决持续的 Lambda 超时问题
- 排除KeyError异常问题

对 API Gateway 集成错误进行故障排除

描述

用户无法使用您的 Transfer Family 服务器进行身份验证，并且在测试您的身份提供商时，您会看到以下错误：

```
{
    "Response": "",
    "StatusCode": 500,
    "Message": "Internal server error"
}
```

原因

API Gateway 集成错误可能由以下原因导致：

- API Gateway 配置不正确
- 未正确处理 Lambda 函数错误
- API Gateway 和 Lambda 之间的权限问题
- 来自 Lambda 函数的响应格式不正确

解决方案

要排除 API Gateway 集成错误，请执行以下操作：

1. 查看您的 Lambda 函数日志，了解详细的错误信息：
   - 在 CloudWatch 控制台中，导航到日志组 >/aws/lambda/your-function-nam e
   - 查找指出根本原因的错误消息或堆栈跟踪
2. 验证您的 Lambda 函数返回的响应格式是否正确：

```
{
    "Role": "arn:aws:iam::123456789012:role/TransferUserRole",
    "HomeDirectory": "/mybucket/home/username"
}
```

3. 为 API Gateway 启用详细 CloudWatch 日志：
   - 在 API Gateway 控制台中，选择你的 API，然后选择阶段
   - 选择您的阶段，然后在 “日志/跟踪” 下启用 “日志” CloudWatch
   - 将日志级别设置为 “错误” 或 “信息”
4. 直接测试您的 API Gateway 终端节点：

```
curl -X POST https://your-api-id.execute-api.region.amazonaws.com/prod/servers/your-
server-id/users/username/config \
    -H "Content-Type: application/json" \
    -d '{"Password": "password"}'
```

5. 验证 API Gateway 和 Lambda 之间的权限：
   - 确保 API Gateway 有权调用您的 Lambda 函数
   - 检查您的 Lambda 函数的执行角色是否具有必要的权限

对 Lambda 函数超时进行故障排除

描述

当用户尝试使用自定义身份提供商向您的 Transfer Family 服务器进行身份验证时，他们会遇到长时间的延迟，然后是身份验证失败。在您的 Lambda 日志中，您会看到超时错误。

原因

用于自定义身份提供商的 Lambda 函数的默认超时时间为 3 秒。如果您的身份验证逻辑花费的时间超过此超时时间（例如，查询外部数据库或对第三方身份提供商进行 API 调用时），则该函数将超时，身份验证将失败。

解决方案

要解决 Lambda 超时问题，请执行以下操作：

1. 增加 Lambda 函数的超时时间：
   - 在 Lambda 控制台中，导航到您的函数并选择配置选项卡
   - 在 “常规配置” 下，单击 “编辑”
   - 增加超时值（对于身份验证功能，建议最多 15 秒）
2. 优化您的 Lambda 函数代码：
   - 使用连接池进行数据库查询
   - 为经常访问的数据实现缓存
   - 在身份验证期间尽量减少外部 API 调用
3. 考虑使用 Lambda 预配置并发来消除冷启动：

```
aws lambda put-provisioned-concurrency-config \
    --function-name my-authentication-function \
    --qualifier prod \
    --provisioned-concurrent-executions 5
```

4. 使用 CloudWatch 指标监控 Lambda 性能并为持续时间阈值设置警报

解决持续的 Lambda 超时问题

描述

使用 Lambda 函数进行身份验证时，用户会遇到持续的超时问题。

原因

Lambda 无法访问用于进行身份验证的相应 Amazon 服务（例如 DynamoDB、Secrets Manager 或其他身份提供商）。

解决方案

验证子网是否可以访问 Amazon 服务。或者，如果连接到互联网身份提供商（例如 Okta），请验证 Lambda 函数的子网是否可以通过 NAT 网关访问互联网

排除KeyError异常问题

描述

在你的 Transfer Family 日志条目中，你会注意到 KeyError “” 异常。

原因

最有可能的原因是用户或identity_provider记录格式错误或缺少必填字段。

解决方案

查看位于ERRORS日志组中的/aws/transfer/*your-server-id*日志以获取线索。

解决工作流程问题

本节介绍托管工作流程问题的可能解决方案。

主题

- 对托管工作流程问题进行故障排除
- 对工作流程解密问题进行故障排除

对托管工作流程问题进行故障排除

本节介绍以下工作流程问题的可能解决方案。

主题

- 使用 Amazon 解决与工作流程相关的错误 CloudWatch
- 对工作流程复制错误进行故障排除

使用 Amazon 解决与工作流程相关的错误 CloudWatch

描述

如果您的工作流程出现问题，可以使用 Amazon CloudWatch 来调查原因。

原因

可能有多种原因。使用 Amazon CloudWatch 日志进行调查。

解决方案

Transfer Family 会将工作流程执行状态发送到 CloudWatch 日志中。 CloudWatch 日志中可能会出现以下类型的工作流程错误：

- `"type": "StepErrored"`
- `"type": "ExecutionErrored"`
- `"type": "ExecutionThrottled"`
- `"Service failure on starting workflow"`

您可以使用不同的筛选器和模式语法来筛选工作流程的执行日志。例如，您可以在日志中创建日志过滤器，以捕获包含该ExecutionErrored消息的工作流程执行日志。 CloudWatch 有关详细信息，请参阅 Amazon Log CloudWatch s 用户指南中的使用订阅实时处理日志数据以及筛选和模式语法。

StepErrored

```
2021-10-29T12:57:26.272-05:00
            {"type":"StepErrored","details":
{"errorType":"BAD_REQUEST","errorMessage":"Cannot
            tag Efs file","stepType":"TAG","stepName":"successful_tag_step"},
            "workflowId":"w-
abcdef01234567890","executionId":"1234abcd-56ef-78gh-90ij-1234klmno567",
            "transferDetails":
{"serverId":"s-1234567890abcdef0","username":"lhr","sessionId":"1234567890abcdef0"}
```

此处，`StepErrored` 表示工作流程中的某个步骤产生了错误。在单个工作流程中，您可以配置多个步骤。此错误会告诉您错误发生在哪个步骤中，并提供错误消息。在此特定示例中，该步骤配置为标记文件；但是，不支持在 Amazon EFS 文件系统中标记文件，因此该步骤生成了一处错误。

ExecutionErrored

```
2021-10-29T12:57:26.618-05:00
            {"type":"ExecutionErrored","details":{},"workflowId":"w-w-
abcdef01234567890",
            "executionId":"1234abcd-56ef-78gh-90ij-1234klmno567","transferDetails":
{"serverId":"s-1234567890abcdef0",
            "username":"lhr","sessionId":"1234567890abcdef0"}}
```

当工作流程无法执行任何步骤时，它会生成 ExecutionErrored 消息。例如，如果您在给定工作流程中配置了单个步骤，并且该步骤无法执行，则整个工作流程将失败。

Executionthrottled

如果工作流程的触发速度超过系统所能支持的速度，则执行受到限制。此日志消息表明您必须降低工作流程的执行速度。如果您无法降低工作流程执行率，请通过 Contact 联系 Amazon Web Services 支持 。 Amazon

启动工作流程时服务失败

无论何时从服务器上移除工作流程并用新的工作流程替换它，或者更新服务器配置（这会影响工作流程的执行角色），都必须等待大约 10 分钟才能执行新的工作流程。Transfer Family 服务器会缓存工作流程细节，服务器需要 10 分钟才能刷新其缓存。

此外，您必须注销所有活动的 SFTP 会话，然后等待 10 分钟重新登录才能看到更改。

对工作流程复制错误进行故障排除

描述

如果您正在执行的工作流程中包含复制已上传文件的步骤，则可能会遇到以下错误：

```
{
  "type": "StepErrored", "details": {
    "errorType": "BAD_REQUEST", "errorMessage": "Bad Request (Service: Amazon S3;
 Status Code: 400; Error Code: 400 Bad Request;
    Request ID: request-ID; S3 Extended Request ID: request-ID Proxy: null)",
 "stepType": "COPY", "stepName": "copy-step-name" },
  "workflowId": "workflow-ID",
  "executionId": "execution-ID",
  "transferDetails": {
     "serverId": "server-ID",
     "username": "user-name",
     "sessionId": "session-ID"
```

```
  }
}
```

原因

源文件位于与目标存储桶不同 Amazon Web Services 区域 的 Amazon S3 存储桶中。

解决方案

如果您正在执行包含复制步骤的工作流程，请确保源存储桶和目标存储桶位于同一 Amazon Web Services 区域存储桶中。

对工作流程解密问题进行故障排除

本节介绍以下加密工作流程问题的可能解决方案。

主题

- 解决匿名收件人加密问题
- 解决签名加密文件出现的错误
- 对 FIPS 算法的错误进行故障排除

解决匿名收件人加密问题

描述

处理某些加密文件时，您的解密工作流程会失败，但可以处理其他加密文件。

原因

文件可能是在没有指定收件人的情况下加密的（匿名加密），这使得工作流程很难确定使用哪个密钥进行解密。

解决方案

始终使用`-r`参数对非匿名收件人进行文件加密。例如：

```
gpg -e -r user@example.com --openpgp file.txt
```

要检查文件是使用特定收件人加密还是匿名加密，请使用以下`--list-packets`命令：

```
gpg --list-packets file.txt.gpg
```

此命令显示 GPG 加密文件的数据包结构，而不对其内容进行解密。查找包含收件人信息的输出，例如：

```
:pubkey enc packet: version 3, algo 1, keyid 1A2B3C4D5E6F7G8H
```

如果您看到 keyid 信息，则表示该文件已针对特定收件人进行了加密。如果缺少此信息，则该文件可能已被匿名加密，这可能会导致 Transfer Family 工作流程中的解密失败。

您也可以使用此命令来验证：

- 使用了哪些加密算法
- 压缩方法（如果有）
- 创建时间戳

要查看 GPG 安装支持的密码算法列表，请使用：

```
gpg --version
```

这些信息可以帮助您确保使用的加密算法与 Transfer Family 工作流程兼容，尤其是在需要符合 FIPS 的情况下。

解决签名加密文件出现的错误

描述

您的解密工作流程失败，并且您收到以下错误：

```
"Encrypted file with signed message unsupported"
```

原因

Transfer Family 目前不支持对加密文件进行签名。

解决方案

在您的 PGP 客户端中，如果可以选择对加密文件进行签名，请务必清除该选项，因为 Transfer Family 目前不支持对加密文件进行签名。

对 FIPS 算法的错误进行故障排除

描述

解密工作流程失败，日志消息如下所示：

```
{
   "type": "StepErrored",
   "details": {
      "errorType": "BAD_REQUEST",
      "errorMessage": "File encryption algorithm not supported with FIPS mode
 enabled.",
      "stepType": "DECRYPT",
      "stepName": "step-name"
   },
   "workflowId": "workflow-ID",
   "executionId": "execution-ID",
   "transferDetails": {
      "serverId": "server-ID",
      "username": "user-name",
      "sessionId": "session-ID"
   }
}
```

原因

Transfer Family 服务器已启用 FIPS 模式和相关的解密工作流程步骤。在上传到 Transfer Family 服务器之前对文件进行加密时，加密客户端可能会生成使用非 FIPS 批准的对称加密算法的加密文件。在这种情况下，工作流程无法解密文件。在以下示例中，GnuPG 版本 2.4.0 使用 OCB（一种非 FIPS 分组密码模式）来加密文件：这会导致工作流程失败。

解决方案

您必须编辑用于加密文件的 GPG 密钥，然后对其重新加密。以下过程描述了您必须采取的步骤。

编辑 PGP 密钥

1. 通过运行 `gpg --list-keys` 来确定必须编辑的密钥

   这将返回密钥列表。每个密钥的详细信息类似于以下内容：

   ```
   pub   ed25519 2022-07-07 [SC]
   ```

```
      wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
uid           [ultimate] Mary Major <marymajor@example.com>
sub   cv25519 2022-07-07 [E]
```

2. 标识要编辑的密钥。在上一步所示的示例中，ID 为 wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY。
3. 运行 gpg --edit-key wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY。

   系统以有关 GnuPG 程序和指定密钥的详细信息进行响应。
4. 在 gpg> 提示符下，输入 showpref。将返回以下详细信息：

```
[ultimate] (1). Mary Major <marymajor@example.com>
   Cipher: AES256, AES192, AES, 3DES
   AEAD: OCB
   Digest: SHA512, SHA384, SHA256, SHA224, SHA1
   Compression: ZLIB, BZIP2, ZIP, Uncompressed
   Features: MDC, AEAD, Keyserver no-modify
```

   请注意，已列出存储在密钥上的首选算法。
5. 我们希望编辑密钥以保留除 OCB 之外的所有算法。运行 setpref 命令，指定要保留的所有算法：

```
gpg> setpref AES256, AES192,AES,3DES,SHA512, SHA384, SHA256, SHA224, SHA1,ZLIB,
 BZIP2, ZIP, Uncompressed
```

   这将返回以下详细信息：

```
Set preference list to:
     Cipher: AES256, AES192, AES, 3DES
     AEAD:
     Digest: SHA512, SHA384, SHA256, SHA224, SHA1
     Compression: ZLIB, BZIP2, ZIP, Uncompressed
     Features: MDC, Keyserver no-modify
Really update the preferences? (y/N)
```

6. 输入 y 进行更新，然后在系统提示确认更改时输入密码。
7. 保存更改。

```
gpg> save
```

在重新运行解密工作流程之前，必须使用编辑后的密钥重新加密文件。

对 EFS 问题进行故障排除

本节介绍了 Amazon EFS 存储问题的可能解决方案。

主题

- 对 Amazon EFS 问题进行故障排除

对 Amazon EFS 问题进行故障排除

本节介绍以下 Amazon EFS 问题的可能解决方案。

主题

- 对 Amazon EFS 服务托管用户进行故障排除
- 对缺失 POSIX 配置文件进行故障排除
- 使用 Amazon EFS 逻辑目录进行故障排除

对 Amazon EFS 服务托管用户进行故障排除

描述

运行 `sftp` 命令时，提示符未出现，而是会看到以下消息：

```
Couldn't canonicalize: Permission denied
           Need cwd
```

原因

您的 Amazon Identity and Access Management (IAM) 用户的角色无权访问亚马逊 Elastic File System (Amazon EFS)。

解决方案

增加用户角色的策略权限。您可以添加 Amazon 托管策略，例如`AmazonElasticFileSystemClientFullAccess`。

对缺失 POSIX 配置文件进行故障排除

描述

如果您在服务器上使用 Amazon EFS 存储，并且使用自定义身份提供商，则必须为 Amazon Lambda 函数提供 POSIX 配置文件。

原因

一个可能的原因是，我们为创建 Amazon Lambda支持的 Amazon API Gateway 方法提供的模板目前不包含 POSIX 信息。

如果您确实提供了 POSIX 信息，那么 Transfer Family 可能无法正确解析您用于提供 POSIX 信息的格式。

解决方案

请务必向 Transfer Family 提供 `PosixProfile` 参数的 JSON 元素。

例如，如果您使用的是 Python，则可以在解析 `PosixProfile` 参数的位置添加以下行：

```
if PosixProfile:
        response_data["PosixProfile"] = json.loads(PosixProfile)
```

或者，在中 JavaScript，您可以添加以下行，其中*`uid-value`*和*`gid-value`*是分别代表用户 ID (UID) 和组 ID (GID) 的整数，即 0 或大于 0 的整数：

```
PosixProfile: {"Uid": uid-value, "Gid": gid-value},
```

这些代码示例将 `PosixProfile` 参数作为 JSON 对象而非字符串发送到 Transfer Family。

此外 Amazon Secrets Manager，您还必须按如下方式存储`PosixProfile`参数。将 *`your-uid`* 和 *`your-gid`* 替换为您的 GID 和 UID 的实际值。

```
{"Uid": your-uid, "Gid": your-gid, "SecondaryGids": []}
```

使用 Amazon EFS 逻辑目录进行故障排除

描述

如果用户的主目录不存在，并且他们运行了 `ls` 命令，则系统会按如下方式做出响应：

```
sftp> ls
remote readdir ("/"): No such file or directory
```

原因

如果 Transfer Family 服务器使用 Amazon EFS，则必须先创建具有读写访问权限的用户主目录，然后用户才能在其逻辑主目录中工作。用户无法自己创建此目录，因为他们将缺乏 `mkdir` 对逻辑主目录的权限。

解决方案

对父目录具有管理访问权限的用户需要创建该用户的逻辑主目录。

对存储和加密问题进行故障排除

本节介绍存储和加密问题的可能解决方案。

主题

- 对加密 Amazon S3 存储桶的策略进行故障排除
- 对 ResourceNotFound 异常进行故障排除

对加密 Amazon S3 存储桶的策略进行故障排除

描述

您有一个加密的 Amazon S3 存储桶，用作您的 Transfer Family 服务器的存储空间。如果您尝试将文件上传到服务器，则会收到错误消息 `Couldn't close file: Permission denied`。

而且，如果您查看服务器日志，则会看到以下错误：

```
ERROR Message="Access denied" Operation=CLOSE Path=/bucket/user/test.txt BytesIn=13
ERROR Message="Access denied"
```

原因

您的 IAM 用户的策略没有权限访问加密存储桶。

解决方案

您必须在策略中指定其他权限才能授予所需的 Amazon Key Management Service (Amazon KMS) 权限。有关更多信息，请参阅 数据保护和加密。

对 ResourceNotFound 异常进行故障排除

描述

您会收到一条找不到资源的错误。例如，如果您运行 UpdateServer，可能会收到如下错误：

```
An error occurred (ResourceNotFoundException) when calling the UpdateServer operation:
 Unknown server
```

原因

收到ResourceNotFoundException消息的原因有多种。在大多数情况下，您在 API 命令中指定的资源不存在。如果您确实指定了现有资源，那么最有可能的原因是您的默认区域与资源的区域不同。例如，如果您的默认区域为 us-east-1，而您的 Transfer Family 服务器在 us-east-2 中，则您将收到未知资源异常。

有关设置默认区域的详细信息，请参阅使用 aws configure 进行快速配置。

解决方案

在 API 命令中添加区域参数，以明确指定在何处查找特定资源。

```
aws transfer -describe-server --server-id server-id --region us-east-2
```

对监控和警报问题进行故障排除

本节提供有关对监控和警报问题进行故障排除的信息 Amazon Transfer Family，包括 CloudWatch 指标缺失或不完整以及 EventBridge 事件缺失。

主题

- 对缺失或不完整的 CloudWatch 指标进行故障排除
- 解决丢失 EventBridge的事件

对缺失或不完整的 CloudWatch 指标进行故障排除

描述

CloudWatch 您的 Transfer Family 服务器的指标缺失、不完整或未按预期更新。

原因

指标缺失或不完整可能是由多种因素造成的：

- 记录配置问题
- 活动水平低，无法在预期的时间范围内生成指标
- 查看维度或时间范围不正确的指标

解决方案

要解决 CloudWatch 指标缺失或不完整的问题，请执行以下操作：

1. 确保已正确配置您的 Transfer Family 服务器的日志记录：
   - 在 Transfer Family 控制台中，在 “服务器详情” > “其他详细信息” > “记录角色” 下检查是否启用了日志记录。
   - 因此，日志记录角色具有必要的权限和信任关系。
2. 在 CloudWatch 控制台中查看指标时：
   - 使用正确的维度，例如服务器级别ServerId的指标
   - 调整时间范围以确保它涵盖活动时段
   - 检查你的输入是否正确 Amazon Web Services 区域
3. 在 Transfer Family 服务器上生成测试活动，确保指标正在生成。

解决丢失 EventBridge的事件

描述

您已将亚马逊 EventBridge 规则配置为捕获 Transfer Family 事件，但事件并未发送到您的目标目的地，也未触发预期的操作。

原因

EventBridge 事件丢失可能是由以下原因造成的：

- 事件模式配置不正确

- 事件目标的权限问题
- 服务限制或限制
- 由于服务器配置，未生成事件

解决方案

要对缺失 EventBridge 的事件进行故障排除：

1. 验证您的活动模式格式是否正确，以匹配 Transfer Family 事件：

```
{
  "source": ["aws.transfer"],
  "detail-type": ["Transfer State Change"],
  "detail": {
    "serverId": ["s-1234567890abcdef0"]
  }
}
```

2. 检查您的事件目标是否具有必要的权限：
   - 对于 Lambda 目标，请确保 Lambda 函数的资源策略允许调用它 EventBridge
   - 对于 SQS 目标，请验证队列策略是否 EventBridge 允许发送消息
   - 对于 SNS 目标，请确认主题策略允许 EventBridge 向其发布内容
3. 通过生成示例事件来测试您的规则：
   - 使用 EventBridge 控制台创建与您的模式相匹配的测试事件
   - 在你的 Transfer Family 服务器上执行应该会生成事件的操作
4. 启用 EventBridge 规则指标以监控规则调用和失败：

```
aws events put-rule --name "TransferStateChangeRule" --event-pattern '{...}' --state
 ENABLED --metrics-enabled
```

5. 查看 CloudWatch 日志，了解与事件传送失败相关的任何错误消息

解决跨区域传输问题

本节介绍与跨界传输文件相关的问题的可能解决方案 Amazon Web Services 区域。

主题

- 解决跨区域转移权限问题
- 解决跨区域传输性能问题

解决跨区域转移权限问题

描述

尝试使用 Transfer Family 工作流程在不同区域的 Amazon S3 存储桶之间传输文件时，您会遇到以下错误：

```
{
  "type": "StepErrored",
  "details": {
    "errorType": "BAD_REQUEST",
    "errorMessage": "Access Denied (Service: Amazon S3; Status Code: 403; Error Code:
 AccessDenied)",
    "stepType": "COPY",
    "stepName": "cross_region_copy"
  }
}
```

原因

跨区域传输需要源存储桶和目标存储桶的特定的 IAM 权限。您的 Transfer Family 服务器或工作流程使用的 IAM 角色可能没有足够的权限访问其他区域的存储桶。

解决方案

要解决跨区域转移权限问题，请执行以下操作：

1. 确保您的 IAM 角色同时拥有源存储桶和目标存储桶的权限：

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
```

```
      "Resource": "arn:aws:s3:::source-bucket-name/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource": "arn:aws:s3:::destination-bucket-name/*"
    }
  ]
}
```

2. 如果使用 KMS 加密，请为源 KMS 密钥和目标 KMS 密钥添加权限：

```
{
  "Effect": "Allow",
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey"
  ],
  "Resource": [
    "arn:aws:kms:source-region:account-id:key/source-key-id",
    "arn:aws:kms:destination-region:account-id:key/destination-key-id"
  ]
}
```

3. 确认两个区域的存储桶策略都允许从您的 Transfer Family 服务器的 IAM 角色进行访问
4. 对于跨账户转账，请确保配置了正确的跨账户权限

解决跨区域传输性能问题

描述

跨区域传输比预期慢得多，或者在大型文件传输期间会超时。

原因

跨区域传输本质上会涉及更大的延迟，并且可能会受到网络条件、文件大小和服务限制的影响。大文件或大量的小文件可能会导致性能下降。

解决方案

要提高跨区域传输性能，请执行以下操作：

- 对于大型文件，可以考虑使用 Amazon S3 Transfer Acceleration：

```
aws s3 cp --source-region us-east-1 --region us-west-2 \
    s3://source-bucket/large-file.zip s3://destination-bucket/large-file.zip \
    --acl bucket-owner-full-control --s3-accelerate
```

- 对于多个小文件，请在传输之前将它们一起批处理：
  - 使用压缩来合并多个文件
  - 使用 Amazon S3 批量操作进行大规模传输
- 考虑使用具有适当超时设置的 Transfer Family SFTP 连接器进行大型传输
- 对于重复传输，请考虑使用 Amazon S3 跨区域复制 (CRR) 而不是临时传输来复制数据
- 使用 Amazon CloudWatch 指标监控传输绩效以识别瓶颈

对 Terraform 部署问题进行故障排除

本节介绍与使用 Terraform 部署 Transfer Family 资源相关的问题的可能解决方案。有关 Transfer Family 的 Terraform 模块的一般信息，请参阅。Transfer Family terraform 模块

主题

- 对 Terraform 资源创建失败进行故障排除
- 对 Terraform 状态管理问题进行故障排除

对 Terraform 资源创建失败进行故障排除

描述

尝试使用 Terraform 创建 Transfer Family 资源时，你会遇到以下错误：

```
Error: error creating Transfer Server: InvalidRequestException: The request is not
 valid.
Error: error creating Transfer User: InvalidRequestException: Unable to create the user
 because the server endpoint type is incompatible with the home directory type.
```

原因

这些错误通常是由于配置参数不兼容或 Terraform 配置中缺少依赖项而发生的。常见原因包括：

- 端点类型和存储配置不兼容
- 缺少必需的 IAM 角色或策略
- 不正确的安全策略规范
- VPC 终端节点配置问题

解决方案

要解决 Terraform 部署问题，请执行以下操作：

- 确保你的 Terraform 配置使用兼容的参数组合：
  - 对于公共终端节点，请确保使用 Amazon S3 进行存储。
  - 对于 VPC 终端节点，请验证正确的 VPC 和安全组配置。
- 使用带有`depends_on`属性的显式依赖关系，以确保按正确的顺序创建资源。
- 确认所有 IAM 角色都具有必要的信任关系和权限。
- 使用最新版本的 Terraform Amazon 提供程序，确保与 Transfer Family 的所有功能兼容。
- 对于复杂的部署和简单的用例，可以考虑使用上 GitHub 提供的官方 Transfer Family Terraform 模块。https://github.com/aws-ia/terraform-aws-transfer-family这些模块提供了涵盖简单和复杂客户用例的大量示例，遵循 Amazon 最佳实践，并且可以为需要基础设施即代码 (IaC) 配置帮助的客户简化部署。

对 Terraform 状态管理问题进行故障排除

描述

在 Terraform 之外对 Transfer Family 资源进行更改后（通过控制台或 Amazon CLI），在运行`terraform plan`或时会遇到状态偏差或错误。`terraform apply`

原因

Terraform 维护着一个状态文件，用于跟踪其管理的资源。在 Terraform 之外进行更改时，状态文件会与实际资源不同步，从而在后续的 Terraform 操作中导致错误或意外行为。

解决方案

要解决使用 Transfer Family 资源的 Terraform 状态管理问题，请执行以下操作：

1. 用于`terraform import`将现有资源置于 Terraform 管理之下：

```
terraform import <transfer_family_server.example> s-<server-id>
terraform import <transfer_family_server.example> s-<server-id>/username
```

2. `terraform refresh`用于使用当前的真实基础架构更新状态文件
3. 对于无法导入或存在复杂状态问题的资源，可以考虑使用`terraform state rm`将其从状态文件中删除，然后使用 Terraform 重新创建它们
4. 实施一项政策，专门通过 Terraform 管理 Transfer Family 资源，以防止将来的状态漂移
5. 使用带锁定的远程状态存储，以防止在团队合作时同时进行修改

Web 应用程序防火墙集成问题疑难解答

本节介绍与Transfer Family集成 Amazon WAF 相关的问题的可能解决方案。

主题

- 排除 WAF 屏蔽合法流量的故障
- 对 WAF 与自定义身份提供商的集成进行故障排除

排除 WAF 屏蔽合法流量的故障

描述

Amazon WAF 使用您的 Transfer Family 端点进行配置后，合法用户将无法连接或遇到间歇性连接故障。您可能会在日志中看到 HTTP 403（禁止）响应。

原因

您的 Amazon WAF 规则可能过于严格或配置不正确，从而导致误报，从而阻止合法流量。常见原因包括：

- 无意中屏蔽公司网络的基于 IP 的规则或 VPNs
- 基于速率的规则，其阈值对于您的正常流量模式来说太低
- 对你的用例来说过于激进的托管规则组

解决方案

要解决误报问题，请执行以下操作：

1. 启用 Amazon WAF 日志记录功能以识别哪些规则触发了封锁。有关说明，请参阅记录 Amazon WAF Web ACL 流量。
2. 查看您的日志，找出被阻止的请求中的模式。
3. 通过以下方式调整您的规则：
   - 将 IP 地址或范围添加到许可名单
   - 提高基于费率的规则的速率限制
   - 将特定规则设置为 Count 模式而不是 Block 模式，以便在不阻塞的情况下进行监控
   - 使用规则组排除项为特定规则创建例外
4. 在完全部署之前，请使用具有代表性的合法流量样本测试更新的配置。

对 WAF 与自定义身份提供商的集成进行故障排除

描述

使用使用自定义身份提供程序的 Transfer Family 服务器进行配置 Amazon WAF 后，身份验证失败或用户会遇到间歇性的身份验证问题。

原因

在 API Gateway 中使用自定义身份提供商时， Amazon WAF 规则可能会干扰 Transfer Family 与您的身份提供商之间的 API 调用。之所以发生这种情况 Amazon WAF ，是因为正在根据其规则集检查并可能阻止 API 流量。

解决方案

要解决与自定义身份提供商有关的问题 Amazon WAF ，请执行以下操作：

- 确保您的 Amazon WAF 配置包括自定义身份提供商使用的 API Gateway 终端节点的例外情况。
- 将 Transfer Family 服务负责人 (transfer.amazonaws.com) 添加到规则的许可名单中。 Amazon WAF
- 如果使用托管规则组，请查看它们以了解可能影响 API 身份验证流程的规则，并考虑禁用这些特定规则。
- 使用 `TestIdentityProvider` API 操作直接测试您的身份提供商，以验证其在 Amazon WAF 不受干扰的情况下正常运行。

解决服务托管用户问题

本节介绍服务托管用户问题的可能解决方案。

主题

- 对服务托管用户进行故障排除

对服务托管用户进行故障排除

本部分介绍了以下问题的可能解决方案。

主题

- 对公有密钥正文过长进行故障排除
- 对添加 SSH 公有密钥失败进行故障排除

对公有密钥正文过长进行故障排除

描述

您在尝试创建服务托管用户时收到以下错误：

```
Failed to create user (1 validation error detected:
'sshPublicKeyBody' failed to satisfy constraint: Member must have length less than or
 equal to 2048)
```

原因

您可能正在为公钥正文输入 PGP 密钥，并且 Amazon Transfer Family 不支持服务托管用户的 PGP 密钥。

解决方案

如果 PGP 密钥是基于 RSA 的，则可以将其转换为 PEM 格式。例如，Ubuntu 在这里提供了一个转换工具：2ssh.1.html https://manpages.ubuntu.com/manpages/ jammy/en/man1/openpgp

对添加 SSH 公有密钥失败进行故障排除

描述

您在尝试为服务托管用户添加公有密钥时收到以下错误：

```
Failed to add SSH public key (Unsupported or invalid SSH public key format)
```

原因

您可能正在尝试导入 SSH2格式化的公钥，但服务托 Amazon Transfer Family 管用户不支持 SSH2格式化的公钥。

解决方案

您需要将密钥转换为 OpenSSH 格式。将 SSH2 密钥转换为 SSH 公钥格式 中介绍了此过程。

AS2 问题疑难解答

本节介绍 AS2 传输问题的可能解决方案。

主题

- AS2 问题疑难解答
- AS2 证书问题
- AS2 MDN 收据问题
- 证书过期监控问题

AS2 问题疑难解答

AS2 错误代码，本指南的 “ AS2 故障代码” 部分介绍了启用适用性声明 2 (AS2) 的服务器的消息和疑难解答提示。

AS2 证书问题

描述

您在转账时遇到了与证书相关的错误。 AS2

原因

常见原因包括证书过期、证书格式不正确或证书链不匹配。

解决方案

请尝试以下解决方案：

- 确认您的证书未过期
- 确保证书格式正确（PEM 用于 Amazon Transfer Family）
- 检查证书链是否完整且有效
- 确认贸易伙伴之间的签名证书和加密证书是否匹配
- 在证书到期之前尽早轮换证书，以避免中断

AS2 MDN 收据问题

描述

您没有收到预期的 AS2传输邮件处置通知 (MDNs)。

原因

MDN 问题可能是由于网络连接问题、端点配置不正确或 MDN 格式不匹配所致。

解决方案

考虑以下解决方案：

- 验证 MDN 网址配置正确且可访问
- 检查 AS2 服务器和 MDN 端点之间的网络连接
- 确保两个贸易伙伴都配置为相同的 MDN 类型（同步或异步）
- 查看 AS2 日志中是否存在任何与 MDN 处理相关的错误
- 如果使用同步 MDNs，请验证超时设置是否正确

证书过期监控问题

本节提供与证书过期监控和 DaysUntilExpiry 指标相关的常见问题的解决方案。

DaysUntilExpiry 指标未出现

问题：导入证书 CloudWatch 后，该 DaysUntilExpiry 指标在 Amazon 中不可见。

解决方案：

- 导入证书后最多等待 24 小时。Transfer Family 可能需要一整天的时间才能将该指标发送到你的账户。
- 确保你在正确的 Amazon 区域和AWS/Transfer命名空间下方查找 CloudWatch。

证书过期警报未触发

问题：证书过期 CloudWatch 警报未按预期触发。

解决方案：

- 验证警报是否配置了Maximum统计数据和 1 天的周期。
- 检查阈值比较是否设置Less than or equal to为所需的天数。
- 确保已Treat missing data as good (not breaching)在警报配置中选择该选项。
- 验证警报尺寸是否与您的证书 CertificateId和描述（如果提供）相匹配。
- 检查警报操作（SNS 主题、电子邮件通知）是否已正确配置并处于活动状态。

Amazon Transfer Family API 参考

Transfer Family 的完整 API 参考指南可在 Amazon Transfer Family API 参考中找到。

Amazon Transfer Family 是一项安全的传输服务，您可以使用它通过以下协议将文件传入和传出亚马逊简单存储服务 (Amazon S3) Storage Service 存储：

- Secure Shell (SSH) 文件传输协议 (SFTP)
- 安全文件传输协议 (FTPS)
- 文件传输协议 (FTP)
- 适用性声明 2 (AS2)

服务器、用户和角色均由其 Amazon 资源名称 (ARN) 标识。您可以为具有 ARN 的实体分配标签（键值对）。标签是可用于分组或搜索这些实体的元数据。标签有用的一个例子是用于会计目的。

在 Amazon Transfer Family ID 格式中应遵守以下惯例：

- `ServerId` 值采用 `s-01234567890abcdef` 形式。
- `SshPublicKeyId` 值采用 `key-01234567890abcdef` 形式。

Amazon 资源名称 (ARN) 格式采用以下形式：

- 对于服务器，ARNs 请使用表格`arn:aws:transfer:`*`region`*`:`*`account-id`*`:server/`*`server-id`*。

  服务器 ARN 的示例是：`arn:aws:transfer:us-east-1:123456789012:server/s-01234567890abcdef`。
- 对于用户，ARNs 请填写表格`arn:aws:transfer:`*`region`*`:`*`account-id`*`:user/`*`server-id`*`/`*`username`*。

  例如，`arn:aws:transfer:us-east-1:123456789012:user/s-01234567890abcdef/user1`。

正在使用的 DNS 条目（端点）如下所示：

- API 终端节点采用 `transfer.`*`region`*`.amazonaws.com` 形式。

- 服务器终端节点采用 `server.transfer.region.amazonaws.com` 形式。

此 API 接口参考 Amazon Transfer Family 包含可用于管理的编程接口的文档 Amazon Transfer Family。参考结构如下所示：

- 有关按字母顺序排列的 API 操作列表，请参阅 Actions.
- 有关按字母顺序排列的数据类型列表，请参见 Types.
- 有关常用查询参数的列表，请参阅常用参数。
- 有关错误代码的描述，请参阅常见错误。

> **Tip**
>
> 您可以将 `--generate-cli-skeleton` 参数与任何 API 调用一起使用来生成和显示参数模板，而不是实际运行命令。然后，您可以使用生成的模板进行自定义，并将其用作后续命令的输入。有关详细信息，请参阅生成并使用参数骨架文件。

的文档历史记录 Amazon Transfer Family

下表描述了此版本的文档 Amazon Transfer Family。

- API 版本：transfer-2018-11-05
- 最新文档更新：2025 年 11 月 19 日

更改	描述	日期
Transfer Family 网络应用程序支持 VPC 终端节点	Amazon Transfer Family Web 应用程序现在支持 VPC 托管的终端节点，允许您将 Web 应用程序终端节点托管在虚拟私有云中，以便在不通过公共互联网的情况下与 Amazon S3 进行私有数据传输。有关更多信息，请参阅 在 VPC 中创建 Transfer Family 网络应用程序。	2025 年 11 月 19 日
IPv6 支持	Amazon Transfer Family 现在支持 SFTP 公共端点的双栈（IPv4 和 IPv6）端点、SFTP/FTPS/FTP/AS 2 的 VPC 内部端点、SFTP 和连接器以及 AS2 API 端点。有关更多信息，请参阅 IPv6 支持 Transfer Family 服务器。	2025 年 6 月 30 日
SFTP 连接器用户体验的增强	• 能够为您的连接器提供自助式并发连接设置 • 能够提供 OpenSSH 格式的 SSH 私钥，用于对连接进行身份验证	2025 年 4 月 9 日

更改	描述	日期
	• 能够使用远程服务器的 SFTP 连接器发现其公共主机密钥 有关更多信息，请参阅 使用服务管理的出口创建一个 SFTP 连接器。	
SFTP 连接器能够删除、重命名和移动远程 SFTP 服务器上的文件	现在，您可以通过删除、重命名源文件或将源文件移至存档位置来整理存储在远程 SFTP 服务器上的文件。 有关更多信息，请参阅 移动或重命名远程 SFTP 服务器上的文件或目录。	2025 年 4 月 7 日
对 Amazon Transfer Family Web 应用程序的支持	Amazon Transfer Family 网络应用程序是一种新资源，客户可以使用它来创建通过网络浏览器访问其在 Amazon S3 中的数据的简单界面。有关更多信息，请参阅 Transfer Family 网络应用程序。	2024 年 12 月 1 日
将 API 参考移至单独的指南中	为了改善客户体验，API 参考现已与用户指南分开发布。有关单独的 API 参考，请参阅欢迎 Amazon Transfer Family 使用 API。	2024 年 7 月 31 日
SFTP 连接器能够列出远程文件和目录	Transfer Family 增加了我们的客户使用 SFTP 连接器列出存储在远程 SFTP 服务器中的文件的功能。有关详细信息，请参阅 列出远程目录的内容	2024 年 4 月 23 日

更改	描述	日期
能够使用贸易伙伴的自签名 TLS 证书进行 AS2消息交换	Amazon Transfer Family 增加了导入和使用贸易伙伴的公开自签名 TLS 证书的选项，用于通过 HTTPS 向其服务器发送适用性声明 2 (AS2) 消息。	2024 年 4 月 12 日
为 SFTP 连接器添加了安全策略	Amazon Transfer Family 添加了用于 SFTP 连接器的安全策略。有关更多信息，请参阅 Amazon Transfer Family SFTP 连接器的安全策略。	2024 年 4 月 5 日
与 Amazon 集成 EventBridge	Amazon Transfer Family 现在会自动将所有文件传输操作的事件发布到 Amazon EventBridge 。有关更多信息，请参阅 使用管理 Transfer Family 事件 Amazon EventBridge。	2024 年 2 月 8 日
增加了新的安全策略	Amazon Transfer Family 添加了新的 FIPS 和非 FIPS 安全策略。此外，分配给服务器的默认安全策略始终是最新的安全策略。有关更多信息，请参阅 Amazon Transfer Family 服务器的安全策略。	2024 年 2 月 5 日
Support 支持 SFTP 连接器的静态 IP 地址以及 AS2	Transfer Family 现在为 SFTP 连接器提供静态 IP 地址，以及。 AS2这样可以与受 IP 许可名单控制保护的远程 SFTP 服务器建立连接。因为 AS2，我们为来自 AS2 服务器的异步 MDN 响应引入了静态 IP 地址。	2024 年 1 月 16 日

更改	描述	日期
对用户指南进行了重新编排，使其与的最新版本更加一致。Amazon Transfer Family	自该指南问世以来，Transfer Family已经增加了多项功能，因此有必要对该指南进行重组。	2024 年 1 月 3 日
逻辑目录映射增强功能 亚马逊 S3 列表性能优化	Transfer Family 现在支持最大为 2.1 MB 的逻辑目录映射。现在，您还可以声明用户映射是否指向文件。有关更多信息，请参阅 使用逻辑目录的规则。 在创建或更新使用 Amazon S3 进行存储的服务器时，您现在可以优化列出 S3 目录（或文件夹）的性能。有关更多信息，请参阅 配置 SFTP、FTPS 或 FTP 服务器端点。	2023 年 11 月 17 日
带有虚拟私有云 (VPC) 端点的 SFTP 服务器的备用端口	现在，您可以为具有 VPC 终端节点的 SFTP Transfer Family 服务器启用备用非标准端口。有关更多信息，请参阅 在虚拟私有云中创建服务器。	2023 年 11 月 17 日
支持 SFTP 连接器	SFTP 连接器扩展了 Amazon Transfer Family 与云端和本地远程服务器通信的功能。有关更多信息，请参阅 使用 SFTP 连接器。	2023 年 7 月 25 日
Support 对 AS2 基本身份验证的支持	Transfer Family 现在支持对使用适用性声明 2 (AS2) 协议的服务器使用基本身份验证。有关更多信息，请参阅 AS2 连接器的基本身份验证。	2023 年 6 月 30 日

更改	描述	日期
支持结构化 JSON 日志记录	Transfer Family 现在支持向亚马逊 CloudWatch传送结构化 JSON 日志、将日志流分组到自定义日志组以及跨协议执行常见日志查询。有关更多信息，请参阅 Amazon Amazon Transfer Family 服务器 CloudWatch 登录。	2023 年 6 月 24 日
支持多种身份验证方法	Transfer Family 支持使用密码、 public/private 密钥对或两者进行身份验证。这适用于使用 SFTP 协议和自定义身份提供商的服务器。有关更多信息，请参阅 创建启用 SFTP 的服务器。	2023 年 5 月 17 日
支持对 Transfer Family 通过工作流程处理的文件进行 Pretty Good Privacy (PGP) 解密。	Transfer Family 内置了对 Prety Good Privacy (PGP) 解密的支持。您可以对通过 SFTP、FTPS 或 FTP 上传到 Amazon Simple Storage Service (Amazon S3) 或 Amazon Elastic File System (Amazon EFS) 的文件使用 PGP 解密。有关更多信息，请参阅生成 PGP 密钥和在工作流程中使用 PGP 解密。	2022 年 12 月 21 日
Transfer Family 服务器对适用性声明 2 (AS2) 文件传输协议的完全托管支持	您可以创建服务器，使用 AS2 协议向 Amazon 环境内部或外部的贸易伙伴发送和接收信息。有关更多信息，请参阅 正在配置 AS2。	2022 年 7 月 25 日

更改	描述	日期
支持在创建服务器时显示横幅	您可以在创建服务器时添加自定义消息。您可以显示预身份验证消息（所有协议）和身份验证后消息（适用于 FTP 和 FTPS 服务器）。有关更多信息，请参阅 创建启用 SFTP 的服务器、创建启用 FTPS 的服务器 或 创建启用 FTP 的服务器。	2022 年 2 月 17 日
Amazon Lambda 作为身份提供者 Support	现在，您可以使用他们的 Tr Amazon Lambda ansfer Family 服务器连接到自定义身份提供商。以前，您必须提供 Amazon API Gateway URL 才能集成自定义身份提供商。有关更多信息，请参阅 Amazon Lambda 用于整合您的身份提供商。	2021 年 11 月 16 日
支持托管文件传输工作流程	托管文件传输工作流程为您提供了当前手动执行的常见任务的上传后处理抽象。有关更多信息，请参阅 Amazon Transfer Family 托管工作流程。	2021 年 9 月 2 日
AWSTransferLoggingAccessV3：新策略	Amazon Transfer Family 添加了新的托管策略AWSTransferLoggingAccessV3，并弃用了该策略AWSTransferLoggingAccessV2。	2021 年 6 月 15 日

更改	描述	日期
Support Amazon Directory Service for Microsoft Active Directory	除了服务托管和自定义身份提供商之外，您现在还可以使用管理用户访问权限 Amazon Directory Service for Microsoft Active Directory 以进行身份验证和授权。有关更多信息，请参阅 使用微软 Active Directory 的 Amazon 目录服务。	2021 年 5 月 24 日
全新 Amazon Web Services 区域	Amazon Transfer Family 现已在非洲（开普敦）地区推出。有关对 Transfer Family 端点的更多信息，请参阅 Amazon Web Services 一般参考 中的 Amazon Transfer Family 端点和限额。	2021 年 2 月 24 日
全新 Amazon Web Services 区域	Amazon Transfer Family 现已在亚太地区（香港）和中东（巴林）地区推出。有关对 Transfer Family 端点的更多信息，请参阅 Amazon Web Services 一般参考 中的 Amazon Transfer Family 端点和限额。	2021 年 2 月 17 日
支持 Amazon EFS 作为数据存储	Transfer Family 现在支持文件传输进出 Amazon Elastic File System (Amazon EFS)。Amazon EFS 是一个简单、可扩展、完全托管的弹性 NFS 文件系统。有关更多信息，请参阅 配置 Amazon EFS 文件系统。	2021 年 1 月 6 日

更改	描述	日期
Support Amazon WAF	Transfer Family 现在支持 Amazon WAF Web 应用程序防火墙，可帮助保护网络应用程序和 API 操作免受攻击。有关更多信息，请参阅 添加 Web 应用程序防火墙。	2020 年 11 月 24 日
支持 Virtual Private Cloud (VPC) 中的多个安全组	现在，您可以将多个安全组附加到 VPC 中的一台服务器。有关更多信息，请参阅 在虚拟私有云中创建服务器。	2020 年 10 月 15 日
全新 Amazon Web Services 区域	Transfer Family 现已在各 Amazon GovCloud (US) 地区推出。有关 Amazon GovCloud (US) 区域的 Transfer Family 终端节点的更多信息，请参阅中的Amazon Transfer Family 终端节点和配额Amazon Web Services 一般参考。有关在 Amazon GovCloud (US) 各地区使用 Transfer Family 的信息，请参阅Amazon GovCloud (US) 用户指南Amazon Transfer Family中的。	2020 年 9 月 30 日
现在可以将支持加密算法的安全策略附加到您的服务器	现在，您可以将包含一组受支持的加密算法的安全策略附加到服务器。有关更多信息，请参阅 Amazon Transfer Family 服务器的安全策略。	2020 年 8 月 12 日

更改	描述	日期
支持联邦信息处理标准 (FIPS) 端点	启用 FIPS 的端点仅在北美 Amazon Web Services 区域可用。有关可用区域，请参阅 Amazon Web Services 一般参考 中的 Amazon Transfer Family 端点和限额。要为启用 SFTP 的服务器端点启用 FIPS，请参阅 创建启用 SFTP 的服务器。要为启用 FTPS 的服务器端点启用 FIPS，请参阅 创建启用 FTPS 的服务器。要为启用 FTP 的服务器端点启用 FIPS，请参阅 创建启用 FTP 的服务器。	2020 年 8 月 12 日
用户名字符长度增加和允许的其他字符	用户名现在可以包含 at 符号 (@) 和句点 (.)，并且最大长度可以为 100 个字符。要添加用户，请参阅 管理服务器端点的用户。	2020 年 8 月 12 日
支持自动创建亚马逊 CloudWatch 日志 Amazon Identity and Access Management (IAM) 角色	Transfer Family 现在支持自动创建 CloudWatch 日志 IAM 角色来查看最终用户活动。有关更多信息，请参阅 创建启用 SFTP 的服务器、创建启用 FTPS 的服务器 或 创建启用 FTP 的服务器。	2020 年 7 月 30 日

更改	描述	日期
Amazon Transfer Family 现在支持将源 IP 作为授权因素。	Transfer Family 增加了对使用最终用户的源 IP 地址作为授权因素的支持，使您在通过安全文件传输协议 (SFTP)、SSL (FTPS) 文件传输协议或文件传输协议 (FTP) 授权访问权限时，可以应用额外的安全层。有关更多信息，请参阅 使用自定义身份提供程序。	2020 年 6 月 9 日
Amazon SFTP 的传输功能现已启用， Amazon Transfer Family 并增加了对 FTP 和 FTPS 的支持。	现在，您可以使用另外两个协议来传输用户的文件：安全文件传输协议 (FTPS) 和文件传输协议 (FTP)。除了现有的安全文件传输协议 (SFTP) 支持外，用户还可以在其中移动、运行 Amazon、保护和集成基于 SSL 的 FTP (FTPS) 和基于纯文本 FTP 的工作流程。	2020 年 4 月 23 日
支持虚拟私有云 (VPC) 安全组和弹性 IP 地址	现在，您可以使用安全组为传入 IP 地址创建许可名单，从而为服务器提供额外的安全保护。您还可以将弹性 IP 地址与服务器的端点相关联。通过这样做，您可以让防火墙后面的用户允许访问该端点。有关更多信息，请参阅 在虚拟私有云中创建服务器。	2020 年 1 月 10 日

更改	描述	日期
支持在 VPC 中工作	您现在可在 VPC 中创建服务器。您可以使用您的服务器通过客户端与 Amazon S3 存储桶往返传输数据而不流经公共互联网。有关更多信息，请参阅 在虚拟私有云中创建服务器。	2019 年 3 月 27 日
Amazon Transfer Family 已发布的第一个版本。	此初始版本包括设置指令、描述如何入门，并提供有关客户端配置、用户配置和监控活动的信息。	2018 年 11 月 25 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。