aws

ONTAP 用户指南

FSx for ONTAP

FSx for ONTAP: ONTAP 用户指南

Table of Contents

什么是适用于 NetApp ONTAP 的 Amazon FSx？

适用于 NetApp ONTAP 的 Amazon FSx 是一项完全托管的服务，它基于 NetApp 广受欢迎的 ONTAP 文件系统提供高度可靠、可扩展、高性能和功能丰富的文件存储。FSx for ONTAP 将 NetApp 文件系统熟悉的特征、性能、功能和 API 操作与完全托管式 AWS 服务 的敏捷性、可扩展性和简单性相结合。

FSx for ONTAP 提供功能丰富、快速且灵活的共享文件存储，可在 AWS 或本地运行的 Linux、Windows 和 macOS 计算实例广泛访问。FSx for ONTAP 提供具有亚毫秒延迟的高性能固态硬盘（SSD）存储。借助 FSx for ONTAP，您在实现工作负载的 SSD 性能级别的同时，只需为一小部分数据支付 SSD 存储费用。

借助 FSx for ONTAP 可以更轻松地管理数据，因为您只需单击一下按钮即可对文件进行快照拍摄、克隆和复制。此外，FSx for ONTAP 会自动将您的数据分层到更低成本的弹性存储，从而减少了您对预置或管理容量的需求。

FSx for ONTAP 还提供高度可用且耐用的存储，提供完全托管的备份，并支持跨区域灾难恢复。为了更轻松地保护您的数据，FSx for ONTAP 支持常见的数据安全和防病毒应用程序。

对于在本地使用 NetApp ONTAP 的客户来说，FSx for ONTAP 是将基于文件的应用程序从本地迁移、备份或扩展到 AWS 的理想解决方案，而无需更改应用程序代码或数据管理方式。

作为一项完全托管式服务，FSx for ONTAP 可以更轻松地在云中启动和扩展可靠、高性能和安全的共享文件存储。借助 FSx for ONTAP，您不必再担心：

- 设置和预置文件服务器和存储卷
- 复制数据
- 安装和修补文件服务器软件
- 检测和解决硬件故障
- 管理失效转移和失效自动恢复
- 手动进行备份

FSx for ONTAP 还提供与其他 AWS 服务的丰富集成，例如 AWS Identity and Access Management（IAM）、Amazon WorkSpaces、AWS Key Management Service（AWS KMS）和 AWS CloudTrail。

主题

FSx for ONTAP 的功能

借助 FSx for ONTAP，您可以获得完全托管的文件存储解决方案，包括：

- 支持单个命名空间中的 PB 级数据集
- 每个文件系统的吞吐量可达数十千兆字节/秒（GBps）
- 使用网络文件系统（NFS）、服务器消息块（SMB）、互联网小型计算机系统接口（iSCSI）和非易失性存储规范（NVMe）协议对数据进行多协议访问
- 高度可用且耐用的多可用区和单可用区部署选项
- 自动数据分层，可根据您的访问模式自动将不常访问的数据转移到成本较低的存储层，从而降低存储成本
- 数据压缩、重复数据删除和压缩可减少存储消耗
- 支持两种网络类型选项，仅限 IPv4 和双堆栈（同时支持 IPv4 和 IPv6），以访问和管理文件系统
- 支持 NetApp 的 SnapMirror 复制功能
- 支持 NetApp 的 FlexCache 本地缓存解决方案
- 支持使用原生 AWS 或 NetApp 工具以及 API 操作进行访问和管理
  - AWS 管理控制台、AWS Command Line Interface（AWS CLI）和 SDK
  - NetApp ONTAP CLI、REST API 和 NetApp 控制台

安全与数据保护

采用责任共担模式，因为这与 适用于 ONTAP 的 Amazon FSx 中的安全 NetApp 有关。Amazon FSx 提供多个级别的安全性和合规性，便于保护您的数据。

FSx for ONTAP 支持以下数据保护、安全和访问控制功能：

- 使用 AWS KMS keys，为文件系统数据和备份加密静态数据

- 使用以下内容，加密传输中数据：
  - SMB Kerberos
  - IPSEC
  - 基于 Nitro 的加密
- 按需防病毒扫描
- 使用 Microsoft Active Directory 进行身份验证和授权
- 文件访问审计
- NetAppSnapLock WORM 支持 Compliance 保留模式和 Enterprise 保留模式

有关更多信息，请参阅 适用于 ONTAP 的 Amazon FSx 中的数据保护 NetApp 和 保护您的数据。

此外，Amazon FSx 还通过高度耐用的文件系统备份来保护您的数据。Amazon FSx 执行每日自动备份，您可以随时进行额外备份。有关更多信息，请参阅 保护您的数据。

监控工具

监控工具包括 CloudWatch、CloudTrail、ONTAP EMS events、NetApp Data Infrastructure Insights 和 NetApp Harvest。

FSx for ONTAP 的定价

文件系统的费用按以下类别来计费：

- SSD 存储容量（GB/月）
- 您预置的 SSD IOPS 超过 3IOPS/GB（IOPS/月）
- 吞吐能力（每兆字节每秒 [MBps]-月）
- 容量池存储消耗量（GB/月）
- 容量池请求（每次读取和写入）
- 备份存储消耗（GB/月）

有关与服务相关的定价和费用等信息，请参阅适用于 NetApp ONTAP 的 Amazon FSx 定价。

AWS re:Post 上的 FSx for ONTAP

如果您在使用 Amazon FSx 时遇到问题，可使用 AWS re:Post 获取 FSx for ONTAP 问题的答案。

您是首次使用 Amazon FSx 的用户吗？

如果您是首次使用 Amazon FSx，建议您按顺序阅读以下部分：

1. 如果您是首次使用 AWS，请参阅设置 FSx for ONTAP以设置 AWS 账户。
2. 如果您已准备好创建您的第一个 Amazon FSx 文件系统，请按照 开始使用适用于 ONTAP 的 Amazon FSx NetApp 中的说明进行操作。
3. 有关性能的信息，请参阅 适用于 ONTAP 性能的 Amazon FS NetApp x。
4. 有关 Amazon FSx 安全性详细信息，请参阅适用于 ONTAP 的 Amazon FSx 中的安全 NetApp。
5. 有关 Amazon FSx API 的更多信息，请参阅 Amazon FSx API 参考。

FSx 适用于 NetApp ONTAP 的 Amazon 是如何运作的

本主题介绍了 Amazon for NetApp ONTAP 文件系统的主要功能及其工作原理，并 FSx 提供了指向包含深入描述、重要实施细节和 step-by-step配置过程的章节的链接。

主题

FSx 适用于 ONTAP 文件系统

文件系统是 ONTAP 资源的主 FSx 系统，类似于本地 NetApp ONTAP 集群。您可以为文件系统指定固态硬盘（SSD）存储容量和吞吐能力，然后选择用于创建文件系统的 Amazon Virtual Private Cloud（VPC）。有关更多信息，请参阅 管理 FSx for ONTAP 文件系统。

根据配置，您的文件系统可以有 1 到 12 个高可用性（HA）对。HA 对由两台文件服务器组成，采用活动-备用配置。第一代 FSx ONTAP 文件系统和第二代多可用区文件系统支持一个 HA 对。第二代单可用区文件系统最多可支持 12 个 HA 对。有关更多信息，请参阅 管理高可用性（HA）对。

存储虚拟机

存储虚拟机（SVM）是一种独立的文件服务器，具有自己的管理和数据访问端点，用于管理和访问数据。当您访问 for ONTAP 文件系统中的数据时，您的客户端和工作站会使用 SVM 的端点 IP 地址与 SVM 进行交互。 FSx 有关更多信息，请参阅 管理 SVMs。

你可以加入 SVMs Microsoft 活动目录进行文件访问身份验证和授权。有关更多信息，请参阅 在 FSx ONTAP 中使用微软 Active Directory。

卷

FSx ONTAP 卷是用于组织和分组数据的虚拟资源。卷是托管在上的逻辑容器 SVMs，存储在其中的数据会消耗文件系统上的物理存储容量。

创建卷时，需要设置其大小，这决定了卷中可存储的物理数据量（无论数据存储在哪个存储层）。您还可以将卷类型设置为 RW（可读写）或 DP（数据保护）。DP 卷是只读的，可用作 NetApp SnapMirror 或 SnapVault 关系中的目的地。

FSx 因为 ONTAP 卷是精简配置的，这意味着它们仅消耗存储在其中的数据的存储容量。使用精简配置卷时，不会提前预留存储容量。相反，存储容量是根据需要动态分配的。删除卷或 LUN 中的数据后，可用空间将重新释放给文件系统。例如，您可以在配置了 10TiB 免费存储容量的文件系统上创建三个 10TiB 卷，只要三个卷中存储的总数据量在任何时候都不超过 10TiB 即可。卷上物理存储的数据量计入总体存储容量消耗量。有关更多信息，请参阅 管理 FSx ONTAP 卷。

存储层

FSx 适用于 ONTAP 的文件系统有两个存储层：主存储和容量池存储。主存储是预配置的可扩展高性能 SSD 存储，专为数据集的活动部分而构建。容量池存储是一个完全弹性的存储层，可扩展至 PB 级大小，并针对不经常访问的数据进行了成本优化。写入卷的数据会消耗存储层的容量。有关更多信息，请参阅 FSx 适用于 ONTAP 存储层。随着存储需求的增长，您可以增加文件系统的 SSD 存储容量。对于第二代文件系统，您还可以在高性能存储需求发生变化时减少 SSD 存储容量，从而优化存储成本。有关更多信息，请参阅 文件系统存储容量和 IOPS。

数据分层

数据分层是 Amazon FSx for NetApp ONTAP 自动在 SSD 和容量池存储层之间移动数据的过程。每个卷都有分层策略，可控制数据在变为非活动状态（冷）时是否将其移动到该容量层。卷分层策略的冷却期决定了数据何时变为非活动状态（冷）。有关更多信息，请参阅 卷数据分层。

存储效率

Amazon FSx NetApp for ONTAP 支持 ONTAP 的块级存储效率功能（压缩、压缩和重复数据删除），以减少数据消耗的存储容量。存储效率功能可以减少数据在 SSD 存储、容量池存储和备份中的占用空间。在不牺牲性能的情况下，通过对 SSD 和容量池存储层进行压缩、去重和紧凑处理，一般用于文件共享工作负载的存储容量通常可以节省 65%。有关更多信息，请参阅 存储效率。

访问 ONTAP 文件 FSx 系统上存储的数据

你可以通过 NFS（v3、v4、v4.1、v4.2）和 SMB 协议从多个 Linux、Windows 或 macOS 客户端同时访问 ONTAP 卷的数据。 FSx 您还可以使用非易失性存储器 Express (NVMe) 和互联网小型计算机系统接口 (iSCSI) 块协议访问数据。有关更多信息，请参阅 访问您的 fo FSx r ONTAP 数据。

管理 FSx ONTAP 资源

您可以通过多种方式与 for ONTAP 文件系统进行交互并管理其资源。 FSx 您可以使用这两种工具和 ONTAP 管理工具来管理您 FSx 的 f NetApp o AWS r ONTAP 资源：

- AWS 管理工具
  - 的 AWS 管理控制台
  - 的 AWS Command Line Interface (AWS CLI)
  - 亚马逊 FSx API 和 SDKs
  - AWS CloudFormation
- NetApp 管理工具：
  - NetApp 控制台
  - NetApp ONTAP CLI
  - NetApp ONTAP REST API

有关更多信息，请参阅 管理资源。

开始使用适用于 ONTAP 的 Amazon FSx NetApp

了解如何开始使用适用于 ONTAP 的 Amazon FSx。 NetApp 此入门练习包括以下步骤。

1. 注册 AWS 账户 并在该帐户中创建管理员用户。
2. 使用亚马逊 FSx 控制台创建适用于 NetApp ONTAP 文件系统的亚马逊 FSx。
3. 从 Amazon EC2 Linux 实例挂载文件系统。
4. 清理您创建的资源。

主题

设置 FSx for ONTAP

在您首次使用 Amazon FSx 之前，请完成以下任务。

主题

注册获取 AWS 账户

首先 AWS，你需要一个 AWS 账户。有关创建的信息 AWS 账户，请参阅《AWS 账户管理 参考指南》 AWS 账户中的入门指南。

后续步骤

要开始使用 FSx for ONTAP，请参阅 开始使用适用于 ONTAP 的 Amazon FSx NetApp 获取有关创建 Amazon FSx 资源的说明。

创建适用于 NetApp ONTAP 文件系统的亚马逊 FSx

Amazon FSx 控制台有两个用于创建文件系统的选项：快速创建和标准创建。要使用服务推荐的配置快速轻松地创建适用于 NetApp ONTAP 的 Amazon FSx 文件系统，请使用快速创建选项。

快速创建选项将此文件系统配置为允许 Linux 实例通过网络文件系统（NFS）协议访问数据。创建文件系统后，您可以根据需要创建其他 SVM 和卷，包括加入 Active Directory 的 SVM，以允许 Windows 和 macOS 客户端通过服务器消息块（SMB）协议进行访问。您还可以根据所选择的部署类型以及创建时添加的 HA 对数量，添加其他高可用性（HA）对。

> **Note**
>
> 使用快速创建选项创建的 FSx for ONTAP 文件系统使用 `IPv4` 的网络类型。要借助 `Dual-stack` 的 网络类型（同时支持 IPv4 和 IPv6）创建文件系统，请使用标准创建选项。

有关使用标准创建选项创建具有自定义配置的文件系统以及使用 AWS CLI 和 API 的信息，请参阅创建文件系统。

要创建文件系统，请执行以下操作：

1. 打开 Amazon FSx 控制台，网址为。https://console.aws.amazon.com/fsx/
2. 在控制面板上，选择创建文件系统以启动文件系统创建向导。
3. 在 “选择文件系统类型” 页面上，选择 “适用于 NetApp ONTAP 的 Amazon FSx”，然后选择 “下一步”。系统显示创建 ONTAP 文件系统页面。
4. 对于创建方法，选择标准创建。
5. 在快速配置部分中，对于文件系统名称 – 可选，输入文件系统的名称。命名文件系统能让您更轻松地进行查找和管理。您最多可以使用 256 个 Unicode 字母、空格和数字以及这些特殊字符：+ - （连字符）= . _（下划线）: /
6. 对于部署类型，选择Multi-AZ或Single-AZ。

   - Multi-AZ文件系统可以复制您的数据，并支持在同一个可用区内跨多个可用区进行故障转移 AWS 区域。
   - Single-AZ文件系统可以复制您的数据，并在单个可用区内提供自动故障切换。

   有关更多信息，请参阅 可用性、持久性和部署选项。

> **Note**
>
> 默认情况下，会选择可供您 AWS 区域 使用的适用于 ONTAP 文件系统的最新一代 FSx。您可以使用 “标准创建” 选项指定文件系统的生成（如果可用 AWS 区域）。有关更多信息，请参阅 创建文件系统。

7. 对于 SSD 存储容量，请指定文件系统的存储容量，以吉字节（GiB）为单位。输入 1024 – 1048576 内的任意整数。有关更多信息，请参阅 创建文件系统（控制台）。

   创建文件系统后，您可以根据需要随时增加存储容量。有关更多信息，请参阅 管理存储容量。

8. 对于吞吐能力，Amazon FSx 根据 SSD 存储自动提供推荐的吞吐能力。您还可以选择文件系统的吞吐量（根据部署类型和 HA 对的数量，最高可达 73,728 MBps）。

9. 对于虚拟私有云（VPC），请选择要与文件系统关联的 Amazon VPC。

10. （Multi-AZ 仅限）端点 IP 地址范围指定创建用于访问文件系统的端点的 IP 地址范围。

    端点 IP 地址范围选择快速创建选项：

    - VPC 中未分配的 IPv4 地址范围：选择此选项以允许 Amazon FSx 使用 VPC 的主要 CIDR 范围中的最后 64 个 IP 地址作为文件系统的端点 IPv4 地址范围。请注意，如果您多次选择此选项，则将在多个文件系统间共享此范围。

      > **Note**
      >
      > - 您创建的每个文件系统都会使用该范围内的两个 IP 地址，一个用于集群，一个用于第一个 SVM。第一个和最后一个 IP 地址也被保留。每增加一个 SVM，文件系统就会再使用一个 IP 地址。例如，托管 10 个 SVM 的文件系统使用 11 个 IP 地址。其他文件系统的工作方式与此相同。它们使用两个初始 IP 地址，每个额外的 SVM 使用一个 IP 地址。使用相同 IP 地址范围（每个都有一个 SVM）的文件系统的最大数量为 31。
      > - 如果子网正在使用 VPC 主要 CIDR 范围中最后 64 个 IP 地址中的任何一个，则此选项将显示为灰色。

    - V@@ PC 之外的浮动 IPv4 地址范围 — 选择此选项可让 Amazon FSx 使用 198.19.x。 0/24 具有相同 VPC 和路由表的任何其他文件系统尚未使用的地址范围。

您也可以在标准创建选项中指定自己的 IP 地址范围。只要不与任何子网重叠，而且尚未经具有相同 VPC 和路由表的其他文件系统使用，您选择的 IP 地址范围可以在 VPC 的 IPv4 地址范围内，也可以在 VPC 的 IPv4 地址范围外。我们建议使用在 VPC 的 IP 地址范围内的范围。

> **Note**
>
> 确保您使用的所有路由表都与您的 Multi-AZ 文件系统相关联。这样做有助于防止失效转移期间出现不可用问题。有关将 Amazon VPC 路由表与文件系统关联的信息，请参阅 更新文件系统。

11. 在存储效率中，选择已启用来启用 ONTAP 存储效率功能（压缩、重复数据删除和紧凑处理），或选择已禁用来禁用此功能。
12. 选择下一步，检查创建 ONTAP 文件系统页面的文件系统配置。请注意创建文件系统后可以修改的文件系统设置。
13. 选择创建文件系统。

快速创建会创建一个包含一个 SVM（名为 `fsx`）和一个卷（名为 `vol1`）的文件系统。该卷的连接路径为 `/vol1`，容量池分层策略为自动（这会自动将所有 31 天内未访问的数据分层到成本较低的容量池存储）。默认快照策略被分配给默认卷。使用您的默认服务托管密 AWS KMS 钥对文件系统数据进行静态加密。

创建微软 Active Directory-joined SVM

创建文件系统后，您可以创建已加入 Microsoft Active Directory 的其他 SVM，以允许 SMB 从 Windows 和 macOS 客户端进行访问。FSx for ONTAP 与 AWS Secrets Manager 集成，以便安全地管理 Microsoft Active Directory 域加入服务账户凭证。

创建 Microsoft Active Directory-joined SVM

1. 在 Amazon FSx 控制台中，从左侧导航窗格中选择存储虚拟机。
2. 选择创建存储虚拟机。
3. 对于文件系统，选择要创建的文件系统。
4. 对于存储虚拟机名称，输入 SVM 的名称。
5. 对于 Microsoft Active Directory 配置，选择加入 Microsoft Active Directory。

6. 对于域加入服务账户凭证，选择在 Secrets Manager 中托管（默认），以使用 Secrets Manager 实现安全的凭证管理。

> **Note**
>
> 使用 Secrets Manager，则无需存储纯文本凭证，并可提供集中式凭证管理。有关更多信息，请参阅 使用存储活动目录凭证 AWS Secrets Manager。

7. 对于密钥，从 Secrets Manager 中选择包含域加入服务账户凭证的现有密钥，或者选择创建新密钥以创建密钥。
8. 根据您的环境需要填写其余的 Microsoft Active Directory 配置字段。
9. 选择创建存储虚拟机。

SVM 将使用存储在 Secrets Manager 中的凭证进行创建并加入 Microsoft Active Directory。现在，您可以在此 SVM 上创建 SMB 共享和卷，用于访问 Windows 和 macOS 客户端。

从 Amazon EC2 Linux 实例挂载文件系统

您可以从 Amazon Elastic Compute Cloud（Amazon EC2）实例挂载您的文件系统。此过程使用运行 Amazon Linux 2 的实例。

从 Amazon EC2 挂载文件系统

1. 打开位于 https://console.aws.amazon.com/ec2/ 的 Amazon EC2 控制台。
2. 创建或选择一个运行 Amazon Linux 2 的 Amazon EC2 实例，该实例与文件系统在同一个虚拟私有云（VPC）中。有关启动实例的更多信息，请参阅《Amazon EC2 用户指南》中的步骤 1：启动实例。
3. 连接到 Amazon EC2 Linux 实例。有关更多信息，请参阅《Amazon EC2 用户指南》中的连接到 Linux 实例。
4. 使用 Secure Shell（SSH）在 Amazon EC2 实例上打开终端，然后使用相应的凭证登录。
5. 使用以下命令在您的 Amazon EC2 实例上创建一个用作卷挂载点的目录。在以下示例中，*mount-point*用您自己的信息替换。

```
$ sudo mkdir /mount-point
```

6. 将适用于 NetApp ONTAP 的 Amazon FSx 文件系统挂载到您创建的目录中。使用类似于下面示例的 mount 命令。在以下示例中，将占位符值替换为您自己的信息。

- *nfs_version* – 您正在使用的 NFS 版本；FSx for ONTAP 支持版本 3、4.0、4.1 和 4.2。
- *nfs-dns-name* – 待挂载的卷所在的存储虚拟机（SVM）的 NFS DNS 名称已存在。您可以在 Amazon FSx 控制台中找到 NFS DNS 名称，方法是选择虚拟存储机，然后选择待挂载的卷所在的 SVM。NFS DNS 的名称位于端点面板上。
- *volume-junction-path* – 待挂载的卷的连接路径。您可以在 Amazon FSx 控制台的卷详情页面的摘要面板上找到卷的连接路径。
- *mount-point* – 您在 EC2 实例上为卷挂载点创建的目录的名称。

```
sudo mount -t nfs -o nfsvers=nfs_version nfs-dns-name:/volume-junction-path /mount-point
```

以下命令使用的是示例值。

```
sudo mount -t nfs -o nfsvers=4.1 svm-abcdef1234567890c.fs-012345abcdef6789b.fsx.us-east-2.amazonaws.com:/vol1 /fsxN
```

如果您的 Amazon EC2 实例遇到问题（例如连接超时），请参阅《Amazon EC2 用户指南》中的 EC2 实例问题排查。

清理资源

完成本练习后，您应按照以下步骤清理资源并保护您的 AWS 账户。

清理资源

1. 在 Amazon EC2 控制台上，终止您的实例。有关更多信息，请参阅《Amazon EC2 用户指南》中的终止实例。
2. 打开 Amazon FSx 控制台，网址为。https://console.aws.amazon.com/fsx/
3. 在 Amazon FSx 控制台上，删除所有非 SVM 根卷的 FSx for ONTAP 卷。有关更多信息，请参阅删除卷。
4. 删除所有 FSx for ONTAP SVM。有关更多信息，请参阅 删除存储虚拟机（SVM）。
5. 在 Amazon FSx 控制台上，删除您的文件系统。删除文件系统时，会自动删除所有自动备份。但是，您仍须删除所有手动创建的备份。下面概括了该进程的具体步骤。

a. 从控制台控制面板中，选择您要为此练习创建的文件系统的名称。
b. 对于操作，选择删除文件系统。
c. 在删除文件系统对话框的文件系统 ID 框中输入要删除的文件系统的 ID。
d. 选择删除文件系统。
e. 当 Amazon FSx 删除文件系统时，其在控制面板中的状态会更改为 DELETING。删除文件系统后，它将不再出现在控制面板中。所有自动备份都将与文件系统一起删除。
f. 现在，您可以删除为文件系统手动创建的任何备份。从左侧导航窗格中，选择备份。
g. 在控制面板中，选择与您删除的文件系统具有相同文件系统 ID 的所有备份，然后选择删除备份。如果您创建了最终备份，请务必保留。
h. 系统将打开删除备份对话框。选中要删除的备份的 ID 对应的复选框，然后选择删除备份。

现在，您的 Amazon FSx 文件系统和所有相关的自动备份以及您选择删除的所有手动备份都已删除。

可用性依据 AWS 区域

适用于 NetApp ONTAP 文件系统的 Amazon FSx 有以下版本 AWS 区域，并指出了每个区域的部署类型支持：

AWS 区域	Single-AZ 1	Multi-AZ 1	Single-AZ 2	Multi-AZ 2		
美国东部（弗吉尼亚州北部）	✓	✓	✓	✓		
美国东部（俄亥俄州）	✓	✓	✓	✓		
美国西部（北加利福尼亚）	✓	✓	✓	✓		
美国西部（俄勒冈州）	✓	✓	✓	✓		
AWS GovCloud (US-East)	✓	✓				
AWS GovCloud (US-West)	✓	✓	✓	✓		
非洲（开普敦）	✓	✓				
亚太地区（香港）	✓	✓				

AWS 区域	Single-AZ 1	Multi-AZ 1	Single-AZ 2	Multi-AZ 2		
亚太地区（东京）	✓	✓	✓	✓		
亚太地区（首尔）	✓	✓	✓	✓		
亚太地区（大阪）	✓	✓				
亚太地区（孟买）	✓	✓	✓	✓		
亚太地区（海得拉巴）	✓	✓	✓	✓		
亚太地区（新加坡）	✓	✓	✓	✓		
亚太地区（悉尼）	✓	✓	✓	✓		
亚太地区（雅加达）	✓	✓				
亚太地区（墨尔本）	✓	✓				
亚太地区（马来西亚）	✓	✓				
亚太地区（新西兰）	✓	✓				

AWS 区域	Single-AZ 1	Multi-AZ 1	Single-AZ 2	Multi-AZ 2		
亚太地区（台北）	✓	✓				
亚太地区（泰国）	✓	✓				
加拿大（中部）	✓	✓	✓	✓		
加拿大西部（卡尔加里）	✓	✓				
欧洲地区（法兰克福）	✓	✓	✓	✓		
欧洲（苏黎世）	✓	✓	✓	✓		
欧洲地区（斯德哥尔摩）	✓	✓	✓	✓		
欧洲地区（米兰）	✓	✓				
欧洲（西班牙）	✓	✓	✓	✓		
欧洲地区（爱尔兰）	✓	✓	✓	✓		
欧洲地区（伦敦）	✓	✓	✓	✓		

AWS 区域	Single-AZ 1	Multi-AZ 1	Single-AZ 2	Multi-AZ 2		
Europe (Paris)	✓	✓				
以色列（特拉维夫）	✓	✓				
墨西哥（中部）	✓	✓				
中东（阿联酋）：	✓	✓				
中东（巴林）	✓	✓				
南美洲（圣保罗）	✓	✓	✓	✓		

访问您的 fo FSx r ONTAP 数据

您可以在本地和本地环境中使用各种支持的客户端和方法访问您的 Amazon FSx 文件系统。 AWS Cloud

每个 SVM 都有四个端点，用于使用 NetApp ONTAP CLI 或 REST API 访问数据或管理 SVM：

- `Nfs`：用于使用网络文件系统（NFS）协议进行连接
- `Smb`：用于使用服务消息块（SMB）协议进行连接（如果您的 SVM 已加入 Active Directory，或者您正在使用工作组。）
- `Iscsi`：用于使用 Internet 小型计算机系统接口（iSCSI）协议进行连接，支持共享块存储。
- `Nvme`— 用于使用非易失性存储器 Express (NVMe) TCP/IP 进行连接，以支持共享块存储。
- `Management`— 用于 SVMs 使用 NetApp ONTAP CLI、API 或控制台进行 NetApp 管理

> **Note**
>
> iSCSI 协议适用于所有拥有 6 个或更少的高可用性（HA）对的文件系统。该 NVMe/TCP 协议适用于具有 6 个或更少 HA 对的第二代文件系统。

主题

- 为 Linux 配置 NVMe/TCP
- 通过 Amazon S3 接入点访问您的数据
- 访问来自其他 AWS 服务的数据

支持的客户端

FSx for ONTAP 文件系统支持访问来自各种计算实例和操作系统的数据。它通过支持使用网络文件系统（NFS）协议（v3、v4.0、v4.1 和 v4.2）、所有版本的服务器消息块（SMB）协议（包括 2.0、3.0 和 3.1.1）以及 Internet 小型计算机系统接口（iSCSI）协议进行访问来实现这一点。

> **Important**
>
> Amazon FSx 不支持从公共互联网访问文件系统。Amazon FSx 会自动分离任何弹性 IP 地址，该地址是可从互联网访问的公有 IP 地址，该地址连接到文件系统的弹性网络接口。

ONTAP 支持以下 AWS 计算实例与 ONTAP 一起 FSx 使用：

- 运行支持 NFS 或 SMB 的 Linux、Microsoft Windows 和 macOS 的 Amazon Elastic Compute Cloud（Amazon EC2）实例。有关更多信息，请参阅 在 Linux 客户端上挂载卷 在 Microsoft Windows 客户端上挂载卷 和 在 macOS 客户端上挂载卷。
- Amazon EC2 Windows 和 Linux 实例上的 Amazon Elastic Container Service（Amazon ECS）Docker 容器。有关更多信息，请参阅 将亚马逊弹性容器服务与 ONTAP FSx 配合使用。
- 亚马逊 ELastic Kubernetes Service — 要了解更多信息，请参阅亚马逊 EKS 用户指南中的 FSx 亚马逊 NetApp ONTAP CSI 驱动程序。
- 开启红帽 OpenShift 服务 AWS (ROSA) — 要了解更多信息，请参阅红帽 OpenShift 服务在做什么 AWS？ 在《红帽 OpenShift 服务 AWS 用户指南》中。
- 亚马逊 WorkSpaces 实例。有关更多信息，请参阅 将 Amazon WorkSpaces 与 FSx for ONTAP 配合使用。
- 亚马逊 AppStream 2.0 实例。
- AWS Lambda — 有关更多信息，请参阅 AWS 博客文章使用 Amazon 为无服务器工作负载启用 SMB 访问权限。 FSx
- 在 VMware 云端 AWS 环境中运行的虚拟机 (VMs)。有关更多信息，请参阅《使用亚马逊 NetApp ONTAP 版部署指南》将 FSx 适用于 ONTAP AWS 的亚马逊配置 FSx 为外部存储和 NetApp 开启 VMware 云。

装载后， FSx ONTAP 文件系统在 NFS 和 SMB 上显示为本地目录或驱动器号，提供完全托管的共享网络文件存储，最多可由成千上万个客户机同时访问。通过 iSCSI 挂载时，iSCSI LUN 可以作为块设备进行访问。

使用块存储协议

Amazon FSx NetApp for ONTAP 支持互联网小型计算机系统接口 (iSCSI) 和基于 TCP 的非易失性内存 Express (NVMe) （ NVMe/TCP) block storage protocols. In Storage Area Network (SAN) environments, storage systems are targets that have storage target devices. For iSCSI, the storage target devices are referred to as logical units (LUNs). For NVMe/TCP，存储目标设备称为命名空间）。

您可以使用 SVM 的 iSCSI 逻辑接口 (LIF) 连接两者和 NVMe iSCSI 块存储。

您可以通过为 iSCSI 创建和 LUNs 为创建命名空间来配置存储。 NVMe LUNs 然后，主机可以使用 iSCSI 或 TCP 协议访问命名空间。

有关配置 iSCSI 和 NVMe/TCP 块存储的更多信息，请参阅：

- 为 Linux 配置 iSCSI
- 为 Windows 配置 iSCSI
- 为 Linux 配置 NVMe/TCP

从内部访问数据 AWS Cloud

每个亚马逊 FSx 文件系统都与虚拟私有云 (VPC) 关联。无论可用区在哪里，您都可以从文件系统 VPC 中的任何位置访问您的 for ONTAP 文件系统。 FSx 您也可以从其他帐户访问您的文件系统 VPCs ，这些帐户可能位于不同的 AWS 帐户或 AWS 区域. 除了以下各节中描述的访问 FSx ONTAP 资源的要求外，您还需要确保配置文件系统的 VPC 安全组，以便数据和管理流量可以在文件系统和客户端之间流动。有关为使用所需端口配置安全组的更多信息，请参阅 Amazon VPC 安全组。

访问同一 VPC 中的数据

创建 FSx 适用于 NetApp ONTAP 的亚马逊文件系统时，您可以选择该文件系统所在的亚马逊 VPC。与 Amazon FSx for NetApp ONTAP 文件系统关联的所有 SVMs 和卷也位于同一 VPC 中。挂载卷时，如果文件系统和装载卷的客户端位于同一 VPC 中 AWS 账户，则可以使用 SVM 的 DNS 名称和卷连接或 SMB 共享，具体取决于客户端。

如果客户端和卷与文件系统的子网位于同一个可用区，或者多可用区文件系统的首选子网中，则可以实现最佳性能。要识别文件系统的子网或首选子网，请在 Amazon FSx 控制台中选择 “文件系统”，然后选择要安装其卷的 ONTAP 文件系统，子网或首选子网（多可用区）将显示在 “子网” 或 “首选子网” 面板中。

从部署 VPC 外部访问数据

本节介绍如何从文件系统的部署 VPC 之外的 AWS 位置访问 FSx 适用于 ONTAP 文件系统的终端节点。

访问多可用区文件系统上的 NFS、SMB 和 ONTAP 管理端点

Amazon 上 FSx 适用于 ONTAP 多可用区文件系统的 NFS、SMB 和 NetApp ONTAP 管理终端节点使用浮动互联网协议 (IP) 地址，因此在故障转移事件期间，连接的客户端可以在首选文件服务器和备用文件服务器之间无缝切换。有关失效转移的更多信息，请参阅FSx for ONTAP 失效转移过程。

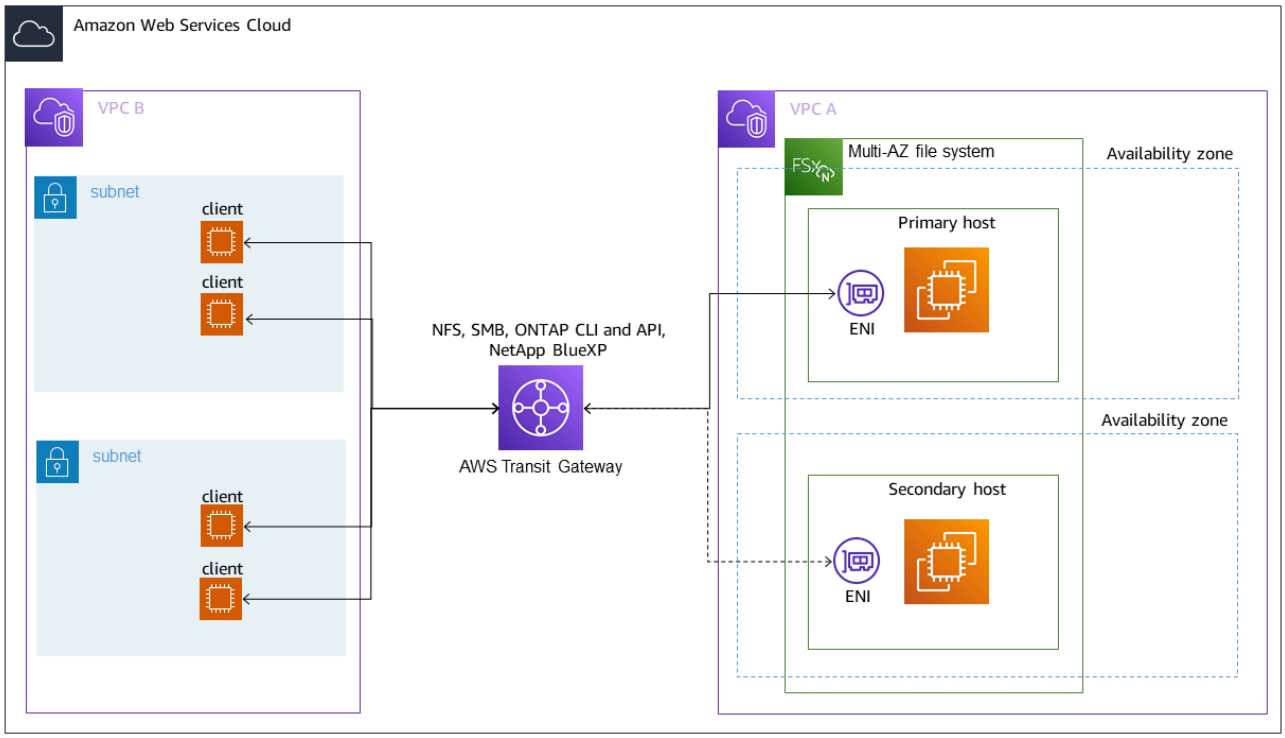
这些浮动 IP 地址在您与文件系统关联的 VPC 路由表中创建，且位于您在创建时所指定文件系统的 `EndpointIPv4AddressRange` 或 `EndpointIPv6AddressRange` 中。根据文件系统的创建方式，端点 IP 地址范围使用以下地址范围：

- 默认情况下，使用亚马逊 FSx 控制台或 Amazon FSx API 创建的多可用区双栈文件系统使用亚马逊 FSx 从 VPC 的 CIDR 范围中选择的可用 /118 IP 地址范围。您可以将部署在同一个 VPC/route 表中的文件系统的端点 IP 地址重叠，只要它们不与任何子网重叠即可。
- 默认情况下，使用 IPv4 Amazon FSx 控制台创建的仅限多可用区的文件系统使用 VPC 主 CIDR 范围中的最后 64 个 IP 地址作为文件系统的终端节点 IP 地址范围。

  默认情况下，使用或 IPv4 A AWS CLI mazon FSx API 创建的仅限多可用区的文件系统使用地址块内的 IP `198.19.0.0/16` 地址范围作为终端节点 IP 地址范围。
- 对于任一网络类型，您也可以在使用标准创建选项时指定自己的 IP 地址范围。只要不与任何子网重叠，而且尚未经具有相同 VPC 和路由表的其他文件系统使用，您选择的 IP 地址范围可以在 VPC 的 IP 地址范围内，也可以在 VPC 的 IP 地址范围外。对于此选项，我们建议使用在 VPC 的 IP 地址范围内的范围。

仅 AWS Transit Gateway 支持路由到浮动 IP 地址，也称为传递的对等。VPC 对等互连 Direct Connect、、 Site-to-Site VPN 不支持传递对等。因此，您需要使用中转网关才能从文件系统 VPC 之外的网络访问这些接口。

下图说明了如何使用 NFS、SMB 或管理端点的中转网关访问多可用区文件系统，该多可用区文件系统与访问它的客户端位于不同的 VPC 中。



> **Note**
>
> 确保您使用的所有路由表都与您的多可用区文件系统相关联。这样做有助于防止失效转移期间出现不可用问题。有关将 Amazon VPC 路由表与文件系统关联的信息，请参阅 更新文件系统。

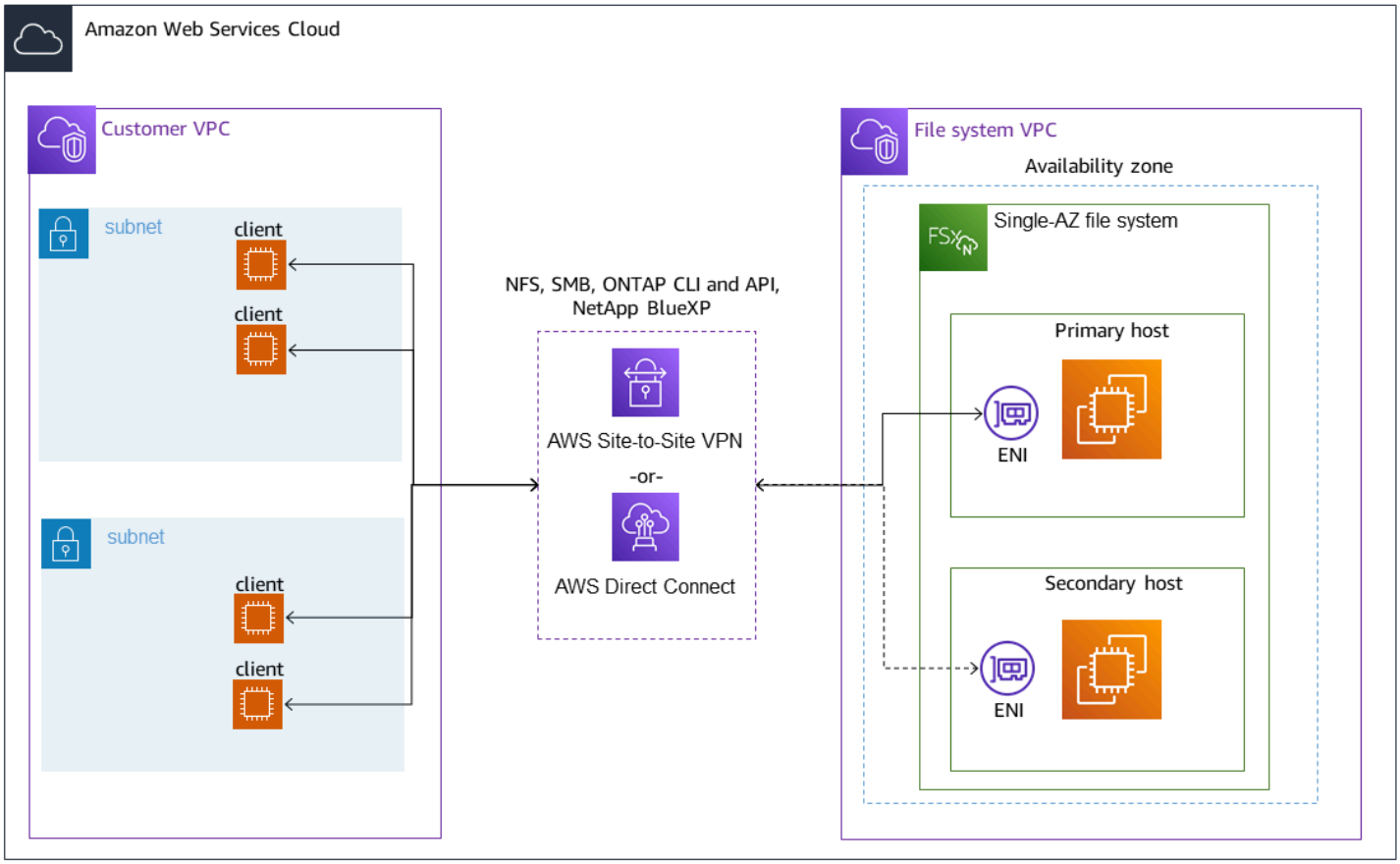
有关何时需要使用 Transit Gateway 访问 FSx 适用于 ONTAP 的文件系统的信息，请参阅什么时候需要中转网关？。

Amazon 使用基于标签的身份验证 FSx 管理多可用区文件系统的 VPC 路由表。这些路由表标有 `Key: AmazonFSx; Value: ManagedByAmazonFSx`。使用 FSx 为 ONTAP 多可用区文件系统创建或更新时，CloudFormation 我们建议您手动添加`Key: AmazonFSx; Value: ManagedByAmazonFSx`标签。

访问单可用区文件系统的 NFS、SMB 或 ONTAP CLI 和 API

用于通过 NFS 或 SMB 访问 FSx ONTAP 单可用区文件系统以及使用 ONTAP CLI 或 REST API 管理文件系统的终端节点是活动文件服务器弹性网卡上的辅助 IP 地址。辅助 IP 地址在 VPC 的 CIDR 范围内，因此客户端可以使用 VPC 对等互连或 Site-to-Site VPN 不要求访问数据和管理端口。 AWS Direct Connect AWS Transit Gateway

下图说明了使用 Site-to-Site VPN 或用 Direct Connect 于 NFS、SMB 或管理访问单可用区文件系统，该单可用区文件系统与访问它的客户端位于不同的 VPC 中。



什么时候需要中转网关？

您的多可用区文件系统是否需要中转网关取决于您访问文件系统数据所使用的方法。单可用区文件系统不需要中转网关。下表描述了何时需要使用 AWS Transit Gateway 访问多可用区文件系统。

数据访问	需要中转网关？
FSx 通过 NFS、SMB 或 NetApp ONTAP REST API、CLI 进行访问。或 NetApp Console	前提是： • 从对等（例如本地）网络进行访问，以及 • 您不是 FSx 通过 NetApp FlexCache 或全局文件缓存实例进行访问的
通过 iSCSI 访问数据	否

数据访问	需要中转网关？
通过访问数据 NVMe	否
将 SVM 加入 Active Directory	否
SnapMirror	否
FlexCache 缓存	否
全局文件缓存	否

在部署 VPC 之外访问 NVMe、iSCSI 和集群间终端节点

您可以使用 VPC 对等互连，也可以从文件系统的部署 VPC 外部访问文件系统 NVMe、iSCSI 和集群间终端节点。 AWS Transit Gateway 您可以使用 VPC 对等互连在两者之间路由 NVMe、iSCSI 和集群间流量。 VPCsVPC 对等连接是两者之间的网络连接 VPCs，用于使用私有 IPv6 地址 IPv4 或地址在两者之间路由流量。您可以使用 VPC 对等互连 VPCs 在同一个 AWS 区域 或不同 AWS 区域的 VPC 之间进行连接。有关 VPC 对等的更多信息，请参阅《Amazon VPC 对等指南》中的什么是 VPC 对等？。

从本地访问数据

您可以使用Site-to-Site VPN和从本地访问您 FSx 的 for ONTAP 文件系统 Direct Connect；以下各节中提供了更具体的用例指南。除了下面列出的从本地访问不同 FSx For ONTAP 资源的任何要求外，您还需要确保文件系统的 VPC 安全组允许数据在文件系统和客户端之间流动；有关所需端口的列表，请参阅 Amazon VPC 安全组。

从本地访问 NFS、SMB 和 ONTAP CLI 及 REST API 端点

本节介绍如何从本地网络访问 ONTAP 文件系统上 FSx 的 NFS、SMB 和 ONTAP 管理端口。

从本地访问多可用区文件系统

Amazon FSx 要求您使用 AWS Transit Gateway 或配置远程 NetApp全局文件缓存 NetApp FlexCache ，或者从本地网络访问多可用区文件系统。为了支持多可用区文件系统的跨可用区域故障转移，Amazon FSx 使用浮动 IP 地址作为用于 NFS、SMB 和 ONTAP 管理终端节点的接口。

由于 NFS、SMB 和管理端点使用浮动 IP 地址，因此必须与本地网络结合使用AWS Transit Gateway AWS Direct Connect 或 Site-to-Site VPN 访问这些接口。用于这些接口的浮动 IP 地址位于您在创建多可用区文件系统时指定的 `EndpointIPv4AddressRange` 或 `EndpointIPv6AddressRange` 范围内。根据文件系统的创建方式，端点 IP 地址范围使用以下地址范围：

- 默认情况下，使用亚马逊 FSx 控制台或 Amazon FSx API 创建的多可用区双栈文件系统使用亚马逊 FSx 从 VPC 的 CIDR 范围中选择的可用 /118 IP 地址范围。您可以将部署在同一个 VPC/route 表中的文件系统的端点 IP 地址重叠，只要它们不与任何子网重叠即可。
- 默认情况下，使用 IPv4 Amazon FSx 控制台创建的仅限多可用区的文件系统使用 VPC 主 CIDR 范围中的最后 64 个 IP 地址作为文件系统的终端节点 IP 地址范围。

  默认情况下，使用或 IPv4 A AWS CLI mazon FSx API 创建的仅限多可用区的文件系统使用地址块内的 IP `198.19.0.0/16` 地址范围作为终端节点 IP 地址范围。
- 对于任一网络类型，您也可以在使用标准创建选项时指定自己的 IP 地址范围。只要不与任何子网重叠，而且尚未经具有相同 VPC 和路由表的其他文件系统使用，您选择的 IP 地址范围可以在 VPC 的 IP 地址范围内，也可以在 VPC 的 IP 地址范围外。对于此选项，我们建议使用在 VPC 的 IP 地址范围内的范围。

浮动 IP 地址用于在需要进行失效转移时将您的客户端无缝过渡到备用文件系统。有关更多信息，请参阅 FSx for ONTAP 失效转移过程。

> **Important**
>
> 要使用中转网关访问多可用区文件系统，必须在其路由表与您的文件系统关联的子网中创建中转网关的每个附件。

有关更多信息，请参阅 配置路由以从本地访问多可用区文件系统。

从本地访问单可用区文件系统

对于单可用区文件系统，不存在从本地网络访问数据的要求。 AWS Transit Gateway 单可用区文件系统部署在单个子网中，无需使用浮动 IP 地址即可在节点之间进行失效转移。取而代之的是，您在单可用区文件系统上访问的 IP 地址将作为文件系统的 VPC CIDR 范围内的辅助 IP 地址实现，从而使您无需 AWS Transit Gateway即可从其他网络访问数据。

从本地访问集群间端点

FSx 对于 ONTAP 的集群间终端节点专门用于 NetApp ONTAP 文件系统之间的复制流量，包括本地 NetApp 部署之间和 FSx ONTAP 之间的复制流量。复制流量包括 SnapMirror、 FlexCache、、存储虚拟机 (SVMs) 与不同文件系统的卷之间的 FlexClone关系，以及 NetApp 全局文件缓存。集群间端点也用于 Active Directory 流量。

由于文件系统的集群间终端节点使用的 IP 地址在您为 ONTAP 创建文件系统时提供的 VPC 的 CIDR 范围内，因此您无需使用 Transit Gateway 在本地和之间路由集群间流量。 FSx AWS Cloud但是，本地客户端仍然必须使用 Site-to-Site VPN 或 Direct Connect 与您的 VPC 建立安全连接。

有关更多信息，请参阅 配置路由以从本地访问多可用区文件系统。

配置路由以从 VPC 之外访问多可用区文件系统

如果您的多可用区文件系统位于`EndpointIPv4AddressRange`或超出您`EndpointIPv6AddressRange`的 VPC 的 IP 地址范围，则需要在中设置额外的路由， AWS Transit Gateway 以便从对等网络或本地网络访问您的文件系统。

> **Important**
>
> 要使用中转网关访问多可用区文件系统，必须在其路由表与您的文件系统关联的子网中创建中转网关的每个附件。

> **Note**
>
> 对于在 VPC 的 IP 地址范围内使用端点 IP 地址范围的单可用区文件系统或多可用区文件系统，无需进行额外的中转网关配置。

使用配置路由 AWS Transit Gateway

1. 打开亚马逊 FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. FSx 为要配置对等网络访问的 ONTAP 文件系统选择。
3. 在网络与安全中，复制端点 IP 地址范围。
4. 向中转网关添加一条路由，将发往此 IP 地址范围的流量路由到您的文件系统的 VPC。有关更多信息，请参阅《Amazon VPC 中转网关》中的使用中转网关。

5. 确认您可以从对等网络访问您 FSx 的 for ONTAP 文件系统。

要将路由表添加到您的文件系统，请参阅 更新文件系统。

> **Note**
>
> 管理、NFS 和 SMB 端点的 DNS 记录只能从与文件系统相同的 VPC 中解析。要挂载卷或从其他网络连接到管理端口，您需要使用端点的 IP 地址。这些 IP 地址不会随着时间的推移而改变。

配置路由以从本地访问多可用区文件系统

配置 AWS Transit Gateway 为从本地访问多可用区文件系统

如果您的多可用区文件系统位于`EndpointIPv4AddressRange`或超出您`EndpointIPv6AddressRange`的 VPC 的 CIDR 范围，则需要在中设置额外的路由，才能从 AWS Transit Gateway 对等网络或本地网络访问您的文件系统。

> **Note**
>
> 对于在 VPC 的 IP 地址范围内使用端点 IP 地址范围的单可用区文件系统或多可用区文件系统，无需进行额外的中转网关配置。

1. 打开亚马逊 FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. FSx 为要配置对等网络访问的 ONTAP 文件系统选择。
3. 在“网络和安全”中，复制端点 IPv4 或 IPv6 地址范围。
4. 向中转网关添加一条路由，将发往此 IP 地址范围的流量路由到您的文件系统的 VPC。有关更多信息，请参阅《Amazon VPC 中转网关用户指南》中的使用中转网关。
5. 确认您可以从对等网络访问您 FSx 的 for ONTAP 文件系统。

> **Important**
>
> 要使用中转网关访问多可用区文件系统，必须在其路由表与您的文件系统关联的子网中创建中转网关的每个附件。如果您有单独的 Transit Gateway 连接子网，则还必须将这些子网的路由表与 Amazon 关联起来， FSx 以便使用亚马逊 FSx 终端节点地址对其进行更新。

要将路由表添加到您的文件系统，请参阅 更新文件系统。

在 Linux 客户端上挂载卷

我们建议您要使用 Linux 客户端装载的卷将安全样式设置为UNIX。有关更多信息，请参阅 管理 FSx ONTAP 卷。

> **Note**
>
> 默认情况下， FSx 对于 ONTAP，NFS 挂载是挂载。hard为了确保在发生失效转移时能够顺利进行失效转移，我们建议您使用默认 hard 挂载选项。

在 Linux 客户端上挂载 ONTAP 卷

1. 打开位于 https://console.aws.amazon.com/ec2/ 的 Amazon EC2 控制台。
2. 创建或选择一个运行 Amazon Linux 2 的 Amazon EC2 实例，该实例与文件系统在同一个 VPC 中。

   有关启动 EC2 Linux 实例的更多信息，请参阅《Amazon EC2 用户指南》中的步骤 1：启动实例。
3. 连接到 Amazon EC2 Linux 实例。有关更多信息，请参阅《Amazon EC2 用户指南》中的连接到 Linux 实例。
4. 使用Secure Shell（SSH）在 EC2 实例上打开终端，然后使用相应的凭证登录。
5. 在 EC2 实例上创建用于挂载 SVM 卷的目录，如下所示：

   ```
   sudo mkdir /fsx
   ```
6. 使用以下命令在您在上一步中创建的目录挂载卷：

```
sudo mount -t nfs svm-dns-name:/volume-junction-path /fsx
```

以下示例使用示例值。

```
sudo mount -t nfs svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-
east-1.amazonaws.com:/vol1 /fsx
```

您也可以使用 SVM 的 IP 地址来代替其 DNS 名称。我们建议使用 DNS 名称将客户端挂载至第二代文件系统，因为这有助于确保客户端在文件系统的高可用性（HA）对中保持平衡。

```
sudo mount -t nfs 198.51.100.1:/vol1 /fsx
```

> **Note**
>
> 对于第二代文件系统，默认启用并行 NFS（PnFS）协议，并默认用于任何挂载 NFS v4.1 或更高版本的卷的客户端。

使用 /etc/fstab 在实例重启时自动挂载

要在 Amazon EC2 Linux 实例重启时自动重新挂载 FSx for ONTAP 卷，请使用 `/etc/fstab` 文件。`/etc/fstab` 文件包含有关文件系统的信息。命令 `mount -a` 会在实例启动期间运行，用于挂载 `/etc/fstab` 中列出的文件系统。

> **Note**
>
> FSx 适用于 ONTAP 文件系统不支持`/etc/fstab`在亚马逊 EC2 Mac 实例上使用自动挂载。

> **Note**
>
> 在更新 EC2 实例`/etc/fstab`的文件之前，请确保您已经创建了 FSx 适用于 ONTAP 的文件系统。有关更多信息，请参阅 创建文件系统。

更新 EC2 实例上的 /etc/fstab 文件

1. 连接到 EC2 实例：

   - 要从运行 macOS 或 Linux 的计算机连接到您的实例，请为 SSH 命令指定 .pem 文件。要执行该操作，请使用 `-i` 选项和私有密钥路径。
   - 要从运行 Windows 的计算机连接到您的实例，您可以使用 MindTerm 或 PuTTY。要使用 PuTTY，您需要安装它并将 .pem 文件转换为 .ppk 文件。

   有关更多信息，请参阅 Amazon EC2 用户指南 中的以下主题：

   - 使用 SSH 连接到 Linux 实例
   - 使用 PuTTY 从 Windows 连接到 Linux 实例

2. 创建用于挂载 SVM 卷的本地目录。

   ```
   sudo mkdir /fsx
   ```

3. 在选定编辑器中打开 `/etc/fstab` 文件。

4. 将以下行添加到 `/etc/fstab` 文件中。在每个参数之间插入一个制表符。它应该显示为一行，不带换行符。

   ```
   svm-dns-name:volume-junction-path /fsx nfs nfsvers=version,defaults 0 0
   ```

   您也可以使用卷的 SVM 的 IP 地址。最后三个参数表示 NFS 选项（我们将其设置为默认值）、文件系统转储和文件系统检查（通常不使用这些选项，因此我们将它们设置为 0）。

5. 保存对文件所做的更改。

6. 现在使用以下命令挂载文件共享。下次系统启动时，该文件夹将自动挂载。

   ```
   sudo mount /fsx
   sudo mount svm-dns-name:volume-junction-path
   ```

您的 EC2 实例现已配置为每次重启时都挂载 ONTAP 卷。

在 Microsoft Windows 客户端上挂载卷

本节介绍如何使用运行 Microsoft Windows 操作系统的客户端访问你 FSx 的 for ONTAP 文件系统中的数据。无论您使用哪种类型的客户端，均请查看以下要求。

此过程假设客户端和文件系统位于同一 VPC 和 AWS 账户中。如果客户端位于本地或其他 VPC 或 AWS 区域中 AWS 账户，则此过程还假设您已使用 AWS Transit Gateway 或使用私有安全隧道设置 AWS Direct Connect 或专用网络连接。 AWS Virtual Private Network有关更多信息，请参阅 从部署 VPC 外部访问数据。

我们建议您使用 SMB 协议将卷附加到 Windows 客户端。

先决条件

要使用 Microsoft Windows 客户端访问 ONTAP 存储卷，您必须满足以下先决条件：

- 您要附加的卷的 SVM 必须加入组织的 Active Directory，或者您必须使用工作组。有关将 SVM 加入 Active Directory 的更多信息，请参阅 管理 FSx ONTAP 存储虚拟机。有关使用工作组的更多信息，请参阅 在工作组中设置 SMB 服务器。
- 要附加的卷的安全风格应设置为 NTFS。有关更多信息，请参阅 卷安全风格。

使用 SMB 和 Active Directory 在 Windows 客户端上挂载卷

1. 打开位于 https://console.aws.amazon.com/ec2/ 的 Amazon EC2 控制台。
2. 创建或选择一个运行 Microsoft Windows 的 Amazon EC2 实例，该实例与文件系统位于同一 VPC 中，并与卷的 SVM 加入同一个 Microsoft Active Directory。

   有关启动实例的更多信息，请参阅《Amazon EC2 用户指南》中的步骤 1：启动实例。

   有关将 SVM 加入 Active Directory 的更多信息，请参阅 管理 FSx ONTAP 存储虚拟机。
3. 连接到您的 Amazon EC2 Windows 实例。有关详细信息，请参阅《Amazon EC2 用户指南》中的连接到 Windows 实例。
4. 打开命令提示符。
5. 运行如下命令。替换以下内容：

   - 将 `Z:` 替换为任何可用的驱动器号。
   - 将 `DNS_NAME` 替换为卷的 SVM 的 SMB 端点的 DNS 名称或 IP 地址。

- 将 SHARE_NAME 替换为 SMB 共享的名称。C$ 是 SVM 命名空间根目录下的默认 SMB 共享，但您不应将其挂载，因为这会将存储暴露给根卷并有可能导致安全问题和服务中断。您应该提供要挂载的 SMB 共享名称，而不是 C$。有关创建 SMB 共享的更多信息，请参阅 管理 SMB 共享。

```
net use Z: \\DNS_NAME\SHARE_NAME
```

以下示例使用示例值。

```
net use Z: \\corp.example.com\group_share
```

您也可以使用 SVM 的 IP 地址来代替其 DNS 名称。我们建议使用 DNS 名称将客户端挂载至第二代文件系统，因为这有助于确保客户端在文件系统的高可用性（HA）对中保持平衡。

```
net use Z: \\198.51.100.5\group_share
```

在 macOS 客户端上挂载卷

本节介绍如何使用运行 macOS 操作系统的客户端访问您 FSx 的 for ONTAP 文件系统中的数据。无论您使用哪种类型的客户端，均请查看以下要求。

此过程假设客户端和文件系统位于同一 VPC 和 AWS 账户中。如果客户端位于本地，或者位于其他 VPC 中， AWS 账户 或者 AWS 区域，您已使用 AWS Transit Gateway 或使用私有、安全的隧道设置 AWS Direct Connect 或专用网络连接。 AWS Virtual Private Network有关更多信息，请参阅 从部署 VPC 外部访问数据。

我们建议您使用 SMB 协议将卷附加到 Mac 客户端。

使用 SMB 在 macOS 客户端上挂载 ONTAP 卷

1. 打开位于 https://console.aws.amazon.com/ec2/ 的 Amazon EC2 控制台。
2. 创建或选择一个运行 macOS 的 Amazon EC2 Mac 实例，该实例与文件系统在同一个 VPC 中。

   有关启动实例的更多信息，请参阅《Amazon EC2 用户指南》中的步骤 1：启动实例。
3. 连接到您的 Amazon EC2 Mac 实例。有关更多信息，请参阅《Amazon EC2 用户指南》中的连接到 Linux 实例。

4. 使用Secure Shell（SSH）在 EC2 实例上打开终端，然后使用相应的凭证登录。
5. 在 EC2 实例上创建用于挂载卷的目录，如下所示：

```
sudo mkdir /fsx
```

6. 使用以下命令挂载卷。

```
sudo mount -t smbfs filesystem-dns-name:/smb-share-name mount-point
```

以下示例使用示例值。

```
sudo mount -t smbfs svm-01234567890abcde2.fs-01234567890abcde5.fsx.us-
east-1.amazonaws.com:/C$ /fsx
```

您也可以使用 SVM 的 IP 地址来代替其 DNS 名称。我们建议使用 DNS 名称将客户端挂载至第二代文件系统，因为这有助于确保客户端在文件系统的高可用性（HA）对中保持平衡。

```
sudo mount -t smbfs 198.51.100.10:/C$ /fsx
```

C$ 是默认 SMB 共享，您可以挂载它来查看 SVM 命名空间根目录。如果您已在 SVM 中创建了任何服务器消息块（SMB）共享，则要提供 SMB 共享名称，而不是 C$。有关创建 SMB 共享的更多信息，请参阅 管理 SMB 共享。

使用 NFS 在 macOS 客户端上挂载 ONTAP 卷

1. 打开位于 https://console.aws.amazon.com/ec2/ 的 Amazon EC2 控制台。
2. 创建或选择一个运行 Amazon Linux 2 的 Amazon EC2 实例，该实例与文件系统在同一个 VPC 中。

   有关启动 EC2 Linux 实例的更多信息，请参阅《Amazon EC2 用户指南》中的步骤 1：启动实例。
3. 连接到 Amazon EC2 Linux 实例。有关更多信息，请参阅《Amazon EC2 用户指南》中的连接到 Linux 实例。
4. 在实例启动期间使用用户数据脚本或运行以下命令，在 Linux EC2 实例上挂载 FSx for ONTAP 卷：

```
sudo mount -t nfs -o nfsvers=NFS_version svm-dns-name:/volume-junction-path /mount-point
```

以下示例使用示例值。

```
sudo mount -t nfs -o nfsvers=4.1
 svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-east-1.amazonaws.com:/vol1 /
fsxontap
```

您也可以使用 SVM 的 IP 地址来代替其 DNS 名称。我们建议使用 DNS 名称将客户端挂载至第二代文件系统，因为这有助于确保客户端在文件系统的 HA 对中保持平衡。

```
sudo mount -t nfs -o nfsvers=4.1 198.51.100.1:/vol1 /fsxontap
```

5. 使用以下命令在您在上一步中创建的目录挂载卷：

```
sudo mount -t nfs svm-dns-name:/volume-junction-path /fsx
```

以下示例使用示例值。

```
sudo mount -t nfs svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-
east-1.amazonaws.com:/vol1 /fsx
```

您也可以使用 SVM 的 IP 地址来代替其 DNS 名称。我们建议使用 DNS 名称将客户端挂载至第二代文件系统，因为这有助于确保客户端在文件系统的高可用性（HA）对中保持平衡。

```
sudo mount -t nfs 198.51.100.1:/vol1 /fsx
```

为 Linux 配置 iSCSI

FSx for ONTAP 支持 iSCSI 协议。您需要在 Linux 客户端和文件系统上配置 iSCSI，才能使用 iSCSI 协议在客户端和文件系统之间传输数据。iSCSI 协议适用于所有拥有 6 个或更少的高可用性（HA）对的文件系统。

在适用于 NetApp ONTAP 的 Amazon FSx 上配置 iSCSI 有三个主要步骤，这些步骤将在以下过程中进行介绍：

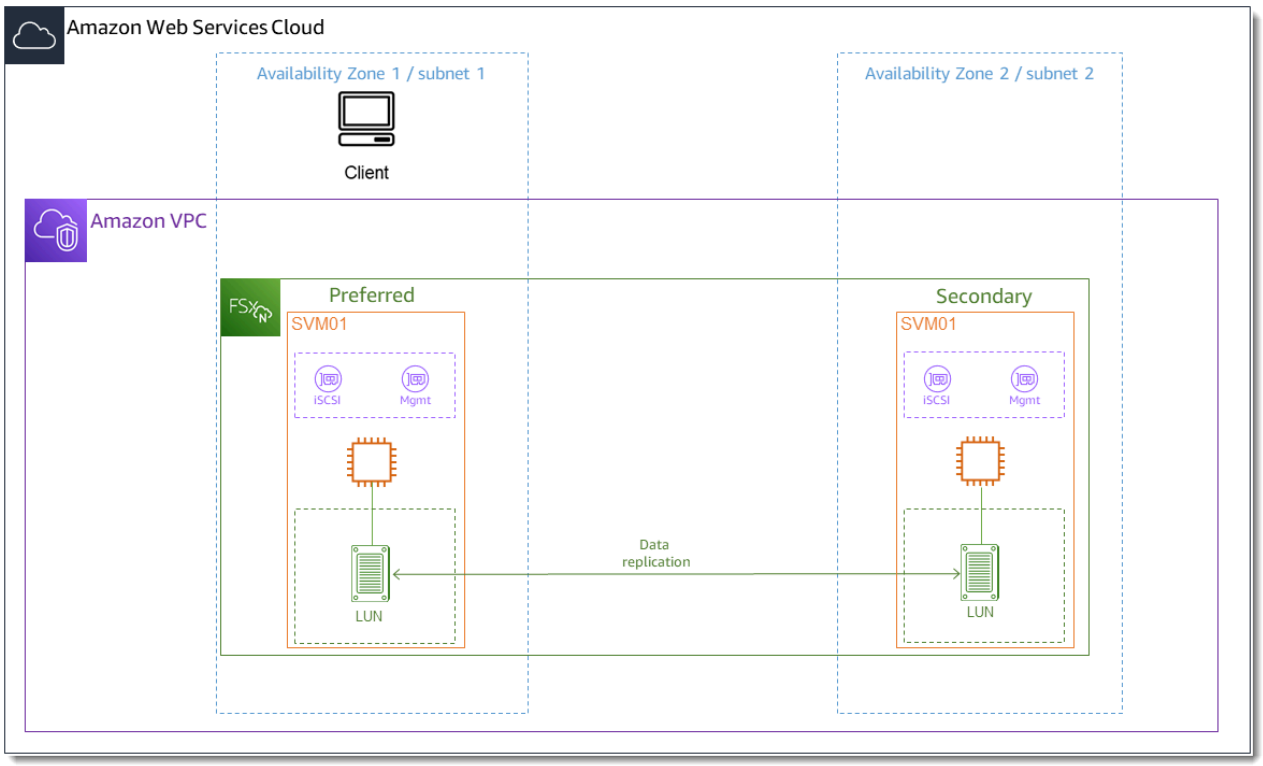
1. 在 Linux 主机上安装和配置 iSCSI 客户端。
2. 在文件系统的 SVM 上配置 iSCSI。
   - 创建 iSCSI 启动器组。
   - 将启动器组映射到 LUN。
3. 在 Linux 客户端上挂载 iSCSI LUN。

开始前的准备工作

在开始为 iSCSI 配置文件系统之前，需要完成以下各项。

- 创建 FSx for ONTAP 文件系统。有关更多信息，请参阅 创建文件系统。
- 在文件系统上创建 iSCSI LUN。有关更多信息，请参阅 创建 iSCSI LUN。
- 在与文件系统相同的 VPC 中创建一个运行 Amazon Linux 2 亚马逊机器映像（AMI）的 Amazon EC2 实例。这是您配置 iSCSI 和访问文件数据所在的 Linux 主机。

  在这些过程的范围之外，如果主机位于其他 VPC 中，则可以使用 VPC 对等连接或 AWS Transit Gateway 来授予其他 VPC 访问该卷的 iSCSI 端点的权限。有关更多信息，请参阅 从部署 VPC 外部访问数据。
- 配置 Linux 主机的 VPC 安全组，允许入站和出站流量，如 使用 Amazon VPC 进行文件系统访问控制 中所述。
- 获取具有 `fsxadmin` 权限的 ONTAP 用户的凭证，此权限用于访问 ONTAP CLI。有关更多信息，请参阅 ONTAP 角色和用户。
- 您将要为 iSCSI 配置并用于访问 FSx for ONTAP 文件系统的 Linux 主机位于同一 VPC 和 AWS 账户中。
- 我们建议您将 EC2 实例与文件系统的首选子网放入同一个可用区，如下图所示。



如果 EC2 实例运行的 Linux AMI 与 Amazon Linux 2 不同，则这些过程和示例中使用的某些实用程序可能已安装，并且您可能会使用不同的命令来安装所需的软件包。除了安装软件包外，本节中使用的命令还适用于其他 EC2 Linux AMI。

主题

- 在 Linux 主机上安装和配置 iSCSI
- 在 FSx for ONTAP 文件系统上配置 iSCSI
- 在 Linux 客户端上挂载 iSCSI LUN

在 Linux 主机上安装和配置 iSCSI

安装 iSCSI 客户端

1. 确认 `iscsi-initiator-utils` 和 `device-mapper-multipath` 并已安装在您的 Linux 设备上。使用 SSH 客户端连接到 Linux 实例。有关更多信息，请参阅使用 SSH 连接到 Linux 实例。
2. 使用以下命令安装 `multipath` 和 iSCSI 客户端。如果您希望在文件服务器之间自动失效转移，则必须安装 `multipath`。

```
~$ sudo yum install -y device-mapper-multipath iscsi-initiator-utils
```

3. 使用 multipath 期间，为了便于在进行文件服务器之间的自动失效转移时更快做出响应，请将 /etc/iscsi/iscsid.conf 文件中的替换超时值设置为值 5，而不是使用默认值 120。

```
~$ sudo sed -i 's/node.session.timeo.replacement_timeout = .*/
node.session.timeo.replacement_timeout = 5/' /etc/iscsi/iscsid.conf; sudo cat /etc/
iscsi/iscsid.conf | grep node.session.timeo.replacement_timeout
```

4. 启动 iSCSI 服务。

```
~$ sudo service iscsid start
```

请注意，根据您的 Linux 版本，您可能需要改为使用以下命令：

```
~$ sudo systemctl start iscsid
```

5. 使用以下命令确认正在运行服务：

```
~$ sudo systemctl status iscsid.service
```

系统将使用以下输出做出响应：

```
iscsid.service - Open-iSCSI
    Loaded: loaded (/usr/lib/systemd/system/iscsid.service; disabled; vendor
 preset: disabled)
    Active: active (running) since Fri 2021-09-02 00:00:00 UTC; 1min ago
    Docs: man:iscsid(8)
    man:iscsiadm(8)
    Process: 14658 ExecStart=/usr/sbin/iscsid (code=exited, status=0/SUCCESS)
    Main PID: 14660 (iscsid)
    CGroup: /system.slice/iscsid.service
    ##14659 /usr/sbin/iscsid
    ##14660 /usr/sbin/iscsid
```

在您的 Linux 客户端上配置 iSCSI

1. 您须要配置多路径来使客户端能够在文件服务器之间自动进行失效转移。使用以下命令：

```
~$ sudo mpathconf --enable --with_multipathd y
```

2. 使用以下命令确定 Linux 主机的启动程序名称。启动程序名称的位置取决于您的 iSCSI 实用程序。如果您正在使用 `iscsi-initiator-utils`，则启动程序名称位于文件 `/etc/iscsi/initiatorname.iscsi` 中。

```
~$ sudo cat /etc/iscsi/initiatorname.iscsi
```

系统使用启动程序名称做出响应。

```
InitiatorName=iqn.1994-05.com.redhat:abcdef12345
```

在 FSx for ONTAP 文件系统上配置 iSCSI

1. 在 FSx for ONTAP 文件系统上，使用以下命令连接到您在其中创建了 iSCSI LUN 的 NetApp ONTAP CLI。有关更多信息，请参阅 使用 NetApp ONTAP CLI。

```
~$ ssh fsxadmin@your_management_endpoint_ip
```

2. 使用 NetApp ONTAP CLI 命令 lun igroup create 创建启动程序组（`igroup`）。启动程序组会映射到 iSCSI LUN，并控制哪些启动程序（客户端）可以访问 LUN。将 `host_initiator_name` 替换为在上一过程中从 Linux 主机中检索到的启动程序名称。

```
::> lun igroup create -vserver svm_name -igroup igroup_name -
initiator host_initiator_name -protocol iscsi -ostype linux
```

如果要使映射到此 igroup 的 LUN 可供多个主机使用，您可以指定多个启动程序名称，以逗号分隔。有关更多信息，请参阅 NetApp ONTAP 文档中心中的创建 LUN igroup。

3. 使用命令 lun igroup show 确认存在 `igroup`：

```
::> lun igroup show
```

系统将使用以下输出做出响应：

```
Vserver   Igroup       Protocol OS Type  Initiators
--------- ------------ -------- -------- ------------------------------------
```

```
svm_name  igroup_name  iscsi    linux    iqn.1994-05.com.redhat:abcdef12345
```

4. 此步骤假定您已创建了 iSCSI LUN。如果您尚未创建，请参阅 创建 iSCSI LUN 的分步说明来创建。

   使用 lun mapping create 来创建从已创建的 LUN 到已创建的 igroup 的映射，并指定以下属性：

   - *svm_name* – 提供 iSCSI 目标的存储虚拟机的名称。主机使用此值来连接 LUN。
   - *vol_name* – 托管 LUN 的卷的名称。
   - *lun_name* – 已分配给 LUN 的名称。
   - *igroup_name* – 启动程序组的名称。
   - *lun_id* – LUN ID 整数是特定于映射的，而不是 LUN 本身。igroup 中的启动程序将其用作逻辑单元号，并在访问存储器时为启动程序使用此值。

   ```
   ::> lun mapping create -vserver svm_name -path /vol/vol_name/lun_name -
   igroup igroup_name -lun-id lun_id
   ```

5. 使用 lun show -path 命令确认 LUN 已创建、已联机且已映射。

   ```
   ::> lun show -path /vol/vol_name/lun_name -fields state,mapped,serial-hex
   ```

   系统将使用以下输出做出响应：

   ```
   Vserver    Path                            serial-hex               state    mapped
   --------- ------------------------------ ------------------------ --------
   --------
   svm_name  /vol/vol_name/lun_name          6c5742314e5d52766e796150 online   mapped
   ```

   保存 serial_hex 值（在本例中为 6c5742314e5d52766e796150），您将在之后的步骤中使用该值为块设备创建易记名称。

6. 使用 network interface show -vserver 命令检索您在其中创建 iSCSI LUN 的 SVM 的 iscsi_1 和 iscsi_2 接口的地址。

   ```
   ::> network interface show -vserver svm_name
   ```

   系统将使用以下输出做出响应：

```
            Logical                Status     Network            Current
        Current Is
Vserver     Interface              Admin/Oper Address/Mask       Node
        Port    Home
----------- ----------             ---------- ------------------ -------------
        ------- ----
svm_name
            iscsi_1                up/up      172.31.0.143/20
 FSxId0123456789abcdef8-01  e0e     true
            iscsi_2                up/up      172.31.21.81/20
 FSxId0123456789abcdef8-02  e0e     true
            nfs_smb_management_1
                                   up/up      198.19.250.177/20
 FSxId0123456789abcdef8-01  e0e     true
3 entries were displayed.
```

在此示例中，iscsi_1 的 IP 地址是 172.31.0.143，iscsi_2 的IP 地址是 172.31.21.81。

在 Linux 客户端上挂载 iSCSI LUN

在 Linux 客户端上挂载 iSCSI LUN 的过程包括三个步骤：

1. 发现目标 iSCSI 节点
2. 对 iSCSI LUN 进行分区
3. 在客户端上挂载 iSCSI LUN

以下过程将详述这些步骤。

发现目标 iSCSI 节点

1. 在 Linux 客户端上，使用以下命令来发现使用 iscsi_1 的 IP 地址 *iSCSI_1_IP* 的目标 iSCSI 节点。

```
~$ sudo iscsiadm --mode discovery --op update --type sendtargets --
portal iscsi_1_IP
```

```
172.31.0.143:3260,1029
 iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3
```

```
172.31.21.81:3260,1028
 iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3
```

在此示例中，iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3 对应于首选可用区中的 iSCSI LUN 的target_initiator。

2. （可选）要为 iSCSI LUN 带来高于 Amazon EC2 单一客户端最大 5Gbps（约 625MBps）的吞吐量，请按照《适用于 Linux 实例的 Amazon Elastic Compute Cloud 用户指南》中的 Amazon EC2 实例网络带宽描述的过程，为提高吞吐量建立更多的会话。

   以下命令会在每个可用区中为每个 ONTAP 节点的每个启动程序建立 8 个会话，使客户端能够向 iSCSI LUN 提供高达 40Gbps（5000MBps）的聚合吞吐量。

```
~$ sudo iscsiadm --mode node -T target_initiator --op update -n
 node.session.nr_sessions -v 8
```

3. 登录到目标启动程序。您的 iSCSI LUN 显示为可用磁盘。

```
~$ sudo iscsiadm --mode node -T target_initiator --login
```

```
Logging in to [iface: default, target:
 iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3, portal:
 172.31.14.66,3260] (multiple)
Login to [iface: default, target:
 iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3, portal:
 172.31.14.66,3260] successful.
```

   上述输出已被截断；您应该会在每个文件服务器上看到针对每个会话的一个 Logging in 和一个 Login successful 响应。如果每个节点有 4 个会话，则会有 8 个 Logging in 和 8 个 Login successful 响应。

4. 使用以下命令，通过显示具有多个策略的单个 LUN 来验证 dm-multipath 是否已识别并合并 iSCSI。列为 active 和列为 enabled 的设备数量应相等。

```
~$ sudo multipath -ll
```

   在输出中，磁盘名称的格式为dm-xyz，其中 xyz 为整数。如果不存在其他多路径磁盘，则此值为 dm-0。

```
3600a09806c5742314e5d52766e79614f dm-xyz NETAPP  ,LUN C-Mode
size=10G features='4 queue_if_no_path pg_init_retries 50 retain_attached_hw_handle'
 hwhandler='0' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| |- 0:0:0:1 sda     8:0   active ready running
| |- 1:0:0:1 sdc     8:32  active ready running
| |- 3:0:0:1 sdg     8:96  active ready running
| `- 4:0:0:1 sdh     8:112 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  |- 2:0:0:1 sdb     8:16  active ready running
  |- 7:0:0:1 sdf     8:80  active ready running
  |- 6:0:0:1 sde     8:64  active ready running
  `- 5:0:0:1 sdd     8:48  active ready running
```

您的块设备现已连接到 Linux 客户端。其位于 /dev/*dm-xyz* 路径之下。您不应将此路径用于管理目的；而应使用 /dev/mapper/*wwid* 路径下的符号链接，其中 *wwid* 是适用于 LUN 的唯一标识符，在不同设备之间保持一致。在下一步中，您需要为 *wwid* 提供一个易记名称，以使其能够其区别于其他多路径磁盘。

为块设备分配一个易记名称

1. 要为您的设备提供易记名称，请在 /etc/multipath.conf 文件中创建别名。为此，请使用首选文本编辑器将以下条目添加到文件中，替换以下占位符：

   - 使用您在 在 FSx for ONTAP 文件系统上配置 iSCSI 过程中保存的值来替换 serial_hex。
   - 如示例所示，将前缀 3600a0980 添加到值 serial_hex 中。这是用于适用于 NetApp ONTAP 的 Amazon FSx 的 NetApp ONTAP 发行版的唯一序言。
   - 将 device_name 替换为您要在设备上使用的易记名称。

```
multipaths {
    multipath {
        wwid 3600a0980serial_hex
        alias device_name
    }
}
```

或者，您可以复制以下脚本并保存为 bash 文件，例如 multipath_alias.sh。您可以使用 sudo 权限运行脚本，使用相应的序列号和期望的易记名称来替换 *serial_hex*（不带 3600a0980 前缀）和 *device_name*。此脚本会在 /etc/multipath.conf 文件中搜索未取消注释的 multipaths 部分。如果存在，它会在该部分中附加一个 multipath 条目；否则，它将创建一个新的 multipaths 部分，其中包含适用于您的块设备的 multipath 条目的。

```
#!/bin/bash
SN=serial_hex
ALIAS=device_name
CONF=/etc/multipath.conf
grep -q '^multipaths {' $CONF
UNCOMMENTED=$?
if [ $UNCOMMENTED -eq 0 ]
then
        sed -i '/^multipaths {/a\\tmultipath {\n\t\twwid 3600a0980'"${SN}"'\n\t
\talias '"${ALIAS}"'\n\t}\n' $CONF
else
        printf "multipaths {\n\tmultipath {\n\t\twwid 3600a0980$SN\n\t\talias
 $ALIAS\n\t}\n}" >> $CONF
fi
```

2. 重新启动 multipathd 服务以使对 /etc/multipathd.conf 的更改生效。

```
~$ systemctl restart multipathd.service
```

对 LUN 进行分区

下一步是使用 fdisk 格式化您的 LUN 并对其进行分区。

1. 使用以下命令验证您的 device_name 路径是否存在。

```
~$ ls /dev/mapper/device_name
```

```
/dev/device_name
```

2. 使用 fdisk 对磁盘进行分区。您需要输入交互式提示。按显示的顺序输入选项。您可以使用小于最后一个扇区的值来创建多个分区（在本例中为 20971519）。

> **Note**
>
> `Last sector` 值将根据 iSCSI LUN 的大小（在本例中为 10 GB）而改变。

```
~$ sudo fdisk /dev/mapper/device_name
```

开始进行 `fsdisk` 交互式提示。

```
Welcome to fdisk (util-linux 2.30.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0x66595cb0.

Command (m for help): n
Partition type
   p primary (0 primary, 0 extended, 4 free)
   e extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-20971519, default 2048): 2048
Last sector, +sectors or +size{K,M,G,T,P} (2048-20971519, default
 20971519): 20971519

Created a new partition 1 of type 'Linux' and of size 512 B.
Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.
```

输入 w 后，您的新分区 /dev/mapper/*partition_name* 即变为可用。*partition_name* 的格式为*<device_name><partition_number>*。1 已用作在上一步 `fdisk` 命令中使用的分区编号。

3. 使用 /dev/mapper/*partition_name* 作为创建文件系统的路径。

```
~$ sudo mkfs.ext4 /dev/mapper/partition_name
```

系统将使用以下输出做出响应：

```
mke2fs 1.42.9 (28-Dec-2013)
Discarding device blocks: done
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=16 blocks
655360 inodes, 2621184 blocks
131059 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2151677952
80 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
     32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632
Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

在 Linux 客户端上挂载 LUN

1. 创建一个目录 *directory_path* 作为文件系统的挂载点。

```
~$ sudo mkdir /directory_path/mount_point
```

2. 使用以下命令挂载文件系统。

```
~$ sudo mount -t ext4 /dev/mapper/partition_name /directory_path/mount_point
```

3. （可选）如果要向特定用户授予挂载目录的所有权，请将 *username* 替换为拥有者的用户名。

```
~$ sudo chown username:username /directory_path/mount_point
```

4. （可选）验证您是否可以从文件系统读取数据和将数据写入文件系统。

```
~$ echo "Hello world!" > /directory_path/mount_point/HelloWorld.txt
```

```
~$ cat directory_path/HelloWorld.txt
Hello world!
```

您已在 Linux 客户端上成功创建并挂载了 iSCSI LUN。

为 Windows 配置 iSCSI

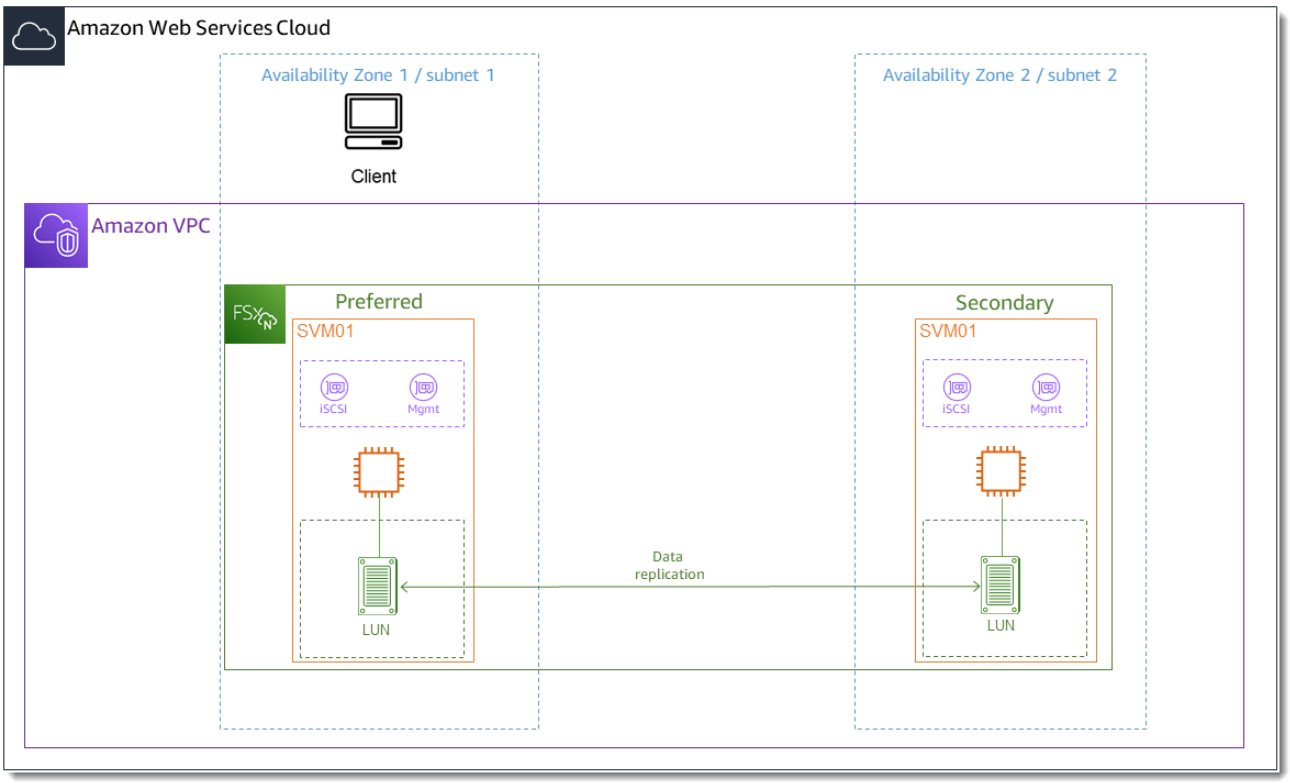
FSx 适用于 ONTAP 支持 iSCSI 协议。您需要在 Windows 客户端和 SVM 及 卷上配置 iSCSI，才能使用 iSCSI 协议在客户端和文件系统之间传输数据。iSCSI 协议适用于所有拥有 6 个或更少的高可用性（HA）对的文件系统。

这些步骤中提供的示例说明了如何在客户端上为 ONTAP 文件系统配置 iSCSI 协议，以及如何使用以下设置： FSx

- 正在挂载到 Windows 主机的 iSCSI LUN 已创建。有关更多信息，请参阅 创建 iSCSI LUN。
- 正在挂载 iSCSI LUN 的 Microsoft Windows 主机是运行 Microsoft Windows Server 2019 亚马逊机器映像（AMI）的 Amazon EC2 实例。为允许入站和出站流量，它已配置 VPC 安全组，如 使用 Amazon VPC 进行文件系统访问控制 中所述。

  您可能需要在设置过程中使用不同的 Microsoft Windows AMI。
- 客户端和文件系统位于同一 VPC 和 AWS 账户中。如果客户端位于其他 VPC 中，则可以使用 VPC 对等互连或 AWS Transit Gateway 向其他人授予对 iSCSI 终端节点的 VPCs 访问权限。有关更多信息，请参阅 从部署 VPC 外部访问数据。

  我们建议您将 EC2 实例与文件系统的首选子网放入同一个可用区，如下图所示。



主题

- 在 Windows 客户端上配置 iSCSI
- 在 ONTAP 文件系统 FSx 上配置 iSCSI
- 在 Windows 客户端上挂载 iSCSI LUN
- 验证 iSCSI 配置

在 Windows 客户端上配置 iSCSI

1. 使用 Windows 远程桌面连接到要在其上挂载 iSCSI LUN 的 Windows 客户端。有关更多信息，请参阅《Amazon Elastic Compute Cloud 用户指南》中的使用 RDP 连接到 Windows 实例。
2. 以管理员 PowerShell 身份打开窗口。使用以下命令在 Windows 实例上启用 iSCSI，并将 iSCSI 服务配置为自动启动。

```
PS C:\> Start-Service MSiSCSI
PS C:\> Set-Service -Name msiscsi -StartupType Automatic
```

3. 检索您的 Windows 实例的启动程序名称。您将使用 ONTAP CLI 在 FSx 适用于 ONTAP 的文件系统上配置 iSCS NetApp I 时使用此值。

```
PS C:\> (Get-InitiatorPort).NodeAddress
```

系统使用启动程序端口做出响应。

```
iqn.1991-05.com.microsoft:ec2amaz-abc123d
```

4. 您需要在 Windows 实例上安装 Multipath-IO（MPIO），以使客户端能够在文件服务器之间自动进行失效转移。使用以下命令：

```
PS C:\> Install-WindowsFeature Multipath-IO
```

5. Multipath-IO 安装完成后重启 Windows 实例。保持您的 Windows 实例处于打开状态，以便执行后续部分中的 iSCSI LUN 挂载步骤。

在 ONTAP 文件系统 FSx 上配置 iSCSI

1. 要访问 ONTAP CLI，请运行以下命令在 Amazon FSx for NetApp ONTAP 文件系统或 SVM 的管理端口上建立 SSH 会话。将 *management_endpoint_ip* 替换为文件系统管理端口的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

有关更多信息，请参阅 使用 ONTAP CLI 管理文件系统。

2. 使用 ONTAP CLI lun igroup create 创建启动程序组或 igroup。启动器组映射到 iSCSI LUNs 并控制哪些启动器（客户端）可以访问。 LUNs将 host_initiator_name 替换为在上一过程中从 Windows 主机中检索到的启动程序名称。

```
::> lun igroup create -vserver svm_name -igroup igroup_name -
initiator host_initiator_name -protocol iscsi -ostype windows
```

如果要将 LUNs 映射到此映射的igroup内容可供多台主机使用，则可以使用 CLI lun igroup createONTAP命令指定多个以逗号分隔的启动器名称。

3. 使用 igroup lun igroup show ONTAP CLI 命令确认是否创建成功：

```
::> lun igroup show
```

系统将使用以下输出做出响应：

```
Vserver    Igroup        Protocol OS Type  Initiators
---------  ------------  -------- -------- ------------------------------------
svm_name   igroup_name   iscsi    windows  iqn.1994-05.com.windows:abcdef12345
```

igroup创建完成后，您就可以创建它们 LUNs 并将其映射到igroup。

4. 此步骤假定您已创建了 iSCSI LUN。如果没有，创建 iSCSI LUN请参见以 step-by-step获取操作说明。

   从 LUN 创建一个新 LUN 的映射到 igroup。

```
::> lun mapping create -vserver svm_name -path /vol/vol_name/lun_name -
igroup igroup_name -lun-id lun_id
```

5. 使用以下命令确认 LUN 已创建、已联机且已映射：

```
::> lun show -path /vol/vol_name/lun_name
Vserver     Path                            State   Mapped   Type     Size
---------   ------------------------------- ------- -------- -------- --------
svm_name    /vol/vol_name/lun_name          online  mapped   windows  10GB
```

   现在，您可以在 Windows 实例上添加 iSCSI 目标。

6. 使用以下命令检索 SVM 的 iscsi_1 和 iscsi_2 接口的 IP 地址：

```
::> network interface show -vserver svm_name
```

```
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
svm_name
            iscsi_1    up/up      172.31.0.143/20    FSxId0123456789abcdef8-01
                                                                   e0e     true
            iscsi_2    up/up      172.31.21.81/20    FSxId0123456789abcdef8-02
                                                                   e0e     true
            nfs_smb_management_1
                       up/up      198.19.250.177/20  FSxId0123456789abcdef8-01
                                                                   e0e     true
3 entries were displayed.
```

在此示例中，iscsi_1 的 IP 地址是 172.31.0.143，iscsi_2 的IP 地址是 172.31.21.81。

在 Windows 客户端上挂载 iSCSI LUN

1. 在你的 Windows 实例上，以管理员身份打开 PowerShell 终端。
2. 您将创建一个用于执行以下操作的 .ps1 脚本：

   - 连接到文件系统的每个 iSCSI 接口。
   - 为 iSCSI 添加和配置 MPIO。
   - 为每个 iSCSI 连接建立 8 个会话，这使客户机能够向 iSCSI LUN 驱动高达 40 Gbps (5,000 MBps) 的聚合吞吐量。拥有 8 个会话可确保单个客户端可以驱动全部的 4,000 MBps 吞吐容量，以达到最高级别 FSx 的 ONTAP 吞吐容量。您可以选择通过修改变量将会话数更改为更高或更少的会话数（每个会话最多可提供 625 MBps 的吞吐RecommendedConnectionCount量）。有关更多信息，请参阅《Amazon Elastic Compute Cloud 用户指南（适用于 Windows 实例）》中的 Amazon EC2 实例网络带宽。

   将以下一组命令复制到文件中，创建 .psl 脚本。

   - 将 iscsi_1 和 iscsi_2 替换为在上一步中检索到的 IP 地址。
   - 将 ec2_ip 替换为 Windows 实例的 IP 地址。

```
Write-Host "Starting iSCSI connection setup..."
     $TargetPortalAddresses = @("iscsi_1","iscsi_2"); $LocaliSCSIAddress = "ec2_ip"
     $RecommendedConnectionCount = 8

     Foreach ($TargetPortalAddress in $TargetPortalAddresses) {
         New-IscsiTargetPortal -TargetPortalAddress $TargetPortalAddress -
TargetPortalPortNumber 3260 -InitiatorPortalAddress $LocaliSCSIAddress
     }

     New-MSDSMSupportedHW -VendorId MSFT2005 -ProductId iSCSIBusType_0x9

     $currentMPIOSettings = Get-MPIOSetting
     if ($currentMPIOSettings.PathVerificationState -ne 'Enabled') {
         Write-Host "Setting MPIO path verification state to Enabled"; Set-
MPIOSetting -NewPathVerificationState Enabled
     } else { Write-Host "MPIO path verification state already Enabled" }
```

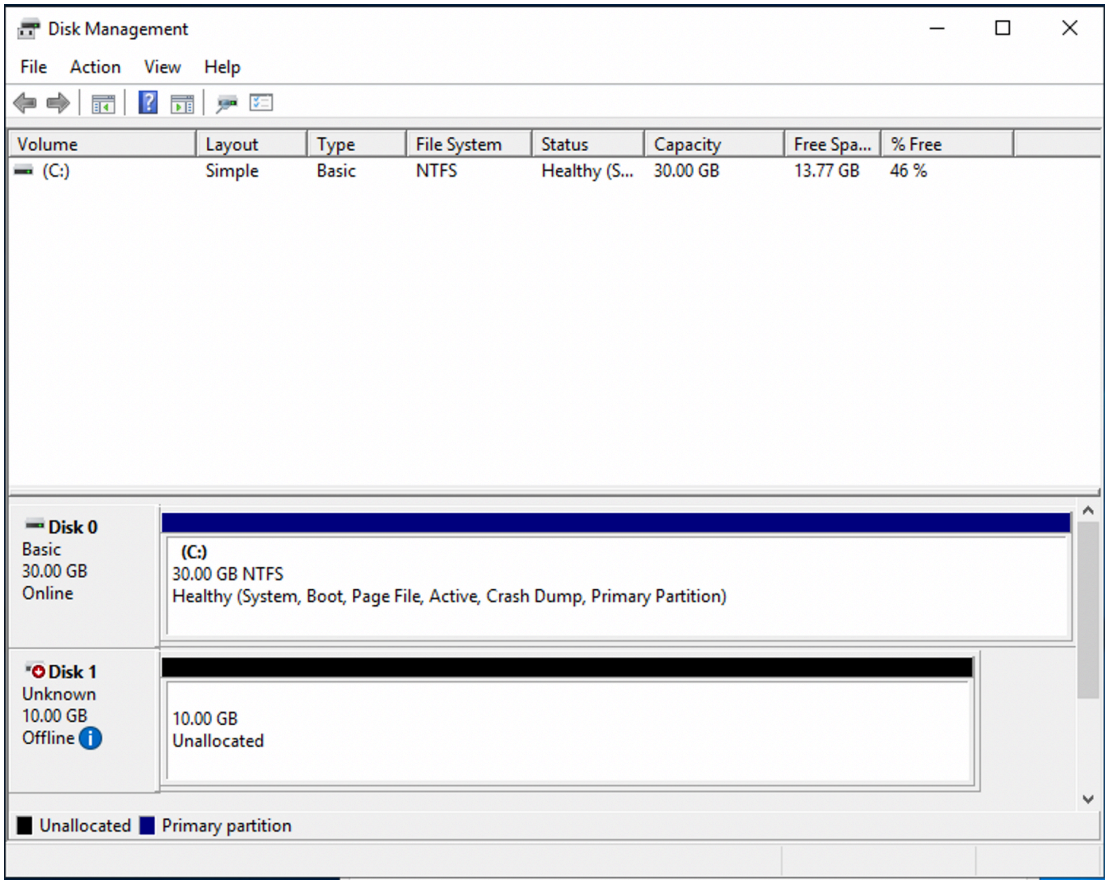
```
    $portalConnectionCounts = @{}
    foreach ($TargetPortalAddress in $TargetPortalAddresses)
{ $portalConnectionCounts[$TargetPortalAddress] = 0 }

    $sessions = Get-IscsiSession
    if ($sessions) {
        foreach ($session in $sessions) {
            if ($session.IsConnected) {
                $targetPortal = (Get-IscsiTargetPortal -iSCSISession
$session).TargetPortalAddress
                if ($portalConnectionCounts.ContainsKey($targetPortal))
{ $portalConnectionCounts[$targetPortal]++ }
            }
        }
    }

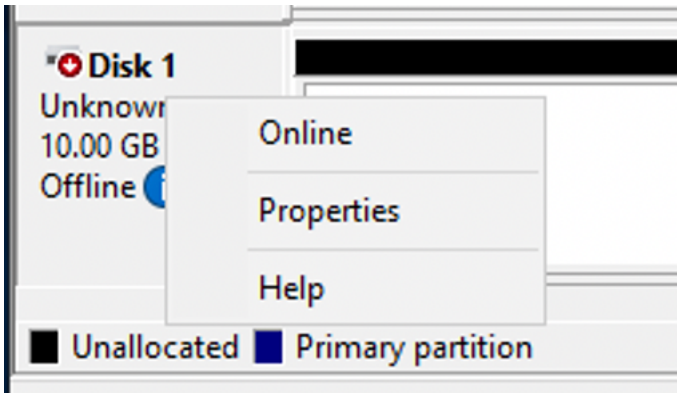
    foreach ($TargetPortalAddress in $TargetPortalAddresses) {
        $existingCount = $portalConnectionCounts[$TargetPortalAddress];
$remainingConnections = $RecommendedConnectionCount - $existingCount
        Write-Host "Portal $TargetPortalAddress has $existingCount
existing connections, $remainingConnections remaining (max recommended:
$RecommendedConnectionCount)"
        if ($remainingConnections -gt 0) {
            Write-Host "Creating $remainingConnections connections for portal
$TargetPortalAddress"
            1..$remainingConnections | ForEach-Object {
                Get-IscsiTarget | Connect-IscsiTarget -IsMultipathEnabled $true -
TargetPortalAddress $TargetPortalAddress -InitiatorPortalAddress $LocaliSCSIAddress
-IsPersistent $true
            }
        } else { Write-Host "Maximum connections (8) reached for portal
$TargetPortalAddress" }
    }

    Set-MSDSMGlobalDefaultLoadBalancePolicy -Policy RR
```

3. 启动 Windows 的“磁盘管理”应用程序。打开 Windows 的“运行”对话框，输入 `diskmgmt.msc`，然后按 Enter。然后，“磁盘管理”应用程序随之打开。



4. 找到未分配的磁盘，那个就是 iSCSI LUN。在此示例中，“Disk 1”即为 iSCSI 磁盘。其处于离线状态。



将光标悬停在 Disk 1 上方，单击右键，然后选择联机，即可使该卷联机。

> **Note**
>
> 您可以修改存储区域网络（SAN）策略，以使新卷能够自动联机。有关更多信息，请参阅 Microsoft Windows Server 命令参考中的 SAN 策略。

5. 要初始化磁盘，请右键单击 Disk 1，然后选择初始化。系统将显示“初始化”对话框。选择确定即可初始化磁盘。
6. 像往常一样格式化磁盘。格式化完成后，iSCSI 驱动器就会在 Windows 客户端上显示为可用驱动器。

验证 iSCSI 配置

我们提供了一个检查 iSCSI 设置是否配置正确的脚本。该脚本检查会话计数、节点分布和多路径 I/O (MPIO) 状态等参数。以下任务介绍了如何安装和使用此脚本。

验证 iSCSI 配置

1. 打开窗户 PowerShell 窗口。
2. 使用以下命令下载脚本。

```
PS C:\> Invoke-WebRequest "https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/
samples/CheckiSCSI.zip" -OutFile "CheckiSCSI.zip"
```

3. 使用以下命令下载 zip 文件。

```
PS C:\> Expand-Archive -Path ".\CheckiSCSI.zip" -DestinationPath "./"
```

4. 使用以下命令运行脚本。

```
PS C:\> ./CheckiSCSI.ps1
```

5. 查看输出以了解配置的当前状态。以下示例演示了成功的 iSCSI 配置。

```
PS C:\> ./CheckiSCSI.ps1

This script checks the iSCSI configuration on the local instance.
It will provide information about the number of connected sessions, connected file
 servers, and MPIO status.

MPIO is installed on this server.

MPIO Load Balance Policy is set to Round Robin (RR).
Initiator: 'iqn.1991-05.com.microsoft:ec2amaz-d2cebnb'
to Target: 'iqn.1992-08.com.netapp:sn.13266b10e61411ee8bc0c76ad263d613:vs.3'
has 16 total sessions (16 active, 0 non-active)
```

```
spread across 2 node(s).
MPIO: Yes
```

为 Linux 配置 NVMe/TCP

FSx for ONTAP 支持基于 TCP 的非易失性存储规范（NVMe/TCP）块存储协议。凭借 NVMe/TCP，您可以使用 ONTAP CLI 配置命名空间和子系统，然后将命名空间映射到子系统，这与配置 LUN 并将其映射到 iSCSI 启动器组（igroup）的方式类似。NVMe/TCP 协议适用于拥有 6 个或更少高可用性（HA）对的第二代文件系统。

> **Note**
>
> FSx for ONTAP 文件系统在 iSCSI 和 NVMe/TCP 块存储协议中均使用 SVM 的 iSCSI 端点。

在适用于 NetApp ONTAP 的 Amazon FSx 上配置 NVMe/TCP 有三个主要步骤，这些步骤将在以下过程中进行介绍：

1. 在 Linux 主机上安装和配置 NVMe 客户端。
2. 在文件系统的 SVM 上配置 NVMe。
   - 创建 NVMe 命名空间。
   - 创建 NVMe 子系统。
   - 将命名空间映射到子系统。
   - 将客户端 NQN 添加到子系统。
3. 在 Linux 客户端上挂载 NVMe 设备。

开始前的准备工作

在开始为 NVMe/TCP 配置文件系统之前，需要完成以下各项。

- 创建 FSx for ONTAP 文件系统。有关更多信息，请参阅 创建文件系统。
- 在与文件系统相同的 VPC 中创建一个运行 Red Hat Enterprise（RHEL）9.3 的 EC2 实例。这是您配置 NVMe 和使用 Linux 版 NVMe/TCP 访问文件数据所在的 Linux 主机。

在这些过程的范围之外，如果主机位于其他 VPC 中，则可以使用 VPC 对等连接或 AWS Transit Gateway 来授予其他 VPC 访问该卷的 iSCSI 端点的权限。有关更多信息，请参阅 从部署 VPC 外部访问数据。

- 配置 Linux 主机的 VPC 安全组，允许入站和出站流量，如 使用 Amazon VPC 进行文件系统访问控制 中所述。
- 获取具有 `fsxadmin` 权限的 ONTAP 用户的凭证，此权限用于访问 ONTAP CLI。有关更多信息，请参阅 ONTAP 角色和用户。
- 您将要为 NVMe 配置并用于访问 FSx for ONTAP 文件系统的 Linux 主机位于同一 VPC 和 AWS 账户 中。
- 我们建议使 EC2 实例与文件系统的首选子网处于同一个可用区。

如果 EC2 实例运行的 Linux AMI 与 RHEL 9.3 不同，则这些过程和示例中使用的某些实用程序可能已安装，并且您可能会使用不同的命令来安装所需的软件包。除了安装软件包外，本节中使用的命令还适用于其他 EC2 Linux AMI。

主题

在 Linux 主机上安装和配置 NVMe

安装 NVMe 客户端

1. 使用 SSH 客户端连接到 Linux 实例。有关更多信息，请参阅使用 SSH 从 Linux 或 macOS 连接到 Linux 实例。
2. 使用以下命令安装 `nvme-cli`：

```
~$ sudo yum install -y nvme-cli
```

3. 将 `nvme-tcp` 模块加载到主机上：

```
$ sudo modprobe nvme-tcp
```

4. 使用以下命令获取 Linux 主机的 NVMe 限定名称（NQN）：

```
$ cat /etc/nvme/hostnqn
nqn.2014-08.org.nvmexpress:uuid:9ed5b327-b9fc-4cf5-97b3-1b5d986345d1
```

请记录响应，以便在后续步骤中使用。

在 FSx for ONTAP 文件系统上配置 NVMe

在文件系统上配置 NVMe

在您计划创建 NVMe 设备所在的 FSx for ONTAP 文件系统上连接 ONTAP CLI。

1. 要访问 ONTAP CLI，请运行以下命令，在适用于 NetApp ONTAP 的 Amazon FSx 文件系统或 SVM 的管理端口上建立 SSH 会话。将 *management_endpoint_ip* 替换为文件系统管理端口的 IP 地址。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   有关更多信息，请参阅 使用 ONTAP CLI 管理文件系统。
2. 在 SVM 上创建一个新的卷以用于访问 NVMe 接口。

   ```
   ::> vol create -vserver fsx -volume nvme_vol1 -aggregate aggr1 -size 1t
        [Job 597] Job succeeded: Successful
   ```
3. 使用 vserver nvme namespace create NetApp ONTAP CLI 命令创建 NVMe 命名空间 ns_1。命名空间映射到启动器（客户端），并控制哪些启动器（客户端）可以访问 NVMe 设备。

   ```
   ::> vserver nvme namespace create -vserver fsx -path /vol/nvme_vol1/ns_1 -size 100g
    -ostype linux
   Created a namespace of size 100GB (107374182400).
   ```
4. 使用 vserver nvme subsystem create NetApp ONTAP CLI 命令创建 NVMe 子系统。

   ```
   ~$ vserver nvme subsystem create -vserver fsx -subsystem sub_1 -ostype linux
   ```
5. 将命名空间映射至刚才创建的子系统。

   ```
   ::> vserver nvme subsystem map add -vserver fsx -subsystem sub_1 -path /vol/
   nvme_vol1/ns_1
   ```

6. 使用之前检索到的 NQN 将客户端添加到子系统。

```
::> vserver nvme subsystem host add -subsystem sub_1 -host-nqn
 nqn.2014-08.org.nvmexpress:uuid:ec21b083-1860-d690-1f29-44528e4f4e0e -vserver fsx
```

如果要将映射到此子系统的设备供多个主机使用，您可以在逗号分隔列表中指定多个启动程序名称。有关更多信息，请参阅 NetApp ONTAP 文档中的虚拟服务器 NVMe 子系统主机的添加。

7. 使用 vserver nvme namespace show 命令确认命名空间存在：

```
::> vserver nvme namespace show -vserver fsx -instance
Vserver Name: fsx
            Namespace Path: /vol/nvme_vol1/ns_1
                      Size: 100GB
                 Size Used: 90.59GB
                   OS Type: linux
                   Comment:
                Block Size: 4KB
                     State: online
         Space Reservation: false
Space Reservations Honored: false
              Is Read Only: false
             Creation Time: 5/20/2024 17:03:08
            Namespace UUID: c51793c0-8840-4a77-903a-c869186e74e3
                 Vdisk ID: 80d42c6f00000000187cca9
      Restore Inaccessible: false
   Inconsistent Filesystem: false
       Inconsistent Blocks: false
                   NVFail: false
Node Hosting the Namespace: FsxId062e9bb6e05143fcb-01
               Volume Name: nvme_vol1
                Qtree Name:
          Mapped Subsystem: sub_1
            Subsystem UUID: db526ec7-16ca-11ef-a612-d320bd5b74a9
              Namespace ID: 00000001h
              ANA Group ID: 00000001h
              Vserver UUID: 656d410a-1460-11ef-a612-d320bd5b74a9
                Vserver ID: 3
              Volume MSID: 2161388655
              Volume DSID: 1029
                 Aggregate: aggr1
            Aggregate UUID: cfa8e6ee-145f-11ef-a612-d320bd5b74a9
 Namespace Container State: online
```

```
        Autodelete Enabled: false
          Application UUID: -
               Application: -
  Has Metadata Provisioned: true

1 entries were displayed.
```

8. 使用 network interface show -vserver 命令检索您在其中创建 NVMe 设备的 SVM 的块存储接口的地址。

```
::> network interface show -vserver svm_name -data-protocol nvme-tcp
            Logical               Status     Network            Current
        Current Is
Vserver     Interface             Admin/Oper Address/Mask       Node
        Port    Home
----------- ----------            ---------- ------------------ -------------
        ------- ----
svm_name
            iscsi_1               up/up      172.31.16.19/20
 FSxId0123456789abcdef8-01  e0e     true
            iscsi_2               up/up      172.31.26.134/20
 FSxId0123456789abcdef8-02  e0e     true
2 entries were displayed.
```

> **Note**
>
> iscsi_1 LIF 对 iSCSI 和 NVMe/TCP 均适用。

在此示例中，iscsi_1 的 IP 地址为 172.31.16.19，iscsi_2 的 IP 地址为 172.31.26.134。

在 Linux 客户端上挂载 NVMe 设备。

在 Linux 客户端上挂载 NVMe 设备的过程包括三个步骤：

1. 发现 NVMe 节点
2. 对 NVMe 设备进行分区
3. 在客户端上挂载 NVMe 设备

以下过程将详述这些步骤。

发现目标 NVMe 节点

1. 在 Linux 客户端上，使用以下命令来发现目标 NVMe 节点。将 *iscsi_1_IP* 替换为 iscsi_1 的 IP 地址以及 *client_IP* 客户端的 IP 地址。

> **Note**
>
> iscsi_1 和 iscsi_2 LIF 对 iSCSI 和 NVMe 存储均适用。

```
~$ sudo nvme discover -t tcp -w client_IP -a iscsi_1_IP
```

```
Discovery Log Number of Records 4, Generation counter 11
=====Discovery Log Entry 0======
trtype:  tcp
adrfam:  ipv4
subtype: current discovery subsystem
treq:    not specified
portid:  0
trsvcid: 8009
subnqn:  nqn.1992-08.com.netapp:sn.656d410a146011efa612d320bd5b74a9:discovery
traddr:  172.31.26.134
eflags:  explicit discovery connections, duplicate discovery information
sectype: none
=====Discovery Log Entry 1======
trtype:  tcp
adrfam:  ipv4
subtype: current discovery subsystem
treq:    not specified
portid:  1
trsvcid: 8009
subnqn:  nqn.1992-08.com.netapp:sn.656d410a146011efa612d320bd5b74a9:discovery
traddr:  172.31.16.19
eflags:  explicit discovery connections, duplicate discovery information
sectype: none
```

2. （可选）要为文件系统的 NVMe 设备带来高于 Amazon EC2 单一客户端最大 5Gbps（约 625MBps）的吞吐量，请按照《适用于 Linux 实例的 Amazon Elastic Compute Cloud 用户指南》中的 Amazon EC2 实例网络带宽描述的过程建立更多的会话。

3. 在控制器断开超时至少达到 1800 秒的情况下，再次使用 iscsi_1 的 IP 地址（*iscsi_1_IP*）和客户端的 IP 地址（*client_IP*）登录目标启动器。NVMe 设备显示为可用磁盘。

```
~$ sudo nvme connect-all -t tcp -w client_IP -a iscsi_1 -l 1800
```

4. 使用以下命令验证 NVMe 堆栈是否已识别并合并多个会话且配置了多路径。如果配置成功，则命令会返回确认 Y。

```
~$ cat /sys/module/nvme_core/parameters/multipath
Y
```

5. 使用以下命令验证相应 ONTAP 命名空间的 NVMe-oF 设置 model 是否设置为 NetApp ONTAP Controller，负载均衡 iopolicy 是否设置为 round-robin，以使 I/O 分布在所有可用的路径上

```
~$ cat /sys/class/nvme-subsystem/nvme-subsys*/model
Amazon Elastic Block Store
NetApp ONTAP Controller
~$ cat /sys/class/nvme-subsystem/nvme-subsys*/iopolicy
numa
round-robin
```

6. 使用以下命令验证是否在主机上创建并正确发现了命名空间。

```
~$ sudo nvme list
Node                  Generic               SN                   Model
                        Namespace  Usage                      Format           FW
 Rev
--------------------- --------------------- --------------------
 ---------------------------------------- ---------- --------------------------
 ---------------- --------
/dev/nvme0n1          /dev/ng0n1            vol05955547c003f0580 Amazon Elastic
 Block Store               0x1         25.77  GB /  25.77  GB    512   B +  0 B
 1.0
/dev/nvme2n1          /dev/ng2n1            lWB12JWY/XLKAAAAAAAC NetApp ONTAP
 Controller                0x1        107.37  GB / 107.37  GB      4 KiB +  0 B
 FFFFFFFF
```

输出中的新设备为 /dev/nvme2n1。根据 Linux 安装情况，此命名方案可能会有所不同。

7. 验证每条路径的控制器状态是否处于活动状态，以及是否具有正确的非对称命名空间访问（ANA）多路径状态：

```
~$ nvme list-subsys /dev/nvme2n1
nvme-subsys2 -
 NQN=nqn.1992-08.com.netapp:sn.656d410a146011efa612d320bd5b74a9:subsystem.rhel
              hostnqn=nqn.2014-08.org.nvmexpress:uuid:ec2a70bf-3ab2-6cb0-
f997-8730057ceb24
              iopolicy=round-robin
\
 +- nvme2 tcp
 traddr=172.31.26.134,trsvcid=4420,host_traddr=172.31.25.143,src_addr=172.31.25.143
 live non-optimized
 +- nvme3 tcp
 traddr=172.31.16.19,trsvcid=4420,host_traddr=172.31.25.143,src_addr=172.31.25.143
 live optimized
```

在此示例中，NVMe 堆栈已自动发现了文件系统的备用 iscsi_2 LIF，即 172.31.26.134。

8. 验证 NetApp 插件是否为每个 ONTAP 命名空间设备显示了正确的值：

```
~$ sudo nvme netapp ontapdevices -o column
Device           Vserver                   Namespace Path
           NSID UUID                                   Size
---------------- ------------------------
 ------------------------------------------------- ----
 ------------------------------------- ---------
/dev/nvme2n1     fsx                       /vol/nvme_vol1/ns_1
           1    0441c609-3db1-4b0b-aa83-790d0d448ece   107.37GB
```

对设备进行分区

1. 使用以下命令验证您的 device_name nvme2n1 路径是否存在。

```
~$ ls /dev/mapper/nvme2n1
/dev/nvme2n1
```

2. 使用 fdisk 对磁盘进行分区。您需要输入交互式提示。按显示的顺序输入选项。您可以使用小于最后一个扇区的值来创建多个分区（在本例中为 20971519）。

> **Note**
>
> Last sector 值根据 NVMe 设备的大小（在本例中为 100 GiB）而不同。

```
~$ sudo fdisk /dev/mapper/nvme2n1
```

开始进行 fsdisk 交互式提示。

```
Welcome to fdisk (util-linux 2.37.4).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0x66595cb0.

Command (m for help): n
Partition type
   p primary (0 primary, 0 extended, 4 free)
   e extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1): 1
First sector (256-26214399, default 256):
Last sector, +sectors or +size{K,M,G,T,P} (256-26214399, default
 26214399): 20971519

Created a new partition 1 of type 'Linux' and of size 100 GiB.
Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.
```

输入 w 后，您的新分区 /dev/nvme2n1 即变为可用。*partition_name* 的格式为 *<device_name><partition_number>*。1 已用作上一步 fdisk 命令中的分区编号。

3. 使用 /dev/nvme2n1 作为创建文件系统的路径。

```
~$ sudo mkfs.ext4 /dev/nvme2n1
```

系统将使用以下输出做出响应：

```
mke2fs 1.46.5 (30-Dec-2021)
Found a dos partition table in /dev/nvme2n1
Proceed anyway? (y,N) y
Creating filesystem with 26214400 4k blocks and 6553600 inodes
Filesystem UUID: 372fb2fd-ae0e-4e74-ac06-3eb3eabd55fb
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
    4096000, 7962624, 11239424, 20480000, 23887872

Allocating group tables: done
Writing inode tables: done
Creating journal (131072 blocks): done
Writing superblocks and filesystem accounting information: done
```

在 Linux 客户端上挂载 NVMe 设备

1. 创建一个目录 *directory_path* 作为 Linux 实例上的文件系统的挂载点。

```
~$ sudo mkdir /directory_path/mount_point
```

2. 使用以下命令挂载文件系统。

```
~$ sudo mount -t ext4 /dev/nvme2n1 /directory_path/mount_point
```

3. （可选）如果要向特定用户授予挂载目录的所有权，请将 *username* 替换为拥有者的用户名。

```
~$ sudo chown username:username /directory_path/mount_point
```

4. （可选）验证您是否可以从文件系统读取数据和将数据写入文件系统。

```
~$ echo "Hello world!" > /directory_path/mount_point/HelloWorld.txt
~$ cat directory_path/HelloWorld.txt
Hello world!
```

您在 Linux 客户端上成功创建并挂载了一个 NVMe 设备。

通过 Amazon S3 接入点访问您的数据

您还可以使用 S3 接入点访问存储在 Amazon FSx 文件系统中的文件数据，就像这些数据存储在 S3 中一样，这样您就可以将其用于与 S3 配合使用的应用程序和服务，而无需更改应用程序或将数据移出文件存储。Amazon S3 接入点是连接到 S3 存储桶或 ONTAP 的 FSX 和 OpenZFS 卷的 fsX 的 S3 终端节点。Amazon S3 接入点简化了任何与 S3 配合使用的应用程序或 AWS 服务的数据访问管理。借助 S3 接入点，拥有共享数据集（包括数据湖、媒体档案和用户生成的内容）的客户可以轻松控制和扩展数百个应用程序、团队或个人的数据访问权限，方法是创建个性化的接入点，并为每个应用程序、团队或个人自定义名称和权限。

连接到 Amazon FSx 的 NetApp ONTAP 卷的 S3 接入点支持对 Amazon S3 终端节点使用 S3 对象操作（例如`GetObject`、`PutObject`、和`ListObjectsV2`）对您的文件数据进行读写访问。

连接到 FSx for ONTAP 文件系统的每个 S3 接入点都有一个 AWS Identity and Access Management (IAM) 接入点策略和一个关联的 UNIX 或 Windows 文件系统用户，用于授权通过该接入点发出的所有请求。对于每个请求，S3 首先评估所有相关策略，包括用户、接入点、S3 VPC 端点和服务控制策略的策略，以授权请求。请求获得 S3 授权后，文件系统会对请求进行授权，文件系统会评估与 S3 接入点关联的文件系统用户是否有权访问文件系统上的数据。您可以将接入点配置为仅接受来自虚拟私有云 (VPC) 的请求，从而限制 Amazon S3 数据访问私有网络。默认情况下，Amazon S3 会对连接到 FSx for ONTAP 卷的所有接入点强制禁止公开访问，并且您无法修改或禁用此设置。

您可以使用 Amazon FSx 控制台、CLI 和 API 创建 S3 接入点并将其连接到 FSx for ONTAP 卷。接入点允许您使用 S3 API 访问文件数据，但您的数据将继续驻留在 FSx for ONTAP 文件系统上，并且您可以继续使用 NFS 和 SMB 协议与 S3 API 一起访问您的数据。

适用于 ONTAP 文件系统的 FSx 的 Amazon S3 接入点提供的延迟在数十毫秒范围内，这与 S3 存储桶访问一致。通过 S3 API 可以驱动到 Amazon FSx 文件系统的吞吐量和每秒请求量取决于文件系统的预配置吞吐量。有关文件系统性能功能的更多信息，请参见 适用于 ONTAP 性能的 Amazon FS NetApp x

主题

- AWS 区域 使用适用于 ONTAP 的 FSx 的 Amazon S3 接入点
- 接入点命名规则、限制和局限性
- 使用接入点别名来引用接入点 ARNs，或 virtual-hosted-style URIs
- 接入点兼容性
- 管理接入点接入
- 创建接入点

- 为 Amazon S3 接入点配置网络访问权限
- 管理 Amazon S3 接入点
- 使用接入点
- 将接入点与 AWS 服务
- 对 S3 接入点问题进行故障排除

AWS 区域 使用适用于 ONTAP 的 FSx 的 Amazon S3 接入点

以下地区支持 FSx for ONTAP 的 Amazon S3 接入点 AWS 区域：非洲（开普敦）、亚太地区（香港、海得拉巴、雅加达、墨尔本、孟买、大阪、首尔、新加坡、悉尼、东京）、加拿大（中部）、加拿大西部（卡尔加里）、欧洲（法兰克福、爱尔兰、伦敦、米兰、巴黎、西班牙、斯德哥尔摩、苏黎世）、以色列（特拉维夫）、中东（巴林、阿联酋）、南美洲（圣保罗）、美国东部（弗吉尼亚北部、俄亥俄州）和美国西部（加利福尼亚北部、俄勒冈州）。

接入点命名规则、限制和局限性

创建 S3 接入点时，您需要为其选择一个名称。以下主题提供有关 S3 接入点命名规则以及限制和限制的信息。

主题

- 接入点命名规则
- 接入点限制和局限性

接入点命名规则

创建 S3 接入点时，您可以选择其名称。接入点名称在 AWS 账户 或之间不必是唯一的 AWS 区域。同样的 AWS 账户 方法可能会创建名称相同的不同接入点， AWS 区域 或者两个不同的接入点 AWS 账户 可能使用相同的接入点名称。但是，在一个 a AWS 区域 中 AWS 账户 可能没有两个名称相同的接入点。

S3 接入点名称不能以后缀结尾`-ext-s3alias`，后缀是为接入点别名保留的。有关接入点命名规则的完整列表，请参阅《亚马逊简单存储服务用户指南》中的 Amazon S3 接入点命名规则。

接入点限制和局限性

连接到 FSx 的 ONTAP 卷的 S3 接入点具有以下限制，这些限制不适用于连接到 S3 存储桶的接入点：

- 您只能使用与要连接的 FSx for ONTAP 卷 AWS 区域 相同的方式创建 S3 接入点。
- 同样 AWS 账户 必须拥有适用于 ONTAP 文件系统的 FSx 和 S3 接入点。您只能为自己拥有的 ONTAP 卷创建连接到 FSx 的 S3 接入点。您无法创建附加到其他卷所拥有的 S3 接入点 AWS 账户。
- 对于运行 NetApp ONTAP 版本 9.17.1 及更高版本的 ONTAP 文件系统，您只能创建 S3 接入点并将其连接到 FSx。

有关所有接入点限制和限制的完整列表，请参阅 Amazon Simple Storage Service 用户指南中的接入点限制和限制。

使用接入点别名来引用接入点 ARNs，或 virtual-hosted-style URIs

创建连接到 for ONTAP 卷 FSx 的接入点后，您可以通过 AWS CLI 和 S3 API 以及兼容 S3 的第三方 AWS 服务和应用程序访问您的数据。在 AWS 服务 或应用程序中提及接入点时，您可以使用 Amazon 资源名称 (ARN)、接入点别名或虚拟托管样式 URI。

主题

- 接入点 ARNs
- 接入点别名
- 虚拟托管类型 URI

接入点 ARNs

接入点有 Amazon 资源名称 (ARNs)。接入点 ARNs 与 S3 存储桶类似 ARNs，但它们是显式键入的，并对接入点 AWS 区域 和接入点所有者的 AWS 账户 ID 进行编码。有关更多信息 ARNs，请参阅AWS Identity and Access Management 用户指南中的使用 Amazon 资源名称识别 AWS 资源 (ARNs)。

接入 ARNs 点采用以下格式：

```
arn:aws::s3:region:account-id:accesspoint/resource
```

`arn:aws:s3:us-west-2:777777777777:accesspoint/test`代表名为的接入点`test`，该接入点归该地区账户 7777777777 所有。`us-west-2`

ARNs 对于通过接入点访问的对象和文件，请使用以下格式：

```
arn:aws::s3:region:account-id:accesspoint/access-point-name/object/resource
```

arn:aws:s3:us-west-2:111122223333:accesspoint/*test*/object/*lions.jpg*表示通过名为的接入点访问的文件 *lions.jpgtest*，该接入点归该地区账户 111122223333 所有。*us-west-2*

有关接入点的更多信息 ARNs，请参阅 Amazon 简单存储服务用户指南 ARNs中的接入点。

接入点别名

创建接入点时，Amazon S3 会自动生成一个接入点别名，您可以在任何可以使用 S3 存储桶名称访问数据的地方使用该别名。

接入点别名无法更改。对于连接到 for ONTAP 卷 FSx 的接入点，接入点别名由以下部分组成：

```
access point prefix-metadata-ext-s3alias
```

下图显示了连接到 for ONTAP 卷的 S3 接入点的 ARN 和接入点别名，这些接入点作为对 CLI 命令describe-s3-access-point-attachments FSx 的响应的一部分返回。 FSx 本示例中的接入点名为my-ontap-ap。

```
...
        "S3AccessPoint": {
            "ResourceARN": "arn:aws:s3:us-east-1:111122223333:accesspoint/my-ontap-ap",
            "Alias": "my-ontap-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias",
...
```

> **Note**
>
> 该-ext-s3alias后缀保留给连接到 for ONTAP 卷的 S3 接入点 FSx 的别名，不能用于接入点名称。

在某些 S3 数据平面操作中，您可以使用接入点别名代替 Amazon S3 接入点 ARN。有关支持的操作的列表，请参阅接入点兼容性。

有关完整的接入点别名限制，请参阅《Amazon 简单存储服务用户指南》中的接入点别名限制。

虚拟托管类型 URI

接入点仅支持 virtual-host-style寻址。在虚拟托管式的 URI 中，接入点名称和 AWS 区域 是 URL 中域名的一部分。 AWS 账户要查看连接到 for ONTAP 卷的接入点的 S3 URI，请在 S3 接入点详细信息下

的接入点详细信息页面中，选择为 S 3 接入点列出的接入点名称。 FSx 这将带您进入 Amazon S3 控制台中的接入点详细信息页面。您可以在 “属性” 下找到 S3 URI。

有关更多信息，请参阅《亚马逊简单存储服务用户指南》中的虚拟托管式 URI。

接入点兼容性

您可以使用访问点访问存储在 for ONTAP 卷上的数据，使用 FSx 以下 Amazon S3 APIs 进行数据访问。下面列出的所有操作都可以接受接入点 ARNs 或接入点别名。

下表是 Amazon S3 操作以及它们是否与接入点兼容的部分列表。下表显示了使用 for ONTAP 卷作为数据源的接入点支持哪些操作。 FSx

S3 操作	连接到 for ONTAP FSx 卷的接入点
AbortMultipartUpload	支持
CompleteMultipartUpload	支持
CopyObject （仅限同区域副本）	如果源和目标位于同一个接入点内，则支持
CreateMultipartUpload	支持
DeleteObject	支持
DeleteObjects	支持
DeleteObjectTagging	支持
GetBucketAcl	不支持
GetBucketCors	不支持
GetBucketLocation	支持
GetBucketNotificationConfiguration	不支持
GetBucketPolicy	不支持
GetObject	支持

S3 操作	连接到 for ONTAP FSx 卷的接入点
GetObjectAcl	不支持
GetObjectAttributes	支持
GetObjectLegalHold	不支持
GetObjectRetention	不支持
GetObjectTagging	支持
HeadBucket	支持
HeadObject	支持
ListMultipartUploads	支持
ListObjects	支持
ListObjectsV2	支持
ListObjectVersions	不支持
ListParts	支持
Presign	不支持
PutObject	支持
PutObjectAcl	不支持
PutObjectLegalHold	不支持
PutObjectRetention	不支持
PutObjectTagging	支持
RestoreObject	不支持
UploadPart	支持

S3 操作	连接到 for ONTAP FSx 卷的接入点
UploadPartCopy （仅限同区域副本）	如果源和目标位于同一个接入点内，则支持

使用 Amazon S3 操作的限制如下：

- 上传的最大对象大小为 5 GB，但您可以下载大于该值的对象
- FSX_ONTAP是唯一支持的存储类别
- SSE-FSX 是唯一支持的服务器端加密模式
- 不支持以下 Amazon S3 功能：请求者付款之外的访问控制列表 (ACLs) bucket-owner-full-control、对象版本控制、对象锁定、对象生命周期、静态网站托管（例如网站重定向）、多因素身份验证 (MFA) 和条件写入

有关使用接入点对文件数据执行数据访问操作的示例，请参见使用接入点。

对象 ETag

实体标签是对象的哈希。仅 ETag 反映对象内容的更改，而不反映其元数据的更改。 ETag 不是对象数据的 MD5 摘要。

对象校验和

您可以使用校验和值来验证所上传数据的完整性。当您上传数据并指定校验和算法时， AWS SDK 会在传输数据之前使用您选择的校验和算法来计算校验和值。然后，Amazon S3 会独立计算您的数据的校验和，并根据提供的校验和值对其进行验证。只有在确认传输到 Amazon S3 期间保持了数据完整性之后，才会接受对象。与 Amazon S3 通用存储桶中对象的校验和不同，校验和值不作为对象元数据存储在 NetApp ONTAP 卷中，也不是对象本 FSx 身。这意味着校验和值不会在响应中返回，也不会用于在下载时验证对象的完整性。

使用亚马逊进行服务器端加密 FSx (SSE-FSX)

所有 Amazon FSx 文件系统都默认配置了加密，并使用使用管理的密钥进行静态加密 AWS Key Management Service。当向文件系统写入数据和从文件系统读取数据时，数据会在文件系统上自动加密和解密。这些流程由 Amazon FSx 以透明方式处理。

分段上传

分段上传允许将单个对象作为一组分段上传。每个分段都是对象数据的连续部分。您可以独立上传以及按任意顺序上传这些对象分段。将 S3 接入点与 for ONTAP 配合 FSx 使用时，分段上传有以下注意事项：

- ONTAP 卷备份中不包含与正在进行的分段上传（即未完成的上传）相关的部分。 FSx
- 与正在进行的分段上传（即未完成的上传）段相关的已用存储空间不会反映在目标卷的`StorageUsed`存储容量 CloudWatch 指标中，而是反映在父文件系统的`StorageUsed`存储容量 CloudWatch 指标中。
- 分段上传操作完成后，关联的段元数据将不再与对象一起存储。这意味着您无法使用`GetObjectAttributes`正在读取的对象的部件号来检索对象部分元数据，也无法通过正在读取的对象的部件号下载对象的单个部分。

访问控制列表（ACL）

使用 Amazon S3 访问控制列表 (ACLs)，您可以管理对存储桶和对象的访问权限。 FSx 仅适用于 S3 的接入点支持 `bucket-owner-full-control` ACL 值。使用任何其他 ACL 值都将导致`InvalidArgument`异常。

管理接入点接入

您可以为每个 S3 接入点配置不同的权限和网络控制，S3 适用于使用该接入点发出的任何请求。S3 接入点支持 AWS Identity and Access Management (IAM) 资源策略，您可以使用这些策略按资源、用户或其他条件控制接入点的使用。要使应用程序或用户通过接入点访问文件，接入点和底层卷都必须允许该请求。有关更多信息，请参阅 IAM 接入点策略。

适用于 ONTAP 的 FSx 的 Amazon S3 接入点使用双层授权模型，将 AWS IAM 权限与文件系统级权限相结合。这种方法可确保在 AWS 服务级别和底层文件系统级别对数据访问请求进行适当授权。

要使应用程序或用户成功地通过接入点访问数据，S3 接入点策略和 ONTAP 卷的底层 FSx 都必须允许该请求。

主题

- 文件系统用户身份和授权
- S3 API 请求授权
- S3 阻止公有访问
- IAM 接入点策略

文件系统用户身份和授权

在为 FSx for ONTAP 卷创建 S3 接入点时，需要指定一个文件系统身份，该身份将用于授权通过该接入点发出的所有文件系统请求。此文件系统标识决定根据文件系统的权限模型授予对底层文件和目录的访问权限级别。文件系统用户是底层 Amazon FSx 文件系统上的用户账户。如果文件系统用户具有只读访问权限，则只有使用访问点发出的读取请求才会获得授权，并且写入请求会被阻止。如果文件系统用户具有读写访问权限，则使用访问点对连接的卷发出的读取和写入请求都将获得授权。

文件系统标识可以是以下两种类型之一：

- UNIX 身份 — 使用 UNIX 安全方式访问卷时使用 UNIX 身份（用户名）
- Windows 身份 — 使用 NTFS 安全模式访问卷时使用 Windows 身份（域和用户名）。

当您指定 UNIX 或 Windows 身份时，通过接入点执行的所有 S3 API 操作都将使用该用户在文件系统上的权限进行授权。

您与接入点关联的文件系统身份决定了对文件和目录的访问级别。例如，如果您将接入点与根 UNIX 身份 (UID 0) 相关联，后者通常对文件系统具有完全的文件访问权限，则所有文件操作都将获得授权。相反，如果您将接入点与受限制的用户身份相关联，则文件操作将仅限于该用户可以访问的内容，具体取决于文件系统的权限模型。

对于具有 UNIX 安全风格的卷，应使用 UNIX 文件系统标识类型，对于具有 NTFS 安全风格的卷，应使用 Windows 标识类型。这种调整可确保授权模型与卷的安全配置相匹配。

对于 UNIX 安全风格的卷，文件系统使用模式位或 NFSv4 ACL 来控制访问权限。对于 NTFS 安全风格的卷，文件系统使用 Windows ACL 来控制访问权限。

> **Important**
>
> 直接通过 NFS 或 SMB 访问卷时，将 S3 接入点连接到 FSx for ONTAP 卷不会改变该卷的行为。所有针对该卷的现有操作都将像以前一样继续运行。您在 S3 接入点策略中包含的限制仅适用于使用接入点发出的请求。

> **Note**
>
> 如果无法在文件系统上解析与接入点关联的文件系统身份，或者连接的卷变为脱机或已卸载，则 S3 接入点可以转换到该`MISCONFIGURED`状态。在此状态下，通过接入点发出的 S3

请求可能会失败。Amazon FSx 会定期检查这些情况，并在问题解决后自动将接入点返回到AVAILABLE。有关更多信息，请参阅 S3 接入点处于配置错误的状态。

S3 API 请求授权

当您通过连接到 FSx for NetApp ONTAP 卷的接入点发出 S3 API 请求时，Amazon S3 会根据接入点的 IAM 资源策略评估调用委托人的 IAM 权限。IAM 委托人调用者必须拥有通过其基于身份的策略授予的必要权限，并且接入点的资源策略也必须允许所请求的操作。

Amazon S3 会评估所有相关策略（包括用户策略、接入点策略、VPC 终端节点策略和服务控制策略），以确定是否对请求进行授权。

您还可以将 S3 接入点配置为仅接受来自特定虚拟私有云 (VPC) 的请求，以限制数据访问。有关更多信息，请参阅 创建限制到 Virtual Private Cloud 的接入点。

S3 阻止公有访问

连接到 FSx for ONTAP 卷的 Amazon S3 接入点会自动配置为启用封锁公有访问，但您无法更改该功能。

IAM 接入点策略

Amazon S3 接入点支持 AWS Identity and Access Management (IAM) 资源策略，允许您根据资源、用户或其他条件控制接入点的使用。为了使应用程序或用户能够通过接入点访问对象，接入点和底层数据源都必须允许该请求。

创建可选接入点策略需要该权限。s3:PutAccessPointPolicy

将 S3 接入点连接到 Amazon FSx 卷后，针对该卷的所有现有操作都将像以前一样继续运行。您在接入点策略中包括的限制仅适用于通过该接入点发出的请求。有关更多信息，请参阅 A mazon 简单存储服务用户指南中的配置 IAM 策略以使用接入点。

使用 Amazon FSx 控制台创建连接到 FSx for ONTAP 卷的接入点时，您可以配置接入点策略。要在现有 S3 接入点上添加、修改或删除接入点策略，可以使用 S3 控制台、CLI 或 API。

创建接入点

您可以使用亚马逊 FSx 控制台、CLI、API 和支持的软件开发工具包创建和管理连接到 Amazon FSx 卷的 S3 接入点。

> **Note**
>
> 由于您可能需要公开 S3 接入点名称以便其他用户可以使用该接入点，因此请避免在 S3 接入点名称中包含敏感信息。接入点名称将在称为域名系统（DNS）的可公开访问的数据库中得以发布。有关接入点名称的更多信息，请参阅接入点命名规则。

所需的权限

创建连接到 Amazon FSx 卷的 S3 接入点需要以下权限：

- `fsx:CreateAndAttachS3AccessPoint`
- `s3:CreateAccessPoint`
- `s3:GetAccessPoint`

使用 Amazon FSx 或 S3 控制台创建可选接入点策略需要该`s3:PutAccessPointPolicy`权限。有关更多信息，请参阅 IAM 接入点策略。

要创建接入点，请参阅以下主题。

主题

- 创建接入点
- 创建限制到 Virtual Private Cloud 的接入点

创建接入点

> **Important**
>
> 要将 S3 接入点连接到 FSx for ONTAP 卷，必须安装该卷（具有接合路径）。有关更多详细信息，请参阅 ONTAP 文档。

在为您的卷创建 S3 接入点时，您的账户中必须已经存在适用于 ONTAP 卷的 FSx。

要创建连接到 FSx for ONTAP 卷的 S3 接入点，请指定以下属性：

- 接入点名称。有关接入点命名规则的信息，请参阅接入点命名规则。

- 用于授权使用接入点发出的文件访问请求的文件系统用户身份。在 UNIX 或 Windows 中指定要包含的 POSIX 用户名。有关更多信息，请参阅 文件系统用户身份和授权。
- 接入点的网络配置决定了接入点是可以从 Internet 访问还是仅限于特定的虚拟私有云 (VPC) 进行访问。有关更多信息，请参阅 创建限制到 Virtual Private Cloud 的接入点。

创建连接到 FSx 卷的 S3 接入点（FSx 控制台）

1. 打开 Amazon FSx 控制台，网址为。https://console.aws.amazon.com/fsx/
2. 在页面顶部的导航栏中，选择要 AWS 区域 在其中创建接入点的。接入点必须在与关联卷相同的区域中创建。
3. 在左侧导航窗格中，选择卷。
4. 在卷页面上，选择要将接入点连接到的 FSx for ONTAP 卷。
5. 从 “操作” 菜单中选择 “创建 S3 接入点”，显示 “创建 S3 接入点” 页面。
6. 在接入点名称中，输入接入点的名称。有关接入点名称的准则和限制的更多信息，请参阅接入点命名规则。

   数据源详细信息中填充了您在步骤 3 中选择的卷的信息。
7. Amazon FSx 使用文件系统用户身份对使用此接入点发出的文件访问请求进行身份验证。请确保您指定的文件系统用户对 FSx for ONTAP 卷具有正确的权限。

   对于文件系统用户身份类型，请选择 UNIX 或 Windows。
8. 在用户名中输入用户的用户名。
9. 在网络配置面板中，您可以选择接入点是可以从 Internet 访问，还是只能访问特定的虚拟私有云。

   对于网络来源，选择 Internet 以使接入点可通过互联网访问，或者选择虚拟私有云 (VPC)，然后输入要限制访问接入点的 VPC ID。

   有关接入点的网络源的更多信息，请参阅创建限制到 Virtual Private Cloud 的接入点。
10. （可选）在 “接入点策略-可选” 下，指定可选的接入点策略。请务必解决所有政策警告、错误和建议。有关指定接入点策略的更多信息，请参阅 A mazon 简单存储服务用户指南中的配置 IAM 策略以使用接入点。
11. 选择创建接入点以查看接入点连接配置。

创建连接到 FSx 卷的 S3 接入点 (CLI)

以下示例命令创建一个名为的接入点*my-ontap-ap*，该接入点连接到账户*fsvol-0123456789abcdef9*中的 FSx for ONTAP 卷。*111122223333*

```
$ aws fsx create-and-attach-s3-access-point --name my-ontap-ap --type ONTAP --ontap-configuration \
   VolumeId=fsvol-0123456789abcdef9,FileSystemIdentity='{Type=UNIX,UnixUser={Name=ec2-user}}' \
   --s3-access-point VpcConfiguration='{VpcId=vpc-0123467},Policy=access-point-policy-json
```

如果请求成功，系统会通过返回新的 S3 接入点附件进行响应。

```
$ {
  {
     "S3AccessPointAttachment": {
        "CreationTime": 1728935791.8,
        "Lifecycle": "CREATING",
        "LifecycleTransitionReason": {
            "Message": "string"
        },
        "Name": "my-ontap-ap",
        "OntapConfiguration": {
            "VolumeId": "fsvol-0123456789abcdef9",
            "FileSystemIdentity": {
                "Type": "UNIX",
                "UnixUser": {
                    "Name": "ec2-user"
                }
            }
        },
        "S3AccessPoint": {
            "ResourceARN": "arn:aws:s3:us-east-1:111122223333:accesspoint/my-ontap-ap",
            "Alias": "my-ontap-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias",
            "VpcConfiguration": {
                "VpcId": "vpc-0123467"
        }
     }
  }
}
```

> **Note**
>
> 创建 S3 接入点并AVAILABLE处于该状态后，MISCONFIGURED如果无法在文件系统上解析与该接入点关联的文件系统身份，或者连接的卷处于脱机状态或已卸载，则该接入点可以转换为。Amazon FSx 会定期检查这些情况，并在潜在问题解决后自动将接入点返回AVAILABLE到该接入点。处于该MISCONFIGURED状态时，通过接入点发出的 S3 请求可能会失败。有关更多信息，请参阅 S3 接入点处于配置错误的状态。

创建限制到 Virtual Private Cloud 的接入点

创建接入点时，您可以选择允许通过互联网访问接入点，也可以指定通过该接入点发出的所有请求都必须来自特定的 Amazon Virtual Private Cloud。可从 Internet 访问的接入点被认为是具有 `Internet` 网络起源。它可以从互联网上的任何地方使用，但要遵守接入点、底层存储桶或 Amazon FSx 卷以及相关资源（例如请求的对象）的任何其他访问限制。只能从指定的 Amazon VPC 访问的接入点的网络来源为VPC，Amazon S3 会拒绝向该接入点发出的并非来自该亚马逊 VPC 的任何请求。

> **Important**
>
> 您只能在创建接入点时指定接入点的网络起源。创建接入点后，无法更改其网络起源。

要将接入点限制为仅限 Amazon VPC 的访问，请在创建接入点的请求中加入`VpcConfiguration`参数。在`VpcConfiguration`参数中，您可以指定您希望能够使用接入点的 Amazon VPC ID。如果请求是通过接入点发出的，则该请求必须来自亚马逊 VPC，否则 Amazon S3 将拒绝该请求。

您可以使用 AWS CLI、 AWS SDKs或 REST 检索接入点的网络来源 APIs。如果接入点指定了 Amazon VPC 配置，则其网络来源为VPC。否则，接入点的网络起源为 `Internet`。

Example

示例：创建仅限于 Amazon VPC 访问的接入点

以下示例在账户`amzn-s3-demo-bucket`中创建了一个名`example-vpc-ap`为存储桶的接入点`123456789012`，该接入点仅允许从 `vpc-1a2b3c` Amazon VPC 进行访问。然后，该示例验证新接入点是否具有 VPC 网络起源。

AWS CLI

```
$ aws fsx create-and-attach-s3-access-point --name example-vpc-ap --type ONTAP --
ontap-configuration \

 VolumeId=fsvol-0123456789abcdef9,FileSystemIdentity='{Type=UNIX,UnixUser={Name=ec2-
user}}' \
   --s3-access-point VpcConfiguration='{VpcId=vpc-id},Policy=access-point-policy-
json
```

```
$ {
  {
     "S3AccessPointAttachment": {
        "Lifecycle": "CREATING",
        "CreationTime": 1728935791.8,
        "Name": "example-vpc-ap",
        "OntapConfiguration": {
            "VolumeId": "fsvol-0123456789abcdef9",
            "FileSystemIdentity": {
                "Type": "UNIX",
                "UnixUser": {
                    "Name": "my-unix-user"
                }
            }
        },
        "S3AccessPoint": {
            "ResourceARN": "arn:aws:s3:us-east-1:111122223333:accesspoint/example-
vpc-ap",
            "Alias": "access-point-abcdef0123456789ab12jj77xy51zacd4-ext-s3alias",
            "VpcConfiguration": {
                "VpcId": "vpc-1a2b3c"
            }
        }
     }
  }
```

要将接入点与 Amazon VPC 配合使用，您必须修改亚马逊 VPC 终端节点的访问策略。亚马逊 VPC 终端节点允许流量从您的亚马逊 VPC 流向亚马逊 S3。他们有访问控制策略，用于控制如何允许 Amazon VPC 内的资源与 Amazon S3 交互。只有当 Amazon VPC 终端节点策略授予访问接入点和底层存储桶的访问权限时，才能通过接入点成功从您的 Amazon VPC 发送到 Amazon S3 的请求。

> **Note**
>
> 要使资源只能在 Amazon VPC 内访问，请务必为您的 Amazon VPC 终端节点创建私有托管区域。要使用私有托管区域，请修改您的 Amazon VPC 设置，将 Amazon VPC 网络enableDnsSupport属enableDnsHostnames性和设置为true。

以下示例策略声明配置了一个允许调用的 Amazon VPC 终端节点GetObject和一个名为example-vpc-ap的接入点。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
    {
        "Principal": "*",
        "Action": [
            "s3:GetObject"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:us-east-1:123456789012:accesspoint/example-vpc-ap/object/
*"
        ]
    }]
}
```

> **Note**
>
> 此示例中的 Resource 声明使用 Amazon 资源名称（ARN）指定接入点。

有关亚马逊 VPC 终端节点策略的更多信息，请参阅 Amazon VP C 用户指南中的 Amaz on S3 网关终端节点。

为 Amazon S3 接入点配置网络访问权限

在为适用于 ONTAP 的 FSx 卷创建 Amazon S3 接入点时，需要配置如何通过网络访问接入点以及谁有权使用该接入点。本节将帮助您为您的环境选择正确的网络和访问控制配置。

本节涵盖网络和 IAM 授权层，具体而言，接入点的网络来源、VPC 终端节点、接入点策略、VPC 终端节点策略、IAM 身份策略和服务控制策略。有关文件系统级授权（UNIX 和 Windows 用户权限）的信息，请参见文件系统用户身份和授权。

主题

Amazon S3 如何评估接入点请求

当通过连接到 FSx for ONTAP 卷的 Amazon S3 接入点发出请求时，该请求必须经过以下所有层的授权：

- 网络来源检查 — 如果接入点有 VPC 网络来源，则请求必须通过绑定 VPC 中的 VPC 终端节点到达。否则，请求将在进行任何策略评估之前被拒绝。
- VPC 终端节点策略 — 如果请求通过 VPC 终端节点，则该终端节点的策略必须允许对接入点资源执行操作。
- 接入点策略-评估接入点的 IAM 资源策略。对于同账号访问，接入点策略或来电者的身份策略都可以授予访问权限。对于跨账户访问，两者都必须允许。
- IAM 身份策略 — 根据接入点资源评估请求委托人的基于身份的策略。
- 服务控制策略 (SCP)-如果账户是 Organizations AWS 组织的一部分，则任何适用的 SCP 都必须允许该操作。

网络起源检查在策略评估之前进行。其余层将作为标准 IAM 授权决策的一部分一起进行评估 — 任何层中的明确拒绝将覆盖其他层中的 Allow 语句。

选择网络来源

创建 Amazon S3 接入点时，您需要选择一个网络来源来决定访问接入点的方式。创建后您无法更改网络来源。

互联网起源

具有互联网网络来源的接入点类似于默认情况下访问 S3 存储桶的方式。所有请求仍需要有效的 IAM 凭证和授权 — 互联网来源并不意味着公开或匿名访问。Amazon S3 在连接到 FSx 的所有接入点上对 ONTAP 卷强制禁止公共访问，您无法禁用此设置。

通过 Internet Origin，经过身份验证的请求可以来自任何地方 — VPC、本地网络、其他 AWS 账户或公共互联网。您可以使用接入点策略和 IAM 身份策略控制允许哪些经过身份验证的来电者。

使用 Internet Origin，您可以使用接入点策略和 IAM 身份策略来控制访问权限。对于同账号来电者，请在接入点策略中使用明确的拒绝语句来限制访问——仅有 Allow-only 策略是不够的，因为呼叫者的 IAM 身份策略可以独立授予访问权限。对于跨账户来电者，接入点策略必须明确允许请求，因此省略“允许” 就足以阻止访问。

VPC 起源

具有 VPC 网络来源的接入点绑定到特定 VPC，其行为实际上是明确的拒绝策略声明，拒绝任何与绑定 VPC `aws:SourceVpc` 不匹配的请求。由于显式拒绝始终优先于任何允许，因此即使是完全允许的接入点策略或 IAM 身份策略也无法向来自绑定 VPC 外部的请求授予访问权限。

如果绑定 VPC 之外的来电者的流量通过绑定 VPC 中的 VPC 终端节点（例如，通过 VPC 对等连接或 Transit Gateway）路由到绑定 VPC 中部署的 Amazon S3 接口终端节点，则仍可以访问接入点。

主要区别

	互联网起源	VPC 起源
网络执法	无 — 访问权限仅受策略控制	对于未通过绑定 VPC 中的 VPC 终端节点到达的请求，实际上是显式拒绝
Multi-VPC access	通过政策条件提供支持	如果来电者通过绑定 VPC 中的接口终端节点（通过 VPC 对等连接或 Transit Gateway）进行路由，则支持此功能

	互联网起源	VPC 起源
更改访问范围	更新政策	必须重新创建接入点才能更改绑定的 VPC
需要 VPC 终端节点	仅当使用`aws:SourceVpc` 条件时	是 — 请求必须通过绑定 VPC 中的终端节点

VPC 起源执法的工作原理

当接入点具有 VPC 网络来源时，其行为实际上就像存在明确的拒绝策略声明一样，该声明拒绝所有`aws:SourceVpc`不等于接入点中指定的 VPC ID 的`VpcConfiguration`请求。此拒绝适用于所有委托人、所有 Amazon S3 操作以及接入点内的所有资源。

由于这是显式拒绝，因此它会覆盖任何 Allow 语句——无论是在接入点策略、呼叫者的 IAM 身份策略还是任何其他策略中。

实际上，这意味着：

- 请求必须通过部署在绑定 VPC 中的 VPC 终端节点（网关或接口）到达，因为只有 VPC 终端节点填充请求的`aws:SourceVpc`属性。
- 来自其他 VPC 的请求会被拒绝，因为它们的 VPC 终端节点填`aws:SourceVpc`充了不同的 VPC ID。
- 来自互联网的请求会被拒绝`aws:SourceVpc`，因为请求中不存在。

这也是为什么拒绝请求的错误消息显示 “基于资源的策略中显式拒绝” 的原因。

> **Important**
>
> 创建接入点后，您无法更改其网络来源。如果您需要从 VPC 源更改为 Internet 来源（反之亦然），则必须删除接入点并创建一个新的接入点。

VPC 来源与带有明确拒绝的互联网来源

VPC-origin 接入点和带有手动写入 “`StringNotEquals aws:SourceVpc`拒绝” 功能的 Internet 源接入点会得到类似的结果，即都拒绝来自指定 VPC 以外的请求。主要区别在于：

- VPC 来源：拒绝内置在接入点的 VPC 配置中。您不能意外将其删除或配置错误。
- 使用 “拒绝” 的互联网起源：您可以自己编写和管理 “拒绝”。这为您提供了更大的灵活性（例如，允许多个 VPC），但也为您提供了更多的责任——如果缺少拒绝或配置错误，则不会强制执行该限制。

使用带有 Amazon S3 接入点的 VPC 终端节点

Amazon S3 接入点适用于这两种类型的 Amazon S3 的 VPC 终端节点。您需要的终端节点类型取决于您的来电者所在的位置。

网关端点

网关终端节点是免费的，并且基于路由表。创建网关终端节点时，会向指定的路由表中添加一条路由，用于引导 Amazon S3 流量通过该终端节点。此路由仅适用于源自 VPC 的流量。

将网关终端节点用于：

- 亚马逊 EC2 实例、Lambda 函数、亚马逊 ECS 任务和 VPC 内的其他计算资源

网关终端节点不会路由从以下来源进入 VPC 的流量：

- On-premises 通过 VPN 或 Direct Connect
- 对等互连 VPC
- 公交 Gateway 连接

有关更多信息，请参阅 Amazon VPC 用户指南中的 Amazon S3 网关终端节点。

接口终端节点

接口终端节点使用您的子网中的私有 IP 地址创建弹性网络接口 (ENI)。流量必须明确定向到终端节点的 DNS 名称或私有 IP。

将接口端点用于：

- On-premises 通过 VPN 或 Direct Connect 访问亚马逊 S3 的来电者
- Cross-account 通过 VPC 对等互连访问亚马逊 S3 的来电者
- 流量从外部进入 VPC 的任何场景

使用接口端点时，呼叫者必须：

- 使用指向接口终端节点的 DNS 名称的`--endpoint-url`参数，或者
- 配置 DNS 以将 Amazon S3 终端节点解析为接口终端节点的私有 IP（使用 Route 53 解析器或本地 DNS 转发）

接口终端节点按小时和每 GB 收费。有关更多信息，请参阅AWS PrivateLink 定价。

同时使用两种端点类型

您可以在同一 VPC 中同时部署网关终端节点和接口终端节点。当您同时拥有 VPC 内呼叫者和本地呼叫者时，此配置非常有用：

- 网关终端节点：处理 VPC 内流量（免费、透明）
- 接口终端节点：处理通过 VPN 或 Direct Connect 进入的本地流量（需要 DNS 配置或`--endpoint-url`）

两种终端节点类型都使用 VPC ID 填充`aws:SourceVpc`属性，因此两者都满足 VPC 源拒绝条件。

VPC 端点策略

VPC 终端节点策略控制可以通过终端节点访问哪些 Amazon S3 资源。默认情况下，VPC 终端节点允许对所有资源执行所有 Amazon S3 操作。您可以将终端节点策略范围限定为仅允许特定的接入点：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:us-east-1:123456789012:accesspoint/my-access-point",
                "arn:aws:s3:us-east-1:123456789012:accesspoint/my-access-point/object/
*"
            ]
        }
    ]
}
```

接入点策略

Amazon S3 接入点支持 AWS Identity and Access Management (IAM) 资源策略，允许您根据资源、用户或其他条件控制接入点的使用。对于跨账户访问，接入点策略和调用方的 IAM 身份策略都必须允许该请求。对于同账户访问，接入点策略或呼叫者的 IAM 身份策略可以单独授予访问权限 — 要限制同账户来电者，请在接入点策略中使用明确的拒绝声明。如果请求通过 VPC 终端节点，则 VPC 终端节点策略还必须允许该请求。

有关接入点策略的更多信息，请参阅 A mazon 简单存储服务用户指南中的配置 IAM 策略以使用接入点。

基于网络的访问控制的条件密钥

IAM 提供全局条件密钥，您可以在接入点策略中使用这些密钥根据请求的网络属性控制访问权限。这些条件键仅在特定情况下才包含在请求上下文中，如下表所述。

条件键	可用性	说明
`aws:SourceVpc`	仅当请求者使用 VPC 终端节点发出请求时，才包含在请求上下文中。	检查请求是否通过 VPC 终端节点所连接的 VPC 传输。使用此密钥仅允许访问特定 VPC。
`aws:SourceVpce`	仅当请求者使用 VPC 终端节点发出请求时，才包含在请求上下文中。	发出请求所通过的 VPC 终端节点的 ID。
`aws:VpcSourceIp`	仅当请求是使用 VPC 终端节点发出时，才包含在请求上下文中。	将发出请求的 IP 地址与您在策略中指定的 IP 地址进行比较。仅当请求来自指定的 IP 地址并通过 VPC 终端节点时才匹配。
`aws:SourceIp`	仅当请求未通过 VPC 终端节点时，才包含在请求上下文中。	来电者的公有 IP 地址。不适用于通过 VPC 终端节点发出的请求。

> **Important**
>
> `aws:SourceIp`并且`aws:VpcSourceIp`是相互排斥的。当请求通过 VPC 终端节点时，不可`aws:SourceIp`用，请`aws:VpcSourceIp`改用。如果请求来自互联网（没有 VPC 终端节点），`aws:VpcSourceIp`则不可用，请`aws:SourceIp`改用。

> **Important**
>
> 条件键区分`aws:VpcSourceIp`大小写。

有关 IAM 全局条件密钥的更多信息，请参阅 I AM 用户指南中的AWS 全局条件上下文密钥。

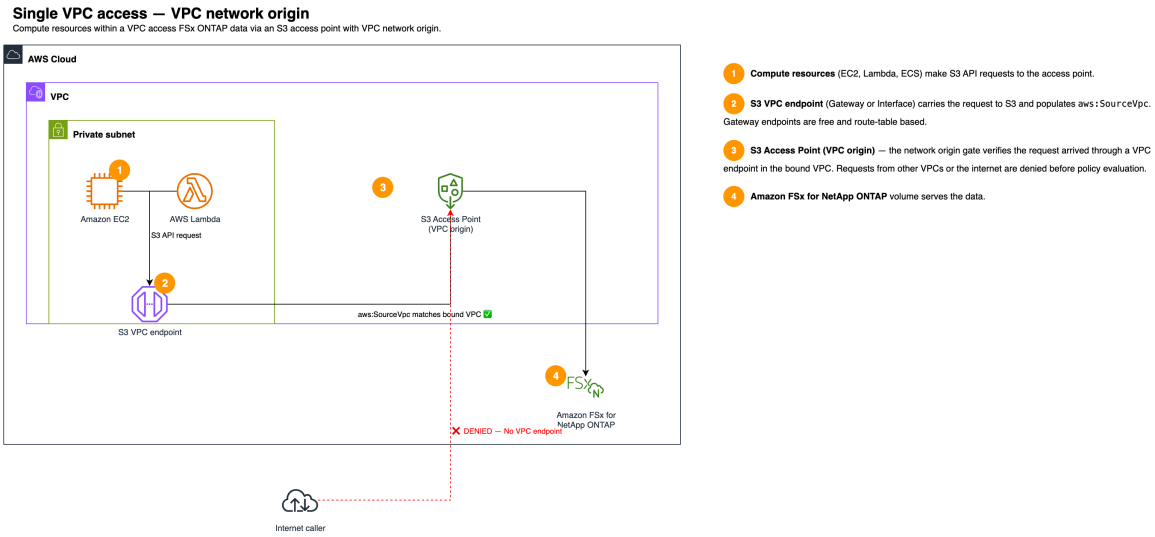
应用场景示例

以下示例场景显示了连接到 FSx 的 ONTAP 卷的 Amazon S3 接入点的常见配置。每种场景都包括推荐的网络来源、VPC 终端节点类型和接入点策略。

单个 VPC 访问权限

用例：单个 VPC 中的亚马逊 EC2 实例、Lambda 函数或亚马逊 ECS 任务访问接入点。无需外部访问。

使用 VPC 网络来源：



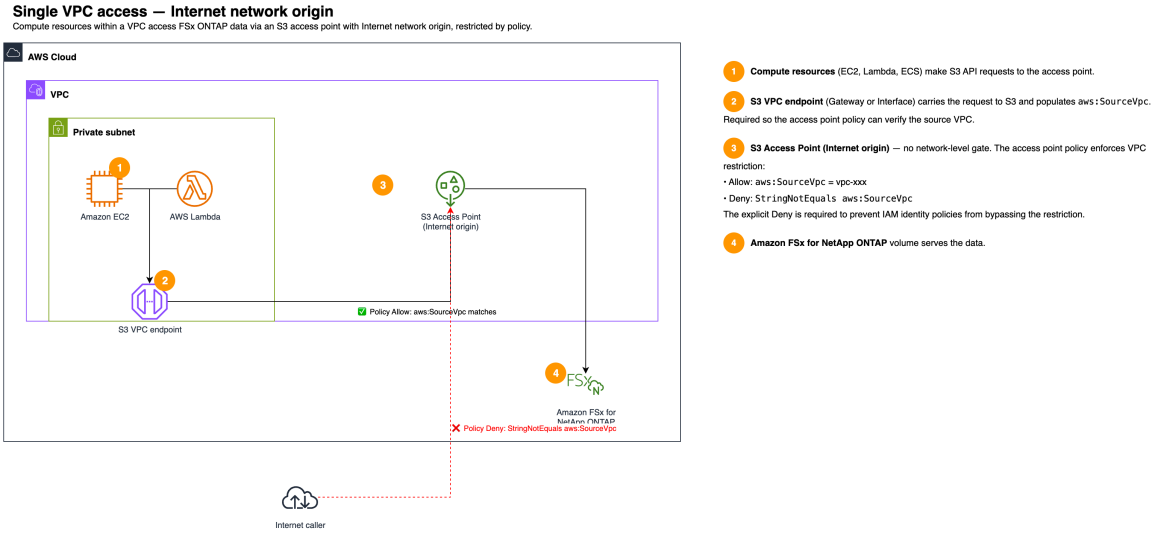
VPC 源配置可以有效地拒绝与绑定 VPC `aws:SourceVpc` 不匹配的请求。来自其他 VPC、互联网或本地网络的请求会被拒绝。您可以使用网关或接口 Amazon S3 VPC 终端节点。

接入点策略示例（VPC 来源）：对于 VPC 来源，网络限制是内置的。接入点策略只需要授予所需的权限。

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

```
        {
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::123456789012:role/my-app-role"},
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:us-east-1:123456789012:accesspoint/my-access-point",
                "arn:aws:s3:us-east-1:123456789012:accesspoint/my-access-point/object/
*"
            ]
        }
    ]
}
```

互联网网络起源：



使用 Internet Origin，您可以使用接入点策略中的`aws:SourceVpc`条件来限制对 VPC 的访问（使用明确的拒绝）。需要一个 VPC 终端节点，以便在请求中填充`aws:SourceVpc`该终端节点。

接入点策略示例（源自 Internet）：该策略既包括带有 VPC 条件的“允许”，也包括拒绝来自 VPC 的请求。

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

```
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::123456789012:role/my-app-role"},
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:us-east-1:123456789012:accesspoint/my-access-point",
                "arn:aws:s3:us-east-1:123456789012:accesspoint/my-access-point/object/
*"
            ],
            "Condition": {
                "StringEquals": {"aws:SourceVpc": "vpc-1a2b3c4d"}
            }
        },
        {
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:us-east-1:123456789012:accesspoint/my-access-point",
                "arn:aws:s3:us-east-1:123456789012:accesspoint/my-access-point/object/
*"
            ],
            "Condition": {
                "StringNotEquals": {"aws:SourceVpc": "vpc-1a2b3c4d"}
            }
        }
    ]
}
```

> **Note**
>
> 接入点策略中都需要使用 Allow 和 Deny 语句。如果没有 Deny 语句，则可能无法对所有呼叫者强制执行 VPC 限制。

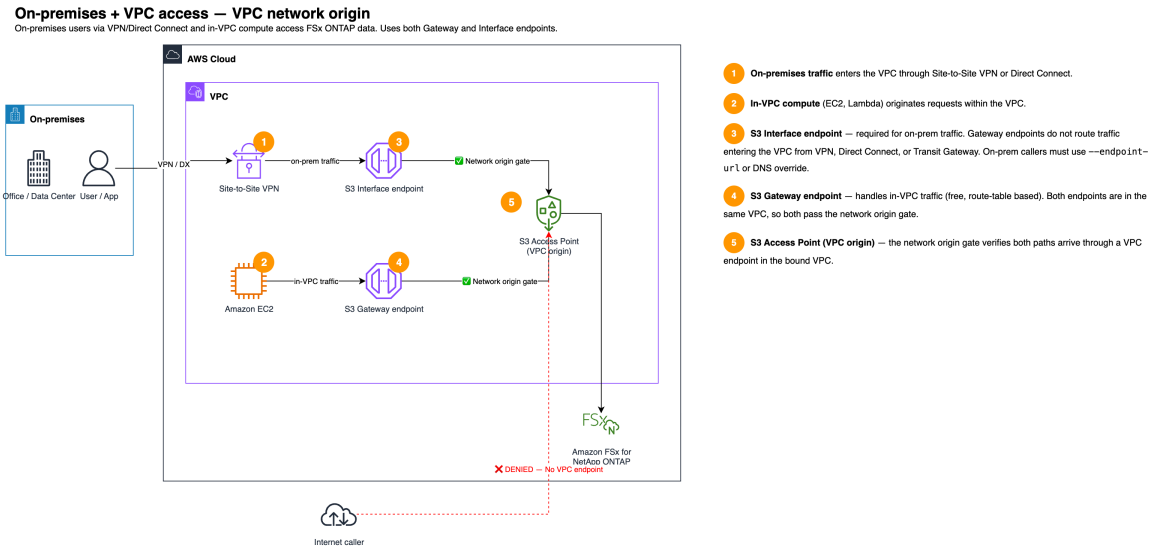
	VPC 起源	互联网起源
网络执法	Built-in 拒绝	Policy-based （ 允许 + 拒绝 ）

	VPC 起源	互联网起源
VPC 端点	必需（网关或接口）	必填项（对于`aws:SourceVpc`）
接入点政策	最小-内置“拒绝”句柄限制	必须包含“`aws:SourceVpc` 允许 + 拒绝”

On-premises 以及 VPC 访问权限

用例：本地用户（通过 VPN 或 Direct Connect）和 VPC 内的计算资源都访问接入点。所有流量都保持私密性。

> **Important**
>
> 网关终端节点不会路由从 VPN、Direct Connect 或 Transit Gateway 连接进入 VPC 的流量。On-premises 呼叫者必须使用 Amazon S3 接口终端节点。有关详细信息，请参阅 使用带有 Amazon S3 接入点的 VPC 终端节点。



网关终端节点（VPC 内流量）和接口终端节点（本地流量）都在同一 VPC 中，因此两者都满足 VPC 源拒绝条件。

	VPC 起源	互联网起源
In-VPC 终端节点	网关（免费）	网关（适用于`aws:SourceVpc`）
On-prem 终端节点	接口（必填）	接口（必填）
On-prem DNS	将 Amazon S3 解析为接口终端节点 IP	将 Amazon S3 解析为接口终端节点 IP

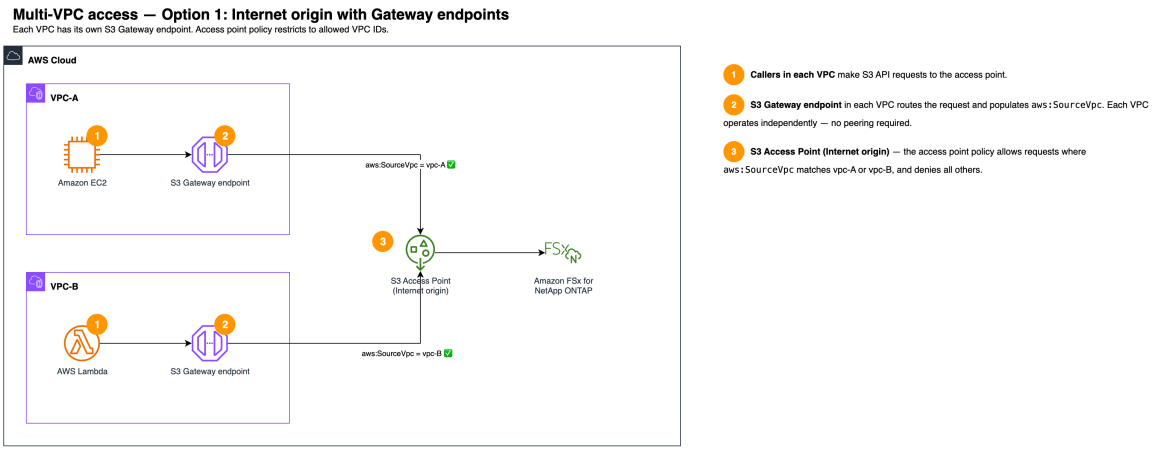
Multi-VPC 访问

用例：多个 VPC 中的呼叫者需要访问同一个接入点。例如，同一账户中位于不同 VPC 中的应用程序，或者通过 VPC 对等互连或 Transit Gateway 连接的不同账户中的 VPC。

多 VPC 访问有两种方法，具体取决于您是要使用基于策略的控制还是 VPC 源网络强制执行。

选项 1：互联网来源，每个 VPC 中都有一个网关终端节点

每个 VPC 都有自己的 Amazon S3 网关终端节点。每个 VPC 中的呼叫者通过其本地网关终端节点访问接入点，该终端节点会`aws:SourceVpc`根据请求填充。接入点策略限制对允许的 VPC ID 的访问。

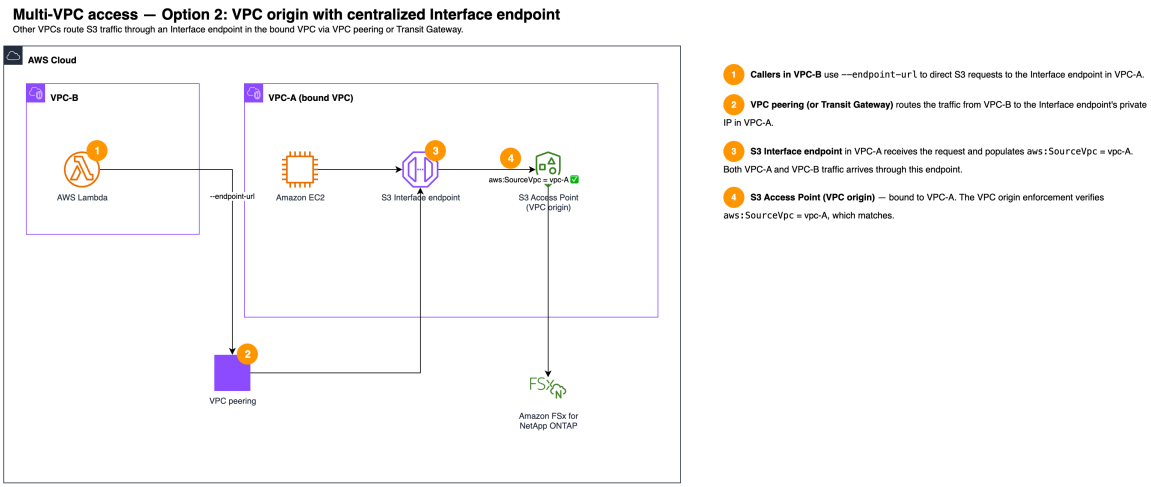


- 网络起源：互联网
- VPC 终端节点：每个 VPC 中的 Amazon S3 网关终端节点（免费，无需额外配置）
- 接入点策略：允许`aws:SourceVpc`列出所有 VPC ID，再加上“拒绝”`StringNotEquals`

> **Note**
>
> 接入点策略中都需要使用 Allow 和 Deny 语句。如果没有 Deny 语句，则可能无法对所有呼叫者强制执行 VPC 限制。

此选项的设置更简单，因为每个 VPC 都独立运行，不需要 VPC 对等互连或 Transit Gateway。要添加或删除 VPC，请更新接入点策略。

选项 2：带有集中式接口终端节点的 VPC 源



一个 VPC 托管一个 Amazon S3 接口终端节点，该接入点是使用绑定到该 VPC 的 VPC 源创建的。其他 VPC 通过 VPC 对等互连或 Transit Gateway 将其 Amazon S3 流量路由到接口终端节点。由于所有请求都通过绑定 VPC 中的终端节点到达，因此它们满足 VPC 源强制执行的要求。

- 网络来源：VPC（绑定到托管接口终端节点的 VPC）
- VPC 终端节点：绑定 VPC 中的 Amazon S3 接口终端节点
- 连接：其他 VPC 与绑定的 VPC 之间的 VPC 对等或 Transit Gateway
- 接入点策略：最小 — VPC 源强制措施处理网络限制
- 来电者配置：其他 VPC 中的呼叫者必须使用`--endpoint-url`或 DNS 配置才能通过接口终端节点路由请求

此选项提供了更强的强制执行，因为无法通过策略更改来绕过 VPC 来源限制。但是，它需要 VPC 对等连接或 Transit Gateway 连接，并且接口终端节点按小时和每 GB 收费。有关接口终端节点的更多信息，AWS PrivateLink请参阅《亚马逊简单存储服务用户指南》中的 Amazon S3。

网络访问问题疑难解答

当 Amazon S3 接入点请求失败时，错误消息通常不会表明哪个授权层拒绝了该请求。使用以下指导来诊断常见问题。

AccessDenied 改为 “在基于资源的策略中明确拒绝”

此错误可能来自多个来源。按顺序完成以下检查：

1。选中 VPC 源拒绝（仅限VPC-origin 接入点）

如果接入点具有 VPC 网络来源，则它实际上会拒绝与绑定 VPC `aws:SourceVpc` 不匹配的请求。验证：

- VPC 终端节点（网关或接口）存在于绑定的 VPC 中。
- 呼叫者的流量正在通过该端点进行路由。对于 vPC 内呼叫者，请验证网关终端节点的路由表是否与呼叫者的子网关联。对于本地呼叫者，请确认他们正在使用接口终端节点（网关终端节点不路由 VPN 或 Direct Connect 流量）。
- 来电者位于绑定的 VPC 中，而不是对等 VPC 中。除非通过绑定 VPC 中的接口终端节点进行路由，否则来自对等 VPC 的请求将被拒绝。

2。查看 VPC 终端节点策略

如果请求通过 VPC 终端节点，则该终端节点的策略必须允许对接入点资源执行操作。默认终端节点策略允许对所有资源执行所有操作。如果您已经确定了策略的范围，请确认它包括接入点 ARN。

3。查看接入点政策

验证接入点策略是否允许请求的主体。检查是否存在条件可能与请求匹配的 Deny 语句。

4。查看来电者的 IAM 身份政策

调用者的 IAM 角色或用户必须具有在接入点 ARN 上执行 Amazon S3 操作的权限。

5。检查服务控制策略 (SCP)

如果该账户是 Organizations AWS 组织的一部分，请确认没有任何 SCP 拒绝接入点上的 Amazon S3 操作。

On-premises 来电者得到 AccessDenied 但在 vpC 内呼叫者成功了

这通常意味着本地流量未通过 VPC 终端节点路由：

- 网关终端节点不路由本地流量。从 VPN、Direct Connect 或 Transit Gateway 连接进入 VPC 的流量不受网关终端节点路由的影响。为本地呼叫者创建 Amazon S3 接口终端节点。
- 验证接口终端节点的安全组允许来自本地 CIDR 的入站 HTTPS（端口 443）。
- 验证本地 DNS 是否将 Amazon S3 终端节点解析为接口终端节点的私有 IP 或呼叫者使用的私有 IP。`--endpoint-url`

接入点策略条件似乎无效

- Allow-only 策略不限制访问。如果您仅在 Allow 语句中使用条件（例如`aws:SourceVpc`），而没有相应的拒绝，则调用者的 IAM 身份策略可以独立授予访问权限。添加带有相反条件的显式 Deny 语句。
- 区分大小写。条件键区分`aws:VpcSourceIp`大小写。
- 互斥的条件键。 `aws:SourceIp`并且`aws:VpcSourceIp`是相互排斥的。 `aws:SourceIp`当请求通过 VPC 终端节点时不可用，请改用`aws:VpcSourceIp`。相反，`aws:VpcSourceIp`不适用于互联网请求——使用`aws:SourceIp`。这适用于使用这些条件密钥的所有策略，包括接入点策略、VPC 终端节点策略和 IAM 身份策略。

管理 Amazon S3 接入点

本节介绍如何使用、或 API 管理和使用您的 Amazon S3 接入点。 AWS 管理控制台 AWS Command Line Interface

S3 接入点附件生命周期

您可以使用 Amazon FSx 控制台或 API 查看 S3 接入点连接的状态。 AWS CLI下表描述了 S3 接入点附件可能的生命周期状态。

生命周期状态	说明
AVAILABLE	接入点附件可供使用。
CREATING	Amazon FSx 正在创建接入点附件。
DELETING	Amazon FSx 正在删除接入点附件。
UPDATING	接入点附件正在更新中。

生命周期状态	说明
MISCONFIGURED	接入点附件存在配置问题，使其无法处理请求。常见原因包括与接入点相关的文件系统身份无法在文件系统上解析，或者连接的卷处于脱机状态或已卸载。Amazon FSx 会定期检查这些情况，并在问题解决后自动将接入点返回到AVAILABLE 。有关更多信息，请参阅 S3 接入点处于配置错误的状态。
FAILED	接入点连接处于终端故障状态。如果接入点创建失败（例如，由于文件系统身份无法解析或 SVM 上的 S3 协议被禁用），或者底层 S3 接入点是直接通过 Amazon S3 而不是通过 Amazon FSx 删除的，则可能会发生这种情况。删除接入点附件并创建新的接入点附件。

主题

列出 S3 接入点附件

本节介绍如何使用 AWS 管理控制台、 AWS Command Line Interface或 REST API 列出 S3 接入点。

列出连接到 FSx for ONTAP 卷的所有 S3 接入点（亚马逊 FSx 控制台）

1. 打开 Amazon FSx 控制台，网址为。https://console.aws.amazon.com/fsx/
2. 在控制台左侧的导航窗格中，选择卷。
3. 在 “卷” 页面上，选择要查看其接入点附件的 ONTAP 卷。
4. 在卷详细信息页面上，选择 S3 以查看连接到该卷的所有 S3 接入点的列表。

列出连接到 FSx for ONTAP 卷的所有 S3 接入点 ()AWS CLI

以下`describe-s3-access-point-attachments`示例命令显示了如何使用列出 S3 接入点附件。AWS CLI

以下命令列出了连接到 FSx for ONTAP 文件系统上卷的所有 S3 接入点 fs-0abcdef123456789。

```
aws fsx describe-s3-access-point-attachments --filter {[Name: file-system-id, Values:
{[fs-0abcdef123456789]}}
```

以下命令列出了连接到 FSx for ONTAP volume 的 S3 接入点 vol-9abcdef123456789]。

```
aws fsx describe-s3-access-point-attachments --filter {[Name: volume-id, Values:
{[vol-9abcdef123456789]}}
```

有关更多信息和示例，请参阅《AWS CLI 命令参考》中的 list-access-points。

查看接入点详情

本节介绍如何使用 AWS 管理控制台、 AWS Command Line Interface或 REST API 查看 S3 接入点的详细信息。

查看连接到 FSx for ONTAP 卷的 S3 接入点的详细信息（亚马逊 FSx 控制台）

1. 打开 Amazon FSx 控制台，网址为。https://console.aws.amazon.com/fsx/
2. 导航到连接到要查看其详细信息的接入点的卷。
3. 选择 S3 以显示连接到该卷的接入点列表。
4. 选择要查看其详细信息的接入点。
5. 在 S3 接入点附件摘要下，查看所选接入点的配置详细信息和属性。

   接入点附件中还列出了文件系统用户身份配置和 S3 接入点权限策略。
6. 要在 Amazon S3 控制台中查看接入点的 S3 配置，请选择 S3 接入点下显示的 S3 接入点名称。它会将您带到 Amazon S3 控制台中接入点的详细信息页面。

删除 S3 接入点附件

本节介绍如何使用 AWS 管理控制台、 AWS Command Line Interface或 REST API 删除 S3 接入点。

删除 S3 接入点附件需
要`fsx:DetatchAndDeleteS3AccessPoint`和`s3control:DeleteAccessPoint`权限。

删除连接到 FSx for ONTAP 卷的 S3 接入点（亚马逊 FSx 控制台）

1. 打开 Amazon FSx 控制台，网址为。https://console.aws.amazon.com/fsx/
2. 导航到要删除的 S3 接入点附件所连接的卷。
3. 选择 S3 以显示连接到该卷的 S3 接入点列表。

4. 选择要删除的 S3 接入点附件。
5. 选择删除。
6. 确认要删除 S3 接入点，然后选择删除。

删除连接到 FSx 的 ONTAP 卷的 S3 接入点 ()AWS CLI

- 要删除 S3 接入点附件，请使用 detachand-delete-s3-access-point CLI 命令（或DetachAndDeleteS3AccessPoint等效的 API 操作），如以下示例所示。使用--name属性指定要删除的 S3 接入点附件的名称。

```
aws fsx detach-and-delete-s3-access-point \
    --region us-east-1 \
    --name my-ontap-ap
```

使用接入点

以下示例演示如何使用 S3 API 使用接入点访问存储在 fo FSx r ONTAP 卷上的文件数据。有关连接到 for ONTAP 卷的接入点所支持的 Amazon S3 API 操作 FSx 的完整列表，请参阅接入点兼容性。

> **Note**
>
> ONTAP 卷上的 FSx 文件以标识StorageClass为。FSX_ONTAP

主题

- 使用 S3 接入点下载文件
- 使用 S3 接入点上传文件
- 使用 S3 接入点列出文件
- 使用 S3 接入点标记文件
- 使用 S3 接入点删除文件

使用 S3 接入点下载文件

以下get-object示例命令显示了如何使用通过接入点下载文件。 AWS CLI 您必须包括一个输出文件，这是已下载对象的文件名。

该示例*my-image.jpg*通过接入点请求文件*my-ontap-ap*并将下载的文件另存为*download.jpg*。

```
$ aws s3api get-object --key my-image.jpg --bucket my-ontap-ap-
hrzrlukc5m36ft7okagglf3gmwluquse1b-ext-s3alias download.jpg
{
    "AcceptRanges": "bytes",
    "LastModified": "Mon, 14 Oct 2024 17:01:48 GMT",
    "ContentLength": 141756,
    "ETag": "\"00751974dc146b76404bb7290f8f51bb-1\"",
    "ContentType": "binary/octet-stream",
    "ServerSideEncryption": "SSE_FSX",
    "Metadata": {},
    "StorageClass": "FSX_ONTAP"
}
```

您也可以使用 REST API 通过接入点下载对象。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 GetObject。

使用 S3 接入点上传文件

以下put-object示例命令显示了如何使用通过接入点上传文件。 AWS CLI 您必须包括一个输出文件，这是上传对象的文件名。

该示例*my-new-image.jpg*通过接入点上传文件*my-ontap-ap*并将上传的文件另存为*my-new-image.jpg*。

```
$ aws s3api put-object --bucket my-ontap-ap-hrzrlukc5m36ft7okagglf3gmwluquse1b-ext-
s3alias --key my-new-image.jpg --body  my-new-image.jpg
```

您也可以使用 REST API 通过接入点上传对象。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 PutObject。

使用 S3 接入点列出文件

以下示例通过区域中账户 ID *my-ontap-ap-hrzrlukc5m36ft7okagglf3gmwluquse1b*-ext-s3alias *111122223333* 拥有的接入点别名列出文件*us-east-2*。

```
$ aws s3api list-objects-v2 --bucket my-ontap-ap-hrzrlukc5m36ft7okagglf3gmwluquse1b-
ext-s3alias
{
    "Contents": [
        {
```

```
            "Key": ".hidden-dir-with-data/file.txt",
            "LastModified": "2024-10-29T14:22:05.4359",
            "ETag": "\"88990077ab44cd55ef66aa77-1\"",
            "Size": 18,
            "StorageClass": "FSX_ONTAP"
        },
        {
            "Key": "documents/report.rtf",
            "LastModified": "2024-11-02T10:18:15.6621",
            "ETag": "\"ab12cd34ef56a89219zg6aa77-1\"",
            "Size": 1048576,
            "StorageClass": "FSX_ONTAP"
        },
    ]
}
```

您也可以使用 REST API 列出您的文件。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 ListObjectsV2。

使用 S3 接入点标记文件

以下put-object-tagging示例命令显示了如何使用通过接入点添加标签集。 AWS CLI 每个标签都是一个键-值对。有更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的使用标签对存储进行分类。

该示例my-image.jpg使用接入点向现有文件添加标签集。*my-ontap-ap*

```
$ aws s3api put-object-tagging --bucket my-ontap-ap-hrzrlukc5m36ft7okagglf3gmwluquse1b-ext-s3alias --key my-image.jpg --tagging TagSet=[{Key="finance",Value="true"}]
```

您还可以使用 REST API 通过接入点向对象添加标签集。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 PutObjectTagging。

使用 S3 接入点删除文件

以下delete-object示例命令显示了如何使用通过接入点删除文件。 AWS CLI

```
$ aws s3api delete-object --bucket my-ontap-ap-hrzrlukc5m36ft7okagglf3gmwluquse1b-ext-s3alias --key my-image.jpg
```

您也可以使用 REST API 通过接入点删除对象。有关更多信息，请参阅《Amazon Simple Storage Service API 参考》中的 DeleteObject。

将接入点与 AWS 服务

您可以将连接到 FSx 的 Amazon S3 接入点用于与 Amazon S3 集成 AWS 服务 的 ONTAP 卷。这样，您就可以在存储在 FSx for ONTAP 中的文件数据上分析、处理和构建 Amazon S3-based 应用程序，而无需将其复制到 Amazon S3 存储桶中。

以下示例用例逐步介绍常见的集成。每个教程都使用连接到 FSx for ONTAP 卷的 Amazon S3 接入点，因此无需将数据复制和同步到 Amazon S3 存储桶 AWS 服务 即可读取和写入您的文件数据。

- 使用 Amazon Athena 使用 SQL 查询文件— 使用 Amazon Athena 和，对你的 FSx for ONTAP 卷上的文件运行临时 SQL 查询。 AWS Glue Data Catalog适用于需要 SQL 访问存放在 NFS 或 SMB 文件共享上的数据的数据分析师。
- 使用 Lambda 以无服务器方式处理文件— 针对您的 FSx for ONTAP 卷上的文件触发 Lambda 函数，以运行无服务器处理工作负载。示例包括生成图像缩略图、从文档中提取文本以及转录音频。
- 使用构建 ETL 管道 AWS Glue— 使用 Apache Spark、Python shell 或 Ray 在 FSx for ONTAP 卷上读取、转换、丰富或分区数据，然后将结果写回 AWS Glue 同一个卷。适用于数据工程团队，利用传统或本地系统生成的文件构建精选数据集。
- 使用 Amazon Bedrock 知识库构建 RAG 应用程序— 构建检索增强生成 (RAG) 应用程序，该应用程序将基础模型响应作为存储在 FSx for ONTAP 卷上的文档中的基础模型响应的基础。适用于在现有文档存储库上构建生成式 AI 体验的团队。
- 使用 Amazon EMR 无服务器运行 Spark 作业— 无需配置集 PySpark 群，即可针对 FSx 上的 ONTAP 卷上的文件运行和 Spark SQL 工作负载。适用于运行超出范围的繁重 Spark 工作负载的数据工程团队 AWS Glue。
- 使用流式传输视频 CloudFront— 使用 FSx 为 ONTAP 音量提供 HLS 自适应比特率视频，边缘缓存可提高性能。 CloudFront适用于其制作工作流程将已完成的内容写入文件共享的媒体和娱乐团队。
- 使用 Transfer Family AWS 传输文件 — 使用 Transfer Family 通过 Amazon S3 接入点将你的 FSx for ONTAP 卷作为 SFTP、FTPS 或 FTP 终端节点公开 AWS 给外部合作伙伴。有关设置说明，请参阅 Transfer Family 用户指南中的使用 Transfer Family 访问适用于 ONTAP 文件系统的 FSx。AWS

主题

- 使用 Amazon EMR 无服务器运行 Spark 作业
- 使用流式传输视频 CloudFront

使用 Amazon Athena 使用 SQL 查询文件

企业系统经常生成基于文件的输出（日志导出、事务提取、清单快照、系统间文件丢弃），这些输出存放在 NFS 或 SMB 文件共享上。

在 FSx for ONTAP 卷上连接了 Amazon S3 接入点后，Amazon Athena 会就地查询文件。您的应用程序和用户继续像往常一样通过 NFS 或 SMB 向卷写入数据，分析人员通过接入点对这些数据运行标准 SQL。由于可以通过 NFS、SMB 和 Amazon S3 API 同时访问适用于 ONTAP 卷的 FSx，因此同一个文件可以由一个协议生成，而另一个协议可以使用，而无需副本。

在本教程中，您将通过 Amazon S3 接入点将示例数据集上传到您的 FSx for ONTAP 卷，在中注册该数据集，然后使用 Amazon Athena 进行查询。 AWS Glue Data Catalog

> **Note**
>
> 本教程大约需要 20 到 30 分钟才能完成。 AWS 服务 使用者会对您创建的资源产生费用。如果您及时完成所有步骤，包括清理部分，则美国东部（弗吉尼亚北部）的预期费用将低于 1美元 AWS 区域。该估算值不包括 FSx 对 ONTAP 容量本身的持续收费。

先决条件

在开始之前，请确保您具有以下各项：

- 连接了 Amazon S3 接入点的 ONTAP 卷的 FSx。接入点必须具有互联网网络来源。有关创建接入点的说明，请参阅创建接入点。
- 配置了查询结果位置的 Athena 工作组。Athena 将查询结果写入亚马逊 S3 存储桶，而不是 ONTAP 卷的 FSx。如果您没有工作组，则可以使用该**primary**工作组并在 Athena 控制台的 “设置” 下配置结果位置。有关更多信息，请参阅 A mazon Athena 用户指南中的管理工作组。
- 附 AWS Glue 带`AWSGlueServiceRole`托管策略的 IAM 角色和授予访问您的 Amazon S3 接入点访问权限的内联策略。如果没有，请按以下步骤操作。

  1. 将以下信任策略另存为`glue-trust-policy.json`。它 AWS Glue 允许扮演这个角色。

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {"Service": "glue.amazonaws.com"},
            "Action": "sts:AssumeRole"
        }
    ]
}
```

2. 将以下权限策略另存为glue-s3-policy.json。它授予访问接入点的权限。用您的值替换*regionaccount-id*、和*access-point-name*。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:region:account-id:accesspoint/access-point-name",
                "arn:aws:s3:region:account-id:accesspoint/access-point-name/
object/*"
            ]
        }
    ]
}
```

3. 创建角色并附加策略。

```
$ aws iam create-role \
    --role-name fsxn-tutorial-glue-role \
    --assume-role-policy-document file://glue-trust-policy.json

aws iam attach-role-policy \
    --role-name fsxn-tutorial-glue-role \
    --policy-arn arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole

aws iam put-role-policy \
    --role-name fsxn-tutorial-glue-role \
    --policy-name s3-access-point-policy \
```

```
    --policy-document file://glue-s3-policy.json
```

- 运行 Athena 查询和访问数据目录的 IAM 权限 AWS Glue 。

> **Important**
>
> Amazon S3 接入点必须使用互联网网络来源。Athena 通过托管基础设施访问 Amazon S3，而不是从您的 VPC。具有 VPC 网络来源的接入点会拒绝来自 Athena 的请求。

步骤 1：将 ONTAP 卷的示例数据上传到您的 FSx

本教程使用纽约市出租车和豪华轿车委员会 (TLC) 旅行记录数据，这是纽约市出租车旅行的公开数据集。数据采用 Apache Parquet 格式，这是一种列式格式，Athena 可以高效地查询该格式。

下载一个月的黄色出租车出行数据，然后通过 Amazon S3 接入点将其上传到您的 FSx 以获取 ONTAP 音量。

```
$ curl -O https://d37ci6vzurychx.cloudfront.net/trip-data/
yellow_tripdata_2024-01.parquet
```

使用接入点别名将文件上传到您的 FSx for ONTAP 卷。*my-ap-alias-ext-s3alias*替换为您的接入点别名。

```
$ aws s3 cp yellow_tripdata_2024-01.parquet \
    s3://my-ap-alias-ext-s3alias/taxi-data/yellow_tripdata_2024-01.parquet
```

验证文件是否可通过接入点访问。

```
$ aws s3 ls s3://my-ap-alias-ext-s3alias/taxi-data/
2024-01-23 02:18:13   49961641 yellow_tripdata_2024-01.parquet
```

步骤 2：在中创建数据库 AWS Glue Data Catalog

在中创建数据库 AWS Glue Data Catalog 以保存表元数据。您可以使用控制 AWS Glue 台、Athena 查询编辑器或. AWS CLI

AWS Glue console

1. 打开 AWS Glue 控制台，网址为https://console.aws.amazon.com/glue/。
2. 在导航窗格中的数据目录下，选择数据库。
3. 选择 Add database（添加数据库）。
4. 对于名称，请输入 *fsxn_taxi_demo*。
5. 选择创建数据库。

Athena 查询编辑器或 AWS CLI

```
$ aws athena start-query-execution \
    --query-string "CREATE DATABASE IF NOT EXISTS fsxn_taxi_demo" \
    --work-group primary
```

步骤 3：将数据注册到 AWS Glue Data Catalog

您可以在 Athena 中使用 AWS Glue 爬虫（推荐）或手动CREATE EXTERNAL TABLE语句注册数据。

选项 A：使用 AWS Glue 爬虫（推荐）

C AWS Glue rawler 会自动发现您的数据架构并在中创建表。 AWS Glue Data Catalog这是推荐的方法，因为爬虫会从 Parquet 文件元数据中推断出正确的列类型。

1. 创建指向接入点别名的爬虫。*my-ap-alias-ext-s3alias*替换为您的接入点别名和 *my-glue-role-arn* l AWS Glue AM 角色的 ARN。

   ```
   $ aws glue create-crawler \
       --name fsxn-taxi-crawler \
       --role my-glue-role-arn \
       --database-name fsxn_taxi_demo \
       --targets '{"S3Targets": [{"Path": "s3://my-ap-alias-ext-s3alias/taxi-
   data/"}]}'
   ```

2. 运行 爬网程序。

   ```
   $ aws glue start-crawler --name fsxn-taxi-crawler
   ```

3. 检查爬虫状态。爬行程序通常在一到两分钟内完成。

   ```
   $ aws glue get-crawler --name fsxn-taxi-crawler \
       --query "Crawler.{State:State,Status:LastCrawl.Status}"
   ```

爬网程序完成后，状态为READY，状态为SUCCEEDED。Crawler 在fsxn_taxi_demo数据库中创建一个名为taxi_data（源自文件夹名称）的表。

选项 B：在 Athena 中手动创建表

如果您已经知道数据的架构，则可以使用语句直接在 Athena 中创建表。CREATE EXTERNAL TABLE在LOCATION子句中使用接入点别名。

```
CREATE EXTERNAL TABLE fsxn_taxi_demo.yellow_taxi_trips (
    VendorID bigint,
    tpep_pickup_datetime timestamp,
    tpep_dropoff_datetime timestamp,
    passenger_count bigint,
    trip_distance double,
    RatecodeID bigint,
    store_and_fwd_flag string,
    PULocationID bigint,
    DOLocationID bigint,
    payment_type bigint,
    fare_amount double,
    extra double,
    mta_tax double,
    tip_amount double,
    tolls_amount double,
    improvement_surcharge double,
    total_amount double,
    congestion_surcharge double,
    Airport_fee double
)
STORED AS PARQUET
LOCATION 's3://my-ap-alias-ext-s3alias/taxi-data/'
```

> **Note**
>
> 列类型必须与 Parquet 文件中的类型相匹配。对于这个数据集，像passenger_count和VendorID这样的字段以 bigint (INT64) 的形式存储在 Parquet 文件中，而不是double。如果类型不匹配，Athena 将返回错误。HIVE_BAD_DATA使用 AWS Glue 爬虫（选项 A）可以避免此问题，因为爬虫会自动推断出正确的类型。

第 4 步：查询您的数据

打开 Athena 查询编辑器或使用 AWS CLI 对您的 FSx 运行 SQL 查询，获取 ONTAP 数据。以下示例使用由 AWS Glue Crawler (`taxi_data`) 创建的表。如果您手动创建了表，请`taxi_data`替换为`yellow_taxi_trips`。

计算行程总数并计算平均值

```
SELECT
    COUNT(*) AS total_trips,
    ROUND(AVG(trip_distance), 2) AS avg_distance_miles,
    ROUND(AVG(total_amount), 2) AS avg_total_usd,
    ROUND(AVG(passenger_count), 1) AS avg_passengers
FROM fsxn_taxi_demo.taxi_data
```

输出示例：

行程总数	平均距离_英里	avg_total_USD	平均乘客数
2964624	3.65	26.80	1.3

查找最繁忙的接送时间

```
SELECT
    HOUR(tpep_pickup_datetime) AS pickup_hour,
    COUNT(*) AS trip_count,
    ROUND(AVG(total_amount), 2) AS avg_fare
FROM fsxn_taxi_demo.taxi_data
GROUP BY HOUR(tpep_pickup_datetime)
ORDER BY trip_count DESC
LIMIT 5
```

查找收入最高的取货地点

```
SELECT
    PULocationID AS pickup_location,
    COUNT(*) AS trip_count,
    ROUND(SUM(total_amount), 2) AS total_revenue
FROM fsxn_taxi_demo.taxi_data
GROUP BY PULocationID
ORDER BY total_revenue DESC
```

```
LIMIT 10
```

注意事项

- Read-only 访问。Athena 通过接入点从 FSx 读取 ONTAP 卷的数据。对于 ONTAP 卷，Athena 的查询结果会写入 Amazon S3 结果存储桶，而不是写回 FSx。
- 需要互联网来源。Athena 从您的 VPC 外部的托管基础设施访问 Amazon S3。`aws:SourceVpc`和`aws:SourceVpce`条件键不适用于 Athena 请求。您必须使用源自互联网的接入点。
- 文件格式。Athena 支持 Parquet、ORC、JSON、CSV 和其他格式。Parquet 和 ORC 等列式格式可提供最佳的查询性能，因为 Athena 只读取查询中引用的列。
- 文件系统用户权限。与接入点关联的文件系统用户必须对所查询的文件具有读取权限。
- AWS Glue Data Catalog 桌子是可重复使用的。在中注册表格后 AWS Glue Data Catalog，其他与之集成的 AWS 分析服务即可使用该表，例如亚马逊 Redshift Spectrum AWS Glue Data Catalog、Amazon EMR 和 ETL 作业。 AWS Glue

清理

为避免持续收费，请删除您在本教程中创建的资源。

1. 删除 Athena 表和数据库。

```
DROP TABLE IF EXISTS fsxn_taxi_demo.taxi_data;
DROP TABLE IF EXISTS fsxn_taxi_demo.yellow_taxi_trips;
DROP DATABASE IF EXISTS fsxn_taxi_demo CASCADE;
```

2. 删除 AWS Glue 爬虫。

```
$ aws glue delete-crawler --name fsxn-taxi-crawler
```

3. 从 FSx 中删除 ONTAP 卷的示例数据。

```
$ aws s3 rm s3://my-ap-alias-ext-s3alias/taxi-data/yellow_tripdata_2024-01.parquet
```

使用 Lambda 以无服务器方式处理文件

文件处理工作流程通常从到达 NFS 或 SMB 文件共享的文件开始，这些文件包括来自分支机构的扫描文档、现场团队上传的图像、从联络中心捕获的音频或合作伙伴提供的数据文件。

通过连接到 FSx for ONTAP 卷的 Amazon S3 接入点， AWS Lambda 函数可以直接使用 Amazon S3 API 读取和写入文件。 File-level 可以针对您的用户和应用程序通过 NFS 和 SMB 访问的相同数据进行无服务器处理操作。

本教程显示了三种常见的文件处理模式。每个示例都通过接入点从卷中读取文件，使用 AWS 服务或库对其进行处理，然后将结果写回卷。

示例	Input	Processing	Output
the section called “示例 1：生成图像缩略图”	JPEG 图片	枕头（图片库）	调整了缩略图大小
the section called “示例 2：从文档中提取文本”	PDF 文档	Amazon Textract	提取的文本 (JSON)
the section called “示例 3：转录音频文件”	MP3 音频	Amazon Transcribe	笔录 (JSON)

> **Note**
>
> 完成本教程大约需要 40 到 60 分钟。 AWS 服务 使用者会对您创建的资源产生费用。如果您及时完成所有步骤，包括清理部分，则美国东部（弗吉尼亚北部）的预期费用将低于 1美元 AWS 区域。该估算值不包括 FSx 对 ONTAP 容量本身的持续费用。

先决条件

在开始之前，请确保您具有以下各项：

- 连接了 Amazon S3 接入点的 ONTAP 卷的 FSx。有关创建接入点的说明，请参阅创建接入点。
- 您的接入点的接入点别名。你可以在 Amazon FSx 控制台中找到它，也可以通过运行来找到。`aws fsx describe-s3-access-point-attachments`

- AWS CLI 已安装并配置版本 1 或版本 2。本教程中的`aws lambda invoke`命令包括`--cli-binary-format raw-in-base64-out`选项，该选项在 AWS CLI 版本 2 中是必需的，这样原始 JSON 负载就不会被解释为 base64。如果您使用 AWS CLI 版本 1，请省略该选项。
- 调用者（运行本教程的用户或角色）的 IAM 权限，用于调用 Lambda 函数 (`lambda:CreateFunction`,`lambda:InvokeFunction`)、访问 Amazon S3 接入点 (`s3:GetObject`,`s3:PutObject`) 和传递 Lambda 执行角色 ()。`iam:PassRole`

> **Note**
>
> 本教程使用默认 Lambda 配置，其中函数在您的 VPC 之外的托管网络中运行。在这种情况下，接入点必须具有互联网网络来源，以便功能可以访问它。如果您将 Lambda 函数附加到 VPC，则可以在接入点上使用 VPC 网络来源；VPC 必须具有 Amazon S3 网关或接口终端节点。有关更多信息，请参阅 为 Amazon S3 接入点配置网络访问权限。

步骤 1：上传示例文件

下载以下示例文件并通过接入点将其上传到您的 FSx for ONTAP 卷。在本教程中*`my-ap-alias-ext-s3alias`*，请使用您的接入点别名替换。

- 示例图片：下载 NASA Blue Marble 图片（公共领域，2.4 MB）并将其另存为`sample-image.jpg`。
- 示例音频：从 Amazon Transcribe 入门教程 (410 KB) 中下载示例音频文件并将其另存为。`sample-audio.mp3`

通过接入点将示例文件上传到您的 FSx for ONTAP 卷。

```
$ aws s3 cp sample-image.jpg s3://my-ap-alias-ext-s3alias/samples/images/sample-image.jpg
aws s3 cp sample-audio.mp3 s3://my-ap-alias-ext-s3alias/samples/audio/sample-audio.mp3
```

> **Note**
>
> 样本图像是美国宇航局的蓝色大理石照片（公共领域，2.4 MB）。示例音频来自 Amazon Transcribe 入门教程 (410 KB)。样本 PDF 是在中生成的the section called “示例 2：从文档中提取文本”。

步骤 2：创建 Lambda 执行角色

Lambda 函数扮演执行角色与其他函数进行交互。 AWS 服务在本教程中，请附上 CloudWatch 日志记录的 AWS托管AWSLambdaBasicExecutionRole策略，然后添加一个内联策略，授予对 Amazon S3 接入点以及示例使用的 Textract 和 Transcribe API 的访问权限。

创建 Lambda 执行角色

用您的值替换*regionaccount-id*、和*access-point-name*。

1. 将以下信任策略另存为trust-policy.json。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {"Service": "lambda.amazonaws.com"},
            "Action": "sts:AssumeRole"
        }
    ]
}
```

2. 将以下内联权限策略另存为permissions-policy.json。它授予访问接入点和示例使用的其他服务的访问权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["s3:GetObject", "s3:PutObject", "s3:ListBucket"],
            "Resource": [
                "arn:aws:s3:region:account-id:accesspoint/access-point-name",
                "arn:aws:s3:region:account-id:accesspoint/access-point-name/object/
*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": ["textract:DetectDocumentText"],
            "Resource": "*"
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "transcribe:StartTranscriptionJob",
                "transcribe:GetTranscriptionJob"
            ],
            "Resource": "*"
        }
    ]
}
```

3. 创建角色，附加托管日志策略并附加内联策略。

```
$ aws iam create-role \
    --role-name fsxn-lambda-file-processor \
    --assume-role-policy-document file://trust-policy.json

aws iam attach-role-policy \
    --role-name fsxn-lambda-file-processor \
    --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole

aws iam put-role-policy \
    --role-name fsxn-lambda-file-processor \
    --policy-name fsxn-access-point-policy \
    --policy-document file://permissions-policy.json
```

集成到您的工作流程中

本教程中的示例使用带有测试事件的手动调用。在生产环境中，您可以使用以下方法自动触发这些函数：

- 亚马逊 EventBridge 日程安排。定期运行该函数（例如，每小时或每天）以处理新文件。该功能可以通过接入点列出文件并处理任何尚未处理的文件。有关更多信息，请参阅亚马逊 EventBridge用户指南 EventBridge中的使用计划 Lambda 函数。
- 亚马逊 API Gateway。将该函数公开为 HTTP API，以便用户或应用程序可以根据需要请求处理特定文件。有关更多信息，请参阅亚马逊 API Gateway 开发者指南中的使用 Lambda 集成 API Gateway RES T API。
- Step Functions。编排组合多个 Lambda 函数的多步骤文件处理管道。例如，一种从文档中提取文本、对其进行翻译并将结果写回卷的工作流程。有关更多信息，请参阅AWS Step Functions 开发人员指南中的使用 Step Functions 调用 Lambda。

示例 1：生成图像缩略图

此示例从 FSx 中读取 ONTAP 音量的 JPEG 图像，使用 Pillow 图像库将其大小调整为 200 像素的缩略图，然后将缩略图写回音量。

Lambda 函数代码

将以下代码另存为`lambda_function.py`。

```
import boto3
from io import BytesIO
from PIL import Image

s3 = boto3.client('s3')

def lambda_handler(event, context):
    bucket = event['access_point_alias']
    key = event['key']

    # Read the image from FSx through the access point
    response = s3.get_object(Bucket=bucket, Key=key)
    image_data = response['Body'].read()

    # Resize to thumbnail
    img = Image.open(BytesIO(image_data))
    img.thumbnail((200, 200))

    # Write the thumbnail back to FSx
    buffer = BytesIO()
    img.save(buffer, format='JPEG', quality=85)
    buffer.seek(0)

    thumbnail_key = key.rsplit('.', 1)[0] + '_thumbnail.jpg'
    s3.put_object(
        Bucket=bucket,
        Key=thumbnail_key,
        Body=buffer.getvalue(),
        ContentType='image/jpeg'
    )

    return {
        'original_size': len(image_data),
        'thumbnail_size': len(buffer.getvalue()),
        'thumbnail_key': thumbnail_key
```

```
    }
```

创建并调用该函数

此功能需要 Pillow 库。创建一个包含专为 Lambda Linux 运行时构建的 Pillow 的部署包。

```
$ # Create a deployment package with Pillow for Lambda (Linux)
mkdir package && pip install Pillow -t package/ \
    --platform manylinux2014_x86_64 --only-binary=:all:
cd package && zip -r ../thumbnail-function.zip .
cd .. && zip thumbnail-function.zip lambda_function.py

# Create the function
aws lambda create-function \
    --function-name fsxn-thumbnail-generator \
    --runtime python3.12 \
    --handler lambda_function.lambda_handler \
    --role arn:aws:iam::account-id:role/fsxn-lambda-file-processor \
    --zip-file fileb://thumbnail-function.zip \
    --timeout 30 \
    --memory-size 256

# Invoke with a test event
aws lambda invoke \
    --function-name fsxn-thumbnail-generator \
    --cli-binary-format raw-in-base64-out \
    --payload '{"access_point_alias": "my-ap-alias-ext-s3alias", "key": "samples/
images/sample-image.jpg"}' \
    response.json

cat response.json
```

验证结果

```
$ aws s3 ls s3://my-ap-alias-ext-s3alias/samples/images/
2024-01-23 12:19:32    2566770 sample-image.jpg
2024-01-23 12:25:49       7065 sample-image_thumbnail.jpg
```

最初的 2.4 MB 图像（5400 × 2700 像素）的大小调整为 7 KB 的缩略图（200 × 100 像素）。

示例 2：从文档中提取文本

此示例从 FSx for ONTAP 卷中读取 PDF 文档，将其发送到 Amazon Textract 以提取文本，然后将提取的文本作为 JSON 文件写回该卷。

创建并上传示例 PDF

在本示例中，你需要在 FSx for ONTAP 卷上有一个 PDF 文档。以下 Python 脚本生成一个简单的发票 PDF 并通过接入点将其上传。在您的本地计算机上运行此脚本（不是 Lambda）。

```
$ pip install fpdf2 boto3
```

```
# create_invoice.py — run locally to generate and upload a sample PDF
from fpdf import FPDF
import boto3

pdf = FPDF()
pdf.add_page()
pdf.set_font("Helvetica", "B", 24)
pdf.cell(0, 15, "INVOICE", new_x="LMARGIN", new_y="NEXT", align="C")
pdf.set_font("Helvetica", "", 12)
pdf.cell(0, 8, "Invoice Number: INV-2024-00142", new_x="LMARGIN", new_y="NEXT")
pdf.cell(0, 8, "Date: January 15, 2024", new_x="LMARGIN", new_y="NEXT")
pdf.cell(0, 8, "Customer: Example Corp", new_x="LMARGIN", new_y="NEXT")
pdf.ln(5)
pdf.set_font("Helvetica", "B", 12)
pdf.cell(80, 8, "Description", border=1)
pdf.cell(30, 8, "Qty", border=1, align="C")
pdf.cell(40, 8, "Unit Price", border=1, align="R")
pdf.cell(40, 8, "Amount", border=1, align="R")
pdf.ln()
pdf.set_font("Helvetica", "", 12)
for desc, qty, price, amt in [
    ("Cloud Storage Service", "1", "$2,400.00", "$2,400.00"),
    ("Data Transfer (TB)", "5", "$90.00", "$450.00"),
    ("Technical Support", "1", "$500.00", "$500.00"),
]:
    pdf.cell(80, 8, desc, border=1)
    pdf.cell(30, 8, qty, border=1, align="C")
    pdf.cell(40, 8, price, border=1, align="R")
    pdf.cell(40, 8, amt, border=1, align="R")
    pdf.ln()
```

```
s3 = boto3.client('s3')
s3.put_object(
    Bucket='my-ap-alias-ext-s3alias',
    Key='samples/documents/invoice.pdf',
    Body=pdf.output(),
    ContentType='application/pdf'
)
print("Uploaded invoice.pdf")
```

```
$ python3 create_invoice.py
```

Lambda 函数代码

将以下代码另存为lambda_function.py。

```
import boto3
import json

s3 = boto3.client('s3')
textract = boto3.client('textract')

def lambda_handler(event, context):
    bucket = event['access_point_alias']
    key = event['key']

    # Read the PDF from FSx through the access point
    response = s3.get_object(Bucket=bucket, Key=key)
    document_bytes = response['Body'].read()

    # Extract text with Textract
    textract_response = textract.detect_document_text(
        Document={'Bytes': document_bytes}
    )

    lines = [
        block['Text']
        for block in textract_response['Blocks']
        if block['BlockType'] == 'LINE'
    ]

    # Write extracted text as JSON back to FSx
    result = {
        'source_file': key,
```

```
        'total_lines': len(lines),
        'extracted_text': lines
    }

    output_key = key.rsplit('.', 1)[0] + '_extracted.json'
    s3.put_object(
        Bucket=bucket,
        Key=output_key,
        Body=json.dumps(result, indent=2),
        ContentType='application/json'
    )

    return {
        'lines_extracted': len(lines),
        'output_key': output_key
    }
```

创建并调用该函数

```
$ zip textract-function.zip lambda_function.py

aws lambda create-function \
    --function-name fsxn-text-extractor \
    --runtime python3.12 \
    --handler lambda_function.lambda_handler \
    --role arn:aws:iam::account-id:role/fsxn-lambda-file-processor \
    --zip-file fileb://textract-function.zip \
    --timeout 30 \
    --memory-size 256

aws lambda invoke \
    --function-name fsxn-text-extractor \
    --cli-binary-format raw-in-base64-out \
    --payload '{"access_point_alias": "my-ap-alias-ext-s3alias", "key": "samples/
documents/invoice.pdf"}' \
    response.json

cat response.json
```

输出示例：

```
{"lines_extracted": 22, "output_key": "samples/documents/invoice_extracted.json"}
```

示例 3：转录音频文件

此示例为存储在 FSx 上的 ONTAP 音量的音频文件启动 Amazon Transcribe 作业。Amazon Transcribe 使用媒体文件 URI 中的接入点别名直接从接入点读取音频文件。作业完成后，该函数会将脚本写回卷中。

Lambda 函数代码

将以下代码另存为`lambda_function.py`。

```
import boto3
import json
import time
import urllib.request

s3 = boto3.client('s3')
transcribe = boto3.client('transcribe')

def lambda_handler(event, context):
    bucket = event['access_point_alias']
    key = event['key']
    media_format = key.rsplit('.', 1)[-1]  # mp3, wav, etc.

    # Start a Transcribe job pointing to the file on FSx
    job_name = f"fsxn-{int(time.time())}"
    transcribe.start_transcription_job(
        TranscriptionJobName=job_name,
        Media={'MediaFileUri': f's3://{bucket}/{key}'},
        MediaFormat=media_format,
        LanguageCode='en-US'
    )

    # Wait for the job to complete
    while True:
        status = transcribe.get_transcription_job(
            TranscriptionJobName=job_name
        )
        state = status['TranscriptionJob']['TranscriptionJobStatus']
        if state in ('COMPLETED', 'FAILED'):
            break
        time.sleep(5)

    if state == 'FAILED':
        raise Exception(
```

```
            status['TranscriptionJob'].get('FailureReason', 'Unknown error')
        )

    # Download the transcript
    transcript_uri = status['TranscriptionJob']['Transcript']['TranscriptFileUri']
    with urllib.request.urlopen(transcript_uri) as resp:
        transcript_data = json.loads(resp.read())

    transcript_text = transcript_data['results']['transcripts'][0]['transcript']

    # Write the transcript back to FSx
    result = {
        'source_file': key,
        'job_name': job_name,
        'transcript': transcript_text
    }

    output_key = key.rsplit('.', 1)[0] + '_transcript.json'
    s3.put_object(
        Bucket=bucket,
        Key=output_key,
        Body=json.dumps(result, indent=2),
        ContentType='application/json'
    )

    return {
        'transcript_length': len(transcript_text),
        'output_key': output_key
    }
```

创建并调用该函数

```
$ zip transcribe-function.zip lambda_function.py

aws lambda create-function \
    --function-name fsxn-audio-transcriber \
    --runtime python3.12 \
    --handler lambda_function.lambda_handler \
    --role arn:aws:iam::account-id:role/fsxn-lambda-file-processor \
    --zip-file fileb://transcribe-function.zip \
    --timeout 120

aws lambda invoke \
```

```
    --function-name fsxn-audio-transcriber \
    --cli-binary-format raw-in-base64-out \
    --payload '{"access_point_alias": "my-ap-alias-ext-s3alias", "key": "samples/audio/
sample-audio.mp3"}' \
    --cli-read-timeout 180 \
    response.json

cat response.json
```

> **Note**
>
> Transcribe 作业通常需要 15 到 45 秒才能完成。为此，该函数的超时设置为 120 秒。

注意事项

- 默认配置需要互联网来源。默认情况下，Lambda 从您的 VPC 之外的托管基础设施访问 Amazon S3，这需要一个源自互联网的接入点。如果您将 Lambda 函数附加到 VPC，则可以改用 VPC-origin 接入点。有关详细信息，请参阅先决条件。
- 文件大小限制。Lambda 函数的最大内存为 10 GB，最长执行时间为 15 分钟。对于大型文件，可以考虑使用范围读取（`GetObject`带`Range`标头）或流式传输响应。
- Textract 限制。同步 `DetectDocumentText` API 接受最大 10 MB 和 1 页的文档。对于多页文档，请使用异步 `StartDocumentTextDetection` API。
- Transcribe 直接从接入点读取。Amazon Transcribe 接受`MediaFileUri`参数 () `s3://ap-alias/key` 中的接入点别名。Lambda 函数不需要下载和重新上传音频文件。
- 文件系统用户权限。与接入点关联的文件系统用户必须具有输入文件的读取权限和输出目录的写入权限。

清理

为避免持续收费，请删除您在本教程中创建的资源。

```
$ # Delete Lambda functions
aws lambda delete-function --function-name fsxn-thumbnail-generator
aws lambda delete-function --function-name fsxn-text-extractor
aws lambda delete-function --function-name fsxn-audio-transcriber

# Delete the IAM role and policies
aws iam delete-role-policy \
```

```
    --role-name fsxn-lambda-file-processor \
    --policy-name fsxn-access-point-policy
aws iam detach-role-policy \
    --role-name fsxn-lambda-file-processor \
    --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole
aws iam delete-role --role-name fsxn-lambda-file-processor

# Delete sample files from your FSx volume
aws s3 rm s3://my-ap-alias-ext-s3alias/samples/ --recursive
```

使用构建 ETL 管道 AWS Glue

数据工程团队通常会通过 NFS 或 SMB 将来自应用程序、每日文件丢弃或合作伙伴集成的 ONTAP 量的原始数据存放到 FSx 上。为下游分析准备这些数据需要大规模读取、转换、丰富或重新分区，并将精选的输出提供给分析师和应用程序。

通过连接到 FSx for ONTAP 卷的 Amazon S3 接入点， AWS Glue 读取源数据，根据你选择的运行时间（Apache Spark、Python shell 或 Ray）对其进行转换，然后将精选的输出写回同一个卷。原始数据集和精选数据集都保留在 FSx for ONTAP 上，因此卷的快照、备份和保留策略在整个管道中统一适用。由于可以通过 NFS、SMB 和 Amazon S3 API 同时访问适用于 ONTAP 卷的 FSx，因此原始数据可以由 NFS 或 SMB 客户端生成，精选的输出可以由这些协议中的任何一个使用。

在本教程中，您将使用教程中的纽约出租车行使用 Amazon Athena 使用 SQL 查询文件程数据集。AWS Glue ETL 作业读取原始 Parquet 数据，添加计算列，筛选无效记录，并将转换后的输出写回按时间分区的卷中。

> **Note**
>
> 本教程大约需要 25 到 35 分钟才能完成。 AWS 服务 使用者会对您创建的资源产生费用。如果您及时完成所有步骤，包括清理部分，则美国东部（弗吉尼亚北部）的预期费用将低于 1美元 AWS 区域。该估算值不包括 FSx 对 ONTAP 容量本身的持续费用。

先决条件

在开始之前，请确保您具有以下各项：

- 完成使用 Amazon Athena 使用 SQL 查询文件本教程的步骤 1 到 3。该过程将 NYC Taxi 数据集上传到接入点，在中 AWS Glue Data Catalog创建`fsxn_taxi_demo`数据库并注册`taxi_data`表。本教程以这些资源为基础，因此在完成本教程之前，请勿运行 Athena 教程的 “清理” 部分。

- 的 IAM 角色 AWS Glue 具有内联策略，该策略授予对 CloudWatch 日志的写 read/write 入权限、访问点的访问权限和对本教程使用的 AWS Glue Data Catalog 数据库的访问权限。以下步骤创建具有本教程所需最低权限的角色。

  1. 将以下信任策略另存为`glue-trust-policy.json`。它 AWS Glue 允许扮演这个角色。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {"Service": "glue.amazonaws.com"},
            "Action": "sts:AssumeRole"
        }
    ]
}
```

  2. 将以下权限策略另存为`glue-permissions.json`。用您的值替换*region*、*account-id*和*access-point-name*。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Logs",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:region:account-id:log-group:/aws-glue/*"
        },
        {
            "Sid": "AccessPoint",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:ListBucket",
                "s3:DeleteObject"
            ],
            "Resource": [
```

```
                "arn:aws:s3:region:account-id:accesspoint/access-point-name",
                "arn:aws:s3:region:account-id:accesspoint/access-point-name/
object/*"
            ]
        },
        {
            "Sid": "DataCatalog",
            "Effect": "Allow",
            "Action": [
                "glue:GetDatabase",
                "glue:GetTable",
                "glue:GetTables",
                "glue:CreateTable",
                "glue:UpdateTable",
                "glue:DeleteTable",
                "glue:BatchCreatePartition",
                "glue:BatchDeletePartition",
                "glue:CreatePartition",
                "glue:UpdatePartition",
                "glue:GetPartition",
                "glue:GetPartitions"
            ],
            "Resource": [
                "arn:aws:glue:region:account-id:catalog",
                "arn:aws:glue:region:account-id:database/fsxn_taxi_demo",
                "arn:aws:glue:region:account-id:table/fsxn_taxi_demo/*"
            ]
        }
    ]
}
```

3. 创建角色并附加内联策略。

```
$ aws iam create-role \
    --role-name fsxn-tutorial-glue-etl-role \
    --assume-role-policy-document file://glue-trust-policy.json

aws iam put-role-policy \
    --role-name fsxn-tutorial-glue-etl-role \
    --policy-name glue-fsxn-access \
    --policy-document file://glue-permissions.json
```

本教程将 ETL 脚本存储在接入点本身，因此不需要单独的 Amazon S3 存储桶。该`AccessPoint`语句涵盖脚本和出租车数据；该`DataCatalog`语句的作用域是对第 4 步中爬虫更新的`fsxn_taxi_demo`数据库的 AWS Glue 目录访问权限。

> **Important**
>
> Amazon S3 接入点必须使用互联网网络来源。 AWS Glue 任务通过托管基础设施访问 Amazon S3，而不是从您的 VPC。

步骤 1：创建 ETL 脚本

以下 PySpark 脚本从 FSx 中读取 ONTAP 音量的原始出租车行程数据，应用转换并将结果写回音量。将此脚本另存为`taxi_transform.py`。

```
import sys
from awsglue.transforms import *
from awsglue.utils import getResolvedOptions
from pyspark.context import SparkContext
from awsglue.context import GlueContext
from awsglue.job import Job
from pyspark.sql.functions import col, hour, dayofweek, when, round as spark_round

args = getResolvedOptions(sys.argv, ['JOB_NAME', 'AP_ALIAS'])
sc = SparkContext()
glueContext = GlueContext(sc)
spark = glueContext.spark_session
job = Job(glueContext)
job.init(args['JOB_NAME'], args)

ap_alias = args['AP_ALIAS']

# Read raw taxi data from FSx through the access point
df = spark.read.parquet(f"s3://{ap_alias}/taxi-data/")

# Transform: filter invalid records, add computed columns
transformed = df \
    .filter(col("trip_distance") > 0) \
    .filter(col("total_amount") > 0) \
    .filter(col("passenger_count") > 0) \
```

```
    .withColumn("pickup_hour", hour(col("tpep_pickup_datetime"))) \
    .withColumn("pickup_day_of_week", dayofweek(col("tpep_pickup_datetime"))) \
    .withColumn("cost_per_mile",
        spark_round(col("total_amount") / col("trip_distance"), 2)) \
    .withColumn("time_of_day",
        when(hour(col("tpep_pickup_datetime")).between(6, 11), "morning")
        .when(hour(col("tpep_pickup_datetime")).between(12, 16), "afternoon")
        .when(hour(col("tpep_pickup_datetime")).between(17, 21), "evening")
        .otherwise("night")
    ) \
    .select(
        "tpep_pickup_datetime", "tpep_dropoff_datetime",
        "passenger_count", "trip_distance",
        "PULocationID", "DOLocationID",
        "fare_amount", "tip_amount", "total_amount",
        "pickup_hour", "pickup_day_of_week",
        "cost_per_mile", "time_of_day"
    )

# Write transformed data back to FSx, partitioned by time of day
transformed.write \
    .mode("overwrite") \
    .partitionBy("time_of_day") \
    .parquet(f"s3://{ap_alias}/taxi-data-transformed/")

job.commit()
```

该脚本执行以下转换：

- 筛选行程距离、票价或乘客人数为零或负的记录。
- 添加计算列：pickup_hour、pickup_day_of_weekcost_per_mile、和time_of_day（上午、下午、晚上或晚上）。
- 选择与分析相关的列子集。
- 对输出进行@@ 分区time_of_day，这样可以提高按时间段筛选时的查询性能。

步骤 2：上传脚本并创建作业

通过接入点将 ETL 脚本上传到您的 FSx for ONTAP 卷，然后 AWS Glue 创建一个引用该脚本的作业。 AWS Glue 在任务启动时从接入点加载脚本，就像从标准 Amazon S3 存储桶加载脚本一样。

```
$ # Upload the script to the access point
```

```
aws s3 cp taxi_transform.py \
    s3://my-ap-alias-ext-s3alias/glue-scripts/taxi_transform.py

# Create the Glue job
aws glue create-job \
    --name fsxn-taxi-transform \
    --role my-glue-role-arn \
    --command '{
        "Name": "glueetl",
        "ScriptLocation": "s3://my-ap-alias-ext-s3alias/glue-scripts/
taxi_transform.py",
        "PythonVersion": "3"
    }' \
    --default-arguments '{
        "--AP_ALIAS": "my-ap-alias-ext-s3alias",
        "--job-language": "python"
    }' \
    --glue-version "4.0" \
    --number-of-workers 2 \
    --worker-type "G.1X"
```

步骤 3：运行作业

```
$ aws glue start-job-run --job-name fsxn-taxi-transform
```

监控作业状态。如果有两名工作 G.1X 人员，工作通常会在一到两分钟内完成。

```
$ aws glue get-job-runs --job-name fsxn-taxi-transform \
    --query "JobRuns[0].{State:JobRunState,Duration:ExecutionTime,Error:ErrorMessage}"
```

任务完成后，在 FSx 上验证 ONTAP 卷的转换后的输出。

```
$ aws s3 ls s3://my-ap-alias-ext-s3alias/taxi-data-transformed/
                           PRE time_of_day=afternoon/
                           PRE time_of_day=evening/
                           PRE time_of_day=morning/
                           PRE time_of_day=night/
```

输出按一天中的时间分为四个目录。每个分区都包含带有转换数据的 Parquet 文件。

步骤 4：查询转换后的数据

对转换后的输出运行 AWS Glue 爬虫以将其注册到中 AWS Glue Data Catalog，然后使用 Athena 进行查询。

```
$ # Create a crawler for the transformed data
aws glue create-crawler \
    --name fsxn-taxi-transformed-crawler \
    --role my-glue-role-arn \
    --database-name fsxn_taxi_demo \
    --targets '{"S3Targets": [{"Path": "s3://my-ap-alias-ext-s3alias/taxi-data-
transformed/"}]}'

# Run the crawler
aws glue start-crawler --name fsxn-taxi-transformed-crawler
```

爬虫完成后，在 Athena 中查询转换后的数据。分区结构允许 Athena 仅扫描相关的分区。

```
-- Average cost per mile by time of day
SELECT
    time_of_day,
    COUNT(*) AS trip_count,
    ROUND(AVG(cost_per_mile), 2) AS avg_cost_per_mile,
    ROUND(AVG(tip_amount), 2) AS avg_tip
FROM fsxn_taxi_demo.taxi_data_transformed
GROUP BY time_of_day
ORDER BY trip_count DESC
```

```
-- Busiest pickup locations during morning rush
SELECT
    PULocationID AS pickup_location,
    COUNT(*) AS trip_count,
    ROUND(AVG(trip_distance), 2) AS avg_distance
FROM fsxn_taxi_demo.taxi_data_transformed
WHERE time_of_day = 'morning'
GROUP BY PULocationID
ORDER BY trip_count DESC
LIMIT 10
```

由于数据是按分区的`time_of_day`，因此第二个查询仅扫描该`morning`分区，从而减少了读取的数据量并提高了查询性能。

注意事项

- 需要互联网来源。 AWS Glue 任务可从您的 VPC 外部的托管基础设施访问 Amazon S3。您必须使用源自互联网的接入点。
- 读和写。 AWS Glue ETL 作业可以通过接入点读取和写入您的 FSx for ONTAP 卷。接入点策略和文件系统用户必须同时允许`s3:GetObject`和`s3:PutObject`。
- 工人尺码。 AWS Glue 工人的数量和类型会影响工作绩效和成本。对于 48 MB 的样本数据集，两个 G.1X 工作人员就足够了。对于较大的数据集，请增加工作人员数量或使用 G.2X 工作线程。
- 分区。编写分区输出可提高 Athena 和其他分析服务的下游查询性能。根据通常的数据查询方式选择分区键。
- 脚本存储。 AWS Glue 在任务启动时从 Amazon S3 加载 ETL 脚本。本教程将脚本存储在接入点上，以便脚本与数据并存，但您也可以将其托管在标准的 Amazon S3 存储桶中。如果您使用独立存储桶，请在脚本存储桶 ARN `s3:GetObject` 上使用该角色的内联策略进行扩展。

清理

为避免持续收费，请删除您在本教程中创建的资源。

在 Athena 查询编辑器中，删除爬虫创建的表：

```
DROP TABLE IF EXISTS fsxn_taxi_demo.taxi_data_transformed;
```

```
$ # Delete the Glue job and crawler
aws glue delete-job --name fsxn-taxi-transform
aws glue delete-crawler --name fsxn-taxi-transformed-crawler

# Delete the ETL script and transformed data from the access point
aws s3 rm s3://my-ap-alias-ext-s3alias/glue-scripts/taxi_transform.py
aws s3 rm s3://my-ap-alias-ext-s3alias/taxi-data-transformed/ --recursive

# Delete the IAM role
aws iam delete-role-policy \
    --role-name fsxn-tutorial-glue-etl-role \
    --policy-name glue-fsxn-access
aws iam delete-role --role-name fsxn-tutorial-glue-etl-role
```

使用 Amazon Bedrock 知识库构建 RAG 应用程序

许多企业在其 NFS 和 SMB 文件共享中积累了大量文档存储库，包括产品手册、政策文档、合同、研究报告、工程规格和用户生成的内容。

通过连接到 FSx for ONTAP 卷的 Amazon S3 接入点，Amazon Bedrock 知识库可以直接从该卷中提取内容。 Foundation-model 回复以您的团队通过 NFS 或 SMB 保存的文档为基础。作者在共享上更新的内容将在下次同步时提供给知识库。

在本教程中，您将通过 Amazon S3 接入点将一小组示例 PDF 上传到 FSx for ONTAP 卷，创建指向接入点的 Amazon Bedrock 知识库，提取文档，然后通过 API 提问。`RetrieveAndGenerate`

> **Note**
>
> 本教程大约需要 35 到 45 分钟才能完成。 AWS 服务 使用者会对您创建的资源产生费用。如果您及时完成所有步骤，包括清理部分，则美国东部（弗吉尼亚北部）的预期费用将低于 1美元 AWS 区域。该估算值不包括 FSx 对 ONTAP 容量本身的持续费用。

先决条件

在开始之前，请确保您具有以下各项：

- 连接了 Amazon S3 接入点的 ONTAP 卷的 FSx。接入点必须具有互联网网络来源，这样 Amazon Bedrock 服务才能访问它。有关创建接入点的说明，请参阅创建接入点。
- 为 Amazon Bedrock 知识库支持的嵌入模型启用模型访问权限，并在其中创建知识库的至少一个文本生成模型（例如`amazon.nova-lite-v1:0`）。 AWS 区域 本教程使用`amazon.titan-embed-text-v2:0`（1024 个维度）作为嵌入模型；还支持 Cohere 嵌入模型。如果您选择其他嵌入模型，请在步骤 2 中调整向量索引维度以匹配模型的输出维度。在 Amazon Bedrock 控制台的“模型访问权限”下启用了模型访问权限。有关更多信息，请参阅《亚马逊 Bedrock 用户指南》中的 Amazon Bedrock 基础模型。
- AWS CLI 安装了版本 2，并配置了可以创建 IAM 角色的证书、Amazon S3 Vectors 资源和 Amazon Bedrock 知识库。

步骤 1：将示例文档上传到接入点

下载一些公共 PDF 作为示例语料库，然后使用 Amazon S3 接入点别名将其上传到您的接入点。

1. 创建本地目录并下载示例 PDF。

```
$ mkdir -p ~/kb-pdfs && cd ~/kb-pdfs
curl -sSL -o aws-overview.pdf https://d1.awsstatic.com/whitepapers/aws-overview.pdf
curl -sSL -o wellarchitected-framework.pdf https://docs.aws.amazon.com/pdfs/
wellarchitected/latest/framework/wellarchitected-framework.pdf
curl -sSL -o s3-userguide.pdf https://docs.aws.amazon.com/pdfs/AmazonS3/latest/
userguide/s3-userguide.pdf
```

2. 将每个文件上传到接入点。*access-point-alias*替换为您的接入点别名（例如，my-kb-ap-a1b2c3d4e5f6g7h8i9j0kl1mnop2uuse1a-ext-s3alias）。您可以在 Amazon FSx 控制台的 “已连接的 Amazon S3 接入点” 下找到该别名，也可以通过运行来找到该别名。aws fsx describe-s3-access-point-attachments

```
$ for f in *.pdf; do
    aws s3 cp "$f" "s3://access-point-alias/$f"
done
```

3. 验证文件已存放在卷上。

```
$ aws s3 ls s3://access-point-alias/
```

> **Note**
>
> Amazon Bedrock 知识库规定每个文档的最大文件大小为 50 MB。摄取期间会跳过大于 50 MB 的文件。

第 2 步：创建矢量存储

知识库将文档嵌入存储在矢量存储中。Amazon Bedrock 知识库支持多个矢量存储；本教程使用 Amazon S3 矢量作为默认存储库，因为它针对 RAG 工作负载进行了成本优化，并且只需最少的设置。还支持 Amazon OpenSearch Serverless；有关这些说明，请参阅本步骤末尾的可折叠部分。

使用控制台创建矢量存储

如果您使用控制台在中创建知识库步骤 4：创建知识库和数据源，请在矢量数据库步骤中选择快速创建新的矢量存储，然后选择 Amazon S3 矢量图（推荐）或 Amazon S OpenSearch erverless。Amazon Bedrock 会自动创建矢量存储和所有必需的配置。向前跳至 步骤 3：为知识库创建 IAM 角色。

要创建 Amazon S3 矢量存储，请使用 AWS CLI

1. 创建 Amazon S3 矢量存储桶。矢量存储桶名称遵循与标准 Amazon S3 存储桶相同的全局唯一性规则。本教程使用`fsxn-kb-vectors`; 替换为唯一的名称。

```
$ aws s3vectors create-vector-bucket --vector-bucket-name fsxn-kb-vectors
```

2. 在存储桶中创建向量索引。索引维度必须与嵌入模型的输出维度匹配；Titan Text Embeddings v2 输出 1024 个维度。该`nonFilterableMetadataKeys`设置将 Bedrock 元数据字段标记为不可筛选，这使它们不受每向量 2 KB 可筛选元数据的限制。

```
$ aws s3vectors create-index --vector-bucket-name fsxn-kb-vectors \
    --index-name bedrock-kb-index \
    --dimension 1024 --distance-metric cosine --data-type float32 \
    --metadata-configuration '{"nonFilterableMetadataKeys":
["AMAZON_BEDROCK_METADATA","AMAZON_BEDROCK_TEXT"]}'
```

请注意响应`indexArn`中的；你在中使用它步骤 4：创建知识库和数据源。

替代方案：使用创建 OpenSearch 服务无服务器矢量存储 AWS CLI

如果您更喜欢无服务器 OpenSearch 服务（用于更高的每秒查询量、高级搜索功能或熟悉现有操作），请使用以下步骤代替上面的 Amazon S3 Vectors 程序。

1. 为集合创建加密和网络安全策略。

```
$ aws opensearchserverless create-security-policy --name kb-enc --type encryption \
    --policy '{"Rules":[{"ResourceType":"collection","Resource":["collection/fsxn-
kb"]}],"AWSOwnedKey":true}'
aws opensearchserverless create-security-policy --name kb-net --type network \
    --policy '[{"Rules":[{"ResourceType":"collection","Resource":["collection/
fsxn-kb"]},{"ResourceType":"dashboard","Resource":["collection/fsxn-
kb"]}],"AllowFromPublic":true}]'
```

2. 创建数据访问策略，向知识库角色和您的当前用户授予读写集合的权限。将 *account-id* 和 *current-user* 替换为您自己的值。

```
$ aws opensearchserverless create-access-policy --name kb-data --type data --policy
 '[{
    "Rules":[
```

```
        {"ResourceType":"index","Resource":["index/fsxn-kb/*"],"Permission":
["aoss:*"]},
        {"ResourceType":"collection","Resource":["collection/fsxn-
kb"],"Permission":["aoss:*"]}
    ],
    "Principal":[
        "arn:aws:iam::account-id:role/fsxn-kb-role",
        "arn:aws:iam::account-id:user/current-user"
    ]
}]'
```

3. 创建收藏并等待它变成ACTIVE。

```
$ aws opensearchserverless create-collection --name fsxn-kb --type VECTORSEARCH
aws opensearchserverless batch-get-collection --names fsxn-kb \
    --query 'collectionDetails[0].{status:status,endpoint:collectionEndpoint}'
```

4. 使用带有签名请求的 Python 脚本在集合上创建向量索引。索引必须使用维度 1024（适用于 Titan Text Embeddings v2）和亚马逊 Bedrock 知识库期望的字段名称。有关完整脚本和后续配置步骤，请参阅 Amazon Bedrock 用户指南中的使用无服务器 OpenSearch 服务的先决条件。使用步骤 4 中生成的集合 ARN 和索引名称，类型storage-configuration为。OPENSEARCH_SERVERLESS

步骤 3：为知识库创建 IAM 角色

知识库需要一个可以代入的 IAM 角色来调用嵌入模型、通过 Amazon S3 接入点读取对象以及访问矢量存储。下方显示的策略授予对 Amazon S3 Vectors 矢量存储的访问权限。如果您改用无服务器 OpenSearch 服务，请将该S3Vectors语句替换为对集合 ARN 授予aoss:APIAccessAll权限的语句。

使用控制台创建角色

在中使用 Amazon Bedrock 控制台创建知识库时步骤 4：创建知识库和数据源，选择创建并使用新的服务角色。Amazon Bedrock 创建了一个具有所需信任和权限的角色，其范围仅限于您的知识库、嵌入模型、矢量存储和数据源。向前跳至 步骤 4：创建知识库和数据源。

要创建角色，请使用 AWS CLI

1. 将以下信任策略另存为kb-trust-policy.json。它允许 Amazon Bedrock 担任这个角色。*account-id*用您的 AWS 账户 身份证替换。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Principal": {"Service": "bedrock.amazonaws.com"},
        "Action": "sts:AssumeRole",
        "Condition": {"StringEquals": {"aws:SourceAccount": "account-id"}}
    }]
}
```

2. 将以下权限策略另存为kb-permissions.json。它允许访问嵌入模型、Amazon S3 接入点和矢量存储。用您的值替换占位符。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "FoundationModel",
            "Effect": "Allow",
            "Action": ["bedrock:InvokeModel"],
            "Resource": ["arn:aws:bedrock:region::foundation-model/amazon.titan-
embed-text-v2:0"]
        },
        {
            "Sid": "S3AccessPoint",
            "Effect": "Allow",
            "Action": ["s3:GetObject", "s3:ListBucket"],
            "Resource": [
                "arn:aws:s3:region:account-id:accesspoint/access-point-name",
                "arn:aws:s3:region:account-id:accesspoint/access-point-name/object/
*"
            ]
        },
        {
            "Sid": "S3Vectors",
            "Effect": "Allow",
            "Action": [
                "s3vectors:GetIndex",
                "s3vectors:PutVectors",
                "s3vectors:GetVectors",
                "s3vectors:ListVectors",
                "s3vectors:DeleteVectors",
```

```
                "s3vectors:QueryVectors"
            ],
            "Resource": [
                "arn:aws:s3vectors:region:account-id:bucket/fsxn-kb-vectors",
                "arn:aws:s3vectors:region:account-id:bucket/fsxn-kb-vectors/index/
*"
            ]
        }
    ]
}
```

3. 创建角色并附加权限策略。

```
$ aws iam create-role --role-name fsxn-kb-role \
    --assume-role-policy-document file://kb-trust-policy.json
aws iam put-role-policy --role-name fsxn-kb-role --policy-name kb-access \
    --policy-document file://kb-permissions.json
```

步骤 4：创建知识库和数据源

数据源指向您的 Amazon S3 接入点别名。Amazon Bedrock 知识库接受接入点别名代替存储桶名称。

使用控制台创建知识库

1. 打开 Amazon Bedrock 控制台，网址为https://console.aws.amazon.com/bedrock/。
2. 在左侧导航窗格中，选择知识库，然后选择创建知识库。
3. 在知识库详细信息下，输入名称（例如fsxn-kb）和描述。
4. 在 IAM 权限下，选择创建并使用新的服务角色。
5. 对于数据源，选择 Amazon S3，然后选择下一步。
6. 输入数据源名称（例如，fsxn-s3ap-source）。
7. 例如，对于 S3 URI，请在s3://接入点别名后输入s3://my-kb-ap-a1b2c3d4e5f6g7h8i9j0kl1mnop2uuse1a-ext-s3alias。控制台在此字段中不区分存储桶名称和接入点别名；接入点别名按原样接受。
8. 选择下一步。
9. 在“嵌入”模型下，选择 Titan 文本嵌入 v2。
10. 在“矢量数据库”下，选择“快速创建新的矢量存储”，然后选择 Amazon S3 矢量图。选择下一步。
11. 查看配置并选择创建知识库。创建知识库可能需要几分钟。

要使用创建知识库 AWS CLI

1. 创建知识库。用您的值替换占位符。`indexArn`是您在步骤 2 中创建的 Amazon S3 向量索引的 ARN。

```
$ aws bedrock-agent create-knowledge-base --name fsxn-kb \
    --role-arn arn:aws:iam::account-id:role/fsxn-kb-role \
    --knowledge-base-configuration '{
        "type":"VECTOR",
        "vectorKnowledgeBaseConfiguration":{
            "embeddingModelArn":"arn:aws:bedrock:region::foundation-model/
amazon.titan-embed-text-v2:0"
        }
    }' \
    --storage-configuration '{
        "type":"S3_VECTORS",
        "s3VectorsConfiguration":{
            "indexArn":"index-arn"
        }
    }'
```

   记下响应中的 `knowledgeBaseId`。

2. 创建数据源。使用表单将 Amazon S3 接入点别名作为存储桶名称传递到`bucketArn`字段中`arn:aws:s3:::access-point-alias`。

```
$ aws bedrock-agent create-data-source \
    --knowledge-base-id knowledge-base-id \
    --name fsxn-s3ap-source \
    --data-source-configuration '{
        "type":"S3",
        "s3Configuration":{"bucketArn":"arn:aws:s3:::access-point-alias"}
    }'
```

   记下响应中的 `dataSourceId`。

第 5 步：收录文档

运行摄取作业，通过接入点对文档进行爬网，生成嵌入内容，并在矢量存储中为它们编制索引。

使用控制台运行摄取

1. 在 Amazon Bedrock 控制台中，打开您的知识库。
2. 在数据源部分，选择您的数据源，然后选择同步。
3. 等待 “同步” 状态显示为 “就绪”。

要使用运行摄取 AWS CLI

1. 启动摄取作业。

```
$ aws bedrock-agent start-ingestion-job \
    --knowledge-base-id knowledge-base-id \
    --data-source-id data-source-id
```

   记下响应中的 `ingestionJobId`。

2. 轮询作业直到其完成。

```
$ aws bedrock-agent get-ingestion-job \
    --knowledge-base-id knowledge-base-id \
    --data-source-id data-source-id \
    --ingestion-job-id ingestion-job-id
```

   该`status`字段从过渡`IN_PROGRESS`到`COMPLETE`。该`statistics`字段显示扫描和索引了多少文档。

步骤 6：查询知识库

向知识库询问一个以摄取的文档为基础的问题。该响应包括通过 Amazon S3 接入点别名引用源文档的引文。

使用控制台进行查询

1. 在 Amazon Bedrock 控制台中，打开您的知识库。
2. 选择测试知识库。
3. 在 “生成响应” 下，选择文本生成模型（例如 Nova Lite）。
4. 输入诸如之类的问题，`What are the pillars of the AWS Well-Architected Framework?`然后选择 “运行”。答案中显示的引文引用链接到 Amazon S3 接入点中的源文档。

要使用进行查询 AWS CLI

使用 `retrieve-and-generate` 命令。用您的值替换占位符。`modelArn`必须参考您有权访问的文本生成模型的推理配置文件。

```
$ aws bedrock-agent-runtime retrieve-and-generate \
    --input '{"text":"What are the pillars of the AWS Well-Architected Framework?"}' \
    --retrieve-and-generate-configuration '{
        "type":"KNOWLEDGE_BASE",
        "knowledgeBaseConfiguration":{
            "knowledgeBaseId":"knowledge-base-id",
            "modelArn":"arn:aws:bedrock:region:account-id:inference-profile/
us.amazon.nova-lite-v1:0"
        }
    }'
```

响应中包含生成的答案`output.text`和`citations`数组中的引文列表。每份引文都包含一个`s3Location.uri`字段，该字段通过表`s3://access-point-alias/file.pdf`单中的接入点别名指向源文档。

问题排查

摄取任务报告文件被忽略

Amazon Bedrock 知识库规定每个文档的最大文件大小为 50 MB。大于 50 MB 的文件将在中列出`failureReasons`并跳过。在上传之前对大型文档进行拆分或压缩。

`ValidationException`: 标记为 Legacy 的型号

您的账户已弃用您指定的文本生成模型。选择有效的推理配置文件，例如`us.amazon.nova-lite-v1:0`或其他当前支持的模型。运行列`aws bedrock list-inference-profiles`出可用的配置文件。

`AccessDeniedException`摄入期间

确认知识库 IAM 角色`s3:ListBucket`在接入点 ARN（而不是底层卷上）上有`s3:GetObject`和，并且接入点是否有互联网网络来源，以便 Amazon Bedrock 服务可以访问它。如果您在步骤 2 中选择了 Serv OpenSearch ice Serverless 替代方案，还要验证数据访问策略是否将该角色列为委托人。

摄取任务成功但查询未返回任何相关段落

确认矢量索引是使用`dimension: 1024`（适用于 Titan Text Embeddings v2）创建的，并且索引映射中的字段名称与知识库中配置的字段名称相匹配。

清理

为避免持续产生费用，请删除您创建的资源：

- Amazon Bedrock 知识库和数据源
- Amazon S3 向量索引和矢量存储桶（如果您在步骤 2 中使用了替代方案，则为无 OpenSearch 服务服务器集合）
- IAM 角色和内联策略
- 上传到接入点的对象（如果不再需要）

```
$ aws bedrock-agent delete-data-source --knowledge-base-id knowledge-base-id --data-source-id data-source-id
aws bedrock-agent delete-knowledge-base --knowledge-base-id knowledge-base-id
aws s3vectors delete-index --vector-bucket-name fsxn-kb-vectors --index-name bedrock-kb-index
aws s3vectors delete-vector-bucket --vector-bucket-name fsxn-kb-vectors
aws iam delete-role-policy --role-name fsxn-kb-role --policy-name kb-access
aws iam delete-role --role-name fsxn-kb-role
```

替代方案：清理 OpenSearch 服务无服务器资源

如果您在步骤 2 中选择了 Serv OpenSearch ice Serverless 替代方案，请将上述`s3vectors`命令替换为以下命令。Idle Serv OpenSearch ice Service Serverless 集合会产生 OCU-hour 费用，因此在完成本教程后请立即将其删除。

```
$ # Get the collection ID (required by delete-collection; the name is not accepted)
COLLECTION_ID=$(aws opensearchserverless batch-get-collection --names fsxn-kb \
    --query 'collectionDetails[0].id' --output text)

# Delete the collection, then the policies
aws opensearchserverless delete-collection --id "$COLLECTION_ID"
aws opensearchserverless delete-access-policy --name kb-data --type data
aws opensearchserverless delete-security-policy --name kb-net --type network
aws opensearchserverless delete-security-policy --name kb-enc --type encryption
```

使用 Amazon EMR 无服务器运行 Spark 作业

运行 Spark 工作负载（用于日志处理、功能工程、复杂 ETL 或科学分析）的数据工程团队通常在 FSx for ONTAP 卷上保存源数据，这些数据由本地摄取管道、NFS 或 SMB 数据移动器或直接挂载卷的应用程序编写。

通过将 Amazon S3 接入点连接到卷，Amazon EMR Serverless 通过接入点读取数据，对其运行 Spark 作业，然后将结果写回同一个卷。Amazon EMR Serverless 会自动处理集群生命周期 — 您提交任务并为其运行的秒数付费。

这种模式适合需要完整 Spark 运行时的工作负载（自定义库、迭代算法、长时间运行的转换或通过 Amazon EMR Studio 实现的交互式笔记本），在这些工作负载中，较轻的选项（适用于 AWS Glue SQL 的 Amazon Athena 和托管 ETL）并不合适。有关这些替代方案的信息，请参阅使用 Amazon Athena 使用 SQL 查询文件和使用构建 ETL 管道 AWS Glue。

在本教程中，您将模拟一个气象小组，汇总了在 FSx for ONTAP 卷上进行的一年的 NOAA 全球表面每日摘要 (GSOD) 观测结果。您提交一份 PySpark 任务，该作业读取原始 CSV 文件，计算每个站点的每月聚合数据（平均温度、总降水量和降水事件发生的天数），并将结果写为 Parquet 按月分区——所有这些都要通过接入点完成。

> **Note**
>
> 本教程大约需要 30 到 40 分钟才能完成。 AWS 服务 使用者会对您创建的资源产生费用。如果您及时完成所有步骤，包括清理部分，则美国东部（弗吉尼亚北部）的预期费用将低于 1美元 AWS 区域。该估算值不包括 FSx 对 ONTAP 容量本身的持续费用。

先决条件

- 连接了 Amazon S3 接入点的 ONTAP 卷的 FSx。接入点必须具有互联网网络来源，这样 Amazon EMR Serverless 服务才能访问该接入点。有关说明，请参阅创建接入点。
- AWS CLI 已安装版本 2，并配置了可以创建 IAM 角色和 Amazon EMR 无服务器资源的证书。

步骤 1：将示例数据集上传到接入点

NOAA GSOD 数据集是每日天气观测的公共数据集，每个站点每年一个 CSV 文件。在本教程中，您将从公共 `noaa-gsod-pds` Amazon S3 存储桶中下载 100 个站点的子集，然后将其上传到您的接入点。

1. 下载 2024 年的前 100 个电台文件。

```
$ mkdir -p ~/gsod && cd ~/gsod
aws s3 ls s3://noaa-gsod-pds/2024/ --no-sign-request | head -100 | awk '{print
 $NF}' > files.txt
while read f; do
```

```
    aws s3 cp "s3://noaa-gsod-pds/2024/$f" "$f" --no-sign-request --only-show-
errors
done < files.txt
ls | wc -l
```

该命令可下载大约 100 个 CSV 文件，总大小约为 7—8 MB。

2. 将文件上传到前gsod/2024/缀下的接入点。*access-point-alias*替换为您的接入点别名。

```
$ aws s3 cp ~/gsod/ "s3://access-point-alias/gsod/2024/" --recursive --exclude
 "files.txt" --only-show-errors
```

第 2 步：写作 PySpark 业

该作业读取输入前缀下的所有 CSV 文件，过滤表示缺失数据的哨兵值，解析FRSHTT位域（雾、雨、雪、冰雹、雷霆、龙卷风）以计算降水事件天数、按(station, month)天进行聚合，并将分区的 Parquet 写回接入点。

1. 将以下脚本保存到名为的文件中gsod_monthly.py。

```
# gsod_monthly.py
import sys
from pyspark.sql import SparkSession
from pyspark.sql import functions as F

INPUT_PATH, OUTPUT_PATH = sys.argv[1], sys.argv[2]

# GSOD sentinels for missing data
TEMP_SENTINEL = 9999.9
PRCP_SENTINEL = 99.99

spark = SparkSession.builder.appName("gsod-monthly-summary").getOrCreate()

raw = spark.read.option("header", True).csv(INPUT_PATH)

cleaned = (raw
    .select(
        F.col("STATION").alias("station"),
        F.col("NAME").alias("station_name"),
        F.col("LATITUDE").cast("double").alias("lat"),
        F.col("LONGITUDE").cast("double").alias("lon"),
        F.to_date("DATE", "yyyy-MM-dd").alias("date"),
```

```
        F.col("TEMP").cast("double").alias("temp_f"),
        F.col("PRCP").cast("double").alias("prcp_in"),
        F.col("FRSHTT").alias("frshtt"),
    )
    .filter(F.col("temp_f") != TEMP_SENTINEL)
    .withColumn("month", F.date_format("date", "yyyy-MM"))
    .withColumn(
        "prcp_in",
        F.when(F.col("prcp_in") == PRCP_SENTINEL,
 None).otherwise(F.col("prcp_in")),
    )
    # FRSHTT is a 6-char bitfield: Fog, Rain, Snow, Hail, Thunder, Tornado.
    # Check only positions 2-4 (Rain, Snow, Hail) for precipitation events.
    .withColumn(
        "had_precip_event",
        F.when(F.col("frshtt").substr(2, 3).rlike("1"), 1).otherwise(0),
    )
)

monthly = (cleaned
    .groupBy("station", "station_name", "lat", "lon", "month")
    .agg(
        F.avg("temp_f").alias("avg_temp_f"),
        F.min("temp_f").alias("min_temp_f"),
        F.max("temp_f").alias("max_temp_f"),
        F.sum("prcp_in").alias("total_prcp_in"),
        F.sum("had_precip_event").alias("precip_event_days"),
        F.count("*").alias("observation_days"),
    )
)

(monthly.write
    .mode("overwrite")
    .partitionBy("month")
    .parquet(OUTPUT_PATH))

spark.stop()
```

2. 将脚本上传到scripts/前缀下的接入点。

```
$ aws s3 cp gsod_monthly.py "s3://access-point-alias/scripts/gsod_monthly.py"
```

步骤 3：创建 Amazon EMR 无服务器工作角色

Amazon EMR Serverless 在运行您的任务时担任 IAM 执行角色。该角色需要权限才能读取和写入接入点以及将日志写入 CloudWatch 日志。展开以下部分了解设置步骤。

创建 Amazon EMR 无服务器工作角色

1. 将以下信任策略另存为`emr-trust-policy.json`。它允许 Amazon EMR Serverless 担任该角色。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Principal": {"Service": "emr-serverless.amazonaws.com"},
        "Action": "sts:AssumeRole"
    }]
}
```

2. 将以下权限策略另存为`emr-permissions.json`。用您的值替换*region*、*account-id*和*access-point-name*。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Logs",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams"
            ],
            "Resource": "*"
        },
        {
            "Sid": "APRead",
            "Effect": "Allow",
            "Action": ["s3:GetObject", "s3:ListBucket"],
            "Resource": [
                "arn:aws:s3:region:account-id:accesspoint/access-point-name",
```

```
                "arn:aws:s3:region:account-id:accesspoint/access-point-name/object/
*"
            ]
        },
        {
            "Sid": "APWrite",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject", "s3:DeleteObject",
                "s3:AbortMultipartUpload", "s3:ListMultipartUploadParts"
            ],
            "Resource": "arn:aws:s3:region:account-id:accesspoint/access-point-
name/object/*"
        }
    ]
}
```

3. 创建角色并附加策略。

```
$ aws iam create-role --role-name fsxn-emr-job-role \
    --assume-role-policy-document file://emr-trust-policy.json
aws iam put-role-policy --role-name fsxn-emr-job-role \
    --policy-name emr-access --policy-document file://emr-permissions.json
```

第 4 步：创建并启动 Amazon EMR 无服务器应用程序

Amazon EMR 无服务器应用程序是针对特定版本标签和引擎（Spark 或 Hive）的长寿命计算环境。您向它提交一份或多份工作。应用程序会根据任务需求自动向上和向下扩展计算，并在没有作业运行时闲置。

1. 使用最新版本的亚马逊 EMR 创建 Spark 应用程序。

```
$ aws emr-serverless create-application \
    --name fsxn-emr-app --type SPARK --release-label emr-7.0.0
```

记下响应中的 `applicationId`。

2. 启动应用程序。启动会预热一小部分工作人员，因此第一个作业运行时不会出现冷启动延迟。

```
$ aws emr-serverless start-application --application-id application-id
```

等待状态变成STARTED。

```
$ aws emr-serverless get-application --application-id application-id \
    --query 'application.state'
```

第 5 步：提交 Spark 任务

使用应用程序 ID 和执行角色提交作业。该作业通过接入点从中读取原始 CSVgsod-monthly/，gsod/2024/并将分区的 Parquet 写入其中。

1. 将作业驱动程序配置另存为job-driver.json。替换占位符。

```
{
    "sparkSubmit": {
        "entryPoint": "s3://access-point-alias/scripts/gsod_monthly.py",
        "entryPointArguments": [
            "s3://access-point-alias/gsod/2024/",
            "s3://access-point-alias/gsod-monthly/"
        ],
        "sparkSubmitParameters": "--conf spark.executor.cores=2 --conf
 spark.executor.memory=4g --conf spark.driver.cores=2 --conf spark.driver.memory=4g
 --conf spark.executor.instances=2"
    }
}
```

2. 将以下监视配置另存为job-config.json。它将驱动程序和执行者日志发送到日 CloudWatch 志。

```
{
    "monitoringConfiguration": {
        "cloudWatchLoggingConfiguration": {
            "enabled": true,
            "logGroupName": "/aws/emr-serverless/fsxn-emr-app"
        }
    }
}
```

3. 提交作业。

```
$ aws emr-serverless start-job-run \
```

```
    --application-id application-id \
    --execution-role-arn arn:aws:iam::account-id:role/fsxn-emr-job-role \
    --name gsod-monthly \
    --job-driver file://job-driver.json \
    --configuration-overrides file://job-config.json
```

记下响应中的 jobRunId。

4. 轮询作业状态。作业从过渡SCHEDULED到RUNNING到SUCCESS。

```
$ aws emr-serverless get-job-run \
    --application-id application-id \
    --job-run-id job-run-id \
    --query 'jobRun.state'
```

> **Note**
>
> 如果作业失败，请在日志组下的“日志”中查看驱动程序 CloudWatch 日志/aws/emr-serverless/fsxn-emr-app。Amazon EMR Serverless 每次作业运行都会写入一个日志流。

步骤 6：检查输出

验证任务每月写入一个 Parquet 分区以及输出是否可读。

1. 列出输出分区。

```
$ aws s3 ls "s3://access-point-alias/gsod-monthly/" --recursive
```

您应该看到每个month=YYYY-MM/分区一个 Parquet 文件，并在根部看到一个_SUCCESS标记。

2. 在本地读取分区以验证内容。

```
$ aws s3 cp "s3://access-point-alias/gsod-monthly/month=2024-06/" . \
    --recursive --exclude "_SUCCESS"
python3 -c "import pyarrow.parquet as pq; \
    t = pq.read_table(next(__import__('glob').iglob('*.parquet'))); \
    print(t.schema); print(t.to_pandas().head())"
```

输出架构包括station、、station_name、latlon、avg_temp_f、min_temp_f、max_temp_f、total_pr和observation_days。

扩展模式

- 使用 Spark SQL 查询输出。将分区输出注册为表， AWS Glue Data Catalog 然后使用 Spark SQL、Athena 或任何其他读取目录表的工具对其进行查询。 AWS Glue 有关注册接入点支持的数据集的说明，请参阅使用 Amazon Athena 使用 SQL 查询文件。
- 使用 Iceberg 进行 ACID 写入。对于更新或合并数据的工作负载，请将作业配置为写入接入点上的 Iceberg 表，而不是普通的 Parquet。Amazon EMR Serverless 默认在最新版本的标签上包含 Iceberg 运行时。
- 与亚马逊 EMR Studio 以交互方式运行。将 Jupyter 笔记本连接到 Amazon EMR 无服务器应用程序，以交互方式浏览数据。在《亚马逊 EMR 无服务器用户指南》中查看使用 Amazon EMR Serverless 进行交互式工作负载。
- 安排作业。使用 Amazon EventBridge Scheduler 或 AWS Step Functions 按定期计划运行作业（例如，当新一天的数据进入卷时）。

问题排查

接入点AccessDenied上的 Job 失败

验证任务角色策略是否在接入点 ARN（而不是存储桶s3:ListBucket上）上授予s3:GetObject和，以及接入点是否有互联网网络来源，以便 Amazon EMR Serverless 服务可以访问它。

Job 成功但输出为空

检查输入路径。Amazon S3 按字面意思ListObjectsV2处理前缀，因此s3://alias/gsod/2024（没有尾部斜杠）和s3://alias/gsod/2024/（尾部斜杠）的行为可能有所不同。指向文件目录时，请包括尾部的斜杠。

驱动程序日志不在 CloudWatch 日志中

监视配置必须在应用程序--configuration-overrides上传递start-job-run，而不是在应用程序上传递。每个作业运行都会在配置的日志组下写入自己的日志流。

清理

停止并删除应用程序，移除 IAM 角色，并删除您不再需要的所有已上传数据。

```
$ aws emr-serverless stop-application --application-id application-id
aws emr-serverless delete-application --application-id application-id
aws iam delete-role-policy --role-name fsxn-emr-job-role --policy-name emr-access
aws iam delete-role --role-name fsxn-emr-job-role
aws s3 rm "s3://access-point-alias/scripts/gsod_monthly.py"
aws s3 rm "s3://access-point-alias/gsod/" --recursive
aws s3 rm "s3://access-point-alias/gsod-monthly/" --recursive
```

使用流式传输视频 CloudFront

媒体工作流通常将完成的内容（视频点播 (VOD) 文件、HTTP 直播 (HLS) 包、图像和图形）存储在 FSx for ONTAP 卷上，编辑、制作人和自动化系统使用 NFS 或 SMB 写入该卷。

通过连接到 FSx for ONTAP 卷的 Amazon S3 接入点， CloudFront 可以直接从该卷中提供内容。编辑和制作系统像往常一样通过 NFS 或 SMB 向卷发布内容，通过接入点 CloudFront 获取内容，观众则从最近的 CloudFront 边缘位置接收内容。

在本教程中，您将示例视频编码为 HLS 自适应比特率包，将输出上传到连接到 FSx for ONTAP 卷的接入点，使用原始访问控制配置 CloudFront 分发以使观众无法绕过直接访问音量，并验证直播是否端 CloudFront 对端播放。

> **Note**
>
> 本教程大约需要 40 到 60 分钟才能完成。 AWS 服务 使用者会对您创建的资源产生费用。如果您及时完成所有步骤，包括清理部分，则美国东部（弗吉尼亚北部）的预期费用将低于 1美元 AWS 区域。该估算值不包括 FSx 对 ONTAP 容量本身的持续收费。

模式是如何运作的

请求流为：

- 观众的播放器（浏览器、移动应用程序、智能电视）向 CloudFront 域请求HLS主播放列表。
- CloudFront 检查其边缘缓存。如果未成功， CloudFront 则使用签名版本 4 (Sigv4) 及其源访问控制 (OAC) 对请求进行签名，然后将其转发到接入点的 Amazon S3 终端节点。

- 接入点根据其访问策略授权请求，该策略允许 CloudFront 服务主体范围限于您的分发，并从 FSx for ONTAP 卷返回请求的对象。
- CloudFront 在边缘缓存响应并将其返回给查看者。

HLS 包混合了两种类型的文件，它们受益于不同的缓存策略：

- 播放列表 (`.m3u8`) 描述了哪些片段构成了直播内容。使用简短的 `Cache-Control` TTL，这样您就可以快速发布更新的播放列表。
- 片段 (`.ts`) 包含编码后的视频和音频。写入后，片段的内容永远不会改变，因此请使用长的、不可变`Cache-Control`的 TTL。

先决条件

- 连接了 Amazon S3 接入点的 ONTAP 卷的 FSx。接入点必须有互联网网络来源，这样 CloudFront 才能到达它。有关说明，请参阅创建接入点。
- AWS CLI 安装并配置了版本 2，其凭据可以创建 CloudFront 分配、源访问控制和接入点策略。
- FFmpeg 安装在本地，用于将示例视频编码为 HLS。
- 源视频文件。本教程使用了Blender基金会的 Sintel预告片，这是一段在知识共享下发布的52秒1080p片段。

第 1 步：将源视频编码为 HLS 包

使用 FFmpeg 制作 360p、720p 和 1080p 的三种变体 HLS 软件包，并具有逼真的过顶 (OTT) 比特率。生成的软件包包括一个主播放列表，该播放列表引用了每个变体的播放列表，每个播放列表都列出了四秒钟的传输流片段。

1. 下载源视频。

```
$ mkdir -p ~/media && cd ~/media
curl -sSL -o sintel-1080p.mp4 \
    https://download.blender.org/durian/trailer/sintel_trailer-1080p.mp4
```

2. 使用三种自适应比特率变体将视频编码为 HLS。

```
$ mkdir hls && cd hls
ffmpeg -i ../sintel-1080p.mp4 \
    -filter_complex "[0:v]split=3[v1][v2][v3]; \
```

```
        [v1]scale=w=640:h=360[v1out]; \
        [v2]scale=w=1280:h=720[v2out]; \
        [v3]scale=w=1920:h=1080[v3out]" \
    -map "[v1out]" -c:v:0 libx264 -b:v:0 800k  -maxrate:v:0 856k  -bufsize:v:0
 1200k \
    -map "[v2out]" -c:v:1 libx264 -b:v:1 3000k -maxrate:v:1 3200k -bufsize:v:1
 4500k \
    -map "[v3out]" -c:v:2 libx264 -b:v:2 5500k -maxrate:v:2 5900k -bufsize:v:2
 8250k \
    -preset veryfast -g 48 -keyint_min 48 -sc_threshold 0 \
    -map a:0 -map a:0 -map a:0 -c:a aac -b:a:0 96k -b:a:1 128k -b:a:2 128k \
    -f hls -hls_time 4 -hls_playlist_type vod -hls_flags independent_segments \
    -hls_segment_filename "stream_%v/seg_%03d.ts" \
    -master_pl_name master.m3u8 \
    -var_stream_map "v:0,a:0,name:360p v:1,a:1,name:720p v:2,a:2,name:1080p" \
    "stream_%v/playlist.m3u8"
```

该命令生成一个目录树，其中包含一个主播放列表、三个变体播放列表以及每个变体的传输流片段。

```
hls/
### master.m3u8
### stream_360p/
#   ### playlist.m3u8
#   ### seg_000.ts
#   ### ...
### stream_720p/
#   ### playlist.m3u8
#   ### seg_000.ts
#   ### ...
### stream_1080p/
    ### playlist.m3u8
    ### seg_000.ts
    ### ...
```

步骤 2：将 HLS 包上传到接入点

上传软件包两次，一次用于包含短 TTL 的播放列表，一次用于具有长且不可变的 TTL 的片段。正确设置Content-Type很重要：大多数玩家都需要 for `.m3u8` 和 `application/vnd.apple.mpegurl` f `video/mp2t` or `.ts`。

*access-point-alias*替换为您的接入点别名。

```
$ # Playlists: short TTL, m3u8 content type
aws s3 cp ~/media/hls/ "s3://access-point-alias/content/sintel/" \
    --recursive --exclude "*" --include "*.m3u8" \
    --content-type "application/vnd.apple.mpegurl" \
    --cache-control "max-age=60"

# Segments: long immutable TTL, ts content type
aws s3 cp ~/media/hls/ "s3://access-point-alias/content/sintel/" \
    --recursive --exclude "*" --include "*.ts" \
    --content-type "video/mp2t" \
    --cache-control "max-age=31536000,immutable"
```

确认上传的两个文件都符合预期的内容类型和缓存标头。

```
$ aws s3api head-object --bucket access-point-alias \
    --key content/sintel/master.m3u8 \
    --query '{ContentType:ContentType,CacheControl:CacheControl}'
```

步骤 3：创建源站访问控制

源访问控制 (OAC) 允许您对接入点的请求进行 CloudFront 签名，因此 CloudFront只能获取对象。如果没有 OAC，则查看者可以通过直接从接入点端点请求对象来绕过 CloudFront 。

```
$ aws cloudfront create-origin-access-control \
    --origin-access-control-config \
    'Name=fsxn-media-
oac,SigningProtocol=sigv4,SigningBehavior=always,OriginAccessControlOriginType=s3'
```

记下响应中的 `Id`。您将在下一步中使用它。

步骤 4：创建分 CloudFront 配

使用接入点别名作为源域创建 CloudFront 分配。使用`CachingOptimized`托管缓存策略，该策略遵循您在步骤 2 中设置的`Cache-Control`标头。

1. 将以下配置保存到名为的文件中`dist.json`，替换占位符。

```
{
    "CallerReference": "fsxn-media-1",
```

```
    "Comment": "FSx for ONTAP media delivery",
    "Enabled": true,
    "DefaultRootObject": "",
    "Origins": {
        "Quantity": 1,
        "Items": [{
            "Id": "fsxn-ap",
            "DomainName": "access-point-alias.s3.region.amazonaws.com",
            "S3OriginConfig": {"OriginAccessIdentity": ""},
            "OriginAccessControlId": "oac-id",
            "ConnectionAttempts": 3,
            "ConnectionTimeout": 10
        }]
    },
    "DefaultCacheBehavior": {
        "TargetOriginId": "fsxn-ap",
        "ViewerProtocolPolicy": "redirect-to-https",
        "AllowedMethods": {
            "Quantity": 2, "Items": ["GET", "HEAD"],
            "CachedMethods": {"Quantity": 2, "Items": ["GET", "HEAD"]}
        },
        "Compress": true,
        "CachePolicyId": "658327ea-f89d-4fab-a63d-7e88639e58f6"
    },
    "PriceClass": "PriceClass_100",
    "ViewerCertificate": {"CloudFrontDefaultCertificate": true}
}
```

> **Note**
>
> PriceClass_100仅在北美和欧洲使用 CloudFront 边缘站点，这样可以降低本教程的成本。对于全局边缘覆盖范围，请将该值更改为PriceClass_All。有关更多信息，请参阅为 CloudFront 分配选择价格等级。

2. 创建发行版。

```
$ aws cloudfront create-distribution --distribution-config file://dist.json \
    --query 'Distribution.{Id:Id,DomainName:DomainName,ARN:ARN}'
```

记下响应中的分发 ID、ARN 和域名。部署该分发大约需要五分钟。部署时，您可以继续执行步骤 5。

步骤 5：附加允许的接入点策略 CloudFront

接入点策略向 CloudFront 服务主体授予读取对象的权限，该权限仅限于使用AWS:SourceArn条件的特定分配。

1. 将以下策略保存到名为的文件中ap-policy.json，替换占位符。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AllowCloudFrontServicePrincipal",
        "Effect": "Allow",
        "Principal": {"Service": "cloudfront.amazonaws.com"},
        "Action": "s3:GetObject",
        "Resource": "arn:aws:s3:region:account-id:accesspoint/access-point-name/
object/*",
        "Condition": {
            "StringEquals": {
                "AWS:SourceArn": "arn:aws:cloudfront::account-
id:distribution/distribution-id"
            }
        }
    }]
}
```

2. 将策略附加到接入点。

```
$ aws s3control put-access-point-policy \
    --account-id account-id \
    --name access-point-name \
    --policy file://ap-policy.json
```

步骤 6：验证播放

等待分发达到Deployed状态。

```
$ aws cloudfront get-distribution --id distribution-id \
    --query 'Distribution.Status'
```

通过获取主播放列表 CloudFront。

```
$ curl -sS "https://distribution-domain/content/sintel/master.m3u8"
```

响应应列出三种变体。

```
#EXTM3U
#EXT-X-VERSION:6
#EXT-X-STREAM-INF:BANDWIDTH=1031744,RESOLUTION=640x360,CODECS="avc1.64001e,mp4a.40.2"
stream_360p/playlist.m3u8

#EXT-X-STREAM-INF:BANDWIDTH=3497301,RESOLUTION=1280x720,CODECS="avc1.64001f,mp4a.40.2"
stream_720p/playlist.m3u8

#EXT-X-STREAM-INF:BANDWIDTH=6311285,RESOLUTION=1920x1080,CODECS="avc1.640028,mp4a.40.2"
stream_1080p/playlist.m3u8
```

检查响应标头的内容类型、缓存控制和缓存状态是否正确。

```
$ curl -sSI "https://distribution-domain/content/sintel/stream_1080p/seg_000.ts"
```

成功的响应会显示`content-type: video/mp2t`和`cache-control: max-age=31536000,immutable`、和一个`x-cache`标头，指示响应是来自边缘还是源头。

最后，使用 FFmpeg 端对端播放直播，以确认所有片段都正确提取和解码。

```
$ ffprobe -v error \
    -show_entries stream=codec_name,width,height \
    -show_entries format=duration \
    "https://distribution-domain/content/sintel/master.m3u8"
```

你也可以在 Safari 或 VLC 中打开主播放列表网址，或者使用诸如 hls.js 之类的 JavaScript 播放器将其嵌入到网页中。

扩展模式

- 使用带有 HTTPS 的自定义域名。为您的域申请 ACM 证书，将其附加到分配中，然后添加指向该 CloudFront 域的 CNAME 记录。有关说明，请参阅将自定义 URL 与配合使用 CloudFront。
- 使用签名网址或签名 Cookie 保护优质内容。对于需要授权的内容（订阅服务、抢先体验预览、地理围栏内容），请使用 CloudFront 签名 URL 或签名 Cookie。请参阅使用签名网址和签名 Cookie 提供私有内容。

- 发布新内容时使缓存失效。替换播放列表或上传新的 HLS 包时，请使用从 `aws cloudfront create-invalidation` edge 中移除旧版本 CloudFront 。对于具有长 TTL 的不可变分段，通常不需要失效，因为每个包的分段文件名都是唯一的。
- 为基于浏览器的玩家启用 CORS。如果其他网域中基于浏览器的 HLS 播放器加载了您的直播，请使用响应`Access-Control-Allow-Origin`标头策略向 CloudFront响应添加标头。
- 记录查看者请求。启用 CloudFront标准日志记录或实时日志，以捕获查看者对分析、计费或滥用检测的请求。

问题排查

403 禁止进入 CloudFront

缺少接入点策略，不包括 CloudFront 服务主体，或者`AWS:SourceArn`条件引用了错误的分发 ARN。使用验证策略`aws s3control get-access-point-policy`并确认分发 ARN 与您的`aws cloudfront create-distribution`回复中的分发 ARN 相匹配。

播放器加载主播放列表但无法播放

检查片段文件是否有`Content-Type: video/mp2t`，播放列表是否有`Content-Type: application/vnd.apple.mpegurl`。一些玩家拒绝使用通用内容类型的片段。 Re-upload 使用正确的`--content-type`标志。

新的播放列表需要时间才能吸引观众

CloudFront 缓存标题设置的 TTL 的播放`Cache-Control`列表。如果您需要较短的 TTL，请使用较小的`max-age`值重新上传播放列表，或者创建无效状态。区段没有这个问题，因为它们的内容不会改变。

`x-cache: Miss from cloudfront`根据每一个请求

当某个区域的查看者第一次请求文件时，这是正常的。 CloudFront 失败时从原点获取并缓存 TTL 的响应。随后从该边缘站点请求相同文件的请求将返回`Hit from cloudfront`。

拒绝直接访问接入点

这是预期行为。OAC 要求来自服务主体的 SigV4-signed 请求 CloudFront，接入点策略限制对 CloudFront 服务主体的访问。观看者只能通过分发域访问内容。

清理

禁用并删除该分配，然后删除其余资源。必须先禁用发行版，然后才能将其删除，这需要几分钟。

禁用需要来自的两个值`get-distribution-config`：ETag`f --if-match` or 和 for 的内部`DistributionConfig`对象`--distribution-config`（完整的响应还包含 ETag，它`update-distribution`不接受）。

```
$ # Capture the current ETag and the DistributionConfig body
GET_ETAG=$(aws cloudfront get-distribution-config --id distribution-id \
    --query 'ETag' --output text)
aws cloudfront get-distribution-config --id distribution-id \
    --query 'DistributionConfig' --output json \
    | jq '.Enabled = false' > dist-updated.json

# Disable the distribution. The response returns a new ETag.
UPDATE_ETAG=$(aws cloudfront update-distribution --id distribution-id \
    --if-match "$GET_ETAG" --distribution-config file://dist-updated.json \
    --query 'ETag' --output text)

# Wait for Status to reach Deployed before deleting.
aws cloudfront get-distribution --id distribution-id \
    --query 'Distribution.Status'

# Delete the distribution using the ETag from the update call.
aws cloudfront delete-distribution --id distribution-id \
    --if-match "$UPDATE_ETAG"

# Fetch the OAC ETag, then delete the OAC.
OAC_ETAG=$(aws cloudfront get-origin-access-control --id oac-id \
    --query 'ETag' --output text)
aws cloudfront delete-origin-access-control --id oac-id \
    --if-match "$OAC_ETAG"
aws s3control delete-access-point-policy \
    --account-id account-id --name access-point-name
aws s3 rm "s3://access-point-alias/content/sintel/" --recursive
```

对 S3 接入点问题进行故障排除

本节介绍从 S3 接入点访问 FSx 数据时遇到问题的症状、原因和解决方案。

S3 接入点处于配置错误的状态

由于以下原因，S3 接入点附件可能会转换到该`MISCONFIGURED`状态：

- 无法解析文件系统标识-无法再在文件系统上解析与接入点关联的 UNIX 或 Windows 用户。如果用户已从名称服务（例如本地文件、LDAP 或 Active Directory）中移除，或者名称服务变得无法访问，则可能会发生这种情况。要解决这个问题，请确保用户存在并且可以在 SVM 上解析。有关更多信息，请参阅 由于文件系统用户身份查询失败，S3 接入点创建失败。
- 连接的卷处于脱机状态或已卸载 — 接入点所连接的卷处于脱机状态或已卸载（不再有接合路径）。要解决此问题，请将该卷重新联机或重新挂载。有关更多详细信息，请参阅 ONTAP 文档。

Amazon FSx 会定期检查这些情况，并在潜在问题解决后自动将接入点返回AVAILABLE到该接入点。

由于文件系统用户身份查询失败，S3 接入点创建失败

创建和连接 S3 接入点时，FileSystemIdentity必须提供。您负责在 ONTAP 中配置提供的 UNIX 或 Windows 用户。

如果提供UnixUser了，则 ONTAP 必须能够将 UnixUser 名称映射到 UNIX UID/GIDs。ONTAP 使用名称服务交换机配置来确定如何执行此映射。

```
> vserver services name-service ns-switch show
```

```
Vserver         Database       Order
--------------- ------------   ---------
svm_1           hosts          files,
                               dns
svm_1           group          files,
                               ldap
svm_1           passwd         files,
                               ldap
svm_1           netgroup       nis,
                               files
```

请确保您在 UnixUser passwd和group数据库中有使用有效来源（filesldap、等）的条目。可以使用vserver services name-service unix-user和vserver services name-service unix-group命令配置files源。可以使用vserver services name-service ldap命令配置ldap源。

如果提供WindowsUser了，则 ONTAP 必须能够在加入的 Active Directory 域中找到该 WindowsUser 名称。

要确认提供的 UnixUser 或映射 WindowsUser 是否正确，fsxadmin可以使用以下命令（替换为 f -unix-user-name o -win-name r WindowsUsers）：

```
> vserver services access-check authentication show-creds -
node FsxId0fd48ff588b9d3eee-01 -vserver svm_name -unix-user-name root -show-partial-
unix-creds true
```

成功输出示例：

```
 UNIX UID: root

 GID: daemon
 Supplementary GIDs:
  daemon
```

不成功的输出示例：

```
Error: Acquire UNIX credentials procedure failed
  [  2 ms] Entry for user-name: unmapped-user not found in the
           current source: FILES. Entry for user-name: unmapped-user
           not found in any of the available sources
**[     3] FAILURE: Unable to retrieve UID for UNIX user
**         unmapped-user

Error: command failed: Failed to resolve user name to a UNIX ID. Reason: "SecD Error:
 object not found".
```

不正确的用户映射可能会导致 S3 Access Denied 出现错误。请参阅下面的失败原因示例。

Entry for user-name not found in the current source: LDAP

如果您配置ns-switch为使用ldap源，请确保 ONTAP 已配置为正确使用您的 LDAP 服务器。有关更多信息 NetApp，请参阅配置 LDAP 的技术报告。

RESULT_ERROR_DNS_CANT_REACH_SERVER 或 RESULT_ERROR_SECD_IN_DISCOVERY

此错误表示 ONTAP 中虚拟服务器的 DNS 配置存在问题。运行以下命令以确保您的虚拟服务器的 DNS 配置正确：

```
> dns check -vserver svm_name
```

NT_STATUS_PENDING

此错误表示与域控制器通信时出现问题。根本原因可能是由于缺乏中小型企业积分。有关更多信息，请参阅 NetApp KB。

由于未装入卷，S3 接入点创建失败。

对于已安装的 ONTAP 卷（具有接合路径），S3 接入点只能连接到 FSx。这也适用于 DP（数据保护）卷类型。有关更多信息，请参阅 ONTAP 卷装载文档。

由于 SVM 上已禁用 S3 协议，S3 接入点创建失败

S3 接入点要求在存储虚拟机 (SVM) 上启用 S3 协议。要启用 S3 协议，请使用`fsxadmin`以下命令在 ONTAP CLI 中运行以下命令：

```
> vserver add-protocols -vserver svm_name -protocols s3
```

要验证协议是否已启用，请执行以下操作：

```
> vserver show -vserver svm_name -fields allowed-protocols,disallowed-protocols
```

文件系统无法处理 S3 请求

如果特定工作负载的 S3 请求量超过文件系统处理流量的容量，则可能会遇到 S3 请求错误（例如`Internal Server Error`、`503 Slow Down`和`Service Unavailable`）。您可以使用 Amazon CloudWatch 指标（例如和`CPU utilization`）主动监控文件系统的性能`Network throughput utilization`并发出警报。如果您发现性能下降，则可以通过增加文件系统的吞吐容量来解决此问题。

使用自动创建的服务角色的默认 S3 接入点权限拒绝访问

某些 S3-integrated AWS 服务将创建自定义服务角色并根据您的特定用例自定义附加权限。将您的 S3 接入点别名指定为 S3 资源时，这些附加的权限可能包括使用存储桶 ARN 格式（例如`arn:aws:s3:::my-fsx-ap-foo7detztxouyjpwtu8krroppxytruse1a-ext-s3alias`）而不是接入点 ARN 格式（例如）的接入点。`arn:aws:s3:us-east-1:1234567890:accesspoint/my-fsx-ap`要解决此问题，请修改策略以使用接入点的 ARN。

访问来自其他 AWS 服务的数据

除了 Amazon EC2 之外，您还可以将其他 AWS 服务与您的卷一起使用来访问您的数据。

主题

- 将 Amazon WorkSpaces 与 FSx for ONTAP 配合使用

- 将亚马逊弹性容器服务与 ONTAP FSx 配合使用
- 将亚马逊弹性 VMware 服务与 ONTAP FSx 配合使用
- 将 VMware 云与 ONTAP 搭 FSx 配使用

将 Amazon WorkSpaces 与 FSx for ONTAP 配合使用

FSx for ONTAP 可与 Amazon WorkSpaces 配合使用，提供共享的网络附属存储（NAS）或存储 Amazon WorkSpaces 账户的漫游配置文件。连接到具有 WorkSpaces 实例的 SMB 文件共享后，用户可以在文件共享上创建和编辑文件。

以下过程说明了如何将 Amazon FSx 与 Amazon WorkSpaces 配合使用，提供漫游配置文件和主文件夹的访问，从而实现一致的体验，并为 Windows 和 Linux WorkSpaces 用户提供共享的团队文件夹。如果您是第一次使用 Amazon WorkSpaces，则可以按照《Amazon WorkSpaces 管理指南》中开始使用 WorkSpaces 快速设置功能中的说明创建您的第一个 Amazon WorkSpaces 环境。

主题

- 提供漫游配置文件支持
- 提供共享文件夹以访问常用文件

提供漫游配置文件支持

您可以使用 Amazon FSx 向组织中的用户提供漫游配置文件支持。用户仅有权访问自己的漫游配置文件。此文件夹将使用 Active Directory 组策略自动连接。借助漫游配置文件，在注销 Amazon FSx 文件共享时，用户的数据和桌面设置得以保存，从而可以在不同的 WorkSpaces 实例之间共享文档和设置，并使用 Amazon FSx 每日自动备份进行自动备份。

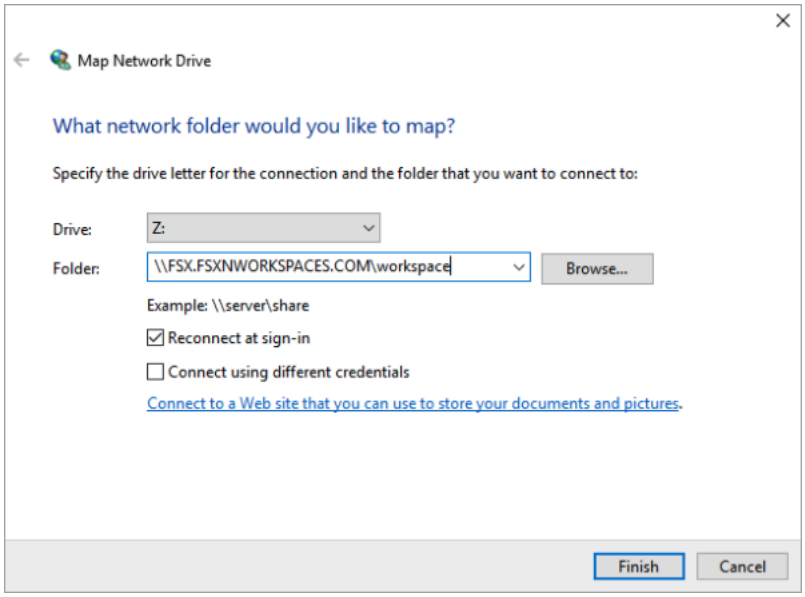
第 1 步：使用 Amazon FSx 为域用户创建配置文件文件夹位置

1. 使用 Amazon FSx 控制台创建 FSx for ONTAP 文件系统。有关更多信息，请参阅 创建文件系统（控制台）。

> **Important**
>
> 每个 FSx for ONTAP 文件系统都有一个端点 IP 地址范围，从该范围创建与文件系统关联的端点。对于多可用区文件系统，FSx for ONTAP 会选择默认未使用的 IP 地址范围 198.19.0.0/16 作为端点 IP 地址范围。如《Amazon WorkSpaces 管理指南》中的 WorkSpaces 的 IP 地址和端口要求所述，WorkSpaces 还使用此 IP 地址范围来管理流量

范围。因此，要从 WorkSpaces 访问 FSx for ONTAP 文件系统的多可用区，必须选择不与 198.19.0.0/16 重叠的端点 IP 地址范围。

2. 如果您还没有将存储虚拟机（SVM）加入 Active Directory，请立即创建一个。例如，您可以配置一个名为 `fsx` 的 SVM，并将安全样式设置为 NTFS。有关更多信息，请参阅 创建存储虚拟机（控制台）。
3. 为您的 SVM 创建卷。例如，您可以创建一个名为 `fsx-vol` 的卷，该卷沿用 SVM 根卷的安全样式。有关更多信息，请参阅 创建 FlexVol 卷（控制台）。
4. 在您的卷上创建 SMB 共享。例如，您可以在名为 `fsx-vol` 的卷上创建一个名为 `workspace` 的共享，在其中创建一个名为 `profiles` 的文件夹。有关更多信息，请参阅 管理 SMB 共享。
5. 从 WorkSpace 或从运行 Windows Server 的 Amazon EC2 实例访问 Amazon FSx SVM。有关更多信息，请参阅 访问您的 fo FSx r ONTAP 数据。
6. 您将共享映射到 Windows WorkSpaces 实例上的 `Z:\`：



步骤 2：将 FSx for ONTAP 文件共享链接至用户账户

1. 在测试用户的 WorkSpace 时，选择 Windows > 系统 > 高级系统设置。
2. 在系统属性中，选择高级选项卡，然后按用户配置文件部分的设置按钮。已登录的用户将具有 `Local` 的配置文件类型。
3. 将测试用户从 WorkSpace 注销。

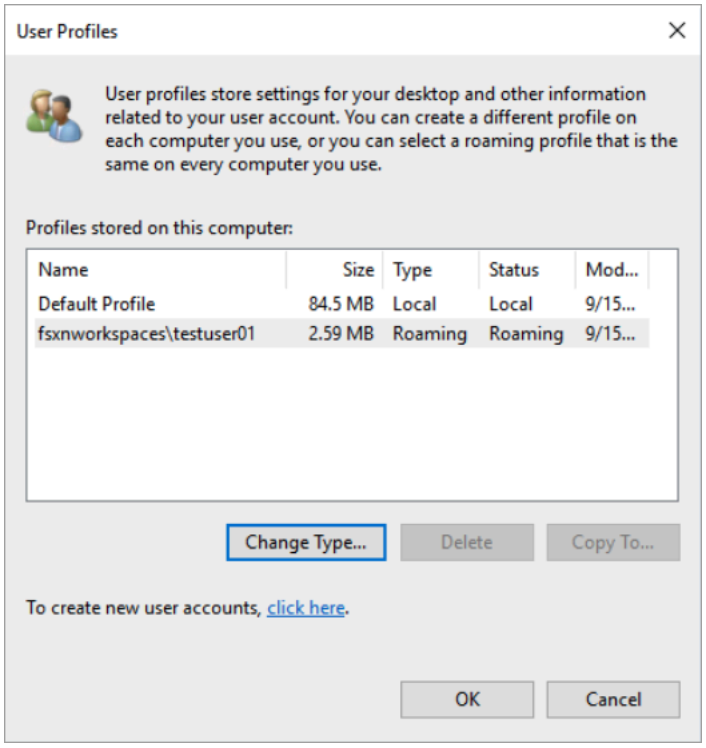
4. 设置测试用户的漫游配置文件位于您的 Amazon FSx 文件系统上。在您的管理员 WorkSpaces 中，打开 PowerShell 控制台并使用类似于以下示例的命令（该示例使用您之前在步骤 1 中创建的 `profiles` 文件夹）：

```
Set-ADUser username -ProfilePath \\filesystem-dns-
name\sharename\foldername\username
```

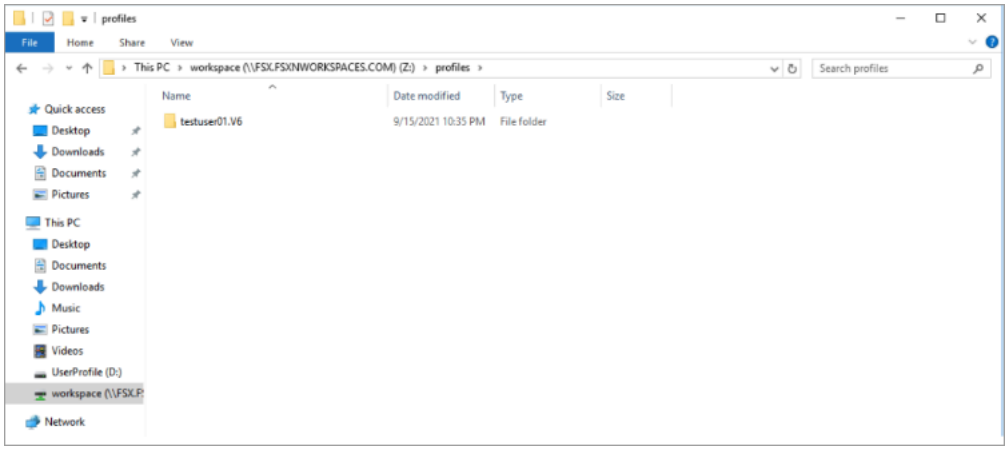
例如：

```
Set-ADUser testuser01 -ProfilePath \\fsx.fsxnworkspaces.com\workspace\profiles
\testuser01
```

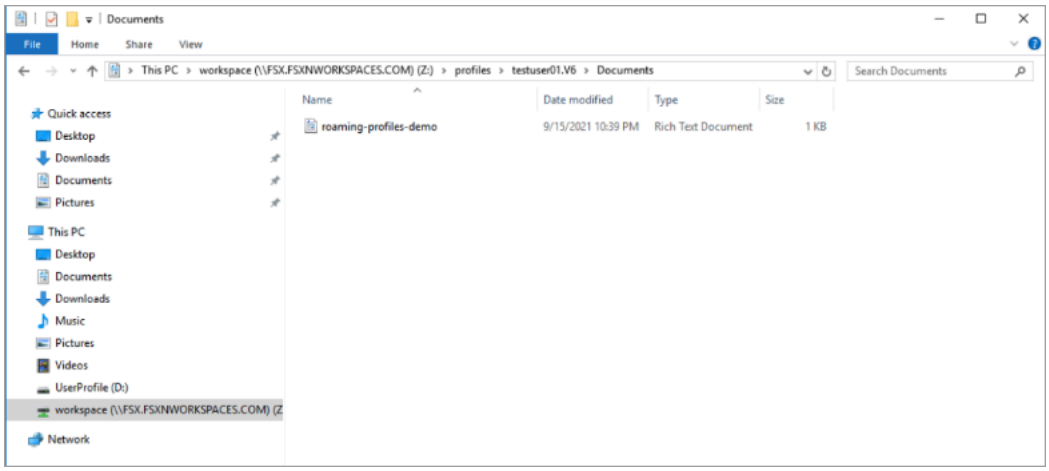
5. 登录到测试用户 WorkSpace。
6. 在系统属性中，选择高级选项卡，然后按用户配置文件部分的设置按钮。已登录的用户将具有 `Roaming` 的配置文件类型。



7. 浏览 FSx 查看 ONTAP 共享文件夹。在 `profiles` 文件夹中，您将看到该用户的文件夹。



8. 在测试用户的 Documents 文件夹中创建文档
9. 将测试用户从其 WorkSpace 注销。
10. 如果您以测试用户的身份重新登录并浏览至他们的配置文件存储位置，则会看到您创建的文档。



提供共享文件夹以访问常用文件

您可以使用 Amazon FSx 向组织中的用户提供共享文件夹。共享文件夹可用于存储您的用户社区使用的文件，例如演示文件、代码示例和所有用户都需要的说明手册。通常，您需为共享文件夹映射驱动器；但是，由于映射的驱动器使用驱动器号，因此您可拥有的共享数量有限。此过程将创建一个 Amazon FSx 共享文件夹，该文件夹无需驱动器号即可使用，这样您就可以更灵活地将共享分配给团队。

挂载共享文件夹，以便从 Linux 和 Windows WorkSpaces 进行跨平台访问

1. 从任务栏中选择位置 > 连接到服务器。
   a. 对于服务器，请输入 *file-system-dns-name*。

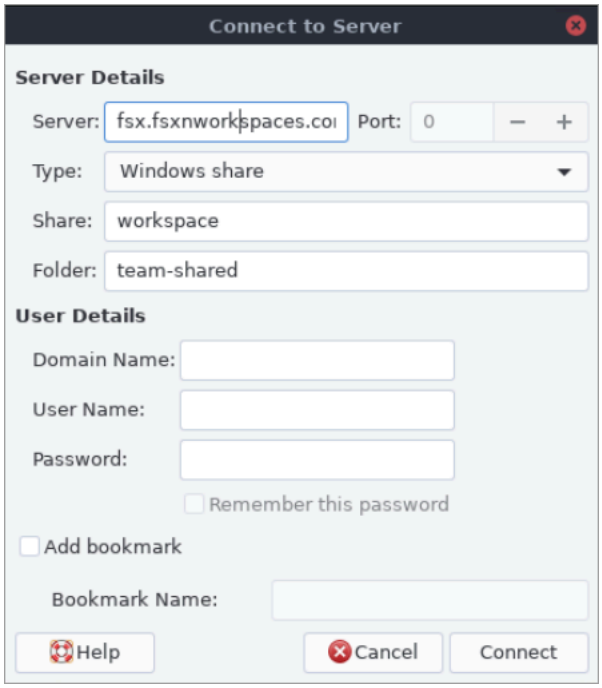
b. 将类型设置为 `Windows share`。

c. 将共享设置为 SMB 共享的名称，例如 `workspace`。

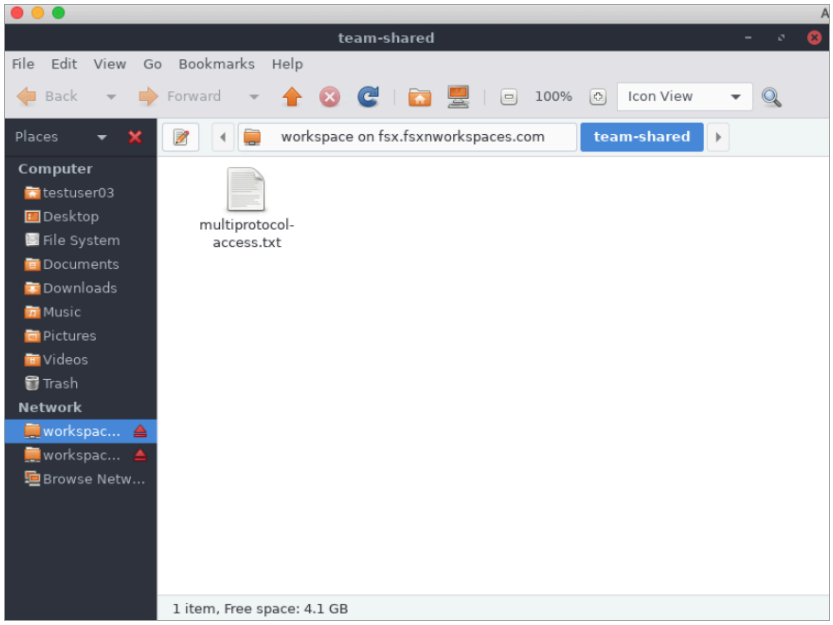
d. 您可以将文件夹保留为 `/` 或将其设置为文件夹，例如名为 `team-shared` 的文件夹。

e. 对于 Linux WorkSpace，如果您的 Linux WorkSpace 与 Amazon FSx 共享位于同一个域中，则无需输入用户详细信息。

f. 选择连接。



2. 建立连接后，您可以在名为 `workspace` 的 SMB 共享中看到共享文件夹（在本示例中名为 `team-shared`）。



将亚马逊弹性容器服务与 ONTAP FSx 配合使用

你可以从亚马逊 EC2 Linux 或 Windows 实例上的亚马逊弹性容器服务 (Amazon ECS) Service Docker 容器访问适用于 NetApp ONTAP 文件系统的亚马逊 FSx。

在 Amazon ECS Linux 容器上挂载

1. 使用 EC2 Linux + 网络集群模板为您的 Linux 容器创建 ECS 集群。有关更多信息，请参阅《Amazon Elastic Container Service 开发人员指南》中的创建集群。
2. 在 EC2 实例上创建用于挂载 SVM 卷的目录，如下所示：

```
sudo mkdir /fsxontap
```

3. 在实例启动期间使用用户数据脚本或运行以下命令，在 Linux EC2 实例上挂载 FSx for ONTAP 卷：

```
sudo mount -t nfs svm-ip-address:/vol1 /fsxontap
```

4. 使用以下命令挂载卷。

```
sudo mount -t nfs -o nfsvers=NFS_version svm-dns-name:/volume-junction-path /
fsxontap
```

以下示例使用示例值。

```
sudo mount -t nfs -o nfsvers=4.1
 svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-east-1.amazonaws.com:/vol1 /
fsxontap
```

您也可以使用 SVM 的 IP 地址来代替其 DNS 名称。

```
sudo mount -t nfs -o nfsvers=4.1 198.51.100.1:/vol1 /fsxontap
```

5. 创建 Amazon ECS 任务定义时，请在 JSON 容器定义中添加以下 `volumes` 和 `mountPoints` 容器属性。将`sourcePath`替换为 for ONTAP 文件系统中的 FSx 挂载点和目录。

```
{
    "volumes": [
        {
            "name": "ontap-volume",
            "host": {
                "sourcePath": "mountpoint"
            }
        }
    ],
    "mountPoints": [
        {
            "containerPath": "containermountpoint",
            "sourceVolume": "ontap-volume"
        }
    ],
    .
    .
    .
}
```

在 Amazon ECS Windows 容器上挂载

1. 使用 EC2 Windows + 网络集群模板为您的 Windows 容器创建 ECS 集群。有关更多信息，请参阅《Amazon Elastic Container Service 开发人员指南》中的创建集群。
2. 将加入域的 Windows EC2 实例添加到 ECS Windows 集群并映射 SMB 共享。

   启动已加入您的 Active Directory 域的 ECS 优化的 Windows EC2 实例，然后通过运行以下命令初始化 ECS 代理。

```
PS C:\Users\user> Initialize-ECSAgent -Cluster windows-fsx-cluster -
EnableTaskIAMRole
```

您也可以将脚本中的信息传递到用户数据文本字段，如下所示。

```
<powershell>
Initialize-ECSAgent -Cluster windows-fsx-cluster -EnableTaskIAMRole
</powershell>
```

3. 在 EC2 实例上创建 SMB 全局映射，以便您可以将 SMB 共享映射到驱动器。将 netbios 或 DNS 名称下方的值替换为 FSx 文件系统和共享名称。挂载在 Linux EC2 实例上的 NFS 卷 vol1 在文件系统上配置为 CIFS 共享 fsxontap。 FSx

```
vserver cifs share show -vserver svm08 -share-name fsxontap


                                Vserver: svm08
                                  Share: fsxontap
                CIFS Server NetBIOS Name: FSXONTAPDEMO
                                  Path: /vol1
                        Share Properties: oplocks
                                          browsable
                                          changenotify
                                          show-previous-versions
                     Symlink Properties: symlinks
                File Mode Creation Mask: -
              Directory Mode Creation Mask: -
                               Share Comment: -
                                   Share ACL: Everyone / Full Control
            File Attribute Cache Lifetime: -
                                 Volume Name: vol1
                               Offline Files: manual
            Vscan File-Operations Profile: standard
         Maximum Tree Connections on Share: 4294967295
               UNIX Group for File Create: -
```

4. 使用以下命令在 EC2 实例上创建 SMB 全局映射：

```
New-SmbGlobalMapping -RemotePath \\fsxontapdemo.fsxontap.com\fsxontap -LocalPath Z:
```

5. 创建 Amazon ECS 任务定义时，请在 JSON 容器定义中添加以下 `volumes` 和 `mountPoints` 容器属性。将`sourcePath`替换为 for ONTAP 文件系统中的 FSx 挂载点和目录。

```
{
    "volumes": [
        {
            "name": "ontap-volume",
            "host": {
                "sourcePath": "mountpoint"
            }
        }
    ],
    "mountPoints": [
        {
            "containerPath": "containermountpoint",
            "sourceVolume": "ontap-volume"
        }
    ],
    .
    .
    .
}
```

将亚马逊弹性 VMware 服务与 ONTAP FSx 配合使用

您可以将 ONTAP 用作亚马逊弹性 VMware 服务 (Amazon EVS) 软件定义数据中心 () 的外部数据存储。 FSx SDDCs有关更多信息，请参阅使用 Amazon FSx for NetApp ONTAP 运行高性能工作负载。有关详细说明，请参阅将适用 FSx 于 NetApp ONTAP 的亚马逊配置为 NFS 数据存储和将适用 FSx 于 ONTA P 的亚马逊配置 NetApp 为 iSCSI 数据存储。

将 VMware 云与 ONTAP 搭 FSx 配使用

您可以将 ONTAP 用作 AWS 软件定义数据中心上 VMware 云的外部数据存储库（ ）。 FSx SDDCs有关更多信息，请参阅《使用亚马逊 NetApp ONTAP 版部署指南》将 FSx 适用于 ONTAP AWS 的亚马逊配置 FSx 为外部存储和 NetApp 开启VMware 云。

可用性、持久性和部署选项

适用于 NetApp ONTAP 的 Amazon FSx 采用单可用区和多可用区部署类型。可以从以下四个选项中选择：单可用区 1、单可用区 2、多可用区 1 和多可用区 2。本主题介绍每种部署类型的可用性与持久性功能，帮助您选择适合您的工作负载的部署类型。有关该服务的可用性 SLA（服务等级协议）的信息，请参阅 Amazon FSx 服务等级协议。

主题

选择文件系统部署类型

以下各节介绍了单可用区和多可用区文件系统部署类型的可用性与持久性功能。

单可用区部署类型

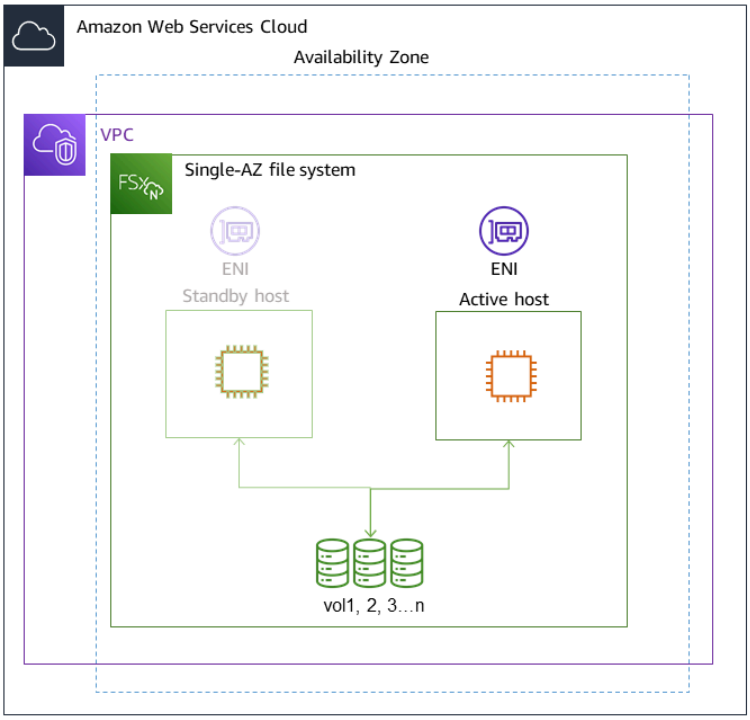
单可用区文件系统可以选择单可用区 1 和单可用区 2。单可用区 1 是具有一个高可用性（HA）对的第一代文件系统，而单可用区 2 是具有 1-12 个 HA 对的第二代文件系统。有关更多信息，请参阅 选择文件系统世代。

创建单可用区文件系统时，Amazon FSx 会自动在主动/备用配置中预置 1 到 12 对文件服务器，并且每对服务器中的主动和备用文件服务器位于 AWS 区域 中单个可用区内的不同故障域中。在计划内的文件系统维护或任何活动文件服务器的计划外服务中断期间，Amazon FSx 通常会在几秒钟内自动、独立地失效转移到备用文件服务器。在失效转移期间，无需手动干预即可继续访问数据。

为了确保高可用性，Amazon FSx 会持续监控硬件故障，并在发生故障时自动更换基础设施组件。为了实现高持久性，Amazon FSx 会自动在可用区内复制您的数据，以保护其免受组件故障的影响。此外，您还可以选择配置文件系统数据的“每日自动备份”。这些备份存储在多个可用区中，为所有备份数据提供多可用区弹性。

单可用区文件系统专为不需要多可用区文件系统的数据弹性模型的用例而设计。它们为开发和测试环境等用例提供了成本优化的解决方案，或者仅通过在单个可用区内复制数据来存储已存储在本地或其他 AWS 区域 中数据的辅助副本。

下图阐明了 FSx for ONTAP 单可用区第一代文件系统的架构。

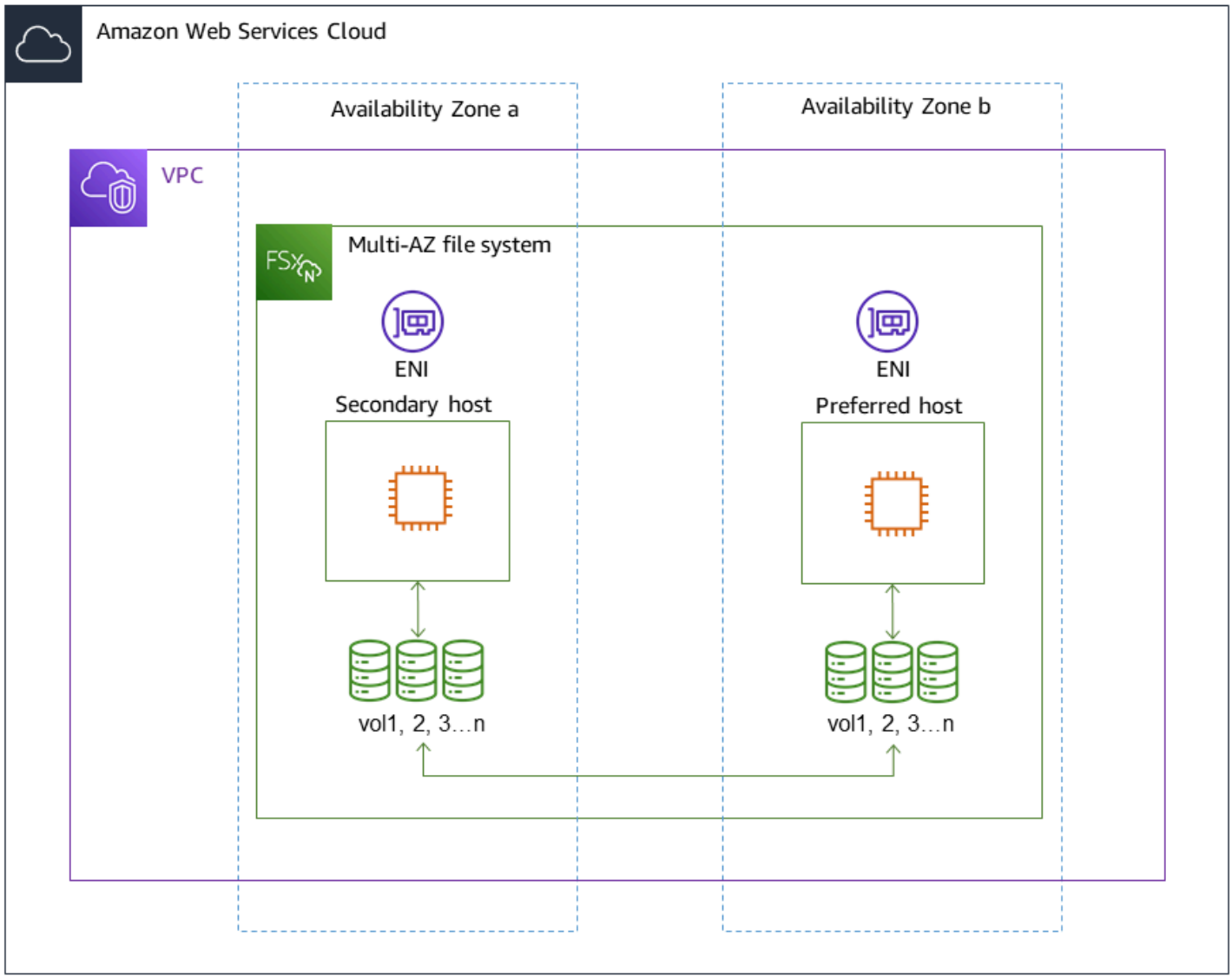


多可用区部署部署类型

多可用区文件系统可以选择多可用区 1 和多可用区 2。多可用区 1 是第一代文件系统，多可用区 2 是第二代文件系统。这两个选项都有一个 HA 对。有关更多信息，请参阅 选择文件系统世代。

多可用区文件系统支持单可用区文件系统的所有可用性与持久性功能。此外，及时可用区不可用，它们都能为数据提供持续可用性。多可用区部署采用单个 HA 对的文件服务器，同一 AWS 区域 的备用文件服务器与活动文件服务器部署在不同的可用区中。写入文件系统的任何更改都会跨可用区同步复制到备用区。

多可用区文件系统专为业务关键型生产工作负载而设计，这些工作负载要求共享 ONTAP 文件数据具有高可用性，并且需要具有跨可用区域内置复制功能的存储。下图阐明了 FSx for ONTAP 多可用区第一代文件系统的架构。



选择文件系统世代

下表说明了第一代和第二代单可用区与多可用区 FSx for ONTAP 文件系统之间的差异。

FSx for ONTAP 文件系统世代

维度	第一代	第二代（单个 HA 对）	第二代（多对）
Deployment type（部署类型）	SINGLE_AZ_1 MULTI_AZ_1	SINGLE_AZ_2 MULTI_AZ_2	SINGLE_AZ_2

维度	第一代	第二代（单个 HA 对）	第二代（多对）
HA 对	1 个 HA 对		1-12 个 HA 对
SSD 和存储	最小值：1 TiB 最大值：192 TiB	最小值：1 TiB 最大值：512 TiB	最小值：1 TiB（每个 HA 对） 最大值：1 PiB（总计）
SSD IOPS	最小值：3 IOPS/GIB SSD 最大值：160000	最小值：3 IOPS/GIB SSD 最大值：200000	最小值：3 IOPS/GIB SSD 最大值：2,400,000（每个 HA 对为 200,000）
吞吐能力	128 MBps；256 MBps；512 MBps；1,024 MBps；2,048 MBps；4,096 MBps	384 MBps；768 MBps；1,536 MBps；3,072 MBps；6,144 MBps	1,536 MBps（每个 HA 对）；3,072 MBps（每个 HA 对）；6,144 MBps（每个 HA 对）

> **Note**
>
> 创建文件系统之后无法更改其部署类型。如果要更改部署类型（例如，从单可用区 1 迁移至单可用区 2），可以备份数据并将其还原到新的文件系统上。您还可以使用 NetApp SnapMirror、AWS DataSync 或第三方数据复制工具来迁移数据。有关更多信息，请参阅 使用 FSx 迁移到 ONTAP NetApp SnapMirror 和 使用 FSx 迁移到 ONTAP AWS DataSync。

FSx for ONTAP 失效转移过程

出现以下情况时，单可用区和多可用区文件系统会自动通过给定的 HA 对从首选文件服务器或活动文件服务器失效转移到备用文件服务器：

- 首选文件服务器或活动文件服务器不可用
- 文件系统的吞吐能力被更改

- 首选文件服务器或活动文件服务器进行计划内维护
- 可用区发生中断（仅限多可用区文件系统）

> **Note**
>
> 对于具有多个 HA 对的第二代文件系统，每个 HA 对的失效转移行为都是独立的。如果一个 HA 对的首选文件服务器不可用，则只有该 HA 对会失效转移到其备用文件服务器。

从一台文件服务器失效转移到另一台文件服务器时，新的活动文件服务器会自动开始处理针对该 HA 对的所有文件系统读取和写入请求。对于多可用区文件系统，当首选文件服务器完全恢复且可供使用时，Amazon FSx 会失效自动恢复到该服务器（失效恢复通常会在 60 秒内完成）。对于单可用区和多可用区文件系统，从在活动文件服务器上检测到故障到将备用文件服务器提升为活动状态，失效转移通常会在 60 秒内完成。由于客户端用于在 NFS 或 SMB 上访问数据的端点 IP 地址保持不变，因此失效转移对 Linux、Windows 和 macOS 应用程序是透明的，这些应用程序无需人工干预即可重新开始文件系统的操作。

要确保失效转移对连接到 FSx for ONTAP 单可用区和多可用区文件系统的客户端透明，请参阅从内部访问数据 AWS Cloud。

在文件系统上测试失效转移

您可以通过修改文件系统的吞吐能力来测试其失效转移。当修改文件系统的吞吐能力时，Amazon FSx 会依次关闭文件系统的文件服务器。当 Amazon FSx 首先替换首选文件服务器时，文件系统会自动失效转移到辅助服务器。更新后，文件系统会失效自动恢复到新的主服务器，Amazon FSx 将替换辅助文件服务器。

您可以在 Amazon FSx 控制台、CLI 和 API 中监控吞吐能力更新请求的进度。有关修改文件系统的吞吐能力和监控请求进度的更多信息，请参阅 管理吞吐能力。

网络资源

本节介绍单可用区和多可用区文件系统所消耗的网络资源。

子网

创建单可用区文件系统时，您需要为该文件系统指定单个子网。您选择的子网将定义您创建的文件系统中的可用区。创建多可用区文件系统时需要指定两个子网，分别用于首选文件服务器和备用文件服务

器。您选择的两个子网必须位于同一 AWS 区域 的不同可用区中。有关 Amazon VPC 的更多信息，请参阅《Amazon Virtual Private Cloud 用户指南》中的Amazon VPC 是什么？。

> **Note**
>
> 无论您指定的是哪个子网，您都可以通过文件系统 VPC 内的任意子网访问文件系统。

文件系统弹性网络接口

对于单可用区文件系统，Amazon FSx 会在您关联到文件系统的子网中配置两个弹性网络接口（ENI）。对于多可用区文件系统，Amazon FSx 会在您关联到文件系统的两个子网中各配置一个弹性网络接口（ENI）。客户端会使用弹性网络接口与 Amazon FSx 文件系统进行通信。这些网络接口被视为在 Amazon FSx 的服务范围内，尽管是您的账户的 VPC 的一部分。多可用区文件系统使用浮动互联网协议（IP）地址，因此在失效转移事件期间，连接的客户端可以在首选文件服务器和备用文件服务器之间无缝切换。

> **Warning**
>
> - 您不得修改或删除与您的文件系统关联的弹性网络接口。修改或删除该网络接口可能会导致永久丢失您的 VPC 和文件系统之间的连接。
> - 与您的文件系统关联的弹性网络接口将自动创建路由，并将其添加到默认 VPC 和子网路由表中。修改或删除这些路由可能会导致文件系统客户端暂时或永久丢失连接。

下表汇总了 FSx for ONTAP 文件系统的各种部署类型的子网、弹性网络接口和 IP 地址资源：

	第一代单可用区	第二代单可用区	多可用区
子网的数量	1	1	2
弹性网络接口的数量	2	每个 HA 对为 2 个	2
各 ENI 的 IP 地址的数量	1 + 文件系统中 SVM 的数量	HA 对计数 + HA 对计数乘以文件系统中的 SVM 数量	1 + 文件系统中 SVM 的数量

	第一代单可用区	第二代单可用区	多可用区
VPC 路由表 路由的数量	不适用	不适用	1 + 文件系统 中 SVM 的数量

创建文件系统或 SVM 后，在删除文件系统之前，其 IP 地址不会更改。

> **Important**
>
> Amazon FSx 不支持从公共互联网访问文件系统，也不支持将文件系统暴露给公共互联网。Amazon FSx 会自动分离任何连接到文件系统的弹性网络接口的弹性 IP 地址，该地址是可从互联网访问的公有 IP 地址。

适用于 ONTAP 性能的 Amazon FS NetApp x

以下是针对 NetApp ONTAP 文件系统性能的 Amazon FSx 的概述，并讨论了可用的性能和吞吐量选项以及有用的性能提示。

主题

如何衡量 FSx for ONTAP 文件系统的性能

文件系统性能由其延迟、吞吐量和每秒 I/O 操作数 (IOPS) 来衡量。

延迟

适用于 NetApp ONTAP 的 Amazon FSx 通过固态硬盘 (SSD) 存储提供亚毫秒的文件操作延迟，为容量池存储提供数十毫秒的延迟。此外，Amazon FSx 在每台文件服务器 [NVMe（非易失性存储规范）驱动器和内存] 上均配备两层读取缓存，以便在您访问最常读取的数据时提供更低的延迟。

吞吐量和 IOPS

每个 Amazon FSx 文件系统可提供多达数十 GBps 的吞吐量和数百万的 IOPS。您的工作负载可以在文件系统上驱动的具体吞吐量和 IOPS 数取决于文件系统的总吞吐能力和存储容量配置，以及工作负载的性质，包括活动工作集的大小。

SMB 多渠道和 NFS nconnect 支持

您可以使用 Amazon FSx 将 SMB 多渠道配置为在单个 SMB 会话中提供 ONTAP 和客户端之间的多个连接。SMB 多通道会在客户端和服务器之间同时使用多个网络连接，以此来聚合网络带宽，从而最大化利用率。有关使用 NetApp ONTAP CLI 配置 SMB 多渠道的信息，请参阅 Configuring SMB Multichannel for performance and redundancy。

NFS 客户端可以使用 nconnect 挂载选项将多个 TCP 连接（最多 16 个）关联到单个 NFS 挂载。此类 NFS 客户端以轮询方式将文件操作多路复用到多个 TCP 连接上，从而从可用的网络带宽中获得更高的吞吐量。NFSv3 和 NFSv4.1 + 支持。nconnect Amazon EC2 实例网络带宽中说明了全双工 5 Gbps 的每个网络流带宽限制。您可以通过将多个网络流与 nconnect 或 SMB 多渠道一起使用来克服此限制。请参阅 NFS 客户端文档，确认您的客户端版本是否支持 nconnect。有关NetApp ONTAP支持的更多信息nconnect，请参阅ONTAP支持 NFSv4.1。

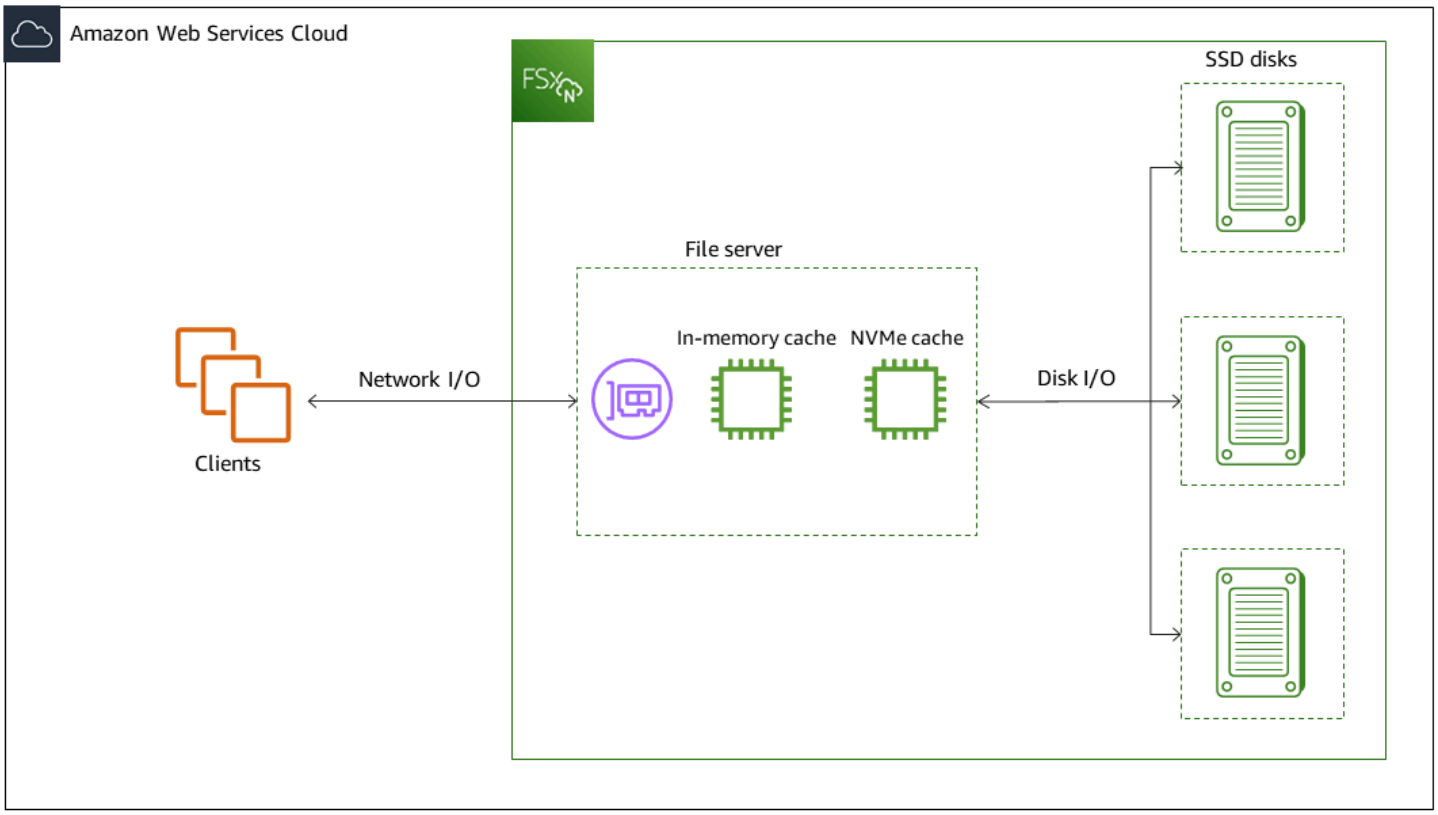
巨型帧

为实现最大的读取或写入吞吐量，我们建议在 Amazon FSx 文件系统的数据路径中所有网络接口上启用巨型帧，包括客户端 EC2 实例。FSx for ONTAP 文件系统上网络接口的默认最大传输单元（MTU）设置为 9001 字节。

性能详情

要详细了解适用于 NetApp ONTAP 的 Amazon FSx 性能模型，您可以检查亚马逊 FSx 文件系统的架构组件。您的客户端计算实例，无论它们存在于本地 AWS 还是本地，都可通过一个或多个弹性网络接口 (ENI) 访问您的文件系统。这些网络接口位于与文件系统关联的 Amazon VPC 中。每个文件系统 ENI 背后都有一个 NetApp ONTAP 文件服务器，这些服务器会通过网络向访问文件系统的客户端提供数据。Amazon FSx 会在每台文件服务器上提供快速的内存缓存和 NVMe 缓存，以增强最常访问数据的性能。每个文件服务器上都附有托管您的文件系统数据的 SSD 磁盘。

这些组件如下图所示。



与这些架构组件（网络接口、内存缓存、NVMe 缓存和存储卷）相对应的是决定整体吞吐量和 IOPS 性能的 Amazon FSX for NetApp ONTAP 文件系统的主要性能特征。

- 网络 I/O 性能： throughput/IOPS 客户机与文件服务器之间请求的性能（总计）
- In-memory 以及文件服务器上的 NVMe 缓存大小：可用于缓存的活动工作集的大小
- 磁盘 I/O 性能： throughput/IOPS 文件服务器和存储磁盘之间的请求

决定文件系统的这些性能特征的因素有两个：SSD IOPS 总数和您为其配置的吞吐能力。前两个性能特征（网络 I/O 性能以及内存和 NVMe 缓存大小）完全由吞吐容量决定，而第三个特征（磁盘 I/O性能）则由吞吐容量和 SSD IOPS 的组合决定。

File-based 工作负载通常很高，其特点是短而密集的高峰期，两次爆发之间 I/O 有充足的空闲时间。为了支持高峰工作负载，除了文件系统可以维持的基准速度外 24/7，Amazon FSx 还提供了在一段时间内突增至更高速度的 I/O 网络和 I/O 磁盘操作的功能。Amazon FSx 使用网络 I/O 积分机制根据平均利用率分配吞吐量和 IOPS — 当文件系统的吞吐量和 IOPS 使用量低于其基准限制时，文件系统会累积积分，并且可以在执行操作时使用这些积分。 I/O

> **Note**
>
> 对于 iSCSI 和 S NVMe/TCP AN 协议，顺序读取客户机操作可以实现文件系统的最大网络 I/O 突发或基准吞吐量。

写入操作使用的网络带宽是读取操作的两倍。写入操作必须在辅助文件服务器上进行复制，因此一次写入操作会产生的两倍的网络吞吐量。

部署类型对性能的影响

您可以使用适用于 ONTAP 的 FSx 创建 Single-AZ 和 Multi-AZ 文件系统。 First-generation 文件系统（包括和 Multi-AZ ）Single-AZ 和第二代 Multi-AZ 文件系统均由一对高可用性 (HA) 提供支持。Second-generation Single-AZ 文件系统由多达 12 个 HA 对提供支持。有关更多信息，请参阅 管理高可用性（HA）对。

适用于 ONTAP Multi-AZ 和 Single-AZ 文件系统的 FSx 为 SSD 存储提供一致的亚毫秒级文件操作延迟，在容量池存储中提供数十毫秒的延迟。此外，满足以下要求的文件系统会提供 NVMe 读取缓存，以减少读取延迟并提高经常读取的数据的 IOPS：

- Multi-AZ 1 和 Multi-AZ 2 文件系统
- Single-AZ 1 个在 2022 年 11 月 28 日之后创建的、吞吐容量至少为 2 Gbps 的文件系统
- Single-AZ 2 个文件系统，每对的吞吐容量至少为 6 Gbps

> **Note**
>
> 对于第二代文件系统（Single-AZ 2 和 Multi-AZ 2），使用 NVMe 缓存可能会导致您的工作负载减少高吞吐量或大型工作负载的总吞吐量。 I/O如果您的工作负载受吞吐量限制，我们建议禁用 NVMe 缓存。有关更多信息，请参阅 管理 NVMe 缓存。

下表显示了文件系统可以扩展到的吞吐容量，具体取决于高可用性 (HA) 对的数量和 AWS 区域 可用性等因素。

First-generation file systems

这些性能规格适用于第一代 Single-AZ 和 Multi-AZ 文件系统。

第一代文件系统的每个 HA 对的 SSD 存储最大吞吐量

	美国东部（俄亥俄州）区域、美国东部（弗吉尼亚州北部）区域、美国西部（俄勒冈州）区域，以及欧洲地区（爱尔兰）		所有其他提供适用于 ONTAP 的 FSx AWS 区域 的地方	
	读取吞吐量（MBps）	写入吞吐量（MBps）	读取吞吐量（MBps）	写入吞吐量（MBps）
Single-AZ	4,096 [1]	1000	2,048	750
Multi-AZ	4,096 [1]	1800	2,048	1,300

> **Note**
>
> [1] 若要预置 4GBps 的吞吐能力，文件系统必须配置最低 5120 GiB 的 SSD 存储和 160000 的 SSD IOPS。

Second-generation file systems

这些性能规格适用于第二代 Single-AZ 和 Multi-AZ 文件系统。通常，第二代文件系统可提供全部的预置吞吐能力用于读取，以及高达三分之一的预置吞吐能力用于写入。唯一的例外是 6,144 MB/s 选项，此表中列出了该选项。

第二代文件系统的每个 HA 对的 SSD 存储最大吞吐量

	读取吞吐量（MBps）	写入吞吐量（MBps）
Single-AZ	6,144 [1]	1,024 [1]
Multi-AZ	6,144	2,048

> **Note**
>
> [1] 每个 HA 对（最多 12 个对）。有关更多信息，请参阅 管理高可用性（HA）对。

存储容量对性能的影响

您的文件系统可以达到的最大磁盘吞吐量和 IOPS 级别是以下两者中较低的一方：

- 文件服务器提供的磁盘性能级别，基于您为文件系统选择的吞吐能力
- 由您为文件系统预置的 SSD IOPS 数提供的磁盘性能级别

默认情况下，文件系统的 SSD 存储提供可达以下级别的磁盘吞吐量和 IOPS：

- 磁盘吞吐量 [每 TiB 存储速率（MBps）]：768
- 磁盘 IOPS（每 TiB 存储的 IOPS 数）：3072

> **Note**
>
> 减少第二代文件系统上的 SSD 存储容量时，对大多数工作负载性能的影响微乎其微。但是，写入密集型工作负载可能会出现暂时的性能下降。当客户端访问被重定向到新磁盘时，您可能还会遇到短 I/O 暂的暂停（最多 60 秒）。
> 为最大限度降低对性能的影响，在执行 SSD 缩减操作之前，确保持续性工作负载不得长期占用超过 50% 的 CPU、50% 的磁盘吞吐量或 50% 的 SSD IOPS。有关减少 SSD 存储容量的更多信息，请参阅 何时减少 SSD 存储容量。

吞吐能力对性能的影响

每个 Amazon FSx 文件系统都有一个您在创建文件系统时为其配置吞吐能力。文件系统的吞吐容量决定了网络 I/O 性能水平，或者是托管文件系统的每台文件服务器通过网络向访问文件的客户端提供文件数据的速度。更高的吞吐量级别来自更多的内存和用于在每个文件服务器上缓存数据的非易失性存储器快速 (NVMe) 存储，以及每个文件服务器支持的更高级别的磁盘 I/O 性能。

在创建文件系统时，您可以选择配置更高级别的 SSD IOPS。即使在预配置了更多 SSD IOPS 时，您的文件系统可以达到的最大 SSD IOPS 水平也取决于文件系统的吞吐能力。

下表所示为吞吐能力的整套规范，以及基准和突增级别，以及相应 AWS 区域中的文件服务器上用于缓存的内存量。

First-generation Single-AZ file system

这些性能规范适用于 2022 年 11 月 28 日之后在指定 AWS 区域版本中创建的第一代 Single-AZ 文件系统。

以下地区的文件系统的性能规格 AWS 区域：美国东部（弗吉尼亚北部）、美国东部（俄亥俄州）、美国西部（俄勒冈）和欧洲（爱尔兰）

FSx 吞吐能力（MBps）	网络吞吐能力（Mbps）		网络 IOPS	In-memory 缓存 (GB)	NVMe 读取缓存（GB）	磁盘吞吐量（MBps）		SSD 驱动器 IOPS *	
	基准	突增				基准	突增	基准	突增
128	188	1500	数万基准	16	–	128	1250	6000	40000
256	375	1500		32	–	256	1250	12000	40000
512	750	1500	数十万基准	64	–	512	1250	20000	40000
1024	1500	–		128	–	1024	1250	40000	–
2,048	3,125	–		256	1,900	2,048	–	80,000	–
4,096	6,250	–		512	5,400	4,096	–	160000	–

> **Note**
>
> * 仅当您访问文件服务器的内存缓存或 NVMe 缓存中未缓存的数据时，才会使用 SSD IOPS。

这些性能规格适用于所有其他提供 FSx for ON AWS 区域 TAP 的第一代 Single-AZ 文件系统。

所有其他提供 FSx for ON AWS 区域 TA P 的文件系统的性能规格

FSx 吞吐能力（Mbps）	网络吞吐能力（Mbps）		网络 IOPS	In-memory 缓存 (GB)	磁盘吞吐量（MBps）		SSD 驱动器 IOPS *	
	基准	突增			基准	突增	基准	突增
128	150	1250	数万基准	16	128	600	6000	18,750
256	300	1250		32	256	600	12000	18,750
512	625	1250	数十万基准	64	512	–	18,750	–
1024	1500	–		128	1024	–	40000	–
2,048	3,125	–		256	2,048	–	80,000	–

> **Note**
>
> * 仅当您访问文件服务器的内存缓存或 NVMe 缓存中未缓存的数据时，才会使用 SSD IOPS。

Second-generation Single-AZ file system

这些性能规范适用于第二代 Single-AZ 文件系统。

第二代 Single-AZ 文件系统的性能规格

FSx 吞吐能力（Mbps）	网络吞吐能力（Mbps）		网络 IOPS	In-memory 缓存 (GB)	NVMe 缓存（GB）	磁盘吞吐量（MBps）		SSD 驱动器 IOPS *	
	基准	突增				基准	突增	基准	突增
384**	781	6,250	数十万基准	16	–	384	3,125	12,500	65000

FSx 吞吐能力（Mbps）	网络吞吐能力（Mbps）		网络 IOPS	In-memory 缓存 (GB)	NVMe 缓存（GB）	磁盘吞吐量（MBps）		SSD 驱动器 IOPS *	
768**	1,563	6,250		32	–	768	3,125	25000	65000
1,536	3,125	6,250		64	–	1,536	3,125	50000	65000
3,072	6,250	–		128	–	3,072	–	100000	–
6,144	12,500	–		256	1,900	6,144	–	200,000	–

> **Note**
>
> * 仅当您访问文件服务器的内存缓存或 NVMe 缓存中未缓存的数据时，才会使用 SSD IOPS。
> ** Second-generation Single-AZ 文件系统支持 384 和 768 吞吐容量，但仅支持一个 HA 对。要添加 HA 对，您的文件系统至少须配置 1,536 MBps 的吞吐能力。

First-generation Multi-AZ file system

这些性能规范适用于 2022 年 11 月 28 日之后在指定 AWS 区域版本中创建的第一代 Multi-AZ 文件系统。

以下地区的文件系统的性能规格 AWS 区域：美国东部（弗吉尼亚北部）、美国东部（俄亥俄州）、美国西部（俄勒冈）和欧洲（爱尔兰）

FSx 吞吐能力（Mbps）	网络吞吐能力（Mbps）		网络 IOPS	In-memory 缓存 (GB)	NVMe 缓存（GB）	磁盘吞吐量（MBps）		SSD 驱动器 IOPS *	
	基准	突增				基准	突增	基准	突增
128	188	1500	数万基准	16	238	128	1250	6000	40000
256	375	1500		32	475	256	1250	12000	40000

FSx 吞吐能力（Mbps）	网络吞吐能力（Mbps）		网络 IOPS	In-memory 缓存 (GB)	NVMe 缓存（GB）	磁盘吞吐量（MBps）		SSD 驱动器 IOPS *	
512	750	1500	数十万基准	64	950	512	1250	20000	40000
1024	1500	–		128	1,900	1024	1250	40000	–
2,048	3,125	–		256	3,800	2,048	–	80,000	–
4,096	6,250	–		512	7,600	4,096	–	160000	–

> **Note**
>
> * 仅当您访问文件服务器的内存缓存或 NVMe 缓存中未缓存的数据时，才会使用 SSD IOPS。

这些性能规格适用于所有其他提供 FSx for ON AWS 区域 TAP 的第一代 Multi-AZ 文件系统。

所有其他提供 FSx for ON AWS 区域 TA P 的文件系统的性能规格

FSx 吞吐能力（Mbps）	网络吞吐能力（Mbps）		网络 IOPS	In-memory 缓存 (GB)	NVMe 缓存（GB）	磁盘吞吐量（MBps）		SSD 驱动器 IOPS *	
	基准	突增				基准	突增	基准	突增
128	150	1250	数万基准	16	150	128	600	6000	18,750
256	300	1250		32	300	256	600	12000	18,750
512	625	1250	数十万基准	64	600	512	–	18,750	–
1024	1500	–		128	1,200	1024	–	40000	–
2,048	3,125	–		256	2400	2,048	–	80,000	–

> **Note**
>
> * 仅当您访问文件服务器的内存缓存或 NVMe 缓存中未缓存的数据时，才会使用 SSD IOPS。

Second-generation Multi-AZ file systems

这些性能规范适用于第二代 Multi-AZ 文件系统。

第二代 Multi-AZ 文件系统的性能规格

FSx 吞吐能力（Mbps）	网络吞吐能力（Mbps）		网络 IOPS	In-memory 缓存 (GB)	NVMe 缓存（GB）	磁盘吞吐量（MBps）		SSD 驱动器 IOPS *	
	基准	突增				基准	突增	基准	突增
384	781	6,250	数十万基准	16	237	384	3,125	12,500	65000
768	1,563	6,250		32	474	768	3,125	25000	65000
1,536	3,125	6,250		64	950	1,536	3,125	50000	65000
3,072	6,250	–		128	1,900	3,072	–	100000	–
6,144	12,500	–		256	3,800	6,144	–	200,000	–

> **Note**
>
> * 仅当您访问文件服务器的内存缓存或 NVMe 缓存中未缓存的数据时，才会使用 SSD IOPS。

示例：存储容量和吞吐能力

以下示例说明了存储容量和吞吐能力对文件系统性能的影响。

配置有 2 TiB SSD 存储容量和 512 MBps 吞吐能力的第一代文件系统具有以下吞吐量级别：

- 网络吞吐量 – 基准为 625Mbps 和 1250Mbps 的突增（参阅吞吐能力表）
- 磁盘吞吐量 – 基准为 512Mbps 和 600Mbps 的突增。

因此，访问文件系统的工作负载将能够提供高达 625Mbps 的基准吞吐量和 1,250Mbps 的突增吞吐量，用于对缓存在文件服务器内存缓存和 NVMe 缓存中主动访问的数据执行文件操作。

管理 FSx for ONTAP 资源

使用 AWS 管理控制台、、 AWS CLI、ONTAP CLI 和 API，您可以对 FSx for ONTAP 资源执行以下管理操作：

- 创建、列出、更新和删除文件系统、存储虚拟机（SVM）、卷、备份和标签。
- 管理现有文件系统挂载目标的访问权限、管理账户和密码、密码要求、SMB 和 iSCSI 协议、网络可访问性

主题

管理存储容量

Amazon FSx for NetApp ONTAP 提供了许多与存储相关的功能，您可以使用这些功能来管理文件系统的存储容量。

主题

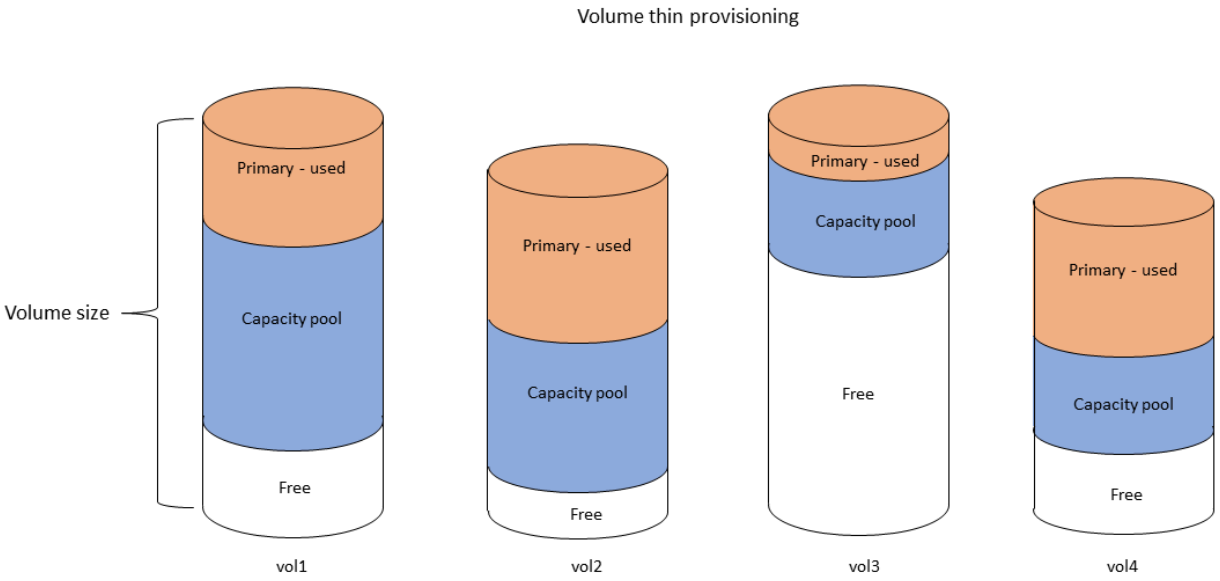
FSx 适用于 ONTAP 存储层

存储层是 Amazon FSx for NetApp ONTAP 文件系统的物理存储介质。 FSx 适用于 ONTAP 提供以下存储层：

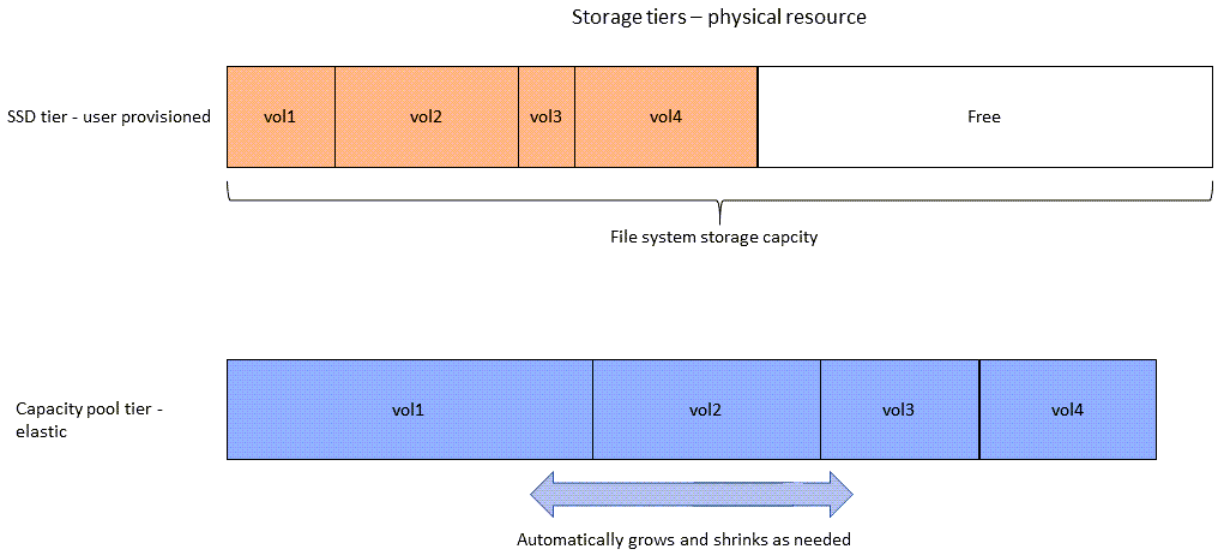
- SSD 层 – 用户预置的高性能固态硬盘（SSD）存储，专为数据集的活跃部分而构建。
- 容量池层 – 完全弹性的存储，可以自动扩展到 PB 级大小，并且针对不经常访问的数据进行成本优化。

FSx 适用于 ONTAP 的卷是一种虚拟资源，与文件夹类似，它不消耗存储容量。您存储的（以及消耗物理存储空间的）数据位于卷内。创建卷时，需要指定其大小，可以在创建卷后对其进行修改。 FSx 对于 ONTAP，卷是精简配置的，并且不会提前预留文件系统存储空间。相反，SSD 和容量池存储空间根据需要动态分配。您在卷级别配置的分层策略决定 SSD 层中存储的数据是否以及何时过渡到容量池层。

下图说明了文件系统中跨多个 FSx ONTAP 卷排列的数据示例。



下图说明了上图四个卷中的数据如何消耗文件系统的物理存储容量。



您可以选择更符合文件系统中每个卷的要求的分层策略，从而降低存储成本。有关更多信息，请参阅卷数据分层。

选择合适容量的文件系统 SSD 存储

在为 onTAP 文件系统选择 SSD 存储容量时，您需要记住以下几点会影响可用于存储数据的 SSD 存储量： FSx

- 为 NetApp ONTAP 软件开销预留的存储容量。
- 文件元数据
- 最近写入的数据
- 您打算在 SSD 存储空间上存储的文件，无论是尚未达到冷却周期的数据，还是您最近读取的数据，都会被检索回 SSD。

SSD 存储的使用方式

文件系统的 SSD 存储用于组合使用 NetApp ONTAP 软件（开销）、文件元数据和数据。

NetApp ONTAP 软件开销

与其他 NetApp ONTAP 文件系统一样，文件系统的 SSD 存储容量中多达 16% 是为 ONTAP 开销预留的，这意味着它不能用于存储您的文件。ONTAP 开销的分配方式如下：

- 11% 留给 NetApp ONTAP 软件。对于 SSD 存储容量超过 30 太字节（TiB）的文件系统，预留 6%。

- 5% 预留给聚合快照。在文件系统的文件服务器之间同步数据时需要聚合快照。

文件元数据

文件元数据通常占用文件消耗的存储容量的 3-7%。该百分比取决于平均文件大小（平均文件大小越小，需要的元数据越多），以及文件的存储效率节省量。请注意，文件元数据无法从存储效率节省中受益。您可以使用以下准则来估算文件系统上元数据使用的 SSD 存储量。

平均文件大小	元数据大小与文件数据百分比的对应关系
4 KB	7%
8 KB	3.5%
32 KB 或更大	1-3%

在调整计划在容量池层上存储的文件元数据所需的 SSD 存储容量时，我们建议采用保守比率，即容量池层上计划存储的每 10GiB 数据对应 1GiB 的 SSD 存储空间。

SSD 层上存储的文件数据

除活跃数据集和所有文件元数据外，写入文件系统的所有数据最初都会写入 SSD 层，然后再分层到容量池存储。无论卷的分层策略如何，都是如此，唯一的例外是，在配置了全部数据分层策略的卷 SnapMirror 上使用时，数据会直接写入容量池存储。

只要 SSD 层的利用率低于 90%，容量池层的随机读取内容就会在 SSD 层中缓存。有关更多信息，请参阅 卷数据分层。

建议的 SSD 容量利用率

我们建议 SSD 存储层的利用率不要一直超过 80%。对于第二代文件系统，我们还建议对文件系统任何聚合的持续利用率不超过 80%。这些建议与针对 ONTAP NetApp 的建议一致。由于文件系统的 SSD 层还用于暂存向容量池层的写入以及从容量池层进行的随机读取，因此，访问模式的任何突然变化都可能很快导致 SSD 层的利用率提高。

当 SSD 利用率为 90% 时，从容量池层读取的数据将不再缓存于 SSD 层，以便剩余的 SSD 容量预留给写入文件系统的新数据。这样会导致，从容量池层重复读取的相同数据会从容量池存储读取，而不是缓存在 SSD 层并从中读取，从而影响文件系统的吞吐能力。

当 SSD 层的利用率达到或高于 98% 时，所有分层功能都会停止。有关更多信息，请参阅 分层阈值。

存储效率

NetApp ONTAP 在卷级别提供块级存储效率功能，包括压缩、紧凑处理和重复数据删除。对于一般文件共享，这些功能最多可节省 65% 的存储容量而不牺牲性能。您可以按卷启用存储效率功能。这些功能可减少数据消耗的存储容量，从而减少 SSD、容量池和备份存储中消耗的存储空间。您可以在每个卷上为 SSD 存储数据启用压缩和重复数据删除功能。当数据分层到容量池存储时，压缩和重复数据删除功能在 SSD 存储中节省的存储空间仍将保留。无论文件系统的存储效率配置如何，备份数据始终启用存储效率功能。

下表列出了典型的存储节省情况。

	仅压缩	仅重复数据删除	压缩和重复数据删除
通用文件共享	50%	30%	65%
虚拟服务器和台式机	55%	70%	70%
数据库	65-70%	0%	65-70%
工程数据	55%	30%	75%
地震数据	40%	3%	40%

对于大多数工作负载，启用压缩和重复数据删除功能不会对文件系统的性能带来不利影响。对于大多数工作负载，压缩功能可提高整体性能。为了提供对 RAM 缓存的快速读取和写入， FSx ONTAP 文件服务器在前端网络接口卡 (NICs) 上配备的网络带宽要高于文件服务器和存储磁盘之间的可用带宽。由于数据压缩减少文件服务器和存储磁盘之间发送的数据量，因此对于大多数工作负载，在使用数据压缩后，文件系统的总体吞吐能力将会增大。一旦文件系统的前端 NIC 饱和后，数据压缩带来的相关吞吐能力的增加将会受到限制。

Amazon FSx for NetApp ONTAP 还支持其他可为您节省空间的ONTAP功能，包括快照、精简配置和 FlexClone 卷。

存储效率功能默认未启用。您可按如下方式将其启用：

- 当创建文件系统时，在 SVM 的根卷上。
- 当创建新卷时。

- 当修改现有卷时。

要查看启用存储效率后在文件系统中节省的存储量，请参阅 监控存储效率节省情况。

计算存储效率节省情况

您可以使用LogicalDataStored和 StorageUsed FSx for ONTAP CloudWatch 文件系统指标来计算压缩、重复数据删除、压缩、快照和所节省的存储空间。FlexClones这些指标使用单个维度 FileSystemId。有关更多信息，请参阅 文件系统指标。

- 要以字节为单位计算存储效率节省，请取给定时段内 StorageUsed 的平均值，然后从相同时段内 LogicalDataStored 的平均值中减去该值。
- 要计算存储效率带来的节省占逻辑数据总大小的百分比，请取某个给定时间段内的 StorageUsed 的 Average，然后从同一时间段的 LogicalDataStored 的 Average 中减去此值。然后使用差值除以同一时间段内的 LogicalDataStored 的 Average。

SSD 大小调整示例

假设您要为某个应用程序存储 100TiB 的数据。该应用程序中 80% 的数据不经常被访问。在这种情况下，80%（80TiB）的数据会自动分层到容量池层，剩余 20%（20TiB）仍保留在 SSD 存储中。根据通用文件共享工作负载的通常存储效率节省为 65%，这相当于 7TiB 的数据。要保持 80% 的 SSD 利用率，您需要使用 8.75TiB 的 SSD 存储容量来存储 20TiB 的活跃访问数据。您预置的 SSD 存储量还需要考虑 16% 的 ONTAP 软件存储开销，如以下计算所示。

```
ssdNeeded = ssdProvisioned * (1 - 0.16)
8.75 TiB / 0.84 = ssdProvisioned
10.42 TiB = ssdProvisioned
```

因此，在本示例中，您需要预置至少 10.42TiB 的 SSD 存储空间。您还将使用 28TiB 的容量池存储空间来存储剩余 80TiB 不经常访问的数据。

文件系统存储容量和 IOPS

创建 FSx 适用于 ONTAP 的文件系统时，需要指定 SSD 层的存储容量。对于第二代单可用区文件系统，您指定的存储容量均匀分布在每个高可用性（HA）对的存储池之间；这些存储池称为聚合。

对于您预配置的每 GiB 固态硬盘存储，Amazon FSx 会自动为文件系统预置每秒 3 次固态硬盘 input/output 操作 (IOPS)，每个文件系统最多可配置 160,000 个 SSD IOPS。对于第二代单可用区文件系

统，SSD IOPS 均匀分布在每个文件系统的聚合中。您可以选择将预调配 SSD IOPS 的级别指定为高于自动设定的 3 SSD IOPS/GiB。有关您可以为适用于 ONTAP 文件系统配置的最大 SSD IOPS 数量 FSx 的更多信息，请参阅。吞吐能力对性能的影响

主题

更新文件系统 SSD 存储和 IOPS

当您需要为数据集的活动部分提供更多存储空间时，可以增加 Amazon for NetApp ONTAP 文件系统 FSx 的 SSD 存储容量。对于第二代文件系统，您甚至可以减少 SSD 存储容量，以适应工作负载不断变化的存储需求。使用亚马逊 FSx 控制台、亚马逊 FSx API 或 AWS Command Line Interface (AWS CLI) 来增加或减少固态硬盘存储容量。有关更多信息，请参阅 更新 SSD 存储容量和预调配 IOPS。

何时增加 SSD 存储容量

如果可用的 SSD 层存储空间即将用完，我们建议您增加文件系统的存储容量。存储空间不足表示 SSD 层太小，无法容纳数据集的活跃部分。

要监控文件系统上的可用存储量，请使用文件系统级别的指标`StorageCapacity`和 `StorageUsed` Amazon CloudWatch 指标。您可以针对指标创建 CloudWatch 警报，并在指标降至特定阈值以下时收到通知。有关更多信息，请参阅 使用 Amazon 进行监控 CloudWatch。

> **Note**
>
> 我们建议您不要超过 80% 的 SSD 存储容量利用率，以确保数据分层、吞吐量扩展和其他维护活动正常运行，并确保有容量可用于存储更多数据。对于第二代文件系统，此建议既适用于所有文件系统聚合的平均利用率，也适用于每个单独聚合的利用率。

有关如何使用文件系统的 SSD 存储以及为文件元数据和操作软件预留多少 SSD 存储空间的更多信息，请参阅选择合适容量的文件系统 SSD 存储。

增加 SSD 存储容量

当您增加 Amazon FSx 文件系统的固态硬盘存储容量时，新容量通常在几分钟内即可使用。新的 SSD 存储容量可用后，您需要为其付费。有关更多信息，请参阅 Amazon f FSx or NetApp ONTAP 定价和。FSx for ONTAP 的 AWS 账单和使用情况报告

增加存储容量后，Amazon FSx 会在后台运行存储优化流程，以重新平衡您的数据。对于大多数文件系统，存储优化需要几个小时，而对工作负载性能几乎没有显著影响。

您可以随时使用 Amazon FSx 控制台和 API 跟踪存储优化过程的进度。 AWS CLI有关更多信息，请参阅 监控存储容量和 IOPS 更新。

增加 SSD 存储容量的注意事项

以下是增加文件系统 SSD 存储容量和 IOPS 时需要考虑的几个重要事项：

- （仅限第一代文件系统）仅增加存储容量：您只能增加文件系统的 SSD 存储容量；您不能减少该存储容量。
- 存储容量最低增量：每次 SSD 存储容量增量必须至少为文件系统当前 SSD 存储容量的 10%，最大为文件系统配置的最大 SSD 存储容量。
- 两次增加的间隔时间：增加文件系统上的 SSD 存储容量、预调配 IOPS 或吞吐能力后，您必须等待至少六个小时，才能再次修改同一个文件系统上的这些配置。这有时也称为冷却时间。
- 预调配 IOPS 模式：对于预调配 IOPS 的更改，您必须指定以下两种 IOPS 模式中的一种：
  - 自动模式 — Amazon FSx 会自动扩展您的固态硬盘 IOPS，以保持每 GiB 固态硬盘存储容量 3 个预配置的固态硬盘 IOPS，最高不超过您的文件系统配置的最大 SSD IOPS。

> **Note**
>
> 有关您可以为适用于 ONTAP 文件系统配置的最大 SSD IOPS 数量 FSx 的更多信息，请参阅。吞吐能力对性能的影响

- 用户预调配模式 – 您可以指定 SSD IOPS 的数量，该数量必须大于或等于 3 IOPS/GiB SSD 存储容量。如果您选择预调配更高的 IOPS 级别，您需要为高于当月所含费率的平均预调配 IOPS 付费，以 IOPS 月数为单位。

有关定价的更多信息，请参阅 Amazon f NetApp o FSx r ONTAP 定价。

何时减少 SSD 存储容量

在以下情况下，您可能需要减少 onTAP 第二代文件系统的 SSD 存储容量： FSx

- 完成不再需要高性能存储的基于项目的工作负载之后
- 完成大规模数据迁移后，该过程使用临时的额外容量来加速数据摄取

减少 SSD 存储容量

当您减少文件系统的 SSD 存储容量时，Amazon 会将一组较小的新磁盘（聚合） FSx 附加到文件系统的每个 HA 对中。 FSx 然后，Amazon 在后台运行存储优化流程，将每个卷的数据从旧磁盘移动到新磁盘。移动每个卷中的数据后，Amazon FSx 会将客户端访问重定向到新磁盘上的卷。 FSx 然后，Amazon 会将旧磁盘从您的文件系统中分离出来。

在整个 SSD 容量缩减操作期间，您需为 SSD 层级中现有容量及新请求的容量付费。例如，当您将 SSD 存储容量从 10 太字节（ TiB ）减少到 5TiB 时，在 SSD 缩减操作期间将按 15TiB 计费，在 SSD 缩减操作完成后则按 5TiB 计费。有关账单的更多信息，请参阅 FSx for ONTAP 的 AWS 账单和使用情况报告。

减少 SSD 存储容量所需的时间可能从数小时到数周不等，具体取决于以下因素：文件系统中存储的数据量、缩减操作期间文件系统接收的净新增写入量，以及文件系统可用的网络和磁盘资源量。

缩减操作期间，您的数据仍可用于读取和写入。大多数工作负载的性能影响微乎其微，但写入密集型工作负载可能会出现短暂的性能下降。当客户端访问被重定向到每个卷的新磁盘时，可能会出现短 I/O 暂的暂停（最长 60 秒）。

为最大限度降低对性能的影响，在执行 SSD 缩减操作之前，应确保文件系统保持足够的余量，具体要求为：持续性工作负载不得长期占用超过 50% 的 CPU、50% 的磁盘吞吐量或 50% 的 SSD IOPS。您可以在 Amazon FSx 控制台中文件系统的 “监控和性能” 选项卡中监控这些利用率指标。

> **Note**
>
> 如果您的 SSD 存储层在降低操作期间超过 80% 的利用率，Amazon 会 FSx 暂停该操作，并在利用率低于 80% 后自动恢复该操作。要降低新磁盘上的 SSD 使用率，您可以将数据分层迁移至容量池，也可以从已成功将客户端访问重定向至新磁盘组的卷中删除数据。

如果您在缩减操作期间需要额外的 SSD 容量，则可以通过调用`update-file-system` AWS CLI 或等效的 UpdateFileSystemAPI 操作并提供新的目标值来提交增加 SSD 容量的请求。Amazon FSx 会优先完成固态硬盘增加请求，以便在恢复固态硬盘缩减操作之前的几分钟内即可使用新的固态硬盘容量。

降低 SSD 存储容量时的注意事项

以下是降低文件系统 SSD 存储容量和预调配 IOPS 时需要考虑的几个重要事项：

- 在缩减操作期间增加存储容量：即使缩减操作正在进行，您仍可增加文件系统的 SSD 存储容量。这种灵活性确保当任何聚合在缩减操作过程中达到容量上限时，您仍能保障系统性能和可用性。如果您将 SSD 容量增加到低于原始容量的大小，Amazon FSx 只会调整新请求的（目标）聚合的大小。但是，如果您将 SSD 容量增加到大于原始容量的大小，Amazon FSx 会增加两个聚合的大小以匹配新的目标值。例如，如果要将存储容量从 10000GiB 减少到 5000GiB，随后又请求增加到 7000GiB，则仅目标聚合增加到 7000GiB，使文件系统的最终 SSD 存储容量为 7000GiB。但是，如果请求增加到 12000GiB，则两个聚合都会增加到 12000GiB。我们建议您进行周密规划，以避免出现必须将 SSD 容量提升至等于或大于原始 SSD 容量的情况。
- 暂停固态硬盘降低 — 如果您对新聚合的利用率超过 80%，Amazon 将 FSx 暂停降低 SSD 的操作，并在利用率降至 80% 以下时自动恢复降低固态硬盘的操作。
- （仅限第二代单可用区文件系统）存储容量分布 - 您为文件系统选择的新存储容量或 SSD IOPS 均匀分布在每个文件系统的聚合中。
- 在存储容量减少期间进行修补 — 如果您的文件系统在 SSD 减少操作期间进行了修补，Amazon 将中 FSx 止为卷移动数据。因此，如果操作期间出现修补程序，则可能会丢失 SSD 缩减操作的进度。补丁操作完成`vol move`后，Amazon FSx 会自动重启。
- 预调配 IOPS 模式：对于预调配 IOPS 的更改，您必须指定以下两种 IOPS 模式中的一种：

- 自动模式 — Amazon FSx 会自动扩展您的固态硬盘 IOPS，以保持每 GiB 固态硬盘存储容量 3 个预配置的固态硬盘 IOPS，最高不超过您的文件系统配置的最大 SSD IOPS。减少 SSD 容量时，自动 SSD IOPS 将按比例缩小。

  > **Note**
  >
  > 有关您可以为适用于 ONTAP 文件系统配置的最大 SSD IOPS 数量 FSx 的更多信息，请参阅。吞吐能力对性能的影响

- 用户预置模式：您提供的 IOPS 值必须等于或高于当前预调配 IOPS。减少 SSD 容量时，只要用户预置的 SSD IOPS 不超过较小聚合支持的最大值（请求的 SSD 容量每 GB 50IOPS），即可保留用户预置的额外 SSD IOPS。如果预调配 IOPS 高于较小聚合支持的最大值，请先降低 IOPS 再减少 SSD 容量。

- 不支持的卷类型 — Amazon FSx 不支持减少包含任何快照的 SnapLock 卷 FlexClones、离线卷或数据保护 (DP) 卷的文件系统的存储容量。
- 收缩期间不支持的操作-在缩减操作期间，您无法脱机卷 FlexClones、移动 SnapLock 卷、创建、创建卷或修改卷的存储效率设置。

减少 SSD 存储容量的限制

减少文件系统的 SSD 存储容量时，会受到以下限制：

- （仅限第二代文件系统）存储容量减少：仅可减少第二代文件系统的存储容量。
- 存储容量最小减量：每次 SSD 存储容量的减量，必须至少达到文件系统当前 SSD 存储容量的 9%。该缩减操作还应确保文件系统在缩减后，其 SSD 容量的利用率不超过 80%。例如，如果您的文件系统具备 10000GiB 的存储容量和 5000GiB 的存储空间，则可将存储容量减少到 6251GiB，从而使 SSD 利用率保持在 80% 以下。您可以将 SSD 存储容量降至每个 HA 对支持的最小值，即 1024GiB。
- 要减少 SSD 层中包含一个或多个数据超过 50 TiB 的卷的文件系统上的 SSD 存储容量，您必须为每个 HA 对预配置至少 1,536 MB/s 的吞吐容量。如果任何卷在 SSD 层中包含超过 100 TiB 的数据，则必须为每个 HA 对预配置至少 3,072 MB/s 的吞吐容量。对于固态硬盘层中数据超过 200 TiB 的卷，您必须为每个 HA 对预置 6,144 个 MB/s 吞吐容量。
- 两次更新的间隔时间：修改文件系统上的 SSD 存储容量、预调配 IOPS 或吞吐能力后，您必须等待至少六个小时，才能再次修改同一个文件系统上的这些配置。这有时也称为冷却时间。
- 您可以增加但不能减少文件系统的吞吞吐能力
- 您无法向文件系统添加 HA 对

- 在将卷中的数据移动到新聚合时，您无法将该卷还原至先前状态状态（使用 `volume snapshot restore`）。但是，您可以在当前未移动的其他卷上运行 `volume snapshot restore`。

为文件系统创建存储容量利用率警报

我们建议平均 SSD 存储容量利用率不要一直超过 80%。允许 SSD 存储利用率偶尔超过 80%。平均利用率保持在 80% 以下，您才有足够的容量来增加存储空间，而不会遇到问题。以下过程说明如何创建 CloudWatch 警报，在文件系统的 SSD 存储利用率接近 80% 时向您发出警报。

创建文件系统存储容量利用率警报

您可以使用该`StorageCapacityUtilization`指标创建警报，当您的 FSx 一个或多个 ONTAP 文件系统达到存储利用率阈值时触发该警报。

1. 打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
2. 在左侧导航窗格中的警报下，选择所有警报。然后选择创建警报。在创建警报向导中，选择选择指标。
3. 在图表资源管理器中，选择多源查询选项卡。
4. 在查询生成器中，选择以下选项：
   - 对于命名空间，选择 AWS/FSx > 详细的文件系统指标。
   - 在 “指标名称” 中，选择 MAX (StorageCapacityUtilization)。
   - 对于筛选依据，可以选择按照 ID 包含或排除特定的文件系统。如果将筛选依据留空，当任何文件系统超过警报的存储容量利用率阈值时就会触发警报。
   - 将其余选项留空，然后选择图表查询。
5. 选择选择指标。回到向导，在指标部分，为指标添加标签。我们建议将周期控制在 5 分钟以内。
6. 在条件下，只要指标大于/等于 80，即可选择静态阈值类型。
7. 选择下一步，进入配置操作页。

配置警报操作

您可以为警报配置各种操作，使其在警报达到配置的阈值时触发。在本示例中，我们选择了一个简单通知服务 (SNS) Simple Notification Service 主题，但您可以在亚马逊用户指南的使用亚马逊警报 CloudWatch 中了解其他操作。 CloudWatch

1. 在通知下，选择当警报处于 ALARM 状态时要通知的 SNS 主题。您可以选择现有主题或创建一个新主题。您将收到订阅通知，您需要确认后才能收到发送至该电子邮件地址的警报通知。

2. 选择下一步。

完成警报

按照以下说明完成 CloudWatch 警报的创建过程。

1. 在添加名称和描述页面上，为警报指定名称和描述（可选），然后选择下一步。
2. 查看您在预览和创建页面中配置的所有内容，然后选择创建警报。

更新 SSD 存储容量和预调配 IOPS

您可以使用 Amazon FSx 控制台、和 API 来增加或减少文件系统中基于 SSD 的存储空间和预配置的 SSD IOPS 量。 AWS CLI

增加文件系统的 SSD 存储容量或预调配 IOPS（控制台）

1. 打开 Amazon FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 在左侧导航窗格中，选择文件系统。在文件系统列表中，选择要更新 SSD 存储容量的 ONTAP 文件系统和 SSD IOPS。 FSx
3. 选择操作 > 更新存储容量。或者，在摘要部分中，在文件系统的 SSD 存储容量值旁边选择更新。
4. 要增加 SSD 存储容量，请选择修改存储容量。
5. 对于输入类型，请选择以下其中一种：
   - 要以当前值的相对百分比更改形式输入新的 SSD 存储容量，请选择百分比。
   - 要以 GiB 为单位输入新值，请选择绝对。
6. 根据输入类型，输入所需百分比增量的值。
   - 对于百分比，请输入百分比增量值。此值必须比当前值至少大 10%。
   - 对于绝对，请以 GiB 为单位输入新值，最大允许值为 196,608GiB。
7. 对于预调配 SSD IOPS，您可以使用两个选项来修改文件系统的预调配 SSD IOPS 数：
   - 如果您希望 Amazon FSx 自动扩展您的固态硬盘 IOPS 以保持每 GiB 固态硬盘存储容量 3 个预配置的固态硬盘 IOPS（最多 160,000），请选择 “自动”。
   - 如果您想指定 SSD IOPS 数，请选择用户预调配。输入绝对 IOPS 数，该数量至少为 SSD 存储层的 GiB 量的三倍，并且小于或等于 16 万。

> **Note**
>
> 有关您可以为适用于 ONTAP 文件系统配置的最大 SSD IOPS 数量 FSx 的更多信息，请参阅。吞吐能力对性能的影响

8. 选择更新。

> **Note**
>
> 在提示的底部显示新 SSD 存储容量和 SSD IOPS 的配置预览。对于第二代文件系统，还会显示该 per-HA-pair值。

增加文件系统的 SSD 存储容量和预调配 IOPS（CLI）

要为适用于 ONTAP 的文件系统增加 SSD 存储容量和预配置 IOPS，请使用 AWS CLI 命令update-file-system或等效UpdateFileSystem的 API 操作。 FSx 使用您的值设置以下参数：

- 将 `--file-system-id` 设置为要更新的文件系统的 ID。
- 要增加 SSD 存储容量，请将 `--storage-capacity` 设置为至少比当前值大 10% 的目标存储容量值。
- 要修改预调配 SSD IOPS，请使用 `--ontap-configuration DiskIopsConfiguration` 属性。此属性有两个参数、`Iops` 和 `Mode`：
  - 如果您想指定预调配 IOPS 数，请使用 `Iops=`*`number_of_IOPS`*（最多 16 万）和 `Mode=USER_PROVISIONED`。IOPS 值必须大于或等于请求的 SSD 存储容量的三倍。如果不增加存储容量，则该 IOPs 值必须大于或等于当前 SSD 存储容量的三倍。
  - 如果您希望 Amazon FSx 自动提高您的固态硬盘 IOPS，请使用`Mode=AUTOMATIC`且不要使用该`Iops`参数。在预配置的固态硬盘存储容量中，亚马逊 FSx 将自动保持每 GiB 3 个固态硬盘 IOPS（最多 160,000 个）。

> **Note**
>
> 有关您可以为适用于 ONTAP 文件系统配置的最大 SSD IOPS 数量 FSx 的更多信息，请参阅。吞吐能力对性能的影响

以下示例将文件系统的 SSD 存储增加至 2000 GiB，并将用户预置 SSD IOPS 的数量设置为 7000。

```
aws fsx update-file-system \
--file-system-id fs-0123456789abcdef0 \
--storage-capacity 2000 \
--ontap-configuration 'DiskIopsConfiguration={Iops=7000,Mode=USER_PROVISIONED}'
```

要监视更新进度，请使用describe-file-systems AWS CLI 命令。在输出中查找 `AdministrativeActions` 部分。

有关更多信息，请参阅《Amazon AdministrativeAction FSx for NetApp ONTAP API 参考》。

减少文件系统的 SSD 存储容量（控制台）

1. 打开 Amazon FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 在左侧导航窗格中，选择文件系统。在文件系统列表中，选择要更新 SSD 存储容量的 ONTAP 文件系统和 SSD IOPS。 FSx
3. 选择操作 > 更新文件系统 > 更新 SSD 存储容量/IOPS。或者，在摘要部分中，在文件系统的 SSD 存储容量值旁边选择更新。
4. 要减少 SSD 存储容量，对于操作类型，选择减少。
5. 对于输入类型，请选择以下其中一种：
   - 要以当前值的相对百分比更改形式输入新的 SSD 存储容量，请选择百分比。
   - 要以 GiB 为单位输入新值，请选择绝对。
6. 根据输入类型，执行以下操作之一。
   - 对于百分比，输入期望的百分比减少值。此值必须比当前值至少小 9%。
   - 对于绝对值，请输入所需存储容量值（以 GiB 为单位）。
7. 选择更新。

> **Note**
>
> 在提示的底部显示新 SSD 存储容量和 SSD IOPS 的配置预览。对于第二代文件系统，还会显示该 per-HA-pair值。

减少文件系统的 SSD 存储容量和预调配 IOPS（CLI）

要降低适用于 ONTAP 文件系统的固态硬盘存储容量和预配置 IOPS，请使用 AWS CLI 命令update-file-system或等效UpdateFileSystem的 API 操作。 FSx 使用您的值设置以下参数：

1. 要减少 SSD 容量，请使用以下命令：

```
aws fsx update-file-system \
--file-system-id fs-0123456789abcdef0 \
--storage-capacity 4096
```

如果您使用的是用户预调配 IOPS 模式，且希望保留当前的 IOPS 级别，请包含 `DiskIopsConfiguration` 参数：

```
aws fsx update-file-system \
--file-system-id fs-0123456789abcdef0 \
--storage-capacity 4096 \
--ontap-configuration 'DiskIopsConfiguration={Iops=15000,Mode=USER_PROVISIONED}'
```

2. 要监控缩减操作的进度，请使用 describe-file-systems 命令：

```
aws fsx describe-file-systems --file-system-id fs-0123456789abcdef0
```

该命令返回有关 `AdministrativeActions` 部分中缩减操作的信息。例如：

```
{
    "FileSystem": {
        "StorageCapacity": 4096,
        "StorageType": "SSD",
        "AdministrativeActions": [
            {
                "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                "Message": "Moving data for [vol1 vol2]. 2 volume(s) remaining.
 https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/troubleshooting.html",
                "ProgressPercent": 4,
                "RequestTime": 1748981251.591,
                "Status": "IN_PROGRESS",
                "TargetFileSystemValues": {
                    "StorageCapacity": 4096
                }
            }
```

```
        ]
    }
}
```

要监视更新进度，请使用`describe-file-systems` AWS CLI 命令。在输出中查找 `AdministrativeActions` 部分。

有关更多信息，请参阅《Amazon `AdministrativeAction` FSx for NetApp ONTAP API 参考》。

动态增加存储容量

当已使用的 SSD 存储容量超过您指定的阈值时，您可以使用以下解决方案动态增加 for ONTAP 文件系统的 SSD 存储容量。 FSx 此 AWS CloudFormation 模板会自动部署定义存储容量阈值所需的所有组件、基于该阈值的 Amazon CloudWatch 警报以及增加文件系统存储容量的 AWS Lambda 功能。

该解决方案会自动部署所需的所有组件，并采用以下参数：

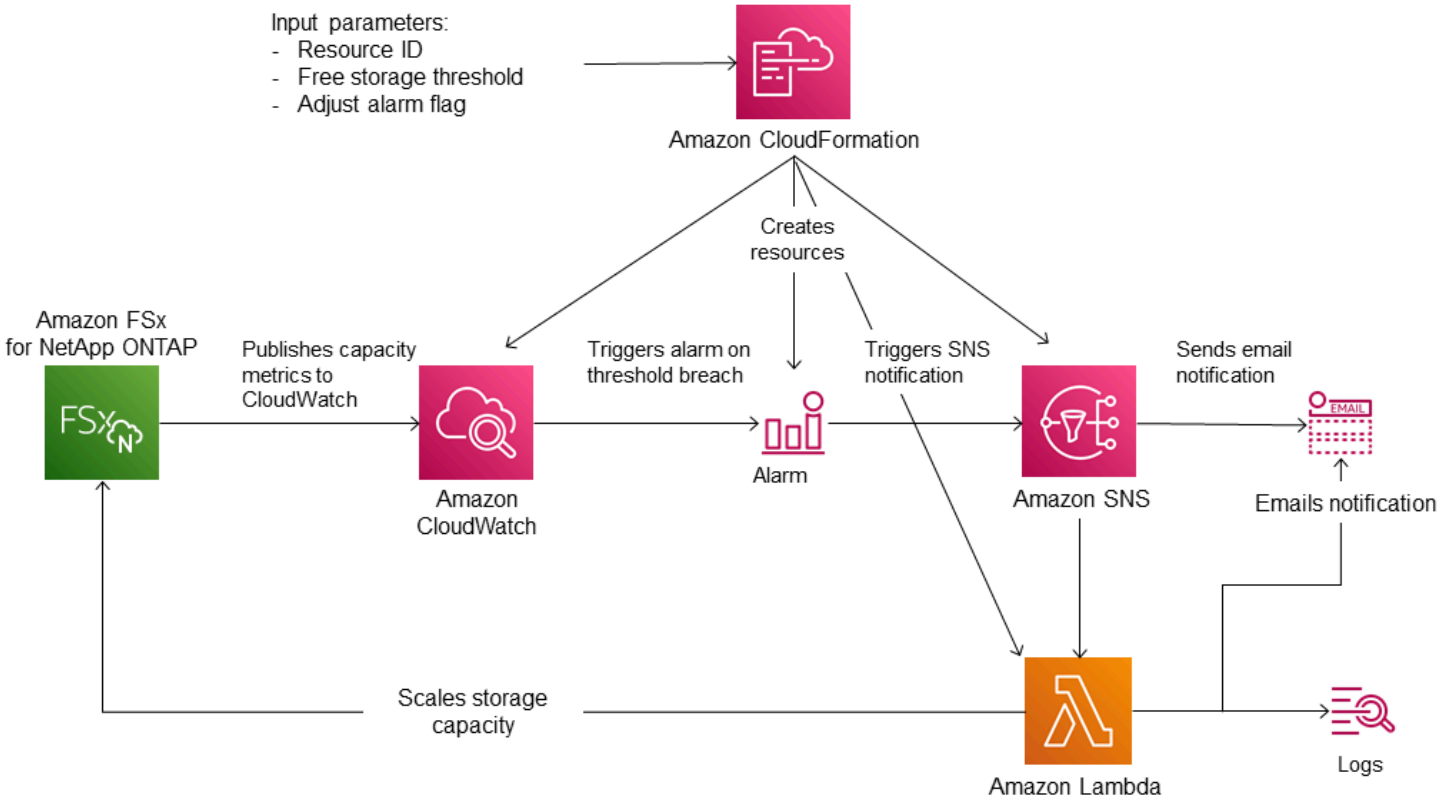
- 您 FSx 的 ONTAP 文件系统 ID。
- 已使用的 SSD 存储容量阈值（数值）。这是触发 CloudWatch 警报的百分比。
- 存储容量的增加百分比（%）。
- 用于接收扩展通知的电子邮件地址。

主题

- 架构概述
- CloudFormation 模板
- 使用自动部署 CloudFormation

架构概述

部署此解决方案将在 AWS Cloud中生成以下资源。



下图说明了以下步骤：

1. 该 CloudFormation 模板部署了 CloudWatch 警报、 AWS Lambda 函数、亚马逊简单通知服务 (Amazon SNS) Service 队列和所有必需 AWS Identity and Access Management 的 (IAM) 角色。IAM 角色授予 Lambda 函数调用亚马逊 FSx API 操作的权限。
2. CloudWatch 当文件系统的已用存储容量超过指定阈值时触发警报，并向 Amazon SNS 队列发送消息。仅当文件系统的已用容量连续 5 分钟超过阈值时，警报才会被触发。
3. 然后，该解决方案会触发订阅此 Amazon SNS 主题的 Lambda 函数。
4. Lambda 函数根据指定的百分比增长值计算新的文件系统存储容量，并设置新的文件系统存储容量。
5. Lambda 函数操作的原始 CloudWatch 警报状态和结果将发送到 Amazon SNS 队列。

要接收有关作为 CloudWatch 警报响应而执行的操作的通知，您必须通过订阅确认电子邮件中提供的链接来确认 Amazon SNS 主题订阅。

CloudFormation 模板

此解决方案 CloudFormation 用于自动部署用于自动增加 for ONTAP 文件系统的存储容量的组件。FSx 要使用此解决方案，请下载FSxOntapDynamicStorageScaling CloudFormation 模板。

该模板使用如下所述的参数。查看模板参数及其默认值，并根据文件系统的需求对它们进行修改。

FileSystemId

无默认值。您想要自动增加存储容量的文件系统的 ID。

LowFreeDataStorageCapacityThreshold

无默认值。指定触发警报并增加文件系统存储容量要达到的已用存储容量的阈值，以文件系统的当前存储容量的百分比（%）形式指定。当已用存储空间超过此阈值时，则视为文件系统的可用存储容量不足。

EmailAddress

无默认值。指定 SNS 订阅使用的电子邮件地址，并接收存储容量阈值警报。

PercentIncrease

默认值为 20%。以当前存储容量的百分比指定存储容量的增量。

> **Note**
>
> 每次 CloudWatch 警报进入ALARM状态时，都会尝试一次存储扩展。如果在尝试存储扩展操作后，SSD 存储容量利用率仍高于阈值，则不会再尝试存储扩展操作。

Max FSx SizeinGi B

默认值为 196608。指定 SSD 存储支持的存储容量上限。

使用自动部署 CloudFormation

以下过程配置和部署 CloudFormation 堆栈以自动增加 for ONTAP 文件系统的存储容量。 FSx 部署需要花几分钟时间。有关创建 CloudFormation 堆栈的更多信息，请参阅《AWS CloudFormation 用户指南》中的在 AWS CloudFormation 控制台上创建堆栈。

> **Note**
>
> 实施此解决方案会产生相关 AWS 服务的账单。有关更多信息，请参阅有关这些服务的定价详细信息页面。

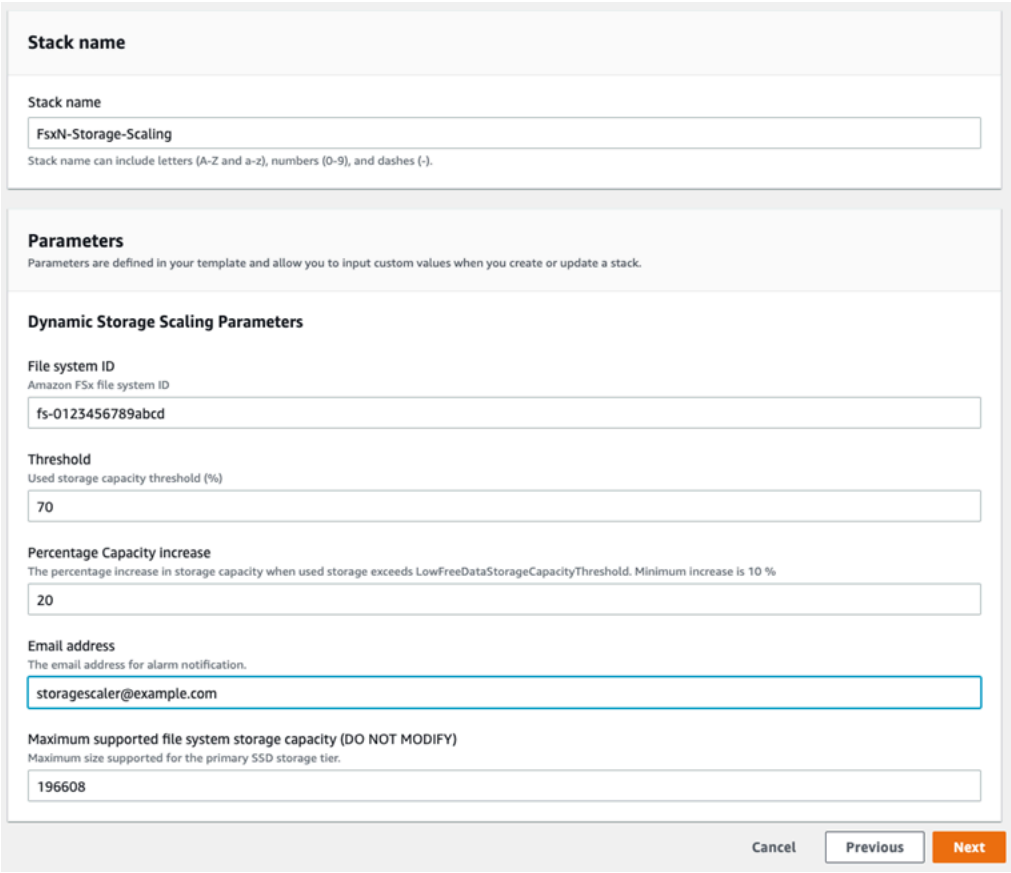
在开始之前，您必须拥有在亚马逊虚拟私有云（亚马逊 VPC）中运行的亚马逊 FSx 文件系统的 ID AWS 账户。有关创建 Amazon FSx 资源的更多信息，请参阅开始使用适用于 ONTAP 的 Amazon FSx NetApp。

启动自动存储容量增加解决方案堆栈

1. 下载 FSxOntapDynamicStorageScaling CloudFormation 模板。

> **Note**
>
> Amazon FSx 目前仅在特定 AWS 地区可用。您必须在可用 Amazon FSx 的 AWS 地区启动此解决方案。有关更多信息，请参阅中的 Amazon FSx 终端节点和配额AWS 一般参考。

2. 在 CloudFormation 控制台中，选择创建堆栈 > 使用新资源。
3. 选择模板已就绪。在指定模板部分中，选择上传模板文件，然后上传您下载的模板。
4. 在指定堆栈详细信息中，输入自动存储容量增加解决方案的值。



5. 输入堆栈名称。

6. 对于参数，请查看模板参数并根据文件系统的需求对其进行修改。然后选择下一步。

> **Note**
>
> 要在尝试使用此 CloudFormation 模板进行扩展时收到电子邮件通知，请确认部署模板后收到的 SNS 订阅电子邮件。

7. 输入自定义解决方案所需的选项设置，然后选择下一步。
8. 对于审核，请审核并确认解决方案设置。必须选择确认模板创建 IAM 资源对应的复选框。
9. 选择创建以部署堆栈。

您可以在 CloudFormation 控制台的 “状态” 列中查看堆栈的状态。您应该会在几分钟后看到 CREATE_COMPLETE 状态。

更新堆栈

创建堆栈后，您可以使用相同的模板并为参数提供新值，从而对其进行更新。有关更多信息，请参阅《AWS CloudFormation 用户指南》中的直接更新堆栈。

监控 SSD 存储利用率

您可以使用各种 AWS 和NetApp工具监控文件系统的 SSD 存储容量利用率。使用 Amazon，CloudWatch 您可以监控存储容量利用率并设置警报，以便在存储容量利用率达到可自定义的阈值时提醒您。

> **Note**
>
> 我们建议 SSD 存储层的存储容量利用率不要超过 80%。这样可以确保分层正常运行，并为新数据提供开销。如果 SSD 存储层的存储容量利用率一直高于 80%，您可以增加 SSD 存储层的容量。有关更多信息，请参阅 更新文件系统 SSD 存储和 IOPS。

您可以在 Amazon FSx 控制台中查看文件系统的可用固态硬盘存储空间和总体存储分布。可用的主存储容量图表显示一段时间内文件系统上可用的 SSD 存储容量。存储分配图表显示文件系统的总体存储容量目前在 3 个类别中的分配情况：

- 容量池层
- SSD 层 – 可用

- SSD 层 – 已使用

您可以使用以下步骤在中监控文件系统的 SSD 存储容量利用率。 AWS 管理控制台

监控文件系统的可用 SSD 层存储容量（控制台）

1. 打开 Amazon FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 在左侧导航栏中选择文件系统，然后选择您要查看其存储容量信息的 ONTAP 文件系统。系统随即显示文件系统详细信息页面。
3. 在第二个面板中，选择监控和性能选项卡，然后选择存储。将显示可用主存储容量和每个聚合的存储容量利用率图表。

监控存储效率节省情况

启用后，您可以在亚马逊控制台、亚马逊 FSx 控制台和 ONTAP CLI 中查看节省了多少存储容量。CloudWatch

查看存储效率节省情况（控制台）

Amazon FSx 控制台中显示的适用 FSx 于 ONTAP 文件系统的存储效率节省包括 FlexClones 和 SnapShots带来的节省。

1. 打开 Amazon FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 从文件系统列表中选择要查看存储效率节省的 ONTAP 文件系统。 FSx
3. 在文件系统详细信息页面的第二个面板上，选择监控和性能选项卡中的摘要。
4. 存储效率节省图表以逻辑数据大小的百分比和物理字节的形式显示节省的空间。

查看存储效率节省情况（ONTAP CLI）

通过使用 ONTAP CLI 运行 `storage aggregate show-efficiency` 命令，您可以查看仅通过压缩、精简和重复数据删除（不受快照和 FlexClones 的影响）而节省的存储效率。有关更多信息，请参阅 NetApp ONTAP 文档中心中的 storage aggregate show-efficiency。

1. 要访问 ONTAP CLI，请运行以下命令在 Amazon FSx for NetApp ONTAP 文件系统或 SVM 的管理端口上建立 SSH 会话。将 *`management_endpoint_ip`* 替换为文件系统管理端口的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

有关更多信息，请参阅 使用 ONTAP CLI 管理文件系统。

2. storage aggregate show-efficiency 命令显示有关所有聚合存储效率的信息。存储效率分为以下四个不同的级别：

   - Total
   - 聚合
   - 卷
   - 快照和 FlexClone 音量

```
::*> aggr show-efficiency

Aggregate: aggr1
     Node: node1

Total Data Reduction Efficiency Ratio:  3.29:1
Total Storage Efficiency Ratio:         4.29:1
Aggregate: aggr2
     Node: node1

Total Data Reduction Efficiency Ratio:  4.50:1
Total Storage Efficiency Ratio:         5.49:1

cluster::*> aggr show-efficiency -details

Aggregate: aggr1
     Node: node1

Total Data Reduction Ratio:                    2.39:1
Total Storage Efficiency Ratio:                4.29:1

Aggregate level Storage Efficiency
(Aggregate Deduplication and Data Compaction): 1.00:1
Volume Deduplication Efficiency:               5.03:1
Compression Efficiency:                        1.00:1

Snapshot Volume Storage Efficiency:            8.81:1
FlexClone Volume Storage Efficiency:           1.00:1
Number of Efficiency Disabled Volumes:         1

Aggregate: aggr2
```

```
     Node: node1
Total Data Reduction Ratio:                    2.39:1
Total Storage Efficiency Ratio:                4.29:1

Aggregate level Storage Efficiency
(Aggregate Deduplication and Data Compaction): 1.00:1
Volume Deduplication Efficiency:               5.03:1
Compression Efficiency:                        1.00:1

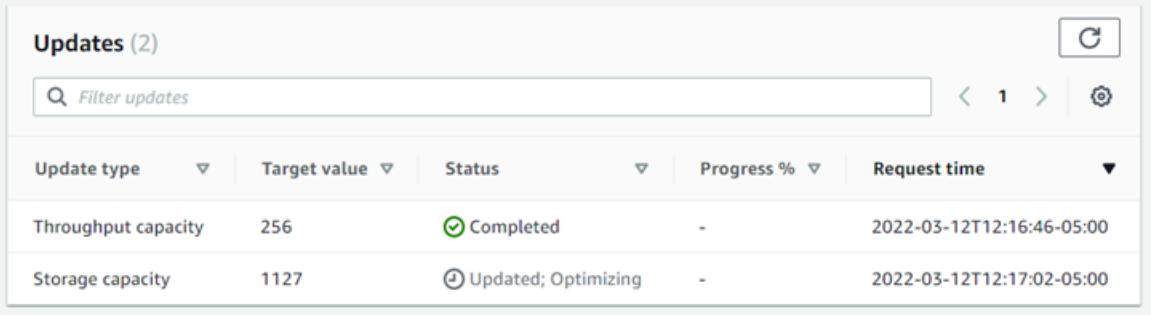
Snapshot Volume Storage Efficiency:            8.81:1
FlexClone Volume Storage Efficiency:           1.00:1
Number of Efficiency Disabled Volumes:         1
```

监控存储容量和 IOPS 更新

您可以使用亚马逊 FSx控制台、CLI 和 API 监控固态硬盘存储容量和 IOPS 更新的进度。

监控存储和 IOPS 更新（控制台）

在 for ONTAP 文件系统的文件系统详细信息页面 FSx 的更新选项卡中，您可以查看每种更新类型的 10 个最新更新。



有关 SSD 存储容量和 IOPS 更新，您可以查看以下信息：

更新类型

支持的类型包括存储容量、模式和 IOPS。为所有存储容量和 IOPS 扩展请求列出模式和 IOPS 值。

目标值

您指定的文件系统 SSD 存储容量或 IOPS 的更新值。

状态

当前更新状态。可能的值如下所示：

- 待处理 — Amazon FSx 已收到更新请求，但尚未开始处理。
- 处理@@ 中 — Amazon FSx 正在处理更新请求。
- 更新；优化 — Amazon FSx 增加了文件系统的固态硬盘存储容量。现在，存储优化流程正在后台重新平衡数据。
- 已完成 – 更新成功完成。
- 已失败 – 更新请求失败。选择问号（？）可查看详细信息。

进度百分比

以完成百分比的形式显示存储优化流程的进度。

请求时间

Amazon FSx 收到更新操作请求的时间。

监控存储和 IOPS 更新（CLI）

您可以使用`describe-file-systems` AWS CLI 命令和 DescribeFileSystemsAPI 操作查看和监控文件系统 SSD 存储容量的增加和减少请求。`AdministrativeActions` 数组列出每种管理操作类型的 10 个最近更新操作。当增加文件系统的 SSD 存储容量时，会生成两个 `AdministrativeActions` 操作：`FILE_SYSTEM_UPDATE` 和 `STORAGE_OPTIMIZATION` 操作。当减少文件系统的 SSD 存储容量时，仅生成一个 `AdministrativeActions` 操作：`FILE_SYSTEM_UPDATE` 操作。

以下示例显示了 CLI 命令 `describe-file-systems` 的响应摘录。文件系统有待处理的管理操作，即，将 SSD 存储容量增加到 2000GiB，将预调配 SSD IOPS 增加到 7000。

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1586797629.095,
        "Status": "PENDING",
        "TargetFileSystemValues": {
            "StorageCapacity": 2000,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "USER_PROVISIONED",
                    "Iops": 7000
                }
             }
        }
```

```
    },
    {
        "AdministrativeActionType": "STORAGE_OPTIMIZATION",
        "RequestTime": 1586797629.095,
        "Status": "PENDING"
    }
]
```

Amazon 首先 FSx 处理该FILE_SYSTEM_UPDATE操作，将新的较大存储磁盘添加到文件系统。当新的存储空间可供文件系统使用时，FILE_SYSTEM_UPDATE 状态将更改为 UPDATED_OPTIMIZING。存储容量显示新的较大值，Amazon FSx 开始处理STORAGE_OPTIMIZATION管理操作。以下 describe-file-systems CLI 命令的响应摘录中显示了该行为。

ProgressPercent 属性显示存储优化流程的进度。存储优化流程成功完成后，FILE_SYSTEM_UPDATE 操作的状态将更改为 COMPLETED，并且 STORAGE_OPTIMIZATION 操作不再显示。

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1586799169.445,
        "Status": "UPDATED_OPTIMIZING",
        "TargetFileSystemValues": {
            "StorageCapacity": 2000,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "USER_PROVISIONED",
                    "Iops": 7000
                }
            }
        }
    },
    {
        "AdministrativeActionType": "STORAGE_OPTIMIZATION",
        "ProgressPercent": 41,
        "RequestTime": 1586799169.445,
        "Status": "IN_PROGRESS"
    }
]
```

减少 SSD 容量时，FILE_SYSTEM_UPDATE 操作包括 Message 属性，该属性提供有关当前正在移动哪些卷以及剩余多少卷的信息。例如：

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "Message": "Moving data for [vol1 vol2]. 2 volume(s) remaining. https://
docs.aws.amazon.com/fsx/latest/ONTAPGuide/troubleshooting.html",
        "ProgressPercent": 8,
        "RequestTime": 1748981251.591,
        "Status": "IN_PROGRESS",
        "TargetFileSystemValues": {
            "StorageCapacity": 4096,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "AUTOMATIC",
                    "Iops": 12288
                }
            }
        }
    }
]
```

如果由于目标聚合的利用率已超过 80% 而暂停 SSD 缩减操作，则状态将更改为 PAUSED，并显示相应提示消息：

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "Message": "Your file system has insufficient free space in its SSD tier.
 Please free up space or increase your file system's storage capacity.",
        "ProgressPercent": 8,
        "RequestTime": 1748981251.591,
        "Status": "PAUSED",
        "TargetFileSystemValues": {
            "StorageCapacity": 4096,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "AUTOMATIC",
                    "Iops": 12288
                }
            }
        }
    }
]
```

如果存储容量或 IOPS 更新请求失败，则 FILE_SYSTEM_UPDATE 操作的状态将更改为 FAILED，如以下示例所示。FailureDetails 属性提供失败信息。

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1586373915.697,
        "Status": "FAILED",
        "TargetFileSystemValues": {
            "StorageCapacity": 2000,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "USER_PROVISIONED",
                    "Iops": 7000
                }
            }
        },
        "FailureDetails": {
            "Message": "failure-message"
        }
    }
]
```

卷存储容量

FSx ONTAP 卷是虚拟资源，用于对数据进行分组、确定数据的存储方式以及确定对数据的访问类型。卷（例如文件夹）本身不会消耗文件系统的存储容量。只有卷中存储的数据才会消耗 SSD 存储空间，而且根据卷的分层策略，还会消耗容量池存储空间。您可以在创建卷时设置其大小，也可以稍后更改大小。您可以使用、和 API 以及 ONTAP CLI 监控和管理 FSx 适用于 ONTAP 的卷的存储容量。 AWS 管理控制台 AWS CLI

主题

- 卷数据分层
- 快照和卷存储容量
- 卷文件容量
- 管理存储效率
- 启用自动调整大小
- 启用云写入模式
- 更新存储容量

- 更新分层策略
- 更新最小冷却天数
- 更新卷的云检索策略
- 更新卷上文件的数量上限
- 监控卷存储容量
- 监控卷的文件容量

卷数据分层

Amazon FSx f NetApp or ONTAP 文件系统有两个存储层：主存储和容量池存储。主存储是预配置的可扩展高性能 SSD 存储，专为数据集的活动部分而构建。容量池存储是完全弹性的存储层，可以自动扩展到 PB 级大小，并且针对不经常访问的数据进行成本优化。

根据卷的分层策略、冷却周期和阈值设置，每个卷上的数据会自动分层到容量池存储层。以下各部分介绍了 ONTAP 卷分层策略，以及在确定何时将数据分层存入容量池时使用的阈值。

> **Note**
>
> FSx for ONTAP 支持将数据分层到所有SnapLock卷上的容量池，无论其类型如何。SnapLock有关更多信息，请参阅 SnapLock 的工作原理。

卷分层策略

您可以通过 FSx 为文件系统上的每个卷选择分层策略来确定如何使用 for ONTAP 文件系统的存储层。您可以在创建卷时选择分层策略，也可以随时使用 Amazon FSx 控制台 AWS CLI、API 或使用NetApp管理工具对其进行修改。您可以选择以下其中一种策略，用于确定哪些数据（如果有）分层到容量池存储。

> **Note**
>
> 分层可以将文件数据和快照数据移至容量池层。但是，文件元数据始终保留在 SSD 层。有关更多信息，请参阅 SSD 存储的使用方式。

- 自动 – 此策略将所有冷数据（用户数据和快照）移动到容量池层。数据的冷却速率由策略的冷却周期决定。冷却周期默认为 31 天，可以配置为 2-183 天之间的值。当底层冷数据块被随机读取时（就像典型文件访问一样），这些冷数据块会变热并写入主存储层。当冷数据块被按顺序读取时（例如，

通过杀毒扫描），这些冷数据块会保持冷却并保留在容量池存储层。这是使用 Amazon FSx 控制台创建卷时的默认策略。

- 仅限快照 – 此策略仅将快照数据移动到容量池存储层。快照分层到容量池的速率由策略的冷却周期决定。冷却周期默认设置为 2 天，可以配置为 2-183 天之间的值。当冷快照数据被读取时，这些数据会变热并写入主存储层。这是使用 AWS CLI、Amazon FSx API 或 NetApp ONTAP CLI 创建卷时的默认策略。
- 全部 – 此策略将所有用户数据和快照数据标记为冷数据，并将其存储于容量池层。当数据块被读取时，这些数据块保持冷却，不会写入主存储层。当数据被写入采用全部分层策略的卷时，这些数据最初仍会写入 SSD 存储层，之后通过后台进程分层到容量池。如果全部策略均应用于已包含数据的卷，则现有数据将从 SSD 分层到容量池。请注意，文件元数据始终保留在 SSD 层。
- 无 – 此策略确保卷的所有数据保留在主存储层，并防止将其移动到容量池存储。如果您在某个卷使用任何其他策略后将其设置为该策略，该卷中位于容量池存储的现有数据（包括快照）会通过后台进程移至 SSD 存储。仅当 SSD 利用率低于 90% 且云检索策略设置为 `promote` 或 `on-read` 时，才会进行这种数据迁移。通过有意读取数据可加快此后台进程。有关更多信息，请参阅 云检索策略。

有关如何设置或修改卷分层策略的更多信息，请参阅 更新分层策略。

作为最佳实践，在迁移您计划长期存储于容量池存储的数据时，我们建议为卷使用自动分层策略。使用自动分层，数据会在 SSD 存储层上至少存储 2 天（具体取决于卷的冷却周期），然后再移动至容量池层。ONTAP 对 SSD 存储层中存储的数据定期运行处理后重复数据删除，根据卷中的数据变化率自动调整频率。频率越高，后处理重复数据删除作业的触发就越频繁。

默认情况下，由于后处理压缩可能会对文件系统上正在进行的工作负载带来性能影响，因此该功能在 ONTAP 中处于禁用状态。在启用后处理压缩之前，应该评估对工作负载性能带来的影响。要启用后处理压缩，假设 ONTAP CLI 中拥有诊断权限级别并运行以下命令：

```
::> volume efficiency inactive-data-compression modify -vserver svm-name -volume vol-name -is-enabled true
```

ONTAP 对在 SSD 存储上至少保留 14 天的数据运行后处理压缩。对于不太可能在较短时间后访问数据的工作负载，可以修改后处理压缩设置，以便更快地运行后处理压缩。例如，要将后处理压缩节省应用于 5 天未访问的数据，请运行以下 ONTAP CLI 命令：

```
::> volume efficiency inactive-data-compression modify -vserver svm-name -volume vol-name -threshold-days 5 -threshold-days-min 2 -threshold-days-max 14
```

有关该命令的更多信息，请参见 inactive-data-compression修改音量效率

通过将数据保留在 SSD 上，可以最大成都地提高所创建卷备份的传输速度，因为 SSD 存储的数据传输速率更高。

分层冷却周期

卷的分层冷却周期设置将 SSD 层中的数据标记为冷数据所需的时间。冷却周期适用于 Auto 和 Snapshot-only 分层策略。您可以将冷却周期设置为 2-183 天之间的值。有关如何设置冷却周期的更多信息，请参阅更新最小冷却天数。

冷却周期到期 24-48 小时后对数据进行分层。分层是一个后台进程，会消耗网络资源，其优先级低于面向客户端的请求。当有面向客户端的持续请求时，分层活动会节流。

云检索策略

卷的云检索策略设置指定何时允许从容量池层读取的数据提升到 SSD 层的条件。当云检索策略设置为 Default 之外的其他任何状态时，该策略将覆盖卷分层策略的检索行为。卷可能具有以下其中一种云检索策略：

- 默认 – 此策略根据卷的底层分层策略来检索分层数据。这是所有卷的默认云检索策略。
- 从不 – 此策略从不检索分层数据，无论读取是顺序读取还是随机读取。这类似于将卷的分层策略设置为全部，不同的是您可以根据最短冷却周期（而不是立即），将其与其他策略（自动、仅限快照）结合使用。
- 读时 – 此策略会检索所有客户端驱动的数据读取的分层数据。使用全部分层策略时，此策略不起作用。
- 提升 – 此策略标记卷在容量池中的所有数据以供检索到 SSD 层。下次运行每日后台分层扫描仪时会对数据进行标记。如果应用程序具有不频繁运行的周期性工作负载，但在运行时需要 SSD 层性能，则该策略对其有益。使用全部分层策略时，此策略不起作用。

有关设置卷的云检索策略的信息，请参阅更新卷的云检索策略。

分层阈值

文件系统的 SSD 存储容量利用率决定 ONTAP 如何管理所有卷的分层行为。根据文件系统的 SSD 存储容量使用情况，以下阈值会如所述设置分层行为。有关如何监控卷的 SSD 存储层的容量利用率的信息，请参阅监控卷存储容量。

> **Note**
>
> 我们建议 SSD 存储层的存储容量利用率不要超过 80%。对于第二代文件系统，此建议既适用于所有文件系统聚合的总平均利用率，也适用于每个单独聚合的利用率。这样可以确保分层正

常运行，并为新数据提供开销。如果 SSD 存储层的存储容量利用率一直高于 80%，您可以增加 SSD 存储层的容量。有关更多信息，请参阅 更新文件系统 SSD 存储和 IOPS。

FSx for ONTAP 使用以下存储容量阈值来管理卷上的分层：

- <= 50% SSD 存储层利用率 – 达到此阈值时，SSD 存储层被认为未充分利用，并且只有使用全部分层策略的卷才会将数据分层到容量池存储。达到此阈值时，采用自动和仅限快照策略的卷不会对数据进行分层。
- > 50% SSD 存储层利用率 – 采用自动和仅限快照分层策略的卷根据分层最短冷却天数设置对数据进行分层。默认设置为 31 天。
- >= 90% 固态硬盘存储层利用率 — 在这个阈值下，Amazon FSx 会优先考虑在 SSD 存储层中保留空间。为采用自动和仅限快照策略的卷读取数据时，容量池层中的冷数据不再移至 SSD 存储层。
- >= 98% SSD 存储层利用率 – 当 SSD 存储层的利用率等于或高于 98% 时，所有分层功能都会停止。您可以继续从存储层读取数据，但不能写入存储层。

快照和卷存储容量

快照是 Amazon FSx for NetApp ONTAP 卷在某个时间点的只读映像。快照可防止卷中的文件被意外删除或修改。用户可通过快照轻松查看和还原早期快照中的单个文件或文件夹。

快照与文件系统的数据一同存储，因此快照会消耗文件系统的存储容量。但是，快照仅消耗文件在上次快照中已更改部分的存储容量。文件系统卷的备份中不包含快照。

默认情况下，使用默认快照策略在卷上启用快照。快照存储于卷根的 `.snapshot` 目录。您可以通过以下方式管理快照的卷存储容量：

- 快照策略 – 选择内置快照策略或选择在 ONTAP CLI 或 REST API 中创建的自定义策略。
- 手动删除快照 – 通过手动删除快照来回收存储容量。
- 创建快照自动删除策略 – 创建策略以删除比默认快照策略更多的快照。
- 关闭自动快照 – 通过关闭自动快照来节省存储容量。

有关更多信息，请参阅 使用快照保护您的数据。

卷文件容量

Amazon FSx for NetApp ONTAP 卷具有文件指针，用于存储文件元数据，例如文件名、上次访问时间、权限、大小，以及用作指向数据块的指针。这些文件指针被称为索引节点，每个卷针对索引节点数量有有限的容量，称为卷文件容量。当卷运行不足或耗尽其可用文件（索引节点）时，您无法向该卷写入其他数据。

卷可以包含的文件系统对象（文件、目录、快照副本）的数量取决于拥有的索引节点数。卷中索引节点的数量随卷的存储容量（以及 FlexGroup 卷的卷组件数量）相应增加。默认情况下，存储容量为 648 GiB 或以上的 FlexVol 卷（或 FlexGroup 组件）都具有相同数量的索引节点：21,251,126。如果您创建了大于 648GiB 的卷，并且希望其索引节点数超过 21,251,126，您必须手动增加索引节点（文件）的数量上限。有关查看卷的最大文件数的信息，请参阅 监控卷的文件容量。

卷上默认索引节点的数量为每 32KiB 卷存储容量为 1 个索引节点，卷大小不超过 648GiB。对于 1GiB 卷：

卷字节数 ×（1 个文件 ÷ 索引节点字节数）= 文件最大数

1,073,741,824 字节 ×（1 个文件 ÷ 32,768 字节）= 32,768 个文件

您可以增加卷可包含的索引节点数上限，即每 4KiB 存储容量最多 1 个索引节点。对于 1GiB 卷，这样会将索引节点或文件的数量上限从 32,768 增加到 262,144：

1,073,741,824 字节 ×（1 个文件 ÷ 4096 字节）= 262,144 个文件

FSx 适用于 ONTAP 的卷最多可以有 20 亿个索引节点。

有关更改卷可存储的最大文件数的信息，请参阅 更新卷上文件的数量上限。

管理存储效率

通过 FSx 为 ONTAP 卷启用存储效率，您可以优化存储利用率、降低存储成本并提高文件系统的整体性能。

> **Note**
>
> 我们建议使用 Amazon FSx 控制台、API 启用存储效率，或者 AWS CLI 确保将最佳存储效率设置应用于您的卷。

ONTAP 将文件组织成 4 千字节（KiB）的数据块。存储效率发生在数据存储块层面，而不是单个文件层面。启用存储效率后，ONTAP 可结合使用数据缩减技术来消除重复数据、压缩数据大小并重新组织数据布局，以实现磁盘使用的最优化。

存储效率有两种应用方式。存储效率应用于内联数据（数据在写入磁盘之前位于内存中），可立即节省存储空间。存储效率还通过定期效率作业应用于 SSD 存储层中的后台数据（数据写入磁盘后），以随着时间的推移优化存储利用率。后台存储效率不在分层到容量池后的数据上运行。但是，如果数据存储在 SSD 中时节省了任何存储空间，则在数据分层到容量池时，这些节省的空间会被保留。

> **Note**
>
> ONTAP 不支持在数据保护（DP）卷上启用存储效率。但是，当数据复制到目标 DP 卷时，源读写（RW）卷中实现的存储节省将得以保留。

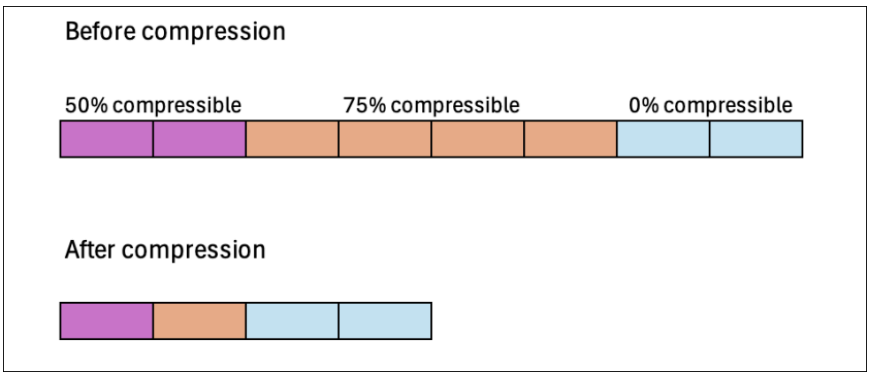
压缩数据块

压缩组是数据的逻辑分组，其中数据作为一个块进行管理和压缩。ONTAP 自动将数据块打包到压缩组中，从而减少磁盘上消耗的空间。为优化性能和存储利用率，ONTAP 可根据数据的访问模式调整应用于数据的压缩程度，从而提供一种均衡的数据管理方法。

默认情况下，使用 8 KB 压缩组对数据进行内联压缩，以确保向卷写入数据时具有最佳性能。或者，您可以在卷上启用非活动数据压缩来进一步压缩 SSD 中的数据，从而对数据应用更大程度的压缩。非活动数据压缩对冷数据使用 32 KB 压缩组，以节省更多存储空间。有关更多信息，请参阅 NetApp ONTAP Documentation Center 中的 `volume efficiency inactive-data-compression modify` 命令。

> **Note**
>
> 非活动数据压缩会消耗额外的 CPU 和磁盘 IOPS，这可能是一项资源密集型任务。在启用此功能之前，我们建议先评估运行非活动数据压缩对工作负载的性能影响。

下图说明了压缩数据块可以节省的存储空间。



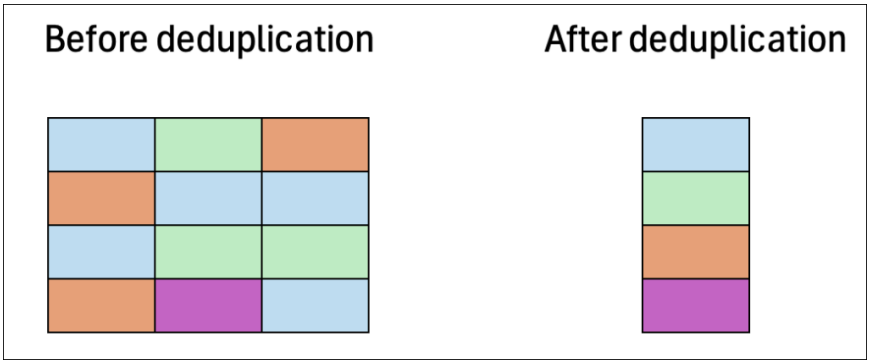
对数据块进行重复数据删除

ONTAP 检测并消除重复的数据块，以减小数据冗余度。重复数据块被替换为对共享唯一数据块的引用。

默认情况下，数据在写入磁盘之前以内联方式删除重复数据，以减小存储占用空间。ONTAP 还会按指定间隔运行后台重复数据删除扫描器，以在重复数据写入磁盘后识别并删除重复数据。在这些计划扫描期间，ONTAP 会处理更改日志，以识别自上次扫描以来尚未删除重复数据的新数据块或修改过的数据块。当发现重复数据时，ONTAP 会更新元数据以指向重复数据块的单个副本，并将冗余数据块标为可以回收的可用空间。

> **Note**
>
> ONTAP 一次对 4 KB 的传入写入数据应用重复数据删除，因此在运行写入数据小于 4 KB 的工作负载时，重复数据删除节省的存储空间可能会降低。
> FSx for ONTAP 不支持跨卷重复数据删除。

下图说明了删除重复数据可以节省的存储空间。

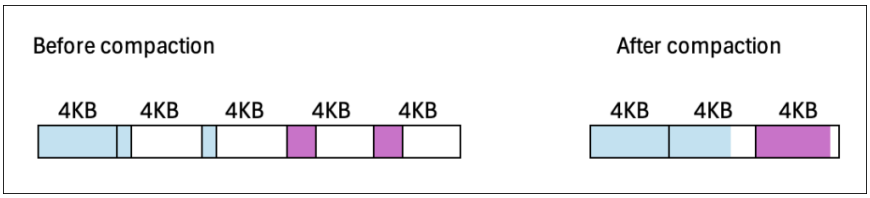


紧凑处理数据块

ONTAP 将每个小于 4 KB 的部分填充数据块整合到一个利用率更高的 4 KB 数据块中。

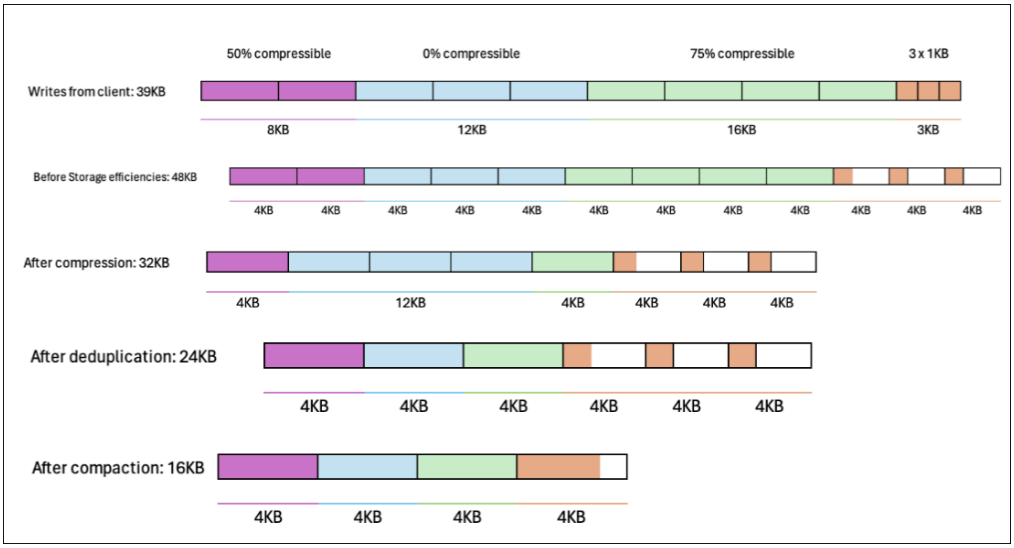
默认情况下，数据以内联方式进行紧凑处理，以优化数据写入磁盘时的布局，从而最大程度地减小存储开销、减少碎片并提高读取性能。

下图说明了紧凑处理可以节省的存储空间。



示例：存储效率

下图说明了存储效率如何应用于数据。



启用自动调整大小

自动调整卷大小，以便卷大小在达到已用存储容量阈值时自动增加到指定大小。您可以使用 ONTAP `volume autosize` CLI 命令对 FlexVol 卷类型（ONTAP FSx 的默认卷类型）执行此操作。

启用卷自动调整大小（ONTAP CLI）

1. 要访问 ONTAP CLI，请运行以下命令在 Amazon FSx for NetApp ONTAP 文件系统或 SVM 的管理端口上建立 SSH 会话。将 *`management_endpoint_ip`* 替换为文件系统管理端口的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

有关更多信息，请参阅 使用 ONTAP CLI 管理文件系统。

2. 使用如下所示的 `volume autosize` 命令，同时替换以下值：

   - 将 *svm_name* 替换为卷创建时所用 SVM 的名称。
   - 将 *vol_name* 替换为要调整大小的卷的名称。
   - 将 *grow_threshold* 替换为已用空间百分比值（例如 90）。达到该值时，卷将自动增大（最大值为 *max_size*）。
   - 将 *max_size* 替换为卷大小的上限。使用格式 *integer*[KB|MB|GB|TB|PB]；例如，300TB。大小上限为 300 TB。默认值为卷大小的 120%。
   - *min_size*替换为音量将缩小到的最小大小。使用与相同的格式*max_size*。
   - 替换为已*shrink_threshold*用空间百分比，在该百分比下，卷的大小将自动缩小。

```
::> volume autosize -vserver svm_name -volume vol_name -mode grow_shrink -
grow-threshold-percent grow_threshold -maximum-size max_size -shrink-threshold-
percent shrink_threshold -minimum-size min_size
```

3. 要显示当前的自动调整大小设置，请运行以下命令。将 *svm_name* 和 *vol_name* 替换为您的信息。

```
::> volume autosize -vserver svm_name -volume vol_name
```

启用云写入模式

使用 `volume modify` ONTAP CLI 命令为现有卷启用或禁用云写入模式。有关更多信息，请参阅 NetApp ONTAP 文档中心`volume modify`中的。

设置云写入模式的先决条件为：

- 卷必须是现有卷。只能在现有卷上启用该功能。
- 卷必须是读写（RW）卷。
- 卷必须具有全部分层策略。有关如何修改卷分层策略的更多信息，请参阅 更新分层策略。

云写入模式对迁移等情况非常有用，例如，使用 NFS 协议将大量数据传输到文件系统。

设置卷的云写入模式（ONTAP CLI）

1. 要访问 ONTAP CLI，请运行以下命令在 Amazon FSx for NetApp ONTAP 文件系统或 SVM 的管理端口上建立 SSH 会话。将 *management_endpoint_ip* 替换为文件系统管理端口的 IP 地址。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   有关更多信息，请参阅 使用 ONTAP CLI 管理文件系统。

2. 使用以下命令进入 ONTAP CLI 高级模式。

   ```
   FSx::> set -privilege advanced
   Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```

3. 使用以下命令设置卷的云写入模式，同时替换以下值：

   - 将 *svm_name* 替换为卷创建时所用 SVM 的名称。
   - 将 *vol_name* 替换为要设置云写入模式的卷的名称。
   - 将 *vol_cw_mode* 替换为 `true` 可以在卷上启用云写入模式，或替换为 `false` 将此模式禁用。

   ```
   FSx::> volume modify -vserver svm_name -volume vol_name -is-cloud-write-
   enabled vol_cw_mode
   ```

   请求成功后，系统会如下响应。

   ```
   Volume modify successful on volume vol_name of Vserver svm_name.
   ```

更新存储容量

您可以使用 AWS 管理控制台、 AWS CLI 和 API 以及 ONTAP CLI 通过手动增加或减小卷大小来管理卷存储容量。您还可以启用卷自动调整大小，以便卷大小在达到某些已用存储容量阈值时自动增加或缩小。您可以使用 ONTAP CLI 来管理卷自动调整大小。

更改卷的存储容量（控制台）

- 您可以使用 Amazon FSx 控制台和 API 增加或减少卷的存储容量。 AWS CLI有关更多信息，请参阅 更新卷。

您还可以通过 ONTAP CLI，使用 `volume modify` 命令来修改卷的存储容量。

修改卷的大小（ONTAP CLI）

1. 要访问 ONTAP CLI，请运行以下命令在 Amazon FSx for NetApp ONTAP 文件系统或 SVM 的管理端口上建立 SSH 会话。将 *`management_endpoint_ip`* 替换为文件系统管理端口的 IP 地址。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   有关更多信息，请参阅 使用 ONTAP CLI 管理文件系统。
2. 使用 volume modify ONTAP CLI 命令修改卷的存储容量。运行以下命令，用您的数据替换以下值：

   - 将 *`svm_name`* 替换为卷创建时所用存储虚拟机（SVM）的名称。
   - 将 *`vol_name`* 替换为要调整大小的卷的名称。
   - 将 *`vol_size`* 替换为以格式 *`integer`*`[KB|MB|GB|TB|PB]` 表示的新的卷大小；例如，`100GB` 表示将卷大小增加到 100GB。

   ```
   ::> volume modify -vserver svm_name -volume vol_name -size vol_size
   ```

更新分层策略

您可以使用 AWS 管理控制台、 AWS CLI 和 API 以及 ONTAP CLI 修改卷的分层策略。

修改卷的数据分层策略（控制台）

按照以下过程，使用 AWS 管理控制台修改卷的数据分层策略。

1. 打开 Amazon FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 在左侧导航窗格中选择卷，然后选择要修改数据分层策略的 ONTAP 卷。
3. 从操作下拉菜单中选择更新卷。更新卷窗口会显示。

4. 对于容量池分层策略，请为卷选择新的策略。有关更多信息，请参阅 卷分层策略。
5. 选择更新，将新策略应用于卷。

设置卷的分层策略（CLI）

- 使用更新卷 CLI 命令 UpdateVolume（等同于 A FSx mazon API 操作）修改卷的分层策略。以下 CLI 命令示例将卷的数据分层策略设置为 SNAPSHOT_ONLY。

```
aws fsx update-volume \
    --volume-id fsxvol-abcde0123456789f
    --ontap-configuration TieringPolicy={Name=SNAPSHOT_ONLY}
```

如果请求成功，系统会返回卷描述。

```
{
    "Volume": {
        "CreationTime": "2021-10-05T14:27:44.332000-04:00",
        "FileSystemId": "fs-abcde0123456789f",
        "Lifecycle": "CREATED",
        "Name": "vol1",
        "OntapConfiguration": {
            "FlexCacheEndpointType": "NONE",
            "JunctionPath": "/vol1",
            "SecurityStyle": "UNIX",
            "SizeInMegabytes": 1048576,
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-abc0123de456789f",
            "StorageVirtualMachineRoot": false,
            "TieringPolicy": {
                "CoolingPeriod": 2,
                "Name": "SNAPSHOT_ONLY"
            },
            "UUID": "aaaa1111-bb22-cc33-dd44-abcde01234f5",
            "OntapVolumeType": "RW"
        },
        "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-
abcde0123456789f/fsvol-abc012def3456789a",
        "VolumeId": "fsvol-abc012def3456789a",
        "VolumeType": "ONTAP"
    }
}
```

修改卷的分层策略（ONTAP CLI）

您可以使用 `volume modify` ONTAP CLI 命令来设置卷的分层策略。有关更多信息，请参阅 NetApp ONTAP 文档中心`volume modify`中的。

1. 要访问 ONTAP CLI，请运行以下命令在 Amazon FSx for NetApp ONTAP 文件系统或 SVM 的管理端口上建立 SSH 会话。将 *`management_endpoint_ip`* 替换为文件系统管理端口的 IP 地址。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   有关更多信息，请参阅 使用 ONTAP CLI 管理文件系统。
2. 使用以下命令进入 ONTAP CLI 高级模式。

   ```
   FSx::> set adv

   Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```
3. 使用以下命令修改卷数据分层策略，同时替换以下值：

   - 将 *`svm_name`* 替换为卷创建时所用 SVM 的名称。
   - 将 *`vol_name`* 替换为要设置数据分层策略的卷的名称。
   - 将 *`tiering_policy`* 替换为所需的策略。有效值为 `snapshot-only`、`auto`、`all` 或 `none`。有关更多信息，请参阅 卷分层策略。

   ```
   FSx::> volume modify -vserver svm_name -volume vol_name -tiering-
   policy tiering_policy
   ```

更新最小冷却天数

卷的最小冷却天数会设置阈值，用于确定哪些数据为热数据，哪些数据为冷数据。您可以使用 AWS CLI 和 API 和 ONTAP CLI 来设置卷的最小冷却天数。

设置卷的最小冷却天数（CLI）

- 使用 up date-volume CLI 命令 UpdateVolume（等同于 A FSx mazon API 操作）修改卷配置。以下 CLI 命令示例将卷的 `CoolingPeriod` 设置为 104 天。

```
aws fsx update-volume \
    --volume-id fsxvol-abcde0123456789f
    --ontap-configuration TieringPolicy={Name=SNAPSHOT_ONLY}
aws fsx update-volume --volume-id fsvol-006530558c14224ac --ontap-configuration
 TieringPolicy={CoolingPeriod=104}
```

如果请求成功，系统会返回卷描述。

```
{
    "Volume": {
        "CreationTime": "2021-10-05T14:27:44.332000-04:00",
        "FileSystemId": "fs-abcde0123456789f",
        "Lifecycle": "CREATED",
        "Name": "vol1",
        "OntapConfiguration": {
            "FlexCacheEndpointType": "NONE",
            "JunctionPath": "/vol1",
            "SecurityStyle": "UNIX",
            "SizeInMegabytes": 1048576,
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-abc0123de456789f",
            "StorageVirtualMachineRoot": false,
            "TieringPolicy": {
                "CoolingPeriod": 104,
                "Name": "SNAPSHOT_ONLY"
            },
            "UUID": "aaaa1111-bb22-cc33-dd44-abcde01234f5",
            "OntapVolumeType": "RW"
        },
        "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-
abcde0123456789f/fsvol-abc012def3456789a",
        "VolumeId": "fsvol-abc012def3456789a",
        "VolumeType": "ONTAP"
    }
}
```

设置卷的最小冷却天数（ONTAP CLI）

使用 `volume modify` ONTAP CLI 命令为现有卷设置最小冷却天数。有关更多信息，请参阅 NetApp ONTAP 文档中心`volume modify`中的。

1. 要访问 ONTAP CLI，请运行以下命令在 Amazon FSx for NetApp ONTAP 文件系统或 SVM 的管理端口上建立 SSH 会话。将 *`management_endpoint_ip`* 替换为文件系统管理端口的 IP 地址。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   有关更多信息，请参阅 使用 ONTAP CLI 管理文件系统。

2. 使用以下命令进入 ONTAP CLI 高级模式。

   ```
   FSx::> set adv

   Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```

3. 使用以下命令来更改卷的分层最小冷却天数，同时替换以下值：

   - 将 *`svm_name`* 替换为卷创建时所用 SVM 的名称。
   - 将 *`vol_name`* 替换为要设置冷却天数的卷的名称。
   - 将 *`cooling_days`* 替换为所需的 2-183 之间的整数。

   ```
   FSx::> volume modify -vserver svm_name -volume vol_name -tiering-minimum-cooling-
   days cooling_days
   ```

   请求成功后，系统会如下响应。

   ```
   Volume modify successful on volume vol_name of Vserver svm_name.
   ```

更新卷的云检索策略

使用 ONTAP CLI 命令 `volume modify` 为现有卷设置云检索策略。有关更多信息，请参阅 NetApp ONTAP 文档中心`volume modify`中的。

设置卷的云检索策略（ONTAP CLI）

1. 要访问 ONTAP CLI，请运行以下命令在 Amazon FSx for NetApp ONTAP 文件系统或 SVM 的管理端口上建立 SSH 会话。将 *management_endpoint_ip* 替换为文件系统管理端口的 IP 地址。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   有关更多信息，请参阅 使用 ONTAP CLI 管理文件系统。

2. 使用以下命令进入 ONTAP CLI 高级模式。

   ```
   FSx::> set adv

   Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```

3. 使用以下命令设置卷的云检索策略，同时替换以下值：

   - 将 *svm_name* 替换为卷创建时所用 SVM 的名称。
   - 将 *vol_name* 替换为要设置云检索策略的卷的名称。
   - 将 *retrieval_policy* 替换为所需的值，即 default、on-read、never 或 promote。

   ```
   FSx::> volume modify -vserver svm_name -volume vol_name -cloud-retrieval-
   policy retrieval_policy
   ```

   请求成功后，系统会如下响应。

   ```
   Volume modify successful on volume vol_name of Vserver svm_name.
   ```

更新卷上文件的数量上限

FSx 对于 ONTAP，当可用信息节点或文件指针的数量用完时，卷可能会耗尽文件容量。

增加卷上文件的数量上限（ONTAP CLI）

您可以使用 `volume modify` ONTAP CLI 命令来增加卷上文件的数量上限。有关更多信息，请参阅 NetApp ONTAP 文档中心中的 volume modify。

1. 要访问 ONTAP CLI，请运行以下命令在 Amazon FSx for NetApp ONTAP 文件系统或 SVM 的管理端口上建立 SSH 会话。将 *management_endpoint_ip* 替换为文件系统管理端口的 IP 地址。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   有关更多信息，请参阅 使用 ONTAP CLI 管理文件系统。

2. 根据您的使用案例执行以下某种操作。将 *svm_name* 和 *vol_name* 替换为您自己的值。

   - 要将卷配置为始终具有最大数量的可用文件（索引节点），请执行以下操作：

     1. 使用以下命令在 ONTAP CLI 中进入高级模式。

        ```
        ::> set adv
        ```

     2. 运行此命令后，您将看到此输出。输入 y 以继续。

        ```
        Warning: These advanced commands are potentially dangerous; use them only
         when
        directed to do so by NetApp personnel.
        Do you want to continue? {y|n}: y
        ```

     3. 输入以下命令，以便在卷上始终使用最大数量的文件：

        ```
        ::> volume modify -vserver svm_name -volume vol_name -files-set-maximum true
        ```

   - 要使用 *max_number_files* = (current_size_of_volume) × (1 file ÷ 4 KiB) 手动指定卷上允许的文件总数（最大可能值为 20 亿），请使用以下命令：

     ```
     ::> volume modify -vserver svm_name -volume vol_name -files max_number_files
     ```

监控卷存储容量

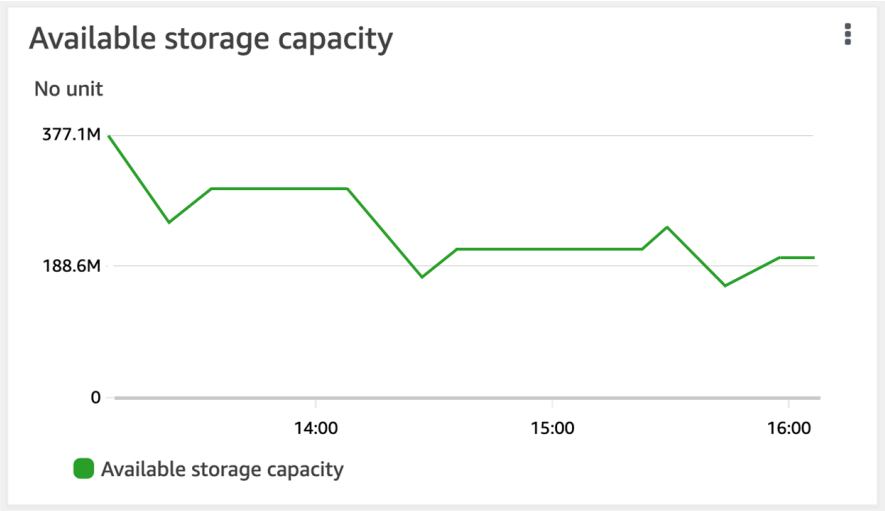
您可以在 AWS 管理控制台、 AWS CLI和 NetApp ONTAP CLI 中查看卷的可用存储空间及其存储分布。

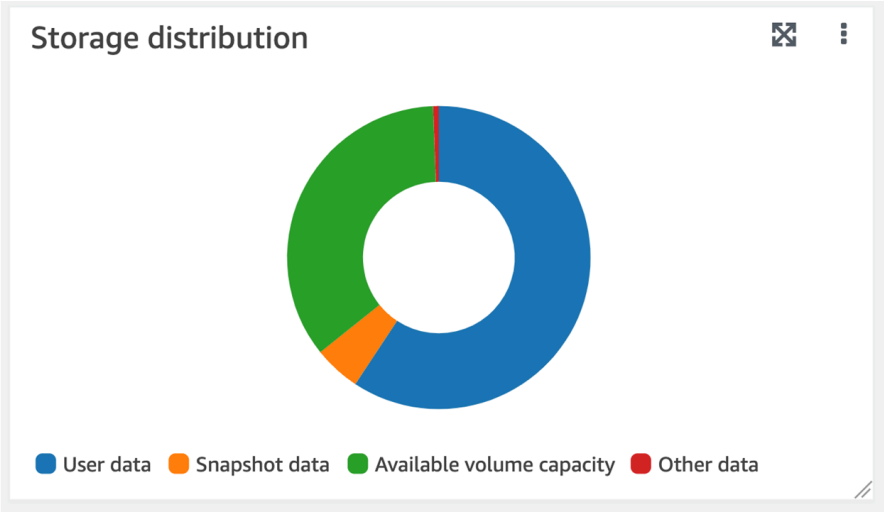
监控卷的存储容量（控制台）

可用存储图表显示一段时间内卷上的可用存储容量。存储分配图表显示卷的存储容量目前在 4 个类别中的分配情况：

- 用户数据
- 快照数据
- 可用卷容量
- 其他数据

1. 打开 Amazon FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 在左侧导航栏中选择卷，然后选择您要查看其存储容量信息的 ONTAP 卷。卷详细信息页面会显示。
3. 在第二个面板中，选择监控选项卡。可用存储和存储分配图表与其他几个图表一起显示。





监控卷的存储容量（ONTAP CLI）

您可以使用 `volume show-space` ONTAP CLI 命令来监控卷存储容量的消耗情况。有关更多信息，请参阅 NetApp ONTAP 文档中心中的 `volume show-space`。

1. 要访问 ONTAP CLI，请运行以下命令在 Amazon FSx for NetApp ONTAP 文件系统或 SVM 的管理端口上建立 SSH 会话。将 *management_endpoint_ip* 替换为文件系统管理端口的 IP 地址。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   有关更多信息，请参阅 使用 ONTAP CLI 管理文件系统。

2. 发出以下命令，同时替换以下值，从而查看卷的存储容量使用情况：

   - 将 *svm_name* 替换为卷创建时所用 SVM 的名称。
   - 将 *vol_name* 替换为要设置数据分层策略的卷的名称。

   ```
   ::> volume show-space -vserver svm_name -volume vol_name
   ```

   如果命令成功，您将看到类似以下内容的输出：

   ```
   Vserver : svm_name
   Volume  : vol_name
   Feature                                     Used      Used%
   --------------------------------     ----------     ------
   User Data                                140KB         0%
   Filesystem Metadata                    164.4MB         1%
   Inodes                                 10.28MB         0%
   Snapshot Reserve                       563.2MB         5%
   Deduplication                             12KB         0%
   Snapshot Spill                          9.31GB        85%
   Performance Metadata                      668KB         0%

   Total Used                             10.03GB        91%

   Total Physical Used                    10.03GB        91%
   ```

   此命令的输出显示不同类型的数据在此卷上占用的实际空间。它还显示每种数据消耗的总卷容量百分比。在本示例中，`Snapshot Spill` 和 `Snapshot Reserve` 总共消耗 90% 的卷容量。

Snapshot Reserve 显示为存储快照副本而预留的磁盘空间量。如果快照副本的存储空间超过预留空间，则会溢出到文件系统，并且此数量在 Snapshot Spill 下方显示。

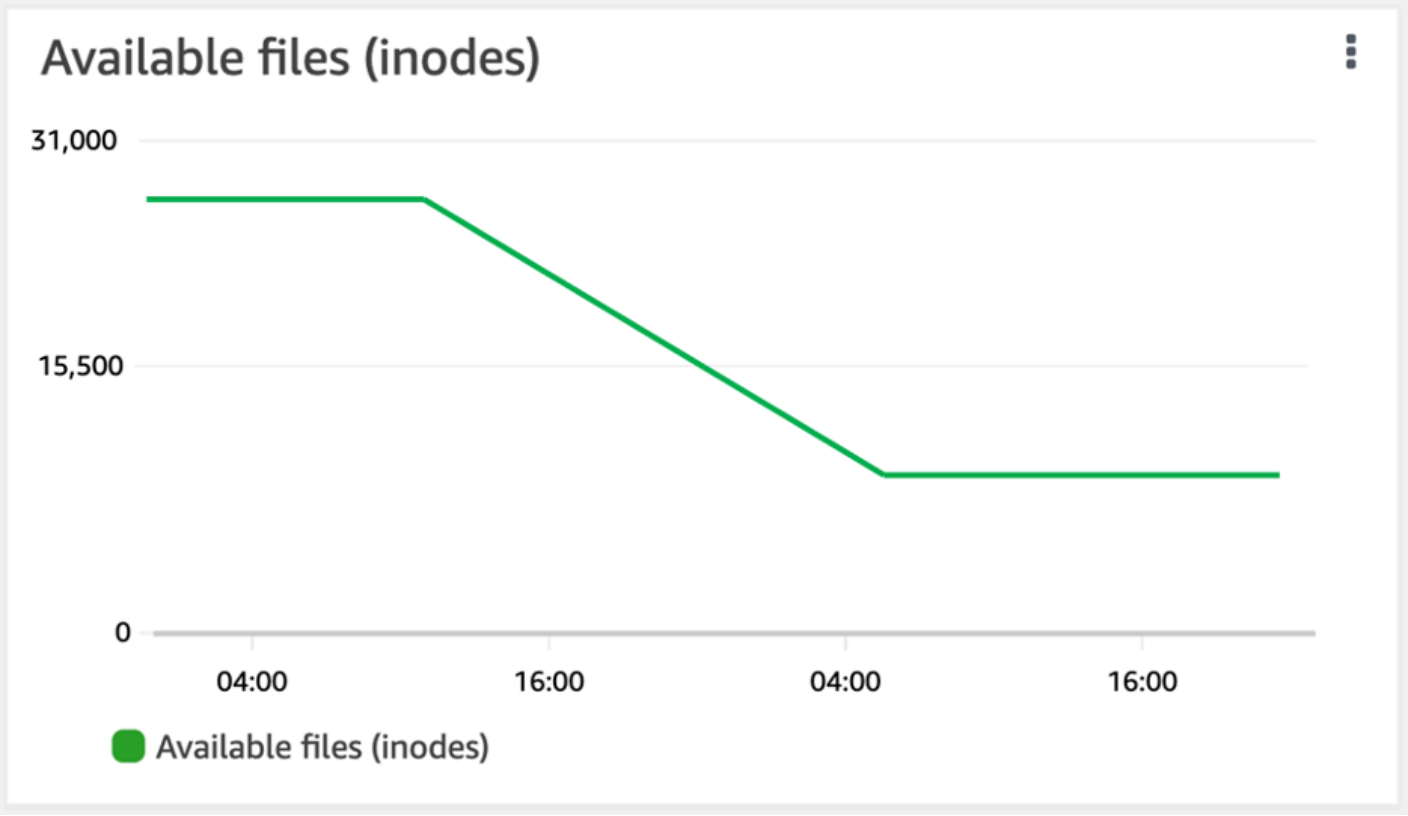
要增加可用空间量，您可以增加卷的大小，也可以删除未使用的快照，如以下过程所示。

对于 FlexVol 卷类型（ONTAP 卷的 FSx 默认卷类型），您也可以启用卷自动调整大小。启用自动调整大小后，卷大小在达到特定阈值时会自动增加。您还可以禁用自动快照。以下部分将介绍这两个功能。

监控卷的文件容量

您可以使用以下任一方法来查看允许的文件数量上限和卷上已用文件的数量。

- CloudWatch 交易量指标FilesCapacity和FilesUsed.
- 在 Amazon FSx 控制台中，导航至卷的 “监控” 选项卡中的 “可用文件 (inode)” 图表。下图显示了一段时间内卷上减少的可用文件（索引节点）。



管理 FSx for ONTAP 文件系统

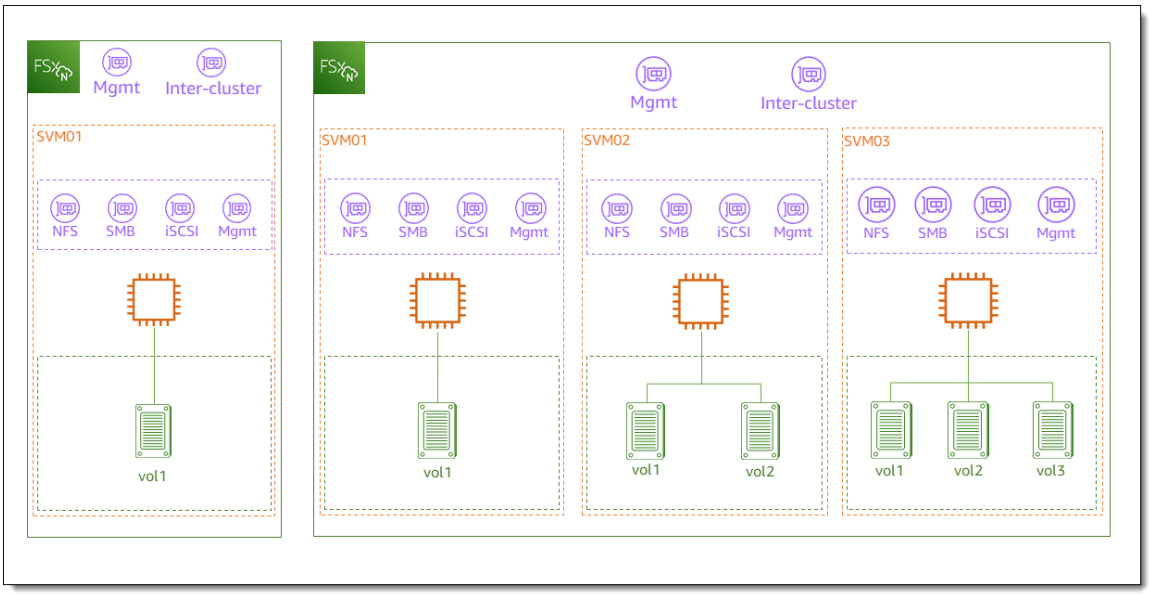
文件系统是主要 Amazon FSx 资源，类似于本地 ONTAP 集群。您可以为文件系统指定固态硬盘（SSD）存储容量和吞吐能力，然后选择用于创建文件系统的虚拟私有云（VPC）。每个文件系统都有一个管理端点，您可以使用该端点通过 ONTAP CLI 或 REST API 管理资源和数据。

文件系统资源

适用于 NetApp ONTAP 文件系统的 Amazon FSx 由以下主要资源组成：

- 文件系统本身的物理硬件包括文件服务器和存储介质。
- 一个或多个高可用性 (HA) 文件服务器对，用于托管您的存储虚拟机 (SVM)。 First-generation 文件系统和 Multi-AZ 第二代文件系统有一对 HA，第二代 Single-AZ 文件系统最多有 12 个 HA 对。每个 HA 对都有一个称为“聚合”的存储池。所有 HA 对的聚合集构成了 SSD 存储层。
- 一个或多个 SVM，托管文件系统卷，并拥有自己的凭证和访问管理。
- 一个或多个卷，虚拟组织数据并由客户端挂载。

下图显示了第一代具有一个 HA 对的 FSx for ONTAP 文件系统的架构及其主要资源之间的关系。左边的 FSx for ONTAP 文件系统是最简单的文件系统，只有一个 SVM 和一个卷。右边的文件系统有多个 SVM，其中一些 SVM 有多个卷。文件系统和 SVM 都有多个管理端点，SVM 也有数据访问端点。



在创建 FSx for ONTAP 文件系统时，您需要定义以下属性：

- 部署类型-文件系统的部署类型（Multi-AZ 或 Single-AZ）。 Single-AZ 文件系统可以复制您的数据，并在单个可用区内提供自动故障切换。 First-generation Single-AZ 文件系统支持一个 HA 对。 Second-generation Single-AZ 文件系统最多支持 12 个 HA 对。 Multi-AZ 文件系统还可以复制您的数据，并支持在同一可用区内的多个可用区之间进行故障转移，从而提高弹性。 AWS 区域 First-generation 和第二代 Multi-AZ 文件系统都支持一个 HA 对。

  > **Note**
  >
  > 创建文件系统之后无法更改其部署类型。如果要更改部署类型（例如，从 Single-AZ 1 移至 Single-AZ 2），则可以备份数据并将其还原到新的文件系统上。您还可以使用 NetApp SnapMirror、 AWS DataSync或第三方数据复制工具来迁移数据。有关更多信息，请参阅使用 FSx 迁移到 ONTAP NetApp SnapMirror和使用 FSx 迁移到 ONTAP AWS DataSync。

- 存储容量 — 这是固态硬盘的存储量，第一代文件系统最多 192 太字节 (TiB)，第二代文件系统高达 512 TiB，第二代文件 Multi-AZ 系统最高 1 PiB (PiB)。 Single-AZ
- SSD IOPS - 默认情况下，每 GB 的 SSD 存储包括三个 SSD IOPS（不超过文件系统配置支持的最大值）。您可以根据需要选择配置额外的 SSD IOPS。
- 吞吐能力 – 文件服务器可以持续提供数据的速度。
- 网络 – 您的文件系统创建的管理和数据访问端点 VPC 和子网。对于 Multi-AZ 文件系统，您还可以定义 IP 地址范围和路由表。
- 加密-用于加密文件系统静态数据的 AWS Key Management Service (AWS KMS) 密钥。
- 管理访问 – 您可以为 `fsxadmin`用户指定密码。您可以使用 NetApp ONTAP CLI 和 REST API 使用此用户来管理文件系统。

您可以使用 ONTAP CLI 或 REST AP NetApp I 管理 ONTAP 文件系统的 FSx。您还可以在 Amazon FSx 文件系统与其他 ONTAP 部署（包括另一个 Amazon FSx 文件系统）之间 SnapVault 建立 SnapMirror 或建立关系。每个 ONTAP 文件系统的 FSx 都有以下文件系统端点，用于访问应用程序：NetApp

- 管理 — 使用此端点通过安全外壳 (SSH) 访问 NetApp ONTAP CLI，或者在文件系统中使用 NetApp ONTAP REST API。
- 群集间-使用设置复制 NetApp SnapMirror 或使用缓存时，请使用此端点。 NetApp FlexCache

有关更多信息，请参阅使用 NetApp 应用程序管理 FSx for ONTAP 资源和使用 NetApp SnapMirror 复制您的数据。

创建文件系统

本节介绍如何使用亚马逊 FSx 控制台或亚马逊 FSx API 为 ONTAP 文件系统创建 FSx。 AWS CLI您可以在自己拥有的虚拟私有云 (VPC) 中创建文件系统，也可以在其他 AWS 账户 人与您共享的 VPC 中创建文件系统。在您参与的 VPC 中创建 Multi-AZ 文件系统时，需要考虑一些注意事项。本主题将讨论这些注意事项。

默认情况下，从 Amazon FSx 控制台创建新文件系统时，Amazon FSx 会自动创建一个包含单个存储虚拟机（SVM）和一个卷的文件系统，允许 Linux 实例通过网络文件系统（NFS）协议快速访问数据。创建文件系统时，您可以选择将 SVM 加入 Active Directory，以允许 Windows 和 macOS 客户端通过服务器消息块（SMB）协议进行访问。创建文件系统后，您可以根据需要创建更多 SVM 和卷。

创建文件系统（控制台）

此过程使用标准创建创建选项，利用您根据需要自定义的配置创建 FSx for ONTAP 文件系统。有关使用快速创建创建选项快速创建具有一组默认配置参数的文件系统的信息，请参阅创建适用于 NetApp ONTAP 文件系统的亚马逊 FSx。

1. 打开 Amazon FSx 控制台，网址为。https://console.aws.amazon.com/fsx/
2. 在控制面板中，选择创建文件系统。
3. 在 “选择文件系统类型” 页面上，在 “文件系统选项” 中，选择 “适用于 NetApp ONTAP 的 Amazon FSx”，然后选择 “下一步”。
4. 在创建方法部分中，选择标准创建。
5. 在文件系统详细信息部分提供以下信息：

   - 在文件系统名称 – 可选部分，输入文件系统的名称。命名文件系统能让您更轻松地进行查找和管理。您最多可以使用 256 个 Unicode 字母、空格和数字以及这些特殊字符：+ - = . _ : /
   - 对于部署类型，请选择 Multi-AZ Single-AZ 2 、2、Multi-AZ 1 或 Single-AZ 1。
     - Multi-AZ文件系统可以复制您的数据，并支持在同一个可用区内跨多个可用区进行故障转移 AWS 区域。 Multi-AZ 1 是适用于 ONTAP 文件系统的第一代 FSx。 Multi-AZ 2 是第二代文件系统。它们都支持一个高可用性（HA）对。
     - Single-AZ文件系统可以复制您的数据，并在单个可用区内提供自动故障切换。 Single-AZ 1 是适用于 ONTAP 文件系统的第一代 FSx，支持一个 HA 对。 Single-AZ 2 是第二代文件系统，最多支持 12 个 HA 对。有关更多信息，请参阅 管理高可用性（HA）对。

       有关部署类型的更多信息，请参阅 可用性、持久性和部署选项。

> **Note**
>
> 创建文件系统之后无法更改其部署类型。如果要更改部署类型（例如，从 Single-AZ 1 移至 Single-AZ 2），则可以备份数据并将其还原到新的文件系统上。您还可以使用 NetApp SnapMirror、 AWS DataSync或第三方数据复制工具来迁移数据。有关更多信息，请参阅使用 FSx 迁移到 ONTAP NetApp SnapMirror和使用 FSx 迁移到 ONTAP AWS DataSync。

- 对于 SSD 存储容量，请输入文件系统的存储容量，以吉字节（GiB）为单位。输入 1,024–1,048,576 GiB 内的任意整数（最多 1 太字节 [Pib]）。

  创建文件系统后，您可以根据需要随时增加存储容量。有关更多信息，请参阅 管理存储容量。

- 对于预调配 SSD IOPS，您有两个为文件系统预调配 IOPS 数量的选项：
  - 如果您希望 Amazon FSx 自动为 SSD 存储配置为 3 IOPS/GiB，请选择自动（默认）。
  - 选择User-provisioned是否要指定 IOPS 数。每个文件系统最多可以预置 20 万 SSD IOPS。

> **Note**
>
> 创建文件系统后，您可以增加预调配的 SSD IOPS。请记住，即使在预置更多 SSD IOPS 时，您的文件系统可以达到的最大 SSD IOPS 水平也取决于文件系统的吞吐能力。有关更多信息，请参阅吞吐能力对性能的影响和管理存储容量。

- 对于吞吐能力，可以使用以下两个选项来确定单位为每秒兆字节（MBps）的吞吐能力：
  - 如果希望 Amazon FSx 根据您选择的存储容量自动选择吞吐能力，请选择建议的吞吐能力。
  - 如果要指定吞吐能力，请选择指定的吞吐能力。如果选择此选项，则会出现吞吐能力下拉列表，其内容根据您选择的部署类型进行填充。您还可以选择 HA 对的数量（最多 12 个）。有关更多信息，请参阅 管理高可用性（HA）对。

  吞吐能力是托管文件系统的文件服务器可以持续提供数据的速度。有关更多信息，请参阅 适用于 ONTAP 性能的 Amazon FS NetApp x。

6. 在联网部分中，提供以下信息：

- 对于虚拟私有云（VPC），请选择要与文件系统关联的 VPC。
- 对于VPC 安全组，您可以选择要与文件系统的网络接口关联的 VPC 安全组。如果没有指定，Amazon FSx 会将 VPC 的默认安全组与您的文件系统相关联。

- （Multi-AZ 仅限）对于首选子网，请从可用子网列表中选择任意值。同时为备用文件服务器选择备用子网。
- （Single-AZ 仅限）对于子网，请从可用子网列表中选择任意值。
- （Multi-AZ 仅限）对于 VPC 路由表，请指定 VPC 路由表以创建文件系统的终端节点。选择与客户端所在子网关联的所有 VPC 路由表。默认情况下，Amazon FSx 会选择 VPC 的默认路由表。有关更多信息，请参阅 从部署 VPC 外部访问数据。

> **Note**
>
> Amazon FSx 使用基于标签的身份验证来管理 Multi-AZ 文件系统的这些路由表。这些路由表标有 `Key: AmazonFSx; Value: ManagedByAmazonFSx`。使用为 ONTAP Multi-AZ 文件系统创建 FSx 时， CloudFormation 我们建议您手动添加标签。`Key: AmazonFSx; Value: ManagedByAmazonFSx`

- 对于网络类型，请选择 IPv4（仅支持 IPv4）或 Dual-stack（同时支持 IPv4 和 IPv6）。可随时更改现有文件系统的网络类型。有关更多信息，请参阅 更改网络类型。

> **Note**
>
> 如果您打算为使用双堆栈模式的 ONTAP 文件系统创建一个 FSx，则必须先为您的 VPC 和子网分配 Amazon-provided IPv6 CIDR 块。有关更多信息，请参阅《Amazon Virtual Private Cloud 用户指南》中的为 VPC 添加 IPv6 支持。

- （Multi-AZ 仅限）端点 IPv4 地址范围指定创建用于访问文件系统的端点的 IPv4 地址范围。

  端点 IPv4 地址范围有三个选项：

  - 未从 VPC 分配 IPv4 地址范围：Amazon FSx 从 VPC 的主要 CIDR 范围中选择最后 64 个 IP 地址作为文件系统的端点 IPv4 地址范围。如果您多次选择此选项，则将在多个文件系统间共享此范围。

> **Note**
>
> 如果子网正在使用 VPC 主要 CIDR 范围中最后 64 个 IP 地址中的任何一个，则此选项将显示为灰色。在这种情况下，您仍然可以通过选择输入 IP 地址范围选项来选择 VPC 内的地址范围（即不在主要 CIDR 范围末尾的范围或不在 VPC 辅助 CIDR 中的范围）。

- V@@ PC 之外的浮动 IPv4 地址范围 — 亚马逊 FSx 选择 198.19.x。 0/24 具有相同 VPC 和路由表的任何其他文件系统尚未使用的地址范围。
- 输入 IPv4 地址范围：您可以提供自己选择的 CIDR 范围。只要不与任何子网重叠，您选择的 IPv4 地址范围可以在 VPC 的 IP 地址范围内，也可以在 VPC 的 IP 地址范围外。

> **Note**
>
> 请勿选择任何属于以下 CIDR 范围的范围，因为它们与 FSx for ONTAP 不兼容：
>
> - 0.0.0。 0/8
> - 127.0.0。 0/8
> - 198.19.0。 0/20
> - 224.0.0。 0/4
> - 240.0.0。 0/4
> - 255.255.255。 255/32

- （Multi-AZ 仅限双栈）端点 IPv6 地址范围指定了创建用于访问文件系统的端点的 IPv6 地址范围。端点 IPv6 地址范围有两个选项：
  - 未从 VPC 分配 IPv6 地址范围：Amazon FSx 从 VPC 的 IPv6 CIDR 范围中选择可用的 1024 个 IPv6 地址块作为文件系统的端点 IPv6 地址范围。
  - 输入 IPv6 地址范围：您可以提供自己选择的 IPv6 CIDR 范围。只要不与任何子网重叠，您选择的 IPv6 地址范围可以在 VPC 的 IPv6 地址范围内，也可以在 VPC 的 IPv6 地址范围外。

7. 在加密部分，对于加密密钥，选择 AWS Key Management Service （AWS KMS）加密密钥以保护文件系统上的静态数据。
8. 在文件系统管理密码中，输入 `fsxadmin` 用户的安全密码。确认密码。

   您可以通过 ONTAP CLI 和 REST API，使用 `fsxadmin` 用户来管理文件系统。有关 `fsxadmin` 用户的更多信息，请参阅使用 ONTAP CLI 管理文件系统。
9. 在默认存储虚拟机配置部分中，提供以下信息：

   - 在存储虚拟机名称字段中，填写存储虚拟机的名称。最多可以使用 47 个字母数字字符，以及下划线（_）特殊字符。
   - 对于 SVM 管理密码，您可以选择指定密码并为 SVM 的 `vsadmin` 用户提供密码。您可以通过 ONTAP CLI 或 REST API，使用 `vsadmin` 用户来管理 SVM。有关 `vsadmin` 用户的更多信息，请参阅使用 ONTAP CLI 管理 SVM。

如果您选择不指定密码（默认），则仍然可以通过 ONTAP CLI 或 REST API 使用文件系统的 `fsxadmin` 用户来管理文件系统，但不能使用 SVM 的 `vsadmin` 用户来执行相同操作。

- 对于卷安全风格，为卷选择 Unix（Linux）或 NTFS。有关更多信息，请参阅 卷安全风格。
- 在 Active Directory 部分，您可以将 Active Directory 加入 SVM。有关更多信息，请参阅 在 FSx ONTAP 中使用微软 Active Directory。

  如果您不想将 SVM 加入 Active Directory，请选择不加入 Active Directory。

  如果要将 SVM 加入自行管理的 Active Directory 域，请选择加入 Active Directory，然后针对 Active Directory 提供以下详细信息：

  - 为 SVM 创建的 Active Directory 计算机对象的 NetBIOS 名称。NetBIOS 名称不超过 15 个字符。
  - Active Directory 的完全限定域名。域名不超过 255 个字符。
  - DNS 服务器 IP 地址：域的域名系统（DNS）服务器的 IPv4 或 IPv6 地址。
  - 服务账户凭证：选择如何提供服务账户凭证：
    - 选项 1： AWS Secrets Manager 秘密 ARN-包含您的 Active Directory 域上服务帐户的用户名和密码的密钥。有关更多信息，请参阅 使用存储活动目录凭证 AWS Secrets Manager。
    - 选项 2：纯文本凭证
      - 服务账户用户名：现有 Microsoft Active Directory 中服务账户的用户名。请勿包含域前缀或后缀。例如，对于 `EXAMPLE\ADMIN`，仅使用 `ADMIN`。
      - 服务账户密码 – 服务账户的密码。
      - 确认密码 – 服务账户的密码。
  - （可选）组织单元（OU）– 文件系统要加入的组织单元的可分辨路径名称。
  - 委托文件系统管理员组 – Active Directory 中可以管理您的文件系统的组的名称。

    如果您正在使用 AWS Managed Microsoft AD，则需要指定一个群组，例如 AWS 委托 FSx 管理员、 AWS 授权管理员或具有向 OU 委派权限的自定义群组。

    如果您要加入自行管理的 AD，请在 AD 中使用该组的名称。默认组为 `Domain Admins`。

10. 在默认卷配置部分，为使用文件系统创建的默认卷提供以下信息：

    - 在卷名字段中，填入卷的名称。最多可以使用 203 个字母数字或下划线（_）字符。

- （只有一个 HA 对的文件系统）对于卷风格，请选择 FlexVol 或 FlexGroup。FlexVol 卷是通用卷，其大小最高可达 300 太字节（TiB）。FlexGroup 卷专为高性能工作负载而设计，其大小最高可达 20PiB。
- 对于卷大小，请为 FlexVol 卷输入一个介于 20 - 314572800 兆字节（MiB）之间的任意整数，或为 FlexGroup 卷的每个 HA 对输入一个介于 800 千兆字节（GiB）- 2400TiB 之间的整数。例如，一个具有 12 个 HA 对的文件系统的最小卷大小为 9,600 GiB，最大卷大小为 20,480 TiB。
- 对于卷类型，选择 Read-Write (RW) 创建可读写卷，或选择 “数据保护” (DP) 创建只读卷，可用作NetAppSnapMirror或SnapVault关系的目标。有关更多信息，请参阅 卷类型。
- 在连接路径中，输入文件系统中用于挂载此卷的位置。该名称必须包含一个前导正斜杠，例如 `/vol3`。
- 在存储效率中选择已启用来启用 ONTAP 存储效率功能（重复数据删除、压缩和紧凑处理）。有关更多信息，请参阅 存储效率。
- 在快照策略中选择用于此卷的快照策略。有关快照策略的更多信息，请参阅快照策略。

  如果选择自定义策略，则必须在 custom-policy 字段中指定策略名称。必须是已存在于 SVM 或文件系统中的自定义策略。您可以通过 ONTAP CLI 或 REST API 创建自定义快照策略。有关更多信息，请参阅《NetApp ONTAP 产品文档》中的创建快照策略。

11. 在默认卷存储分层部分的容量池分层策略中，选择用于此卷的存储池分层策略，该策略可以是自动（默认）、仅快照、全部或无。有关容量池分层策略的更多信息，请参阅卷分层策略。

    对于分层策略冷却期，如果您已将存储分层设置为 `Auto` 和 `Snapshot-only` 策略之一，则有效值为 2–183 天。卷的分层策略冷却周期定义了将未被访问的数据标记为“冷”并移动到容量池存储之前的天数。

12. 在 “默认卷 SnapLock 配置” 部分中，在 “SnapLock配置” 中选择 “启用” 和 “禁用”。有关配置 SnapLock Compliance 卷或 SnapLock Enterprise 卷的更多信息，请参阅 了解 SnapLock Compliance 和 了解 SnapLock Enterprise。有关 SnapLock的更多信息，请参阅使用 SnapLock 保护您的数据。
13. 在备份和维护 – 可选中，您可以设置以下选项：

    - 对于每日自动备份，请为每日自动备份选择已启用。默认情况下，此选项处于启用状态。
    - 对于每日自动备份时段，以协调世界时（UTC）设置您希望每日自动备份时段开始的时间。时段为从该指定时间开始的 30 分钟。此时段不能与每周维护备份时段重叠。
    - 对于自动备份保留期，请将要保留自动备份的期限设置为 1–90 天。

- 对于每周维护时段，您可以设置希望维护时段在一周中开始的时间。第 1 天是星期一，第 2 天是星期二，依此类推。时段为从该指定时间开始的 30 分钟。此时段不能与每日自动备份时段重叠。

14. 对于标签 – 可选，您可以输入键和值以将标签添加到您的文件系统。标签是区分大小写的键值对，能够帮助您管理、筛选和搜索文件系统。

    选择下一步。

15. 检查创建文件系统页面上显示的文件系统配置。注意，创建文件系统后可以修改的文件系统设置，以供参考。

16. 选择创建文件系统。

创建文件系统（CLI）

- 要为 ONTAP 文件系统创建 FSx，请使用 create-file-system CLI 命令（或等效的 CreateFileSystemAPI 操作），如以下示例所示。

> **Note**
>
> 创建文件系统之后无法更改其部署类型。如果要更改部署类型（例如，从 Single-AZ 1 移至 Single-AZ 2），则可以备份数据并将其还原到新的文件系统上。您还可以使用 NetApp SnapMirror、 AWS DataSync或第三方数据复制工具来迁移数据。有关更多信息，请参阅使用 FSx 迁移到 ONTAP NetApp SnapMirror和使用 FSx 迁移到 ONTAP AWS DataSync。

```
aws fsx create-file-system \
    --file-system-type ONTAP \
    --storage-capacity 1024 \
    --storage-type SSD \
    --security-group-ids security-group-id \

    --subnet-ids subnet-abcdef1234567890b subnet-abcdef1234567890c \
    --ontap-configuration DeploymentType=MULTI_AZ_1,
        ThroughputCapacity=512,PreferredSubnetId=subnet-abcdef1234567890b
```

在成功创建文件系统后，Amazon FSx 以 JSON 格式返回文件系统描述，如以下示例所示。

```
{
  "FileSystem": {
    "OwnerId": "111122223333",
    "CreationTime": 1625066825.306,
    "FileSystemId": "fs-0123456789abcdef0",
    "FileSystemType": "ONTAP",
    "Lifecycle": "CREATING",
    "StorageCapacity": 1024,
    "StorageType": "SSD",
    "VpcId": "vpc-11223344556677aab",
    "SubnetIds": [
      "subnet-abcdef1234567890b",
      "subnet-abcdef1234567890c"
    ],
    "KmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
    "ResourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/
fs-0123456789abcdef0",
    "Tags": [],
    "OntapConfiguration": {
      "DeploymentType": "MULTI_AZ_HA_1",
      "EndpointIpAddressRange": "198.19.0.0/24",
      "Endpoints": {
        "Management": {
          "DnsName": "management.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com"
        },
        "Intercluster": {
          "DnsName": "intercluster.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com"
        }
      },
      "DiskIopsConfiguration": {
                "Mode": "AUTOMATIC",
                "Iops": 3072
      },
      "PreferredSubnetId": "subnet-abcdef1234567890b",
      "RouteTableIds": [
        "rtb-abcdef1234567890e",
        "rtb-abcd1234ef567890b"
      ],
      "ThroughputCapacity": 512,
      "WeeklyMaintenanceStartTime": "4:10:00"
    }
  }
```

```
}
```

> **Note**
>
> 与在控制台中创建文件系统的过程不同，`create-file-system` CLI 命令和 `CreateFileSystem` API 操作不会创建默认 SVM 和卷。要创建 SVM，请参阅创建存储虚拟机（SVM）；要创建卷，请参阅创建卷。

在共享子网中创建 FSx for ONTAP 文件系统

VPC 共享允许多 AWS 账户 人将资源创建到共享的、集中管理的虚拟私有云 (VPC) 中。在此模型中，拥有 VPC 的账户（所有者）与属于同一组织的其他账户（参与者）共享一个或多个子网。 AWS Organizations

参与者账户可以在所有者账户与其共享的 VPC 子网中为 ONTAP Single-AZ 和 Multi-AZ 文件系统创建 FSx。要让参与者账户创建 Multi-AZ 文件系统，所有者账户还需要授予 Amazon FSx 代表参与者账户修改共享子网中路由表的权限。有关更多信息，请参阅 管理 Multi-AZ 文件系统的共享 VPC 支持。

> **Note**
>
> 参与者账户有责任与 VPC 拥有者协调，防止创建任何与参与者文件系统的 VPC 内 CIDR 重叠的后续 VPC 子网。如果子网确实重叠，则通向文件系统的流量可能会中断。

共享子网要求和注意事项

在共享子网中创建 FSx for ONTAP 文件系统时，请注意以下几点：

- VPC 子网的拥有者必须与参与者账户共享一个子网，该账户才能在其中创建 FSx for ONTAP 集群。
- 您不能使用 VPC 的默认安全组启动资源，因为此安全组属于拥有者。此外，参与者账户无法使用其他参与者或拥有者拥有的安全组启动资源。
- 在共享子网中，参与者和拥有者分别控制各自账户中的安全组。账户拥有者可以看到参与者创建的安全组，但不能对其执行任何操作。如果账户拥有者想要删除或修改安全组，则创建安全组的参与者必须执行该操作。
- 参与者帐户可以查看、创建、修改和删除所有者帐户与其共享的子网中的 Single-AZ 文件系统及其关联资源。

- 参与者帐户可以创建、查看、修改和删除所有者帐户与其共享的子网中的 Multi-AZ 文件系统及其关联资源。此外，拥有者账户还必须向 Amazon FSx 服务授予代表参与者账户在共享子网中修改路由表的权限。有关更多信息，请参阅 管理 Multi-AZ 文件系统的共享 VPC 支持。
- 共享 VPC 拥有者无法查看、修改或删除参与者在共享子网中创建的资源。这是对每个账户具有不同访问权限的 VPC 资源的补充。有关更多信息，请参阅 Amazon VPC 用户指南中的拥有者和参与者的责任和权限。

有关更多信息，请参阅《Amazon VPC 用户指南》中的与其他账户共享 VPC。

共享 VPC 子网时

与将在共享子网中创建 FSx for ONTAP 文件系统的参与者账户共享子网时，需要执行以下操作：

- VPC 所有者需要使用安全 AWS Resource Access Manager 地与其他人共享 VPC 和子网。 AWS 账户有关更多信息，请参阅《 AWS Resource Access Manager 用户指南》中的共享 AWS 资源。
- VPC 拥有者需要与参与者账户共享一个或多个 VPC。有关更多信息，请参阅《Amazon Virtual Private Cloud 用户指南》中的与其他账户共享 VPC。
- 要使参与者账户为 ONTAP Multi-AZ 文件系统创建 FSx，VPC 所有者还必须向 Amazon FSx 服务授予代表参与者账户在共享子网中创建和修改路由表的权限。这是因为 ONTAP Multi-AZ 文件系统的 FSx 使用浮动 IP 地址，因此在故障转移事件期间，连接的客户端可以在首选文件服务器和备用文件服务器之间无缝切换。发生失效转移事件时，Amazon FSx 会更新与文件系统关联的所有路由表中的所有路由，使其指向当前处于活动状态的文件服务器。

管理 Multi-AZ 文件系统的共享 VPC 支持

所有者账户可以管理参与者账户是否可以在所有者使用、和 API 与参与者共享的 VPC 子网中为 ONTAP 文件系统创建 Multi-AZ FSx AWS 管理控制台 AWS CLI，如以下各节所述。

管理 Multi-AZ 文件系统的 VPC 共享（控制台）

打开 Amazon FSx 控制台，网址为。https://console.aws.amazon.com/fsx/

1. 在导航窗格中，选择设置。
2. 在 “设置” 页面上找到Multi-AZ 共享 VPC 设置。
    - 要为您共享的 VPC 子网中的 Multi-AZ 文件系统启用 VPC 共享，请选择启用参与者账户的路由表更新。

- 要对您拥有的所有 VPC 中的 Multi-AZ 文件系统禁用 VPC 共享，请选择禁用参与者账户的路由表更新。此时将显示确认屏幕。

> **Important**
>
> 我们强烈建议先删除参与者在共享 VPC 中创建 Multi-AZ 的文件系统，然后再禁用此功能。禁用此功能后，这些文件系统将进入 `MISCONFIGURED` 状态且面临不可用的风险。

3. 输入 **`confirm`** 并选择确认禁用此功能。

管理 Multi-AZ 文件系统的 VPC 共享 (AWS CLI)

1. 要查看 Multi-AZ VPC 共享的当前设置，请使用 d escribe-shared-vpc-config uration CLI 命令或等效的 API 命令，如下所示 DescribeSharedVpcConfiguration：

```
$ aws fsx describe-shared-vpc-configuration
```

服务对成功请求的响应如下：

```
{
    "EnableFsxRouteTableUpdatesFromParticipantAccounts": "false"
}
```

2. 要管理 Multi-AZ 共享 VPC 配置，请使用 up date-shared-vpc-configuration CLI 命令或等效的 API 命令。UpdateSharedVpcConfiguration以下示例为 Multi-AZ 文件系统启用 VPC 共享。

```
$ aws fsx update-shared-vpc-configuration --enable-fsx-route-table-updates-from-participant-accounts true
```

服务对成功请求的响应如下：

```
{
    "EnableFsxRouteTableUpdatesFromParticipantAccounts": "true"
}
```

3. 要禁用此功能，可将 `EnableFsxRouteTableUpdatesFromParticipantAccounts` 设置为 `false`，如以下示例所示。

```
$ aws fsx update-shared-vpc-configuration --enable-fsx-route-table-updates-from-participant-accounts false
```

服务对成功请求的响应如下：

```
{
    "EnableFsxRouteTableUpdatesFromParticipantAccounts": "false"
}
```

更新文件系统

本主题介绍您可以更新现有文件系统的哪些属性，并提供使用 Amazon FSx 控制台和 CLI 进行操作的过程。您可以使用 Amazon FSx 控制台和 API 更新以下 FSx for ONTAP 文件系统属性： AWS CLI

- 每日自动备份。开启或关闭每日自动备份，修改备份时段和备份保留期。有关更多信息，请参阅 每日自动备份。
- 每周维护时段。设置 Amazon FSx 执行文件系统维护和更新在星期几的什么时间发生。有关更多信息，请参阅 使用 Amazon FSx 维护时段进行性能优化。
- 文件系统管理密码。更改文件系统 `fsxadmin` 用户的密码。您可以通过 ONTAP CLI 和 REST API，使用 `fsxadmin` 用户来管理文件系统。有关 `fsxadmin` 用户的更多信息，请参阅使用 ONTAP CLI 管理文件系统。
- Amazon VPC 路由表。使用适用于 ONTAP 文件系统的 Multi-AZ FSx，用于通过 NFS 或 SMB 访问数据的终端节点以及用于访问 ONTAP CLI、API 和 NetApp 控制台的管理终端节点使用与文件系统关联的 Amazon VPC 路由表中的浮动 IP 地址。您可以将您创建的新路由表与现有 Multi-AZ 文件系统相关联，这样您就可以配置哪些客户端可以访问您的数据，即使您的网络不断发展。您也可以解除（删除）现有路由表与文件系统的关联。

> **Note**
>
> Amazon FSx 使用基于标签的身份验证来管理 Multi-AZ 文件系统的 VPC 路由表。这些路由表标有 `Key: AmazonFSx; Value: ManagedByAmazonFSx`。使用为 ONTAP Multi-AZ 文件系统创建或更新 FSx 时， CloudFormation 我们建议您手动添加标签。`Key: AmazonFSx; Value: ManagedByAmazonFSx`

更新文件系统（控制台）

以下过程提供了有关如何使用 AWS 管理控制台更新现有 FSx for ONTAP 文件系统的说明。

更新每日自动备份

1. 打开 Amazon FSx 控制台，网址为。https://console.aws.amazon.com/fsx/
2. 要显示文件系统详细信息页面，请在左侧导航窗格中选择文件系统，然后选择要更新的 FSx for ONTAP 文件系统。
3. 在页面上的第二个面板中选择备份选项卡。
4. 选择更新。
5. 修改此文件系统的每日自动备份设置。
6. 选择 保存 以保存您的更改。

更新每周维护时段

1. 打开 Amazon FSx 控制台，网址为。https://console.aws.amazon.com/fsx/
2. 要显示文件系统详细信息页面，请在左侧导航窗格中选择文件系统，然后选择要更新的 FSx for ONTAP 文件系统。
3. 在页面上的第二个面板中选择管理选项卡。
4. 在维护窗格中，选择更新。
5. 修改此文件系统每周维护时段的时间。
6. 选择 保存 以保存您的更改。

更改文件系统管理密码

1. 打开 Amazon FSx 控制台，网址为。https://console.aws.amazon.com/fsx/
2. 要显示文件系统详细信息页面，请在左侧导航窗格中选择文件系统，然后选择要更新的 FSx for ONTAP 文件系统。
3. 选择管理选项卡。
4. 在 ONTAP 管理窗格中，选择 ONTAP 管理员密码下的更新。
5. 在更新 ONTAP 管理员凭证对话框的 ONTAP 管理密码字段中输入新密码。
6. 使用确认密码字段确认密码。

7. 单击更新凭证以保存您的更改。

> **Note**
>
> 如果收到表示新密码不符合密码要求的错误消息，可以使用 `security login role config show` ONTAP CLI 命令查看文件系统中的密码要求设置。有关更多信息（包括有关如何更改密码设置的说明），请参阅 更新 fsxadmin #####败。

更新 Multi-AZ 文件系统上的 VPC 路由表

1. 打开 Amazon FSx 控制台，网址为。https://console.aws.amazon.com/fsx/
2. 要显示文件系统详细信息页面，请在左侧导航窗格中选择文件系统，然后选择要更新的 FSx for ONTAP 文件系统。
3. 对于操作，选择更新文件系统 > 更新路由表。或者，在网络和安全面板中，选择文件系统的路由表旁边的管理。
4. 在管理路由表对话框中，执行下列操作之一：
   - 要关联新的 VPC 路由表，请从关联新路由表下拉列表中选择一个路由表，然后选择关联。
   - 要取消关联现有 VPC 路由表，请从当前路由表窗格中选择一个路由表，然后选择取消关联。
5. 选择关闭。

更新文件系统（CLI）

以下过程说明了有关如何使用 AWS CLI更新现有 FSx for ONTAP 文件系统。

1. 要更新适用于 ONTAP 文件系统的 FSx 的配置，请使用 update-file-system CLI 命令（或等效的 UpdateFileSystemAPI 操作），如以下示例所示。

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --ontap-configuration
 AutomaticBackupRetentionDays=30,DailyAutomaticBackupStartTime=01:00, \
      WeeklyMaintenanceStartTime=1:01:30,AddRouteTableIds=rtb-0123abcd, \
      FsxAdminPassword=new-fsx-admin-password
```

2. 要禁用每日自动备份，可将 AutomaticBackupRetentionDays 属性设置为 0。将其设置为 0 将禁用自动备份，并删除文件系统卷的所有现有自动备份。

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --ontap-configuration AutomaticBackupRetentionDays=0
```

管理高可用性（HA）对

每个 FSx for ONTAP 文件系统由一个或多个高可用性（HA）对的文件服务器提供支持，这些服务器采用活动-备用配置。在此配置中，首选文件服务器主动提供流量，第二个文件服务器在活动服务器不可用时进行接管。FSx for ONTAP 第一代文件系统由一个 HA 对提供支持，可提供高达 4 GBps 的吞吐能力和 16 万的 SSD IOPS。适用于 ONTAP 第二代 Multi-AZ 文件系统的 FSx 也由一个 HA 对提供支持，它们可提供高达 6 Gbps 的吞吐容量和 200,000 个固态硬盘 IOPS。适用于 ONTAP 第二代 Single-AZ 文件系统的 FSx 由多达 12 个 HA 对提供支持，可提供高达 72 Gbps 的吞吐容量和 2,400,000 个固态硬盘 IOPS（每对 HA 有 6 Gbps 的吞吐容量和 200,000 个固态硬盘 IOPS）。

从 Amazon FSx 控制台创建文件系统时，Amazon FSx 会根据您需要的 SSD 存储建议应使用的 HA 对数。您也可以根据工作负载和性能要求手动选择 HA 对数。如果您的文件系统需要高达 6 GBps 的吞吐能力和 20 万的 SSD IOP，我们建议使用单个 HA 对；如果您的工作负载需要更高级别的性能可扩展性，我们建议使用多个 HA 对。

每个 HA 对都有一个聚合，这是一组逻辑物理磁盘。

> **Note**
>
> 您可以将 HA 对添加到第二代 Single-AZ 文件系统。有关更多信息，请参阅 添加高可用性（HA）对。否则，您可以使用SnapMirror、或通过将数据从备份恢复到新的文件系统来在文件系统（具有不同 HA 对）之间迁移数据。 AWS DataSync

添加高可用性（HA）对

适用于 ONTAP 文件系统的 FSx 由一对或多个 HA 文件服务器组成。 First-generation 文件系统和第二代 Multi-AZ 文件系统支持一个 HA 对，而第二代 Single-AZ 文件系统最多支持 12 个 HA 对。您还可以在创建第二代 Single-AZ 文件系统后添加更多 HA 对（最多 12 个）。添加 HA 对不具有破坏性，通常只需要几分钟即可完成。

向文件系统添加 HA 对时，请考虑以下几点：

- 向文件系统添加 HA 对会引入采用自有存储（或聚合）的新文件服务器。新的 HA 对与文件系统现有的 HA 对具有相同的吞吐能力和存储容量。例如，假设文件系统有两个 HA 对，总吞吐能力为 12GBps，SSD 存储空间为 2 太字节（TiB）。如果添加一个新的 HA 对，则文件系统将拥有 18 GBps 的吞吐能力和 3 TiB 的 SSD 存储空间。
- 要从新 HA 对增加的性能中受益，您需要将部分现有卷迁移至新的 HA 对，然后重新挂载客户端进行连接。有关更多信息，请参阅 跨 HA 对平衡工作负载。
- 在添加 HA 对或正在对添加 HA 对进行更新时，您无法修改文件系统的吞吐能力、SSD 存储容量或预置 SSD IOPS。
- 添加 HA 对后无法将其删除。如果您暂时需要更高的性能（假设您的文件系统没有达到最高吞吐能力），我们建议扩展文件系统的吞吐能力。这可以增加文件系统现有 HA 对的吞吐能力。
- iSCSI 协议适用于拥有六个或更少的高可用性对（HA 对）的文件系统。该 NVMe/TCP 协议适用于具有六个或更少 HA 对的第二代文件系统。有关更多信息，请参阅 访问您的 fo FSx r ONTAP 数据。
- 向文件系统添加新的 HA 对时，默认为新的文件系统节点启用 NVMe 缓存。对于高吞吐量的工作负载，我们建议将其禁用。有关更多信息，请参阅 管理 NVMe 缓存。

添加 HA 对

1. 打开 Amazon FSx 控制台，网址为。https://console.aws.amazon.com/fsx/
2. 要显示文件系统详细信息页面，请在左侧导航窗格中选择文件系统，然后选择要更新的 FSx for ONTAP 文件系统。
3. 在摘要面板上，对于 HA 对的数量，选择更新。
4. 从 HA 对下拉列表中，选择要添加到文件系统的 HA 对数。
5. 选择更新按钮。

添加 HA 对后，必须重新平衡现有数据，以确保在文件系统的 HA 对中 I/O 保持均匀分布。有关更多信息，请参阅 跨 HA 对平衡工作负载。

跨 HA 对平衡工作负载

如果您的文件系统具有多个高可用性 (HA) 对，则其吞吐量和存储将分布在每个 HA 对中。 FSx for ONTAP 会在将文件写入文件系统时自动平衡文件，但添加高可用性对后，工作负载数据和 I/O 工作负载数据将不再平衡。此外，在极少数情况下，您的工作负载数据 I/O 可能会在文件系统的现有 HA 对之间变得不平衡，这可能会影响工作负载的整体性能。如果工作负载不平衡，则可以在文件系统的每个 HA 对（及其相应的文件服务器和聚合，即构成主存储层的存储池）之间进行重新平衡。

主题

主存储利用率平衡

文件系统的主存储容量在各个 HA 中之间平均分配给称为聚合的存储池中。每个 HA 对都有一个聚合。我们建议将主存储层的平均利用率持续保持在不高于 80% 的水平。对于具有多个 HA 对的文件系统，我们建议将每个聚合的平均利用率保持在 80% 以下。

保持 80% 的利用率可确保为新的传入数据预留可用空间，并为可能临时占用聚合上可用空间的维护操作保持合理的开销。

如果发现聚合不平衡，可以增加文件系统的主存储容量（相应地增加每个聚合的存储容量），或者也可以在聚合之间移动卷。有关更多信息，请参阅 在聚合之间移动卷。

文件服务器和磁盘性能利用率不平衡

文件系统的总体性能（例如网络吞吐量、文件服务器到磁盘的吞吐量和 IOPS 以及磁盘 IOPS）平均分配给文件系统的 HA 对。对于各种性能限制，我们建议将平均利用率持续保持在 50% 以下（最大峰值利用率低于 80%），这既适用于文件系统文件服务器资源在所有 HA 对中的总体利用率，也适用于每个文件服务器的利用率。

如果发现文件服务器性能利用率不平衡，工作负载不平衡的文件服务器的持续利用率超过 80%，则可以使用 ONTAP CLI 和 REST API 进一步诊断性能不平衡的原因并进行修复。下表列出了可能的不平衡指标以及进行进一步诊断的后续步骤。

如果文件系统...	则...
文件服务器磁盘吞吐量或文件服务器磁盘 IOPS 不平衡	您可能会在高可用性对子集（包含大量正在访问的数据的卷子集）上遇到 I/O 热点，这可能会限制工作负载的整体性能，因为它在高可用性对子集上存在瓶颈。对于各个高利用率文件服务器，请检查利用率最高的卷，查看聚合中哪些卷的活动最多。有关此过程的更多信息，请参阅重新平衡卷。

如果文件系统...	则...
网络吞吐量不平衡，但文件服务器磁盘吞吐量、文件服务器磁盘 IOPS 或磁盘 IOPS 未出现不平衡	数据在 HA 对之间均匀分布，但客户端分布不均匀。对于网络吞吐量利用率较高的文件服务器，请检查各个文件服务器的主要客户端，然后通过从这些客户端上卸载任何卷，并在不同 HA 对上挂载至不同的端点来重新平衡这些客户端。有关此过程的更多信息，请参阅重新平衡客户端。

将 CloudWatch 维度映射到 ONTAP CLI 和 REST API 资源

您的第二代文件系统具有带`FileServer`或`Aggregate`维度的 Amazon CloudWatch 指标。为了进一步诊断不平衡情况，需要将这些维度值映射到 ONTAP CLI 或 REST API 中的特定文件服务器（或节点）和聚合。

- 对于文件服务器，各个文件服务器名称均映射到 ONTAP 中的文件服务器（或节点）名称（例如 `FsxId01234567890abcdef-01`）。奇数文件服务器为首选文件服务器（也就是说，除非文件系统已失效转移至辅助文件服务器，否则将由这些服务器提供流量），而偶数文件服务器为辅助文件服务器（也就是说，它们仅在伙伴服务器不可用时提供流量）。因此，辅助文件服务器的利用率通常低于首选文件服务器。
- 对于聚合，各个聚合名称均映射到 ONTAP 中的聚合（例如 `aggr1`）。每个 HA 对都有一个聚合，这意味着聚合 `aggr1` 由 HA 对中的文件服务器 `FsxId01234567890abcdef-01`（活动文件服务器）和 `FsxId01234567890abcdef-02`（辅助文件服务器）共享，聚合 `aggr2` 由文件服务器 `FsxId01234567890abcdef-03` 和 `FsxId01234567890abcdef-04` 共享，依此类推。

可以使用 ONTAP CLI 查看所有聚合和文件服务器之间的映射。

1. 要通过 SSH 登录文件系统的 NetApp ONTAP CLI，请按照《Amazon for NetApp ONTAP 用户指南》中记录的步骤 FSx 进行操作。使用 NetApp ONTAP CLI

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. 使用 storage aggregate show 命令，并指定 `-fields node` 参数。

   ```
   ::> storage aggregate show -fields node
   aggregate                      node
   ------------------------------ -------------------------
   aggr1                          FsxId01234567890abcdef-01
   aggr2                          FsxId01234567890abcdef-03
   ```

```
aggr3                              FsxId01234567890abcdef-05
aggr4                              FsxId01234567890abcdef-07
aggr5                              FsxId01234567890abcdef-09
aggr6                              FsxId01234567890abcdef-11
6 entries were displayed.
```

重新平衡客户端

添加 HA 对后，或者如果文件服务器之间出现 I/O 不平衡（特别是网络吞吐量利用率），则可以重新平衡客户端。如果在添加 HA 对后要重新平衡客户端，可以跳至 重新挂载客户端。否则，应先确定要移动的高流量客户端，以便重新平衡工作负载 I/O。

如果您遇到文件服务器之间 I/O 不平衡的问题（特别是在网络吞吐量利用率方面），则可能是导致 I/O 客户端过高的原因。要识别高流量客户端，应使用 ONTAP CLI。

识别高流量客户端

1. 要通过 SSH 登录文件系统的 NetApp ONTAP CLI，请按照《Amazon for NetApp ONTAP 用户指南》中记录的步骤 FSx 进行操作。使用 NetApp ONTAP CLI

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. 要查看流量最高的客户端，应使用 statistics top client show ONTAP CLI 命令。您可以选择指定 -node 参数，从而仅查看特定文件服务器的主要客户端。如果要诊断特定文件服务器的不平衡问题，应使用 -node 参数，并将 node_name 替换为文件服务器的名称（例如，FsxId01234567890abcdef-01）。

   您可以选择添加 -interval 参数，提供输出各报告之前的测量间隔（单位为秒）。延长间隔（例如，延长至最长 300 秒）可以为每个卷的流量提供时间更长的样本。默认值为 5（秒）。

   ```
   ::> statistics top client show -node FsxId01234567890abcdef-01 [-interval [5,300]]
   ```

   在输出中，主要客户端按其 IP 地址和端口显示。

   ```
                                                    *Total     Total
              Client   Vserver          Node           Ops     (Bps)
   ------------------ --------- ------------------------- ------ ---------
    172.17.236.53:938 svm01     FsxId01234567890abcdef-01   2143 140443648
   172.17.236.160:898 svm02     FsxId01234567890abcdef-01    812  53215232
   ```

重新挂载客户端

- 可以将客户端重新平衡到其他 HA 对。为此，请从客户端卸载该卷，然后使用 SVM 端 NFS/SMB 点的 DNS 名称重新挂载该卷，这将返回一个与随机 HA 对相对应的随机端点。

  我们建议重复使用 DNS 名称，但您可以明确选择特定客户端挂载的 HA 对。为确保将客户端挂载到不同的端点，您可以改为指定一个与大流量文件服务器的对应端点 IP 地址不同的 IP 地址。您可以使用以下命令进行这项操作：

  ```
  ::> network interface show -vserver svm_name -lif nfs_smb_management* -fields
   address,curr-node
  vserver   lif                  address      curr-node
  --------- -------------------- ------------ -------------------------
  svm01 nfs_smb_management_1 172.31.15.89 FsxId01234567890abcdef-01
  svm01 nfs_smb_management_3 172.31.8.112 FsxId01234567890abcdef-03
  2 entries were displayed.
  ```

  根据 `statistics top client show` 命令的示例输出可知，客户端 `172.17.236.53` 正在向 `FsxId01234567890abcdef-01` 发送大量流量。`network interface show` 命令的输出表明这是地址 `172.31.15.89`。要挂载到不同的端点，请选择其他任何地址（在本例中，其他唯一地址为 `172.31.8.112`，对应于 `FsxId01234567890abcdef-03`）。

重新平衡卷

如果您的卷或聚合之间出现 I/O 不平衡的情况，则可以重新平衡交易量，以便在各卷之间重新分配 I/O 流量。

> **Note**
>
> 如果您的聚合之间存在存储利用率不平衡的问题，则通常不会对性能产生任何影响，除非高利用率与 I/O 不平衡相结合。虽然您可以在聚合之间移动卷以平衡存储利用率，但我们建议您仅在看到性能影响时才移动卷，因为如果您不考虑考虑要移动的每个卷的 I/O 驱动器，则移动卷可能会对性能产生不利影响。

1. 要通过 SSH 登录文件系统的 NetApp ONTAP CLI，请按照《Amazon for NetApp ONTAP 用户指南》中记录的步骤 FSx 进行操作。使用 NetApp ONTAP CLI

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. 使用 statistics volume show ONTAP CLI 命令并进行以下更改，查看给定聚合的最高流量：

   - *aggregate_name*替换为聚合的名称（例如，aggr1）。
   - 您可以选择添加 -interval 参数，提供输出各报告之前的测量间隔（单位为秒）。延长间隔（例如，延长至最长 300 秒）可以为每个卷的流量提供时间更长的样本。默认值为 5（秒）。

```
::> statistics volume show -aggregate aggregate_name -sort-key total_ops [-interval
 [5,300]]
```

   根据所选择的时间间隔，显示数据最多可能需要 5 分钟。该命令显示聚合中的所有卷，以及当前流向各个聚合的流量。

```
                           *Total Read Write Other      Read Write Latency
    Volume Vserver Aggregate    Ops  Ops   Ops   Ops     (Bps) (Bps)    (us)
---------- ------- --------- ------ ---- ----- ----- --------- ----- -------
vol1__0007    svm1     aggr1   4078 4078     0     0 267255808     0    1092
vol1__0005    svm1     aggr1   4078 4078     0     0 267255808     0    1086
vol1__0003    svm1     aggr1   4077 4077     0     0 267223040     0    1086
vol1__0001    svm1     aggr1   4077 4077     0     0 267239424     0    1087
vol1__0008    svm1     aggr2   2314 2314     0     0 151650304     0    1112
vol1__0006    svm1     aggr2   2144 2144     0     0 140509184     0    1104
vol1__0002    svm1     aggr2   2183 2183     0     0 143065088     0    1106
vol1__0004    svm1     aggr2   2183 2183     0     0 143065088     0    1103
```

   卷统计数据按组件显示（例如，vol1__0015 是 FlexGroup vol1 的第 15 个组件）。从示例输出中可以看出，aggr1 组件的利用率比 aggr2 组件更高。要平衡聚合之间的流量，可以在聚合之间移动组成卷，以使流量分布更为均匀。

3. 如果添加了新的 HA 对，应将现有卷移至新的聚合。有关更多信息，请参阅 在聚合之间移动卷。

管理 NVMe 缓存

第二代文件系统默认启用 NVMe 缓存。如果第二代文件系统的工作负载吞吐量大，则可以禁用 NVMe 缓存以提高性能。以下过程介绍如何启用、禁用和验证文件系统的 NVMe 缓存。

管理 NVMe 缓存

1. 通过 SSH 连接到 ONTAP 文件系统。有关更多信息，请参阅 the section called “使用 NetApp ONTAP CLI”。

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. 使用 system node external-cache modify ONTAP CLI 命令。选择 **true** 启用 NVMe 缓存，或选择 **false** 将其禁用。

```
::> system node external-cache modify -node * -is-enabled [true|false]
```

3. 使用 system node external-cache show ONTAP CLI 命令检查 NVMe 缓存是启用还是禁用。

```
::> system node external-cache show -node * -fields is-enabled
```

NVMe 缓存是按节点启用或禁用的。向文件系统添加新的高可用性（HA）对时，每个新节点的默认行为与新文件系统的节点相同。因此，即使现有节点禁用了 NVMe 缓存，文件系统上的任何新节点也将启用 NVMe 缓存。有关更多信息，请参阅 添加高可用性（HA）对。

管理网络类型

创建 FSx for ONTAP 文件系统时，必须指定网络类型，该类型必须为以下选项之一：

- `IPv4` 允许文件系统使用仅互联网协议版本 4（IPv4）进行通信。
- `Dual-stack` 允许文件系统同时使用互联网协议版本 6（IPv6）和 IPv4 进行通信。

您可以随时使用 Amazon FSx 管理控制台、AWS CLI、AWS API 或其中一个 AWS SDK，以更改现有 FSx for ONTAP 文件系统的网络类型。例如，如果您的子网同时支持 IPv4 和 IPv6 寻址，则可以将现有文件系统从仅 IPv4 模式更新为双堆栈模式，也可以将双堆栈文件系统更新为仅 IPv4。

使用双堆栈模式

如果您需要从 IPv6 客户端本地访问和管理 Amazon FSx 文件系统，则应使用双堆栈模式。通过将您的 Amazon FSx 文件系统配置为使用双堆栈寻址，您可以从 IPv6 客户端以及 IPv4 客户端在同一 Amazon VPC、另一个 AWS 账户 的 VPC 或本地网络中访问您的文件数据。例如，借助已配置为使用双堆栈的 Amazon FSx 文件系统，可让现有 IPv4 客户端和新的 IPv6 客户端访问存储在文件系统上的文件数据。

默认情况下，Amazon FSx 和 Amazon VPC 使用 IPv4 寻址协议。因此，作为使用 IPv6 的先决条件，您必须首先为您的 VPC 和子网分配 Amazon 提供的 IPv6 无类域间范围（CIDR）数据块，然后才能

将 IPv6 与 Amazon FSx 文件系统一起使用。有关为 VPC 启用 IPv6 的信息，请参阅《Amazon Virtual Private Cloud 用户指南》中的为 VPC 添加 IPv6 支持。

在为设置为双堆栈模式的 FSx for ONTAP 文件系统创建时，除现有的 IPv4 地址范围外，您还可指定 IPv6 地址范围，用于创建访问该文件系统的端点。默认情况下，Amazon FSx 会从 VPC 的 IPv6 CIDR 范围中选择包含 1024 个 IP 地址的数据块作为文件系统的端点 IPv6 地址范围。

更改网络类型

您可以使用 Amazon FSx 控制台、AWS Command Line Interface（AWS CLI）或 Amazon FSx API 修改文件系统的网络类型。

更改文件系统的网络类型（控制台）

1. 通过以下网址打开 Amazon FSx 控制台：https://console.aws.amazon.com/fsx/。
2. 导航到文件系统，然后选择要为其更改网络类型的 FSx for ONTAP 文件系统。
3. 对于操作，选择更新网络类型。或者，在网络和安全面板中，选择文件系统的网络类型旁边的管理。

   此时将显示更新网络类型窗口。
4. 对于所需的网络类型，选择 IPv4 或双堆栈。
   - 如果选择 `IPv4`，则无需作进一步配置。
   - 如果选择 `Dual-stack`，则指定文件系统端点将使用的 IPv6 地址范围：
     - 未从 VPC 分配 IPv6 地址范围：Amazon FSx 从 VPC 的 IPv6 CIDR 范围中选择可用的 /118 个 IP 地址作为文件系统的端点 IPv6 地址范围。
     - 输入 IPv6 地址范围：您可以提供自己选择的 IPv6 CIDR 范围。只要不与任何子网重叠，您选择的 IP 地址范围可以在 VPC 的 IP 地址范围内，也可以在 VPC 的 IP 地址范围外。
5. 选择更新。

修改文件系统的网络类型（CLI）

- 要修改文件系统的网络类型，请使用 CLI 命令 update-file-system（或等效的 UpdateFileSystem API 操作），如下例所示。

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
```

```
    --network-type DUAL
```

监控文件系统详细信息

您可以使用 Amazon FSx 控制台、API 和支持的软件开发工具包查看适用于 ONTAP 的 FSx 文件系统的详细配置信息。 AWS CLI AWS

查看文件系统详细信息：

- 使用控制台 – 选择一个文件系统，查看该文件系统详细信息页面。摘要面板显示文件系统的 ID、生命周期状态、部署类型、SSD 存储容量、吞吐能力、预调配 IOPS、可用区和创建时间。

  以下选项卡为可以修改的属性提供了详细的配置信息和编辑：

  - 网络和安全：显示以下文件系统管理信息：
    - 默认 Amazon VPC
    - 与 Multi-AZ 文件系统关联的 Amazon VPC 路由表
    - 文件系统的网络类型（IPv4-only 或双栈）
    - 端点 IPv4 或 IPv6 地址范围
    - AWS Key Management Service (AWS KMS) 密钥 ID
  - 监控和性能-显示您创建的 CloudWatch 警报以及以下类别的指标和警告：
    - 摘要：文件系统活动指标的总体摘要
    - 文件系统存储容量
    - 文件服务器和磁盘性能

    有关更多信息，请参阅 使用 Amazon 进行监控 CloudWatch。
  - 管理 - 显示以下文件系统管理信息：
    - 文件系统管理和集群间端点的 DNS 名称和 IP 地址。
    - ONTAP 管理员用户名。
    - 更新 ONTAP 管理员密码的选项。
  - 文件系统的 SVM 列表
  - 文件系统的卷列表
  - 备份设置 - 更改文件系统的每日自动备份设置。
  - 更新 - 显示用户对文件系统配置发起的更新的状态。
  - 标签-查看、编辑、添加、删除标签 Key:Value 对。

- 使用 CLI 或 API — 使用 describe -file-system s CLI 命令或 API 操作。DescribeFileSystems

FSx for ONTAP 文件系统状态

您可以使用 Amazon FSx 控制台、d escribe-file- systems AWS CLI 命令或 API 操作查看 Amazon FSx 文件系统的状态。DescribeFileSystems

文件系统状态	说明
AVAILABLE	文件系统已成功创建并可供使用。
CREATING	Amazon FSx 正在创建新的文件系统。
DELETING	Amazon FSx 正在删除现有文件系统。
MISCONFIGURED	文件系统处于错误配置但可恢复的状态。
FAILED	1. 文件系统故障，且 Amazon FSx 无法恢复。 2. 创建新文件系统时，Amazon FSx 无法再创建新的文件系统。

删除文件系统

您可以使用亚马逊 FSx 控制台、Amazon FSx API 和软件开发工具包删除适用于 ONTAP 文件系统 AWS CLI的 FSx。

删除文件系统：

- 使用控制台 – 按照清理资源中所述的步骤操作。
- 使用 CLI 或 API – 首先删除文件系统上的所有卷和 SVM。然后使用删除文件系统 CLI 命令或 DeleteFileSystemAPI 操作。

管理 FSx ONTAP 存储虚拟机

在 FSx ONTAP 中，卷托管在称为存储虚拟机 (SVMs) 的虚拟文件服务器上。SVM 是独立的文件服务器，拥有自己的管理凭证和端点，用于管理和访问数据。当您访问 ONTAP 中的 FSx 数据时，您的客户端和工作站会使用 SVM 的终端节点（IP 地址）挂载由 SVM 托管的卷、SMB 共享或 iSCSI LUN。

当您使用创建文件系统时，Amazon FSx 会自动在您的文件系统上创建默认 SVM。 AWS 管理控制台您可以随时使用控制台、 AWS CLI或 Amazon FSx API 和在文件系统 SVMs 上创建其他内容 SDKs。您无法 SVMs 使用 ONTAP CLI 或 REST API 进行创建。

你可以加入 Microsoft 活动目录进行文件访问身份验证和授权。 SVMs 有关更多信息，请参阅 在 FSx ONTAP 中使用微软 Active Directory。

SVMs 每个文件系统的最大数量

下表列出了您可以 SVMs 为文件系统创建的最大数量。的最大数量 SVMs 取决于预配置的吞吐容量（以每秒兆字节为单位MBps），也取决于文件系统的网络类型。

高可用性（HA）对	吞吐容量 (MBps)	SVMs 每个文件系统的最大数量（IPv4仅限模式）	SVMs 每个文件系统的最大数量（双栈模式）
1 个 HA 对	128	6	6
	256	6	6
	384	6	6
	512	14	11
	768	6	6
	1024	14	11
	1,536	14	11
	2,048	24	11
	3,072	14	11
	4,096	24	11
	6,144	24	11
2-12 个 HA 对	任何	11	11

主题

创建存储虚拟机（SVM）

您可以使用 AWS 管理控制台、 AWS CLI和 API 创建 FSx 适用于 ONTAP 的 SVM。

SVMs 您可以为文件系统创建的最大数量取决于您的文件系统的部署类型、网络类型和预配置的吞吐容量。有关更多信息，请参阅 SVMs 每个文件系统的最大数量。

SVM 属性

创建 SVM 时，需要定义以下属性：

- 它 FSx 所属的 ONTAP 文件系统。
- Microsoft Active Directory（AD）配置 – 您可以选择性将 SVM 加入自行管理的 AD，对 Windows 和 macOS 客户端进行身份验证和访问控制。有关更多信息，请参阅 在 FSx ONTAP 中使用微软 Active Directory。
- 根卷安全风格：设置根卷安全风格（Unix 或 NTFS），与您在 SVM 中访问数据时使用的客户端类型保持一致。有关更多信息，请参阅 卷安全风格。
- SVM 管理密码 – 您可以选择性地为 SVM 的 `vsadmin` 用户设置密码。有关更多信息，请参阅 使用 ONTAP CLI 管理 SVM。

创建存储虚拟机（控制台）

1. 打开亚马逊 FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 在左侧导航窗格中，选择存储虚拟机。
3. 选择创建新的存储虚拟机。
4. 在文件系统中，选择存储虚拟机创建时使用的文件系统。

5. 在存储虚拟机名称字段中，填写存储虚拟机的名称。最多可以使用 47 个字母数字字符，以及下划线（_）特殊字符。
6. 对于 SVM 管理密码，您可以选择指定密码并为 SVM 的 vsadmin 用户提供密码。您可以通过 ONTAP CLI 或 REST API，使用 vsadmin 用户来管理 SVM。有关 vsadmin 用户的更多信息，请参阅使用 ONTAP CLI 管理 SVM。

   如果您选择不指定密码（默认），则仍然可以通过 ONTAP CLI 或 REST API 使用文件系统的 fsxadmin 用户来管理文件系统，但不能使用 SVM 的 vsadmin 用户来执行相同操作。
7. 对于 Active Directory，有以下选项：

   - 如果您不想将文件系统加入 Active Directory（AD），请选择不加入 Active Directory。
   - 如果您要将 SVM 加入自行管理的 Active Directory 域，请选择加入 Active Directory，然后提供 AD 的以下详细信息。有关更多信息，请参阅 将 SVM 加入自行管理的 Microsoft AD 的先决条件。
     - 为 SVM 创建的 Active Directory 计算机对象的 NetBIOS 名称。NetBIOS 名称不超过 15 个字符。这是 Active Directory 中此 SVM 的名称。
     - Active Directory 域的完全限定域名（FQDN）。FQDN 不能超过 255 个字符。
     - DNS 服务器 IP 地址-您的域的 DNS 服务器的 IPv4 或 IPv6 地址。
     - 服务账户凭证：选择如何提供服务账户凭证：
       - 选项 1： AWS Secrets Manager 秘密 ARN-包含您的 Active Directory 域上服务帐户的用户名和密码的密钥。有关更多信息，请参阅 使用存储活动目录凭证 AWS Secrets Manager。
       - 选项 2：纯文本凭证
         - 服务账户用户名：现有 Microsoft Active Directory 中服务账户的用户名。请勿包含域前缀或后缀。例如，对于 EXAMPLE\ADMIN，仅使用 ADMIN。
         - 服务账户密码 – 服务账户的密码。
         - 确认密码 – 服务账户的密码。
     - （可选）组织单元（OU）– 文件系统要加入的组织单元的可分辨路径名称。
     - 委托的文件系统管理员组 – AD 中可以管理文件系统的组的名称。

       如果您正在使用 AWS Managed Microsoft AD，则必须指定一个群组，例如 AWS 委派 FSx 管理员、 AWS 授权管理员或具有向 OU 委派权限的自定义群组。

       如果您要加入自行管理的 AD，请在 AD 中使用该组的名称。默认组为 Domain Admins。

8. 对于 SVM 根卷安全风格，请根据访问数据的客户端类型选择 SVM 的安全风格。如果您主要使用 Linux 客户端访问数据，请选择 Unix（Linux）；如果您主要使用 Windows 客户端访问数据，请选择 NTFS。有关更多信息，请参阅 卷安全风格。
9. 选择确认以创建存储虚拟机。

您可以访问文件系统详细信息页面，在存储虚拟机窗格的状态列中监控更新进度。当状态为已创建时，存储虚拟机可供使用。

创建存储虚拟机（CLI）

- 要创建 FSx 适用于 ONTAP 存储的虚拟机 (SVM)，请使用 C create-storage-virtual-machineLI 命令（或等效CreateStorageVirtualMachine的 API 操作），如以下示例所示。

```
aws fsx create-storage-virtual-machine \
    --file-system-id fs-0123456789abcdef0 \
    --name svm1 \
    --svm-admin-password password \
    --active-directory-configuration
 SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",FileSystemAd
 \
UserName="FSxService",Password="password", \
   DnsIps=["10.0.1.18"]}',NetBiosName=amznfsx12345
```

成功创建存储虚拟机后，Amazon 以 JSON 格式 FSx 返回其描述，如以下示例所示。

```
{
  "StorageVirtualMachine": {
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
```

```
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.7", "198.19.0.8"]
      }
    },
    "FileSystemId": "fs-0123456789abcdef0",
    "Lifecycle": "CREATING",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/
fs-0123456789abcdef0/svm-abcdef0123456789a",
    "StorageVirtualMachineId": "svm-abcdef0123456789a",
    "Subtype": "default",
    "Tags": [],
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
  }
}
```

更新存储虚拟机（SVM）

您可以使用亚马逊 FSx 控制台和亚马逊 FSx API 更新以下存储虚拟机 (SVM) 配置属性： AWS CLI

- SVM 管理账户密码。

- SVM Active Directory（AD）配置 – 您可以将 SVM 加入 AD，也可以修改已加入 AD 的 SVM 的 AD 配置。有关更多信息，请参阅 管理 SVM Microsoft Active Directory 配置。

更新 SVM 管理员账户凭证（控制台）

1. 打开亚马逊 FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 按如下所示方法选择要更新的 SVM：
   - 在左侧导航窗格中，选择文件系统，然后选择要更新 SVM 的 ONTAP 文件系统。
   - 选择存储虚拟机选项卡。

   –或–
   - 要显示当前版本中所有 SVMs 可用虚拟机的列表 AWS 区域，请 AWS 账户 展开 ONTAP 并选择存储虚拟机。
3. 选择要更新的存储虚拟机。
4. 选择操作 > 更新管理员密码。更新 SVM 管理凭证窗口会显示。
5. 输入 `vsadmin` 用户的新密码并进行确认。
6. 选择更新凭证以保存新密码。

更新 SVM 管理员账户凭证（CLI）

- 要更新 FSx 适用于 ONTAP 的 SVM 的配置，请使用 CL update-storage-virtual-machineI 命令（或等效UpdateStorageVirtualMachine的 API 操作），如以下示例所示。

```
aws fsx update-storage-virtual-machine \
--storage-virtual-machine-id svm-abcdef01234567890 \
--svm-admin-password new-svm-password \
```

成功创建存储虚拟机后，Amazon 以 JSON 格式 FSx 返回其描述，如以下示例所示。

```
{
  "StorageVirtualMachine": {
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
```

```
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.7", "198.19.0.8"]
      }
    },
    "FileSystemId": "fs-0123456789abcdef0",
    "Lifecycle": "CREATING",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/
fs-0123456789abcdef0/svm-abcdef01234567890",
    "StorageVirtualMachineId": "svm-abcdef01234567890",
    "Subtype": "default",
    "Tags": [],
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
  }
}
```

管理 SVM Microsoft Active Directory 配置

你可以将 SVM 加入微软 Active Directory，也可以修改已经加入微软 Active Directory 的 SVM 的微软 Active Directory 配置。 FSx for ONTAP 与集成 AWS Secrets Manager ，可安全地管理您的域加入服务帐户凭据。

更新 SVM Microsoft Active Directory 配置（控制台）

1. 打开亚马逊 FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 按如下所示方法选择要更新的 SVM：
   - 在左侧导航窗格中，选择文件系统，然后选择要更新 SVM 的 ONTAP 文件系统。
   - 选择存储虚拟机选项卡。

   –或–
   - 要显示当前版本中所有 SVMs 可用虚拟机的列表 AWS 区域，请 AWS 账户 展开ONTAP并选择存储虚拟机。
3. 选择要更新的存储虚拟机。
4. 选择操作 > 更新 Microsoft Active Directory 配置。此时将显示更新 Microsoft Active Directory 配置窗口。
5. 对于域加入服务账户凭证，选择在 Secrets Manager 中托管（建议），以使用 Secrets Manager 实现安全的凭证管理。

   > **Note**
   >
   > 使用 Secrets Manager，则无需存储纯文本凭证，并可提供集中式凭证管理。有关更多信息，请参阅 使用存储活动目录凭证 AWS Secrets Manager。
6. 对于密钥，从 Secrets Manager 中选择包含已更新域加入服务账户凭证的现有密钥，或者选择创建新密钥以创建密钥。
7. 根据您的环境需要更新其他 Microsoft Active Directory 配置字段。
8. 选择更新配置以保存更改。

更新 SVM Microsoft Active Directory 配置（CLI）

- 要更新 FSx 适用于 ONTAP 的 SVM 的 Microsoft Active Directory 配置，请使用带有`--active-directory-configuration`参数的 update-storage-virtual-machineCLI 命令，如下例所示。

```
aws fsx update-storage-virtual-machine \
--storage-virtual-machine-id svm-abcdef01234567890 \
--active-directory-configuration DomainJoinServiceAccountSecret=secret-arn
```

审计文件访问

适用于 NetApp ONTAP 的 Amazon FSx 支持审计最终用户对虚拟存储机（SVM）中文件和目录的访问权限。

主题

- 文件访问审计概述
- 设置文件访问审计的任务概览

文件访问审计概述

文件访问审计能让您根据您定义的审计策略记录最终用户对单个文件和目录的访问权限。文件访问审计可以帮助您提高系统的安全性，降低未经授权访问系统数据的风险。文件访问审计可帮助您的组织遵守数据保护要求，尽早发现潜在威胁，并降低数据泄露的风险。

在文件和目录访问中，Amazon FSx 支持记录成功的尝试（例如拥有足够权限的用户成功访问文件）、失败的尝试或两者兼而有之。您还可以随时关闭文件访问审计。

默认情况下，审计事件日志以 EVTX 文件格式存储，允许您使用 Microsoft 事件查看器进行查看。

可以审计的 SMB 访问事件

下表列出了可以审计的 SMB 文件和文件夹访问事件。

事件 ID（EVT/EVTX）	事件	描述	类别
560/4656	打开对象/创建对象	OBJECT ACCESS：打开对象（文件或目录）	文件访问

事件 ID（EVT/EVTX）	事件	描述	类别
563/4659	打开要删除的对象	OBJECT ACCESS：为了删除而请求对象（文件或目录）句柄	文件访问
564/4660	删除对象	OBJECT ACCESS：删除对象（文件或目录）当 Windows 客户端尝试删除对象（文件或目录）时，ONTAP 会生成此事件	文件访问

事件 ID（EVT/EVTX）	事件	描述	类别
567/4663	读取对象/写入对象/获取对象属性/设置对象属性	OBJECT ACCESS：对象访问尝试（读取、写入、获取属性、设置属性）。 **Note** 对于此事件，ONTAP 仅审计对象上的第一个 SMB 读取和第一个 SMB 写入操作（成功或失败）。这样可以防止 ONTAP 在单个客户端打开对象并对同一对象执行多次连续读取或写入操作时创建过多的日志条目。	文件访问
N/A/4664	硬链接	OBJECT ACCESS：尝试创建硬链接	文件访问

事件 ID（EVT/EVTX）	事件	描述	类别
N/A/N/A ONTAP 事件 ID 9999	重命名对象	OBJECT ACCESS：已重命名对象。这是一个 ONTAP 事件。Windows 目前不支持将其作为单一事件。	文件访问
N/A/N/A ONTAP 事件 ID 9998	取消关联对象	OBJECT ACCESS：对象已取消关联。这是一个 ONTAP 事件。Windows 目前不支持将其作为单一事件。	文件访问

可以审计的 NFS 访问事件

以下 NFS 文件和文件夹访问事件可以审计。

- READ
- OPEN
- CLOSE
- READDIR
- WRITE
- SETATTR
- CREATE
- LINK
- OPENATTR
- REMOVE
- GETATTR
- VERIFY
- NVERIFY

- RENAME

设置文件访问审计的任务概览

设置 FSx for ONTAP 以进行文件访问审计涉及以下高级任务：

1. 熟悉文件访问审计要求和注意事项。
2. 在特定 SVM 上创建审计配置。
3. 在该 SVM 上启用审计。
4. 对您的文件和目录配置审计策略。
5. 在 FSx for ONTAP 发出审计事件日志后查看审计事件日志。

任务详细信息可见于以下过程。

对文件系统上要为其启用文件访问审计的任何其他 SVM 重复这些任务。

审计要求

在 SVM 上配置和启用审计之前，您应了解以下要求和注意事项。

- NFS 审计支持指定为 u 类型的审计访问控制条目（ACE），尝试访问对象时，这些条目会生成审计日志条目。对于 NFS 审计，模式位和审计 ACE 之间无映射。将 ACL 转换为模式位时，会跳过审计 ACE。将模式位转换为 ACL 时，不会生成审计 ACE。
- 审计取决于暂存卷中的可用空间。（暂存卷是由 ONTAP 创建的用于存储暂存文件的专用卷，这些文件是单个节点上的中间二进制文件，审计记录在转换为 EVTX 或 XML 文件格式之前存储在这些节点上。）您必须确保在包含已审计卷的聚合中有足够的空间容纳暂存卷。
- 审计取决于存储转换后审计事件日志的目录所在的卷中是否有可用空间。必须确保卷中有足够的空间用于存储事件日志。您可以在创建审计配置时使用 `-rotate-limit` 参数来指定要在审计目录中保留的审计日志数量，这有助于确保卷中有足够的可用空间存放审计日志。

在 SVM 上创建审计配置

在开始审计文件和目录事件之前，必须先在存储虚拟机（SVM）上创建审计配置。创建审计配置之后，您必须在 SVM 上启用。

在使用 `vserver audit create` 命令创建审计配置之前，请确保已创建用作日志目标的目录，且该目录没有符号链接。您可以使用 `-destination` 参数指定目标目录。

您可以创建根据日志大小或计划轮换审计日志的审计配置，如下所示：

- 要根据日志大小轮换审计日志，请使用以下命令：

```
vserver audit create -vserver svm_name -destination path [-format {xml|evtx}] [-
rotate-limit integer] [-rotate-size {integer[KB|MB|GB|TB|PB]}]
```

以下示例为名为 svm1 的 SVM 创建审计配置，使用基于大小的轮换来审计文件操作以及 CIFS（SMB）登录和注销事件（默认）。日志格式为 EVTX（默认），日志存储在 /audit_log 目录中，每次只有一个日志文件（最大 200MB）。

```
vserver audit create -vserver svm1 -destination /audit_log -rotate-size 200MB
```

- 要根据计划轮换审计日志，请使用以下命令：

```
vserver audit create -vserver svm_name -destination path [-format {xml|evtx}]
        [-rotate-limit integer] [-rotate-schedule-month chron_month]
        [-rotate-schedule-dayofweek chron_dayofweek] [-rotate-schedule-
day chron_dayofmonth]
        [-rotate-schedule-hour chron_hour] [-rotate-schedule-minute chron_minute]
```

如果您要配置基于时间的审计日志轮换，则需要 -rotate-schedule-minute 参数。

以下示例使用基于时间的轮换为名为 svm2 的 SVM 创建审计配置。日志格式为 EVTX（默认），审计日志每月轮换，时间为每日中午 12:30。

```
vserver audit create -vserver svm2 -destination /audit_log -rotate-size 200MB  -
rotate-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour 12 -
rotate-schedule-minute 30
```

您可以使用 -format 参数来指定审计日志是以转换后的 EVTX 格式（默认）还是以 XML 文件格式创建。EVTX 格式允许您使用 Microsoft 事件查看器查看日志文件。

默认情况下，要审计的事件类别包括文件访问事件（SMB 和 NFS）、CIFS（SMB）登录和注销事件以及授权策略更改事件。您可以通过 -events 参数更好地控制要记录哪些事件，其格式如下：

```
-events {file-ops|cifs-logon-logoff|cap-staging|file-share|audit-policy-change|user-
account|authorization-policy-change|security-group}
```

例如，使用 `-events file-share` 可以对文件共享事件进行审计。

有关 `vserver audit create` 命令的更多信息，请参阅创建审计配置。

在 SVM 上启用审计

设置审计配置之后，您必须在 SVM 上启用审计。为此，请使用以下命令：

```
vserver audit enable -vserver svm_name
```

例如，使用以下命令启用名为 `svm1` 的 SVM 的审计。

```
vserver audit enable -vserver svm1
```

您可以随时禁用访问审计。例如，使用以下命令禁用名为 `svm4` 的 SVM 的审计。

```
vserver audit disable -vserver svm4
```

禁用审计后，不会删除 SVM 上的审计配置，这意味着您可以随时在该 SVM 上重新启用审计。

配置文件和文件夹审计策略

您需要为要审计用户访问尝试的文件和文件夹配置审计策略。您可以配置审计策略来监控成功和失败的访问尝试。

SMB 和 NFS 两种审计策略均可配置。根据卷的安全样式，SMB 和 NFS 审计策略具有不同的配置要求和审计功能。

NTFS 安全样式文件和目录的审计策略

您可以使用“Windows 安全”选项卡或 ONTAP CLI 配置 NTFS 审计策略。

要配置 NTFS 审计策略（“Windows 安全”选项卡），请执行以下操作：

您可以通过向 NTFS SACL 中添加与 NTFS 安全描述符关联的条目来配置 NTFS 审计策略。然后将安全描述符应用于 NTFS 文件和目录。这些任务由 Windows GUI 自动处理。安全描述符可以包含用于应用文件和文件夹访问权限的自主访问控制列表（DACL）、用于文件和文件夹审计的 SACL，或者同时包含 SACL 和 DACL。

1. 从 Windows 资源管理器的工具菜单中，选择映射网络驱动器。
2. 填写映射网络驱动程序框：

a. 选择驱动器号。

b. 在文件夹框中，键入包含共享的 SMB（CIFS）服务器名称，其中包含要审计的数据和共享的名称。

c. 选择完成。

您选择的驱动器已安装并准备就绪，Windows 资源管理器窗口显示共享中包含的文件和文件夹。

3. 选择要为其启用审计访问的文件或目录。
4. 右键单击文件或目录，然后选择属性。
5. 选择安全性选项卡。
6. 单击高级。
7. 选择审计选项卡。
8. 执行所需的操作：

如果要...	执行以下操作：
为新用户或组设置审计	1. 选择添加。 2. 在输入要选择的对象名称框中，键入要添加的用户或组的名称。 3. 选择确定。
从用户或组中删除审计	1. 在输入要选择的对象名称框中，选择要删除的用户或组。 2. 选择删除。 3. 选择确定。 4. 跳过此过程中的其余步骤。
更改对用户或组的审计	1. 在输入要选择的对象名称框中，选择要更改的用户或组。 2. 选择编辑。 3. 选择确定。

如果要对用户或组设置审计，或者要更改对现有用户或组的审计，则打开**##**的审计条目框。

9. 在应用于框中，选择要如何应用此审计条目。

如果要对单个文件设置审计，则应用于框处于非活动状态，因为它默认为“仅限此对象”。

10. 在访问权限框中，选择要审计的内容，以及是要审计成功的事件、失败的事件还是两者兼而有之。

    - 要审计成功的事件，请选择成功框。
    - 要审计失败的事件，请选择失败框。

    选择需要监控的操作以满足您的安全要求。有关这些可审计事件的更多信息，请参阅 Windows 文档。您可以审计以下事件：

    - 完全控制
    - 遍历文件夹/执行文件
    - 列出文件夹/读取数据
    - 读取属性
    - 读取扩展属性
    - 创建文件/写入数据
    - 创建文件夹/追加数据
    - 写入属性
    - 写入扩展属性
    - 删除子文件夹和文件
    - 删除
    - 读取权限
    - 更改权限
    - 获取所有权
11. 如果您不希望将审计设置传播到原始容器的后续文件和文件夹，请选择仅将这些审计条目应用于此容器中的对象和/或容器框。
12. 选择应用。
13. 添加、删除或编辑审计条目后，选择确定。

    ##的审计条目框关闭。
14. 在审计框中，选择此文件夹的继承设置。仅选择提供符合您安全要求的审计事件的最低级别。

    您可以选择以下任一种密钥：

    - 选择包括此对象父项中可继承的审计条目框。
    - 选择用此对象中的可继承审计条目替换所有子代上的现有可继承审计条目框。

- 两个都选。
- 两个都不选。

如果您在单个文件上设置 SACL，则审计框中不会显示用此对象中的可继承审计条目替换所有子代上的现有可继承审计条目。

15. 选择确定。

要配置 NTFS 审计策略（ONTAP CLI），请执行以下操作：

通过使用 ONTAP CLI，您可以配置 NTFS 审计策略，而无需在 Windows 客户端上使用 SMB 共享连接到数据。

- 您可以使用 vserver security file-directory ntfs sacl add 命令系列来配置 NTFS 审计策略。

例如，以下命令为名为 vs0 的 SVM创建名为 p1 的安全策略。

```
vserver security file-directory policy create -policy-name p1 -vserver vs0
```

然后，以下命令将 p1 安全策略应用于 vs0 SVM。

```
vserver security file-directory apply -vserver vs0 -policy-name p1
```

UNIX 安全样式文件和目录的审计策略

您可以通过向 NFS v4.x ACL（访问控制列表）中添加审计 ACE（访问控制表达式）来配置对 UNIX 安全样式文件和目录的审计。出于安全考虑，这允许您监控某些 NFS 文件和目录访问事件。

> **Note**
>
> 对于 NFS v4.x，自主 ACE 和系统 ACE 都存储在同一 ACL 中。因此，在向现有 ACL 中添加审计 ACE 时必须小心，以免覆盖和丢失现有 ACL。将审计 ACE 添加到现有 ACL 的顺序无关紧要。

要配置 UNIX 审计策略，请执行以下操作：

1. 使用 nfs4_getfacl 或等效命令检索文件或目录的现有 ACL。

2. 附加所需的审计 ACE。
3. 使用 `nfs4_setfacl` 或等效命令将更新后的 ACL 应用于文件或目录。

   此示例使用 `-a` 选项授予用户（名为 `testuser`）读取名为 `file1` 的文件的权限。

   ```
   nfs4_setfacl -a "A::testuser@example.com:R" file1
   ```

查看审计事件日志

您可以查看以 EVTX 或 XML 文件格式保存的审计事件日志。

- EVTX 文件格式 – 您可以使用 Microsoft 事件查看器将转换后的 EVTX 审计事件日志作为保存的文件打开。

  使用事件查看器查看事件日志时，有两个选项可供选择：
  - 一般视图：显示事件记录中所有事件的通用信息。不显示事件记录中特定于事件的数据。您可以使用详细视图来显示特定事件的数据。
  - 详细视图：提供友好视图和 XML 视图。友好视图和 XML 视图既显示所有事件的通用信息，也显示事件记录中特定事件的数据。
- XML 文件格式 – 您可以查看和处理支持 XML 文件格式的第三方应用程序上的 XML 审计事件日志。只要您具有 XML 架构和有关 XML 字段定义的信息，就可以使用 XML 查看工具来查看审计日志。

在工作组中设置 SMB 服务器

如果 Microsoft Active Directory 域基础设施不可用，可在 SVM 的工作组中配置服务器消息块（SMB）服务器，作为将 SVM 加入 Microsoft Active Directory 的替代方案。工作组是使用 SMB 协议的对等联网，且仅包含本地账户和本地组。

将 SMB 服务器设置为工作组成员的过程包括：

- 在存储虚拟机（SVM）上创建 SMB 服务器。
- 创建本地用户和组。
- 将本地用户或组添加为工作组的成员。

请记住，工作组模式下的 SMB 服务器不支持以下 SMB 功能：

- SMB3 见证协议

- SMB3 CA 共享
- 通过 SMB 的 SQL
- 文件夹重定向
- 漫游配置文件
- 组策略对象（GPO）
- 卷快照服务（VSS）

此外，工作组模式下的 SMB 服务器仅支持 NTLM 身份验证，而不支持 Kerberos 身份验证。

以下流程将引导您完成在工作组的 SVM 上设置 SMB 服务器、创建本地账户，以及将这些账户添加到工作组成员资格。您将使用文件系统或 SVM 管理界面中的 NetApp ONTAP CLI 以实施这些流程。有关更多信息，请参阅 使用 NetApp ONTAP CLI。

主题

- 在工作组中创建 SMB 服务器
- 在 SMB 服务器上创建本地用户账户
- 在 SMB 服务器上创建本地组
- 将本地用户添加到本地组

在工作组中创建 SMB 服务器

您可以使用 vserver cifs createONTAP CLI 命令在 SVM 上创建 SMB 服务器，并指定该服务器所属的工作组。

开始前的准备工作

用于提供数据的 SVM 及卷（和接口）必须已配置为允许 SMB 协议。

LIF 必须能够连接到 SVM 上配置的 DNS 服务器。文件系统可能需要 CIFS 许可证，但如果 SMB 服务器仅用于身份验证，则不需要 CIFS 许可证。

在工作组中创建 SMB 服务器

1. 要访问 ONTAP CLI，请运行以下命令，在适用于 NetApp ONTAP 的 Amazon FSx 文件系统或 SVM 的管理端口上建立 SSH 会话。将 *management_endpoint_ip* 替换为文件系统管理端口的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

有关更多信息，请参阅 使用 ONTAP CLI 管理文件系统。

2. 在工作组中创建 SMB 服务器：

```
FSxIdabcde123456::> vserver cifs create -vserver vserver_name -cifs-
server cifs_server_name -workgroup workgroup_name [-comment workgroup_description]
```

以下命令在工作组 workgroup01 中创建 SMB 服务器 smb_server01：

```
FSxIdabcde123456::> vserver cifs create -vserver svm1 -cifs-server SMB_SERVER01 -
workgroup workgroup01
```

如果已连接到 SVM 的管理端口，则无需指定 -vserver。

3. 使用 vserver cifs show 命令验证 SMB 服务器配置。

在以下示例中，命令输出显示在工作组 workgroup01 的 SVM svm1 上创建了名为 smb_server01 的 SMB 服务器：

```
FSxIdabcde123456::> vserver cifs show -vserver svm1

                                          Vserver: svm1
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: workgroup01
                     Fully Qualified Domain Name: -
                             Organizational Unit: -
Default Site Used by LIFs Without Site Membership: -
                                   Workgroup Name: workgroup01
                              Authentication Style: workgroup
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: -
```

在 SMB 服务器上创建本地用户账户

您可以创建本地用户账户，用于授权通过 SMB 连接访问 SVM 中包含的数据。创建 SMB 会话时，也可使用本地用户账户进行身份验证。创建 SVM 时，默认启用本地用户功能。创建本地用户账户时，必须指定用户名，还必须指定要与该账户关联的 SVM。

在 SMB 服务器上创建本地用户账户

1. 使用 vserver cifs users-and-groups local-user create ONTAP CLI 命令创建本地用户：

   ```
   vserver cifs users-and-groups local-user create -vserver svm_name -user-
   name user_name optional_parameters
   ```

   以下可选参数可能有所助益：

   - `-full-name`：用户的全名。
   - `-description`：对本地用户的描述。
   - `-is-account-disabled {true|false}`：指定启用还是禁用用户账户。如果未指定此参数，则默认启用用户账户。

   该命令提示输入本地用户的密码。
2. 输入本地用户的密码，然后确认该密码。
3. 验证用户是否已成功创建：

   ```
   vserver cifs users-and-groups local-user show -vserver svm_name
   ```

以下示例创建本地用户 `SMB_SERVER01\sue`，其全名为 `Sue Chang`，且与 SVM `svm1` 关联：

```
FSxIdabcde123456::> vserver cifs users-and-groups local-user create -vserver svm1
 -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:
```

```
FSxIdabcde123456::> vserver cifs users-and-groups local-user show
Vserver  User Name                  Full Name  Description
-------- -------------------------- ---------- -------------
```

```
svm1     SMB_SERVER01\Administrator            Built-in administrator account
svm1     SMB_SERVER01\sue           Sue Chang
```

在 SMB 服务器上创建本地组

您可以创建本地组，用于授权通过 SMB 连接访问与 SVM 相关联的数据。您还可以分配权限，以定义组成员拥有的用户权限或功能。

创建 SVM 时，默认启用本地组功能。创建本地组时，必须指定组的名称，还必须指定要与该组关联的 SVM。您可以指定包含或不包含本地域名的组名，也可以选择性地为本地组指定描述。您无法将一个本地组添加到另一个本地组。

在 SMB 服务器上创建本地组

1. 使用 vserver cifs users-and-groups local-group create ONTAP CLI 命令创建本地组。

   ```
   vserver cifs users-and-groups local-group create -vserver svm_name -group-
   name group_name [-description local_group_description
   ```

   为本地组添加描述会有所助益。
2. 验证组是否已成功创建：

   ```
   vserver cifs users-and-groups local-group show -vserver svm_name
   ```

以下示例创建与 SVM svm1 关联的本地组 SMB_SERVER01\engineering：

```
FSxIdabcde123456::> vserver cifs users-and-groups local-group create -vserver svm1 -
group-name SMB_SERVER01\engineering
```

```
FSxIdabcde123456::> vserver cifs users-and-groups local-group show -vserver svm1

Vserver          Group Name                   Description
---------------- ---------------------------- ----------------------------
svm1             BUILTIN\Administrators       Built-in Administrators group
svm1             BUILTIN\Backup Operators     Backup Operators group
svm1             BUILTIN\Guests               Built-in Guests group
svm1             BUILTIN\Power Users          Restricted administrative privileges
svm1             BUILTIN\Users                All users
svm1             SMB_SERVER01\engineering
```

将本地用户添加到本地组

您可以通过添加和删除本地或域用户，或添加和删除域组来管理本地组成员资格。如果您需要根据对组设置的访问控制来控制对数据的访问权限，或者您希望用户拥有与该组关联的权限，则此功能非常有用。如果您不再希望本地用户、域用户或域组基于其所属组的成员资格享有访问权限或特权，可将其从该组中移除。

向本地组添加成员时，请注意以下事项：

- 您无法向特殊的所有人组添加用户。
- 您无法将一个本地组添加到另一个本地组。
- 要将域用户或组添加到本地组，ONTAP 必须能够将名称解析为 SID。

从本地组中移除成员时，请注意以下事项：

- 您无法从特殊的所有人组中移除成员。
- 要从本地组中移除成员，ONTAP 必须能够将其名称解析为 SID。

您需要具备 `fsxadmin` 角色才能运行此过程中使用的命令。有关更多信息，请参阅 ONTAP 角色和用户。

管理本地组成员资格

- 使用 vserver cifs users-and-groups local-group add-members 和 vserver cifs users-and-groups local-group remove-members ONTAP CLI 命令，向组添加成员或从组中移除成员。
  - 要向工作组添加成员，请执行以下操作：

    ```
    vserver cifs users-and-groups local-group add-members -vserver svm_name -group-name group_name -member-names name[,...]
    ```

    您可以指定以逗号分隔的本地用户、域用户或域组列表，以添加至指定的本地组。
  - 要查看工作组的成员，请执行以下操作：

    ```
    vserver cifs users-and-groups local-group show-members -vserver svm_name -group-name group_name
    ```
  - 要从工作组中移除成员，请执行以下操作：

```
vserver cifs users-and-groups local-group remove-members -vserver svm_name -
group-name group_name -member-names name[,...]
```

您可以指定以逗号分隔的本地用户、域用户或域组列表，以从指定的本地组中移除。

以下示例将本地用户 SMB_SERVER01\sue 添加到 SVM svm1 上的本地组 SMB_SERVER01\engineering：

```
FSxIdabcde123456::> vserver cifs users-and-groups local-group add-members -vserver svm1
 -group-name SMB_SERVER01\engineering -member-names SMB_SERVER01\sue
```

以下示例将本地用户 SMB_SERVER01\sue 和 SMB_SERVER01\james 从 SVM svm1 上的本地组 SMB_SERVER01\engineering 中移除：

```
FSxIdabcde123456::> vserver cifs users-and-groups local-group remove-
members -vserver svm1 -group-name SMB_SERVER01\engineering -member-names
 SMB_SERVER01\sue,SMB_SERVER01\james
```

以下示例列出本地组 SMB_SERVER01\engineering 的成员：

```
FsxIdabcdef01234::> vserver cifs users-and-groups local-group show-members -
vserver svm_name -group-name group_name

           Vserver: svm1
       Domain Name: SMB_SERVER01
        Group Name: SMB_SERVER01\engineering
       Member Name: SMB_SERVER01\anita
                    SMB_SERVER01\james
                    SMB_SERVER01\liang
```

监控存储虚拟机（SVM）配置详细信息

您可以使用亚马逊 FSx 控制台、和 Amazon FSx API 查看当前位于文件系统中的 ONTAP 存储虚拟机。 FSx AWS CLI

要查看文件系统上的存储虚拟机，请执行以下操作：

- 使用控制台 – 选择一个文件系统，查看其文件系统详细信息页面。要列出文件系统上的所有存储虚拟机，请选择存储虚拟机选项卡，然后选择要查看的存储虚拟机。

- 使用 CLI 或 API-使用 describe-storage-virtual-machinesCLI 命令或 DescribeStorageVirtualMachinesAPI 操作。

  系统响应是您账户 SVMs 中所有内容的完整描述列表 AWS 区域。

删除存储虚拟机（SVM）

您只能使用亚马逊 FSx 控制台、和 API 删除 FSx 适用于 ONTAP 的 AWS CLI SVM。在删除 SVM 之前，您必须先删除 SVM 上附加的所有非根卷。

> **Important**
>
> 您无法使用 NetApp ONTAP CLI 或 API 删除 SVM。

> **Note**
>
> 在删除存储虚拟机之前，请确保没有应用程序正在访问 SVM 中的数据，并且已删除 SVM 上附加的所有非根卷。

删除存储虚拟机（控制台）

1. 打开亚马逊 FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 按以下方式选择要删除的 SVM：
   - 在左侧导航窗格中，选择文件系统，然后选择要删除 SVM 的 ONTAP 文件系统。
   - 选择存储虚拟机选项卡。

     –或–
   - 要显示所有 SVMs 可用虚拟机的列表，请展开 ONTAP 并选择存储虚拟机。

   从列表中选择要删除的 SVM。
3. 在卷选项卡中，查看 SVM 上附加的卷的列表。在删除 SVM 之前，您必须先删除 SVM 上附加的所有非根卷（如果有）。请参阅 删除卷 以了解更多信息。
4. 从操作菜单中选择删除存储虚拟机。
5. 在“删除确认”对话框中，请选择删除存储虚拟机。

删除存储虚拟机（CLI）

- 要删除 FSx 适用于 ONTAP 存储的虚拟机，请使用 delete-storage-virtual-machineCLI 命令（或等效DeleteStorageVirtualMachine的 API 操作），如以下示例所示。

```
aws fsx delete-storage-virtual-machine --storage-virtual-machine-id svm-
abcdef0123456789d
```

管理 FSx ONTAP 卷

for ONTAP 文件系统上的每个存储虚拟机 (SVM) 可以有一个或多个卷。 FSx 卷是文件、目录或 iSCSI 逻辑存储单元的隔离数据容器（LUNs）。卷是精简配置，这意味着它们只会为存储在其中的数据消耗存储容量。

您可以通过网络文件系统 (NFS) 协议、服务器消息块 (SMB) 协议从 Linux、Windows 或 macOS 客户机访问卷，也可以通过创建 iSCSI LUN（共享块存储）通过互联网小型计算机系统接口 (iSCSI) 协议访问卷。 FSx for ONTAP 还支持对同一卷进行多协议访问（并发 NFS 和 SMB 访问）。

您可以使用 AWS 管理控制台、 AWS CLI、Amazon FSx API 或来创建卷NetApp Console。您还可以使用文件系统或 SVM 的管理端点，通过 NetApp ONTAP CLI 或 REST API 来创建、更新和删除卷。

> **Note**
>
> 每个 HA 对可以创建 500 个卷，所有 HA 对最多可以创建 1,000 个卷。 FlexGroup 组成卷计入此限制。默认情况下，每个 FlexGroup 的每个聚合有八个组成卷。

创建卷时，需要定义以下属性：

- 卷风格 - 卷风格可以是 FlexVol，也可以是 FlexGroup。
- 卷名称 - 卷的名称。
- 卷类型 – 卷类型可以是“读写（RW）”或“数据保护（DP）”。DP 卷为只读卷，用作 NetApp SnapMirror 或 SnapVault 关系中的目标卷。
- 卷大小 – 卷可以存储的最大数据量，与存储层无关。
- 连接路径 – SVM 命名空间中挂载卷的位置。
- 存储效率 - 存储效率功能（包括数据紧凑处理、压缩和重复数据删除）可为通用文件共享工作负载节省 65% 的典型存储。

- 卷的安全风格（Unix 或 NTFS）– 决定在授权用户访问卷数据时所使用的权限类型。
- 数据分层 – 分层策略定义要将哪些数据存储在经济高效的容量池层中。
- 分层策略冷却期 - 定义何时将数据标记为“冷”并移至容量池存储。
- 快照策略 – 快照策略定义系统为卷创建快照的方式。您可以从三个预定义的安全策略中选择，也可以使用您使用 ONTAP CLI 或 REST API 创建的自定义策略。
- 将@@ 标签复制到备份 — Amazon FSx 会使用此选项自动将所有标签从您的卷复制到备份中。您可以使用 AWS CLI 或 Amazon FSx API 设置此选项。

主题

卷风格

FSx for ONTAP 提供了两种风格的卷，您可以将其用于不同的目的。您可以使用亚马逊 FSx 控制台 AWS CLI、和 Amazon FSx API 创建 FlexVol 或 FlexGroup 卷。

- FlexVol 卷为拥有一个高可用性（HA）对的文件系统带来了最简单的体验，因此这种卷是具有一个 HA 对的第一代文件系统和第二代文件系统的默认卷风格。FlexVol 卷大小最小为 20 兆字节（MiB），最大为 314,572,800 MiB。
- FlexGroup 卷由多个 FlexVol 组成卷构成，与拥有多个 HA 对的文件系统的 FlexVol 卷相比，这种卷能够提供更高的性能和存储可扩展性。FlexGroup 卷是拥有多个 HA 对的第二代文件系统的默认卷风格。FlexGroup 卷大小最小为每个组件 100 千兆字节（GiB），最大为 20 拍字节（PiB）。

您可以使用 ONTAP CLI 将 FlexVol 风格的卷转换为 FlexGroup 风格，该命令可创建一个包含单个组件的 FlexGroup。但是，我们建议您使用 AWS DataSync 在FlexVol卷和新FlexGroup卷之间移动数据，以确保数据在各FlexGroup's组成部分之间均匀分布。有关更多信息，请参阅 FlexGroup 组件。

> **Note**
>
> 如果要使用 ONTAP CLI 将 FlexVol 卷转换为 FlexGroup 卷，务必确保在转换之前删除 FlexVol 卷的所有备份。ONTAP 不会在转换过程中自动重新平衡数据，因此 FlexGroup 组件之间的数据可能会不平衡。

FlexGroup 组件

一个 FlexGroup 卷由多个组件构成，组件为 FlexVol 卷。默认情况下，ONTAP 会 FSx 为每个 HA 对的FlexGroup卷分配八个成分。

创建 FlexGroup 卷时，其大小在其组件之间平均分配。例如，如果创建一个 800 千兆字节（GB）的 FlexGroup 卷包含八个组件，则每个组件的大小为 100GB。FlexGroup 卷大小可以介于 100 GB 到 20 PiB 之间，但总大小取决于各组件的大小。每个组件的大小最小为 100 GB，最大为 300 TiB。例如，一个 FlexGroup 卷包含八个组件，其大小最小为 800 GB，最大为 20 PiB。

ONTAP 在各个组件之间进行文件级的数据分布。在 FlexGroup 卷的每个组件中，最多可以存储 20 亿个文件。

当更新 FlexGroup 卷的大小时，新大小将均匀分布在现有组件中。

您还可以使用 ONTAP CLI 或 REST API 向 FlexGroup 卷添加更多组件。但是，我们建议仅在需要额外存储容量且所有组件均已达到最大容量（每个组件 300 TiB）时才这么做。添加成分可能会导致数据和 I/O 各成分之间的不平衡。在各组件实现平衡之前，写入吞吐量可能比平衡的 FlexGroup 卷低 5-10%。当向 FlexGroup 卷写入新数据时，ONTAP 会将数据优先分布在新组件中，直到各组件实现平衡。如果确实添加了新的组件，我们建议选择一个偶数，且每个聚合的组件不超过八个。

> **Note**
>
> 如果添加新的组件，则现有快照将成为部分快照；因此，无法使用这些快照将 FlexGroup 卷完全还原到之前的状态。之前的快照无法提供您的FlexGroup卷的完整 point-in-time图像，因为新的成分还不存在。但是，可以使用部分快照恢复单个文件和目录、创建新卷或使用 SnapMirror 进行复制。

卷类型

FSx for ONTAP 提供了两种类型的卷，您可以使用亚马逊 FSx 控制台和亚马逊 FSx API 创建这些卷。AWS CLI

- 大多数情况下使用的是读写（RW）卷。顾名思义，这种卷是可读写的。
- 数据保护（DP）卷为只读卷，用作 NetApp SnapMirror 或 SnapVault 关系的目标。若要迁移或保护单个卷的数据，应使用 DP 卷。

FlexVol 和 FlexGroup 卷可以是 RW 卷，也可以是 DP 卷。

> **Note**
>
> 创建卷后即无法更新卷类型。

卷安全风格

创建 FSx 适用于 ONTAP 的卷时，您可以从两种安全样式中进行选择：Unix 和 NTFS。每种安全风格对数据权限的处理方式有着不同的影响。您必须了解这些不同的影响，以确保为自己的用途选择合适的安全风格。

重要的是要明白，安全风格不能决定哪些客户端类型可以或不可以访问数据。安全风格仅确定 ONTAP FSx 用于控制数据访问的权限类型以及可以修改这些权限的客户端类型。

用于确定卷安全风格的两个因素是负责管理文件系统的管理员的类型和访问卷数据的用户或服务的类型。

在 Amazon FSx 控制台、CLI 和 API 中创建卷时，安全风格会自动设置为根卷的安全风格。您可以使用 AWS CLI 或 API 修改卷的安全风格。创建卷后仍可以修改此设置。请参阅更新卷了解更多信息。

在配置卷的安全风格时，请考虑环境的需求，确保选择最佳的安全风格，避免在管理权限时出现问题。请记住，安全风格并不能决定哪些客户端类型可以访问数据。安全风格决定的是用于允许数据访问的权限以及能够修改这些权限的客户端类型。以下是可以帮助您确定选择哪种卷安全风格的注意事项：

- Unix（Linux）– 如果文件系统由 Unix 管理员管理，则大多数用户是 NFS 客户端，而访问数据的应用程序使用 Unix 用户作为服务账户，应选择此安全风格。只有 Linux 客户端可以使用 Unix 安全风格修改权限，并且用于文件和目录的权限类型为 mode-bits 或 NFS v4.x。 ACLs
- NTFS – 如果文件系统由 Windows 管理员管理，则大多数用户是 SMB 客户端，而访问数据的应用程序使用 Windows 用户作为服务账户，应选择此安全风格。如果需要使用 Windows 访问卷，则建议您使用 NTFS 安全风格。只有 Windows 客户端可以使用 NTFS 安全风格修改权限，并且文件和目录使用的权限类型是 NT ACLs FS。

创建卷

除了 ONTAP 命令行界面 (CLI) 和 RES FSx T API 之外 AWS CLI，您还可以使用亚马逊 FSx 控制台、和亚马逊 API 创建 NetApp ONTAP FlexVol 或FlexGroup卷。 FSx

创建 FlexVol 卷（控制台）

> **Note**
>
> 卷的安全风格会被自动设置为根卷的安全风格。

1. 打开 Amazon FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 在左侧导航窗格中，选择卷。
3. 选择创建卷。
4. 对于文件系统类型，请为 NetApp ONTAP 选择亚马逊 FSx 。
5. 在文件系统详细信息部分中，提供以下信息：
   - 在文件系统中选择要在其中创建卷的文件系统。
   - 在存储虚拟机中选择要在其中创建卷的存储虚拟机（SVM）。
6. 在卷风格部分中，选择 FlexVol。
7. 在卷详细信息部分中，提供以下信息：
   - 在卷名字段中，填入卷的名称。最多可以使用 203 个字母数字或下划线（_）字符。
   - 在卷大小中输入 20–314572800 之间的任意整数来指定卷大小，单位为兆字节（MiB）。
   - 对于卷类型，选择读写（RW）来创建可以读取和写入的卷，或者选择数据保护（DP）来创建仅可读取且可用作 NetApp SnapMirror 或 SnapVault 关系的目标的卷。有关更多信息，请参阅卷类型。
   - 在连接路径中，输入文件系统中用于挂载此卷的位置。该名称必须包含一个前导正斜杠，例如 `/vol3`。
   - 在存储效率中选择已启用以在此卷上启用 ONTAP 存储效率功能（重复数据删除、压缩和紧凑处理）。有关更多信息，请参阅 存储效率。
   - 对于卷安全风格，为卷选择 Unix（Linux）或 NTFS。有关更多信息，请参阅 卷安全风格。
   - 在快照策略中选择用于此卷的快照策略。有关快照策略的更多信息，请参阅快照策略。

如果选择自定义策略，则必须在 custom-policy 字段中指定策略名称。必须是已存在于 SVM 或文件系统中的自定义策略。您可以通过 ONTAP CLI 或 REST API 创建自定义快照策略。有关更多信息，请参阅《NetApp ONTAP 产品文档》中的创建快照策略。

8. 在存储分层 部分中，提供以下信息：
   - 在容量池分层策略中，为该卷选择存储池分层策略，该策略可以是自动（默认）、仅快照、全部或无。有关更多信息，请参阅 卷分层策略。
   - 若选择的是自动或仅限快照，则可设置分层策略冷却周期，以定义将未被访问的数据标记为“冷”并移动到容量池存储之前的天数。您可以提供一个 2 到 183 天之间的值。默认设置为 31 天。
9. 在高级部分的 SnapLock 配置中选择已启用或已禁用。有关配置 SnapLock Compliance 卷或 SnapLock Enterprise 卷的更多信息，请参阅 了解 SnapLock Compliance 和 了解 SnapLock Enterprise。有关 SnapLock的更多信息，请参阅使用 SnapLock 保护您的数据。
10. 选择确认即可创建卷。

您可以通过卷窗格的状态列中的文件系统详细信息页面监控更新进度。卷状态为已创建时，说明卷已可使用。

创建 FlexGroup 卷（控制台）

> **Note**
>
> 您只能使用 Amazon FSx 控制台为具有多个 HA 对的文件系统创建FlexGroup卷。要为具有多个 HA 对的文件系统创建FlexVol卷，请使用 AWS CLI、Amazon FSx API 或 NetApp 管理工具。

1. 打开 Amazon FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 在左侧导航窗格中，选择卷。
3. 选择创建卷。
4. 对于文件系统类型，请为 NetApp ONTAP 选择亚马逊 FSx 。
5. 在文件系统详细信息部分中，提供以下信息：
   - 在文件系统中选择要在其中创建卷的文件系统。
   - 在存储虚拟机中选择要在其中创建卷的存储虚拟机（SVM）。

6. 在卷风格部分中，选择 FlexGroup。
7. 在卷详细信息部分中，提供以下信息：

   - 在卷名字段中，填入卷的名称。最多可以使用 203 个字母数字或下划线（_）字符。
   - 对于卷大小，请为每个 HA 对输入一个介于 800 千兆字节（GiB）- 2400 太字节（TiB）范围内的任意整数。例如，一个具有 12 个高可用性（HA）对的文件系统的最小卷大小为 9600GiB，最大卷大小为 20480TiB。
   - 对于卷类型，选择读写（RW）来创建可以读取和写入的卷，或者选择数据保护（DP）来创建仅可读取且可用作 NetApp SnapMirror 或 SnapVault 关系的目标的卷。有关更多信息，请参阅卷类型。
   - 在连接路径中，输入文件系统中用于挂载此卷的位置。该名称必须包含一个前导正斜杠，例如 `/vol3`。
   - 在存储效率中选择已启用来启用 ONTAP 存储效率功能（重复数据删除、压缩和紧凑处理）。有关更多信息，请参阅 存储效率。
   - 对于卷安全风格，为卷选择 Unix（Linux）或 NTFS。有关更多信息，请参阅 卷安全风格。

     > **Note**
     >
     > 卷的安全风格会被自动设置为根卷的安全风格。

   - 在快照策略中选择用于此卷的快照策略。有关快照策略的更多信息，请参阅快照策略。

     如果选择自定义策略，则必须在 custom-policy 字段中指定策略名称。必须是已存在于 SVM 或文件系统中的自定义策略。您可以通过 ONTAP CLI 或 REST API 创建自定义快照策略。有关更多信息，请参阅《NetApp ONTAP 产品文档》中的创建快照策略。
8. 在存储分层 部分中，提供以下信息：

   - 在容量池分层策略中，为该卷选择存储池分层策略，该策略可以是自动（默认）、仅快照、全部或无。有关更多信息，请参阅 卷分层策略。
   - 若选择的是自动或仅限快照，则可设置分层策略冷却周期，以定义将未被访问的数据标记为“冷”并移动到容量池存储之前的天数。您可以提供一个 2 到 183 天之间的值。默认设置为 31 天。
9. 在高级部分的 SnapLock 配置中选择已启用或已禁用。有关配置 SnapLock Compliance 卷或 SnapLock Enterprise 卷的更多信息，请参阅 了解 SnapLock Compliance 和 了解 SnapLock Enterprise。有关 SnapLock的更多信息，请参阅使用 SnapLock 保护您的数据。
10. 选择确认即可创建卷。

您可以通过卷窗格的状态列中的文件系统详细信息页面监控更新进度。卷状态为已创建时，说明卷已可使用。

创建卷（CLI）

- 要 FSx 为 ONTAP 创建卷，请使用 create-vol ume CLI 命令（或CreateVolume等效的 API 操作），如以下示例所示。

```
aws fsx create-volume \
    --volume-type ONTAP \
    --name vol1 \
    --ontap-configuration CopyTagsToBackups=true,JunctionPath=/
vol1,SecurityStyle=NTFS, \
          SizeInMegabytes=1024,SnapshotPolicy=default, \
          StorageVirtualMachineId=svm-abcdef0123456789a,OntapVolumeType=RW, \
          StorageEfficiencyEnabled=true
```

成功创建卷后，Amazon 将以 JSON 格式 FSx 返回其描述，如以下示例所示。

```
{
    "Volume": {
        "CreationTime": "2022-08-12T13:03:37.625000-04:00",
        "FileSystemId": "fs-abcdef0123456789c",
        "Lifecycle": "CREATING",
        "Name": "vol1",
        "OntapConfiguration": {
            "CopyTagsToBackups": true,
            "FlexCacheEndpointType": "NONE",
            "JunctionPath": "/vol1",
            "SecurityStyle": "NTFS",
            "SizeInMegabytes": 1024,
            "SnapshotPolicy": "default",
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-abcdef0123456789a",
            "StorageVirtualMachineRoot": false,
            "TieringPolicy": {
                "Name": "NONE"
            },
            "OntapVolumeType": "RW"
        },
        "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-abcdef0123456789c/
fsvol-abcdef0123456789b",
```

```
        "VolumeId": "fsvol-abcdef0123456789b",
        "VolumeType": "ONTAP"


    }
}
```

您还可以通过向新卷还原卷备份来创建新卷。有关更多信息，请参阅 将备份还原至新卷。

更新卷

除了 ONTAP 命令行界面 (CLI) 和 REST API 之外 AWS CLI，您还可以使用亚马逊 FSx 控制台、和亚马逊 FSx API 更新 FSx 适用于 NetApp ONTAP 的卷的配置。您可以修改现有 ONTAP 卷 FSx 的以下属性：

- 卷名
- 连接路径
- 卷大小
- 存储效率
- 容量池分层策略
- 卷安全风格
- 快照策略
- 分层策略冷却周期
- 将标签复制到备份（使用 AWS CLI 和 Amazon FSx API）

有关更多信息，请参阅 管理 FSx ONTAP 卷。

更新卷配置（控制台）

1. 打开 Amazon FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 导航到文件系统，然后选择要为其更新卷的 ONTAP 文件系统。
3. 选择卷选项卡。
4. 选择要更新的卷。
5. 在操作中，选择更新卷。

   系统将显示更新卷对话框，其中包含该卷的当前设置。

6. 在连接路径中，输入文件系统中的一个现有位置，用于安装此卷。该名称中必须包含前导正斜杠，例如 `/vol5`。
7. 对于卷大小，您可以在 Amazon FSx 控制台中指定的范围内增加或减小卷的大小。对于 FlexVol 卷，最大大小为 300 TiB。对于 FlexGroup 卷，最大大小为 300 TiB 乘以 FlexGroup 拥有的总组成卷数，最大值为 20 PiB。
8. 在存储效率中，选择已启用以在卷上启用 ONTAP 存储效率功能（重复数据删除、压缩和紧凑处理），或选择已禁用来禁用此功能。
9. 在容量池分层策略中，为该卷选择新的存储池分层策略，该策略可以是自动（默认）、仅快照、全部或无。有关容量池分层策略的更多信息，请参阅卷分层策略。
10. 在卷安全风格中，选择 Unix（Linux）、NTFS 或混合。卷的安全风格决定了是优先选择 NTFS 还是 UNIX ACLs 进行多协议访问。“混合”模式不是多协议访问的必要条件，仅推荐高级用户使用。
11. 在快照策略中选择用于此卷的快照策略。有关快照策略的更多信息，请参阅快照策略。

    如果选择自定义策略，则必须在 custom-policy 字段中指定策略名称。必须是已存在于 SVM 或文件系统中的自定义策略。您可以通过 ONTAP CLI 或 REST API 创建自定义快照策略。有关更多信息，请参阅《NetApp ONTAP 产品文档》中的创建快照策略。
12. 分层策略冷却周期的有效值为 2–183 天。卷的分层策略冷却周期定义了将未被访问的数据标记为“冷”并移动到容量池存储之前的天数。此设置仅会对 `Auto` 和 `Snapshot-only` 策略造成影响。
13. 选择更新即可更新卷。

更新卷配置（CLI）

- 要更新 FSx 适用于 ONTAP 的卷的配置，请使用更新卷 CLI 命令（或UpdateVolume等效的 API 操作），如以下示例所示。

```
aws fsx update-volume \
    --volume-id fsvol-1234567890abcdefa \
    --name new_vol \
    --ontap-configuration CopyTagsToBackups=true,JunctionPath=/new_vol, \
           SizeInMegabytes=2048,SnapshotPolicy=default-1weekly, \
           StorageEfficiencyEnabled=true, \
           TieringPolicy=all
```

扩展 FlexGroup 卷

您可以使用 ONTAP CLI 中的 `volume expand` 命令向 FlexGroup 卷添加其他组成卷。这是向文件系统添加高可用性（HA）对之后的最佳做法，因为它能确保 FlexGroup 卷保持平衡。

在扩展 FlexGroup 卷 之前，应考虑以下几点：

- 所有 FlexGroup's 组成卷都具有相同的存储容量。当用更多的组件来扩展 FlexGroup 卷时，每个组件的大小与现有组件相同。因此，在添加组件之前务必确保每个聚合有足够的可用空间。
- AWS 建议每个卷的每个总量保持八个成分FlexGroup卷。每个聚合八个组成卷可最大程度地提高 FlexGroup 卷的并行性，并为工作负载提供最佳性能。一般来说，只有在添加 HA 对时，我们才建议使用更多的组件来扩展 FlexGroup 卷。这是唯一需要添加组件以维持每个聚合八个组件的情况。
- 如果 FlexGroup 卷处于 SnapMirror 关系中，则源和目标 FlexGroup 卷都需要具有相同的组件数。否则，SnapMirror 传输将失败。SnapMirror 在组件层面工作，并在每个单独组件之间传输数据。因此，如果用更多的组成卷来扩展 FlexGroup 卷，则还必须手动扩展与其存在 SnapMirror 关系的任何卷。
- 当用更多的组件来扩展 FlexGroup 卷时，其现存所有快照副本都将变成“部分”副本。部分副本无法还原，但可以浏览这些副本并还原单个文件。此外，这会导致 Amazon FSx 备份、 AWS 备份或 SnapMirror关系的任何增量丢失。
- 一旦添加了组成卷，就无法将其删除。

添加 FlexGroup 卷组件

可以使用 ONTAP CLI 将为 FlexGroup 卷添加组成卷。

添加 FlexGroup 卷组件

1. 要访问 NetApp ONTAP CLI，请运行以下命令在 Amazon FSx for NetApp ONTAP 文件系统的管理端口上建立 SSH 会话。将 *`management_endpoint_ip`* 替换为文件系统管理端口的 IP 地址。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   有关更多信息，请参阅 使用 ONTAP CLI 管理文件系统。
2. 使用 volume expand ONTAP CLI 命令，用更多的组件扩展 FlexGroup 卷。替换以下值：

   - 将 `svm_name` 替换为托管 FlexGroup 卷的存储虚拟机（SVM）的名称（例如 `svm1`）。
   - 将 `vol_name` 替换为要扩展的 FlexGroup 卷的名称（例如 `vol1`）。

- 将 `aggregates` 替换为要向其添加 FlexGroup 组成卷的聚合的逗号分隔列表。例如，单个聚合为 `aggr1`，多个聚合为 `aggr1,aggr2`。
- 将 `constituent_per_aggregate` 替换为要将其添加到每个指定 `aggregates` 的其他组件的数量。添加的组件应当只够确保 FlexGroup 卷在其所处的聚合中保持均衡的组件数。

```
::> volume expand -vserver svm_name -volume vol_name -aggr-list aggregates -aggr-
list-multiplier constituents_per_aggregate
```

> **Important**
>
> 添加 FlexGroup 组件后无法将其删除，因此在运行上一个命令之前要先检查输入。

在聚合之间移动卷

向文件系统添加高可用性（HA）对时，需要通过向新聚合迁移卷来重新平衡现有的数据。要在聚合之间移动卷，可以使用 ONTAP CLI 中的 `volume move` 命令。

在使用 `volume move` 命令之前，应考虑以下几点：

- 使用 `volume move` 命令会影响性能，因为该命令会消耗文件系统上的网络和磁盘资源。因此，我们建议在低活动时期进行聚合间卷移动。或者，可以在移动卷时将文件系统的网络吞吐量利用率和磁盘吞吐量利用率降低至不超过 50%。
- 为了减少对文件系统的性能影响，我们建议每次在两个 HA 对和聚合之间移动单个卷。例如，如果文件系统有四个 HA 对，我们建议每次移动两个卷（假设不是从相同的 HA 对移动卷，也不是向同一 HA 对移动卷）。ONTAP 支持在每个 HA 对上一次最多移动八个卷，但是更多的同步卷移动会降低客户端 I/O 和任何正在进行的卷移动的性能。
- 存储在受影响卷的 SSD 层上的任何数据以物理方式移动到不同文件服务器上的一组不同磁盘中。此操作在后台进行，需要一定的时间。传输所需的时间取决于文件系统的吞吐能力以及文件系统上的活动量。但是，可以对卷移动进行限制。有关更多信息，请参阅 限制卷移动。
- 存储在容量池中的数据并非以物理方式进行移动，因为 HA 对具有相同的容量池存储。相反，ONTAP 会移动能够完整描述容量池中每个数据块的元数据（合乎逻辑的移动）。请记住，文件元数据始终存储在 SSD 层。有关更多信息，请参阅 卷数据分层。

卷移动阶段

卷移动操作分为以下两个阶段：复制阶段和割接阶段。在复制阶段，现有数据被复制到卷的新聚合中。在割接阶段，ONTAP 尝试最后一次快速传输到卷的新聚合。这包括传输在传输阶段写入的所有数据，以及将新流量重定向到卷的新聚合。默认情况下，转换窗口为 30 秒，所有音量都会暂停 I/O 。如果 ONTAP 无法在割接窗口内执行所有这些步骤，就会失败。默认情况下，ONTAP 将尝试连续进行三次割接。如果连续三次尝试均告失败，则 ONTAP 将每小时重试一次，直到成功为止。您可以通过在切换阶段开始之前减少或暂停卷 I/O 流量来减少文件系统的负载，从而确保转换阶段成功。

开始卷移动

启动卷移动

1. 要访问 NetApp ONTAP CLI，请运行以下命令在 Amazon FSx for NetApp ONTAP 文件系统的管理端口上建立 SSH 会话。将 *management_endpoint_ip* 替换为文件系统管理端口的 IP 地址。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   有关更多信息，请参阅 使用 ONTAP CLI 管理文件系统。

2. 运行 volume move start ONTAP CLI 命令。替换以下值：

   - 将 `vserver_name` 替换为托管当前移动卷的 SVM 的名称。
   - 将 `volume_name` 替换为卷组件的名称（例如，`vol1__0001`）。
   - 将 `aggregate_name` 替换为卷的目标聚合的名称。
   - `-enforce-network-throttling` 可限制卷移动的总吞吐量。这是可选的。

   ```
   ::> volume move start -vserver svm_name -volume volume_name --destination-
   aggregate aggregate_name -foreground false
   [Job 1] Job is queued: Move "vol1__0001" in Vserver "svm01" to aggregate "aggr1".
    Use the "volume move show -vserver svm01 -volume vol1__0001" command to view the
    status of this operation.
   ```

> **Important**
>
> 移动卷会消耗源和目标文件服务器的网络与磁盘资源。因此，工作负载的性能会受到任何进行中卷移动的影响。此外，在卷移动的切换阶段，您的卷 I/O 流量将暂时暂停。

监控卷移动

监控卷移动

- 要查看卷移动操作的状态，可使用 `volume move show` ONTAP CLI 命令。

```
::> volume move show -vserver svm_name -volume volume_name

Vserver Name: svm01
Volume Name: vol1__0001
Actual Completion Time: -
Bytes Remaining: 1.00TB
Specified Action For Cutover: retry_on_failure
Specified Cutover Time Window: 30
Destination Aggregate: aggr2
Destination Node: FsxId01234567890abcdef-03
Detailed Status: Transferring data: 12.23GB sent.
Percentage Complete: 1%
Move Phase: replicating
Prior Issues Encountered: -
Estimated Remaining Duration: 00:40:25
Replication Throughput: 434.3MB/s
Duration of Move: 00:00:27
Source Aggregate: aggr1
Source Node: FsxId01234567890abcdef-01
Move State: healthy
```

命令输出显示完成移动的估计时间。完成后，`Move phase` 将显示 `completed` 状态。

保持 FlexGroup 卷平衡

为了使工作负载以最佳方式运行，FlexGroup 卷应涵盖所有聚合，且每个聚合的组成卷数应保持平均。我们建议每个聚合有八个组件。在重新平衡 FlexGroup 卷时，应考虑以下情况：

- 在现有聚合之间移动 FlexGroup 组件：如果将 FlexGroup's 组成卷移动到原本平衡的 FlexGroup 的另一个聚合，则应将另一个利用率较低的组件移动到原始聚合。这样可以确保 FlexGroup 的每个聚合保持平均的组件数。

  添加 HA 对后将 FlexGroup 组件移动到新聚合中：如果在添加 HA 对后将 FlexGroup's 组成卷移动到新聚合，则应在丢失组件的聚合上用更多的组件来扩展 FlexGroup。这样可以确保 FlexGroup 的每个聚合保持平均的组件数。有关更多信息，请参阅 the section called “扩展 FlexGroup 卷”。

限制卷移动

如果要限制在文件系统上进行卷移动的带宽，可以在操作开始时添加 `-enforce-network-throttling` 选项。

> **Note**
>
> 使用此选项会影响文件系统的传入 SnapMirror 复制数据传输。跟踪如何配置文件系统的复制选项，因为设置这些选项后就无法查看。

限制卷移动

1. 该限制操作使用全局复制节流。要设置全局复制节流，应在 ONTAP CLI 中使用以下命令。

```
::> options -option-name replication.throttle.enable on
```

2. 指定复制可使用的最大总带宽，并替换以下选项：

   - 将 `kbs_throttle` 替换为用于任何复制（包括 SnapMirror 和卷移动）的所需最大吞吐量，单位为千字节/秒。

```
::> options -option-name replication.throttle.incoming.max_kbs kbs_throttle
::> options -option-name replication.throttle.outgoing.max_kbs kbs_throttle
```

监控卷

您可以使用亚马逊 FSx 控制台、、Amazon FSx API 和 AWS CLI，查看文件系统中当前存在的卷 SDKs。

监控文件系统上的卷：

- 使用控制台 – 选择一个文件系统，查看该文件系统详细信息页面。选择卷选项卡，列出文件系统上的所有卷，然后选择要查看的卷。
- 使用 CLI 或 API — 使用 desc ribe-volumes CLI 命令或 API 操作DescribeVolumes。

```
$ aws fsx describe-volumes
{
```

```
    "Volumes": [
        {
            "CreationTime": "2024-03-04T20:17:44+00:00",
            "FileSystemId": "fs-abcdef0123a0bb087",
            "Lifecycle": "CREATED",
            "Name": "SVM8_ext_root",
            "OntapConfiguration": {
                "FlexCacheEndpointType": "NONE",
                "JunctionPath": "/",
                "SecurityStyle": "NTFS",
                "SizeInMegabytes": 1024,
                "StorageEfficiencyEnabled": false,
                "StorageVirtualMachineId": "svm-01234567890abcdef",
                "StorageVirtualMachineRoot": true,
                "TieringPolicy": {
                    "Name": "NONE"
                },
                "UUID": "42ce3de0-da64-11ee-a22d-7f7cdfb8d381",
                "OntapVolumeType": "RW",
                "SnapshotPolicy": "default",
                "CopyTagsToBackups": false,
                "VolumeStyle": "FLEXVOL",
                "AggregateConfiguration": {
                    "Aggregates": [
                        "aggr1"
                    ]
                },
                "SizeInBytes": 1073741824
            },
            "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-
abcdef0123a0bb087/fsvol-abcdef0123456789a",
            "VolumeId": "fsvol-abcdef0123456789a",
            "VolumeType": "ONTAP"
        }
    ]
}
```


查看离线卷

当源卷离线时，就无法创建或删除卷备份。可以使用 `volume show` ONTAP CLI 命令来确定卷的当前状态。

```
volume show -vserver svm-name
```

有关在文件系统上访问 ONTAP CLI 的信息，请参阅 使用 NetApp ONTAP CLI。

```
FsxIdabc12345::> volume show -vserver vs1
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
vs1       vol1         aggr1        online     RW          2GB      1.9GB    5%
vs1       vol1_dr      aggr0_dp     online     DP        200GB    160.0GB   20%
vs1       vol2         aggr0        online     RW        150GB    110.3GB   26%
vs1       vol2_dr      aggr0_dp     online     DP        150GB    110.3GB   26%
vs1       vol3         aggr1        online     RW        150GB    120.0GB   20%
vs1       vol3_dr      aggr1_dp     online     DP        150GB    120.0GB   20%
vs1       vol4         aggr1        online     RW        200GB    159.8GB   20%
7 entries were displayed.
```

要使离线卷恢复在线，应使用 `volume online` ONTAP CLI 命令，如以下示例所示。如果仅存在一个 SVM（虚拟服务器），则无需指定 `-vserver` 参数。

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

删除卷

除了 ONTAP 命令行界面 (CLI) 和 RES FSx T API 之外 AWS CLI，您还可以使用亚马逊 FSx 控制台、和亚马逊 API 删除 FSx 适用于 NetApp ONTAP 的卷。

在删除卷之前，请确保没有应用程序正在访问要删除的卷中的数据。

> **Important**
>
> 只有在卷启用了亚马逊 FSx 备份的情况下，您才能使用亚马逊 FSx 控制台、API 或 CLI 删除该卷。

进行最终卷备份

使用 Amazon FSx 控制台删除卷时，您可以选择对该卷进行最终备份。作为最佳实践，我们建议您选择进行最终备份。如果您在一段时间后发现不需要它，则可以删除此备份和其他手动创建的卷备份。当您使用 `delete-volume` CLI 命令删除卷时，Amaz FSx on 会默认进行最终备份。

有关卷备份的更多信息，请参阅 使用卷备份保护数据。

删除卷（控制台）

1. 打开 Amazon FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 在左侧导航窗格中，选择文件系统，然后选择要从中删除卷的 ONTAP 文件系统。
3. 选择卷选项卡。
4. 选择要删除的卷。
5. 在操作中选择删除卷。
6. （仅限SnapLock Enterprise卷）对于 “绕过 SnapLock 企业保留”，请选择 “是”。
7. 在确认对话框的创建最终备份中，为您提供了两个选项：
   - 选择是即可创建卷的最终备份。将显示最终备份名称。
   - 如果您不希望进行卷的最终备份，请选择否。系统此时会要求您确认：删除该卷后自动备份将不再可用。
8. 在 Confirm delete 字段中输入 delete 即可确认删除卷。
9. 选择删除卷。

删除卷（CLI）

- 要删除 FSx 适用于 ONTAP 的卷，请使用删除卷 CLI 命令（或DeleteVolume等效的 API 操作），如以下示例所示。

```
aws fsx delete-volume --volume-id fsvol-1234567890abcde
```

删除 SnapLock 卷

本节介绍了如何删除 SnapLock 卷。

如果 SnapLock Compliance 卷上所有“一次写入、多次读取”（WORM）文件的保留期已过期，则可以将其删除。

> **Note**
>
> 当您关闭包含SnapLock Enterprise或Compliance卷的时 AWS 账户 ， FSx 对于 ONTAP AWS ，请暂停您的帐户 90 天，保持数据完好无损。如果您在这 90 天内没有重新开设账户，则无论您的保留设置如何，都会 AWS 删除您的数据，包括SnapLock批量数据。

如果您拥有所需的权限，则可以随时删除 SnapLock Enterprise 卷。要使用 ONTAP CLI 删除 SnapLock Enterprise 卷，您必须拥有 `fsxadmin` 角色。有关更多信息，请参阅 文件系统管理员角色和用户。

要使用亚马逊 FSx 控制台、CLI 或 Amazon FSx API 删除包含具有有效保留策略的 WORM 数据的 SnapLock企业卷，您必须拥有 `fsx:BypassSnapLockEnterpriseRetention` IAM 权限。

> **Warning**
>
> SnapLock 审计日志卷的最短保留期为六个月。在此保留期到期之前，您无法删除 SnapLock 审计日志卷、存储虚拟机（SVM）或与 SVM 关联的文件系统，即使该卷是在 SnapLock Enterprise 模式下创建的。有关更多信息，请参阅 SnapLock 审计日志卷。

创建 iSCSI LUN

此过程介绍如何使用 CLI 命令在 Amazon FSx for NetApp ONTAP 文件系统上创建 iSCSI L NetApp ONTAP UN。lun create有关更多信息，请参阅 NetApp ONTAP 文档中心中的 lun create。

> **Note**
>
> HA 对超过六个的文件系统不支持 iSCSI 协议。

此过程假设您已经在文件系统上创建了一个卷。有关更多信息，请参阅 创建卷。

1. 要访问 ONTAP CLI，请运行以下命令，在适用于 NetApp ONTAP 文件系统的 Amazon FSx 或 SVM 的管理端口上建立 SSH 会话。将 *`management_endpoint_ip`* 替换为文件系统管理端口的 IP 地址。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

有关更多信息，请参阅 使用 ONTAP CLI 管理文件系统。

2. 使用 lun create NetApp CLI CLI 命令创建 LUN，替换以下值：

   - ***svm_name*** – 提供 iSCSI 目标的存储虚拟机（SVM）的名称。主机使用此值来连接 LUN。
   - ***vol_name*** – 托管 LUN 的卷的名称。
   - ***lun_name*** – 要分配给 LUN 的名称。
   - ***size*** – LUN 的大小，以字节为单位。您可以创建的最大 LUN 大小为 128TB。

     > **Note**
     >
     > 我们建议您使用比 LUN 大小至少大 5% 的卷。此幅度为卷快照留出了空间。

   - ***ostype*** – 主机的操作系统，`windows_2008` 或 `linux`。对所有版本的 Windows 使用 `windows_2008`；这可确保 LUN 具有适合操作系统的块偏移量并优化性能。

   > **Note**
   >
   > 我们建议在 LUN 上启用空间分配。启用空间分配后，ONTAP 可以在 LUN 容量不足时通知您的主机，并且可以在您从 LUN 中删除数据时回收空间。

   有关更多信息，请参阅 NetApp ONTAP CLI 文档`lun create`中的。

   ```
   > lun create -vserver svm_name -path /vol/vol_name/lun_name -size size -
   ostype ostype -space-allocation enabled
   ```

   ```
   Created a LUN of size 10g (10737418240)
   ```

3. 确认 LUN 已创建、已联机且已映射。

   ```
   > lun show
   ```

   系统将使用以下输出做出响应：

   ```
   Vserver   Path                            State   Mapped   Type         Size
   --------- ------------------------------- ------- -------- ------------ --------
   ```

```
svm_name
          /vol/vol_name/lun_name          online  unmapped windows_2008 10GB
```

后续步骤

现在，您已经创建了 iSCSI LUN，那么将 iSCSI LUN 作为块存储过程的下一步便是将 LUN 映射到 igroup。有关更多信息，请参阅为 Linux 配置 iSCSI或为 Windows 配置 iSCSI。

使用 Amazon FSx 维护时段进行性能优化

作为一项完全托管的服务，FSx for ONTAP 会定期维护和更新文件系统。这种维护对大多数工作负载没有影响。对于性能敏感的工作负载，在极少数情况下，您可能会注意到维护时性能会受到短暂影响（<60 秒）；Amazon FSx 允许您通过维护时段控制任何此类潜在维护活动的发生时间。

打补丁很少发生，通常每隔几周发生一次。进行修补时，文件系统的每个文件服务器逐个打补丁，通常每个文件服务器最多需要一个小时才能完成修补。在 HA 对中对任何文件服务器进行修补之前，文件系统会自动失效转移到文件服务器的 HA 配对服务器，这可能会导致定向到该 HA 对的任何 I/O 出现短暂（小于 60 秒）的 I/O 暂停。您的文件系统随后将进行故障恢复，这可能导致另一次短暂（少于 60 秒）的 I/O 暂停。您可以在创建文件系统期间选择维护时段开始时间。如果您没有选择时段，则会自动分配一个时段。

> **Important**
>
> 为确保可成功修补您的文件系统，FSx for ONTAP 将在修补过程中使所有离线卷联机。Amazon FSx 恢复联机的任何卷均不可供客户端访问。

FSx for ONTAP 允许您根据需要调整维护时段，来适应您的工作负载和操作要求。您可以根据需要频繁更改维护时段，但至少每 14 天出现一个维护时段。如果已发布补丁但在 14 天内未出现维护时段，则 FSx for ONTAP 会继续维护文件系统，以确保其安全性和可靠性。

> **Note**
>
> 为了确保维护活动期间的数据完整性，FSx for ONTAP 会在维护开始之前关闭所有机会性锁定，并完成对托管文件系统的底层存储卷的所有待处理写入操作。

您可以使用 Amazon FSx 管理控制台、AWS CLI、AWS API 或某个 AWS SDK 来更改文件系统的维护时段。

更改每周维护时段（控制台）

1. 通过以下网址打开 Amazon FSx 控制台：https://console.aws.amazon.com/fsx/。
2. 在左侧导航栏中选择文件系统。
3. 选择要更改每周维护时段的文件系统。随即显示摘要文件系统详细信息页面。
4. 选择管理，会显示文件系统管理设置面板。
5. 选择更新，会显示更改维护时段窗口。
6. 输入您希望每周维护时段开始的新日期和时间。
7. 选择保存以保存您的更改。文件系统管理设置面板中会显示新的维护开始时间。

要使用 update-file-system 命令更改每周维护时段，请参阅更新文件系统（CLI）。

管理吞吐能力

FSx for ONTAP 会在创建文件系统时配置吞吐容量。您可以随时修改文件系统的吞吐能力。请记住，文件系统需要通过特定配置来实现最大吞吐能力。例如，要为第一代文件系统预置 4 GBps 的吞吐容量，您的文件系统需要至少具有 5,120 GiB 的固态硬盘存储容量和 160,000 个 SSD IOPS 的配置。有关更多信息，请参阅 吞吐能力对性能的影响。

吞吐能力是决定负责托管文件系统的文件服务器在为文件数据提供服务时的速度的因素之一。吞吐能力的级别越高，文件服务器上的网络、磁盘每秒读取 I/O 操作（IOPS）数和数据缓存容量水平也就越高。有关更多信息，请参阅 性能。

当您修改文件系统的吞吐容量时，Amazon 会 FSx 切换为文件系统提供动力的文件服务器。在此期间，单可用区和多可用区文件系统都会经历自动失效转移和失效自动恢复进程，这通常需要几分钟时间来完成。失效转移和失效自动恢复进程对 NFS（网络文件系统）、SMB（服务器消息块）以及 iSCSI（Internet 小型计算机系统接口）客户端是透明的，因此您的工作负载能够继续运行，不会中断，且无需人工干预。您的文件系统可以使用新的吞吐能力量后，就会向您收取费用。

> **Note**
>
> 为了确保维护活动期间的数据完整性， FSx for ONTAP 会在维护开始之前关闭所有机会性锁定，并完成对托管文件系统的底层存储卷的所有待处理写入操作。在文件系统的计划维护时段

中，系统修改（例如对吞吐能力的修改）可能会出现延迟。系统维护会导致这些更改排队等待处理。有关更多信息，请参阅 the section called “更新维护时段”。

主题

何时修改吞吐能力

Amazon 与 Amazon FSx 集成 CloudWatch，可帮助您监控文件系统的持续吞吐量使用水平。除了文件系统的吞吐能力外，您可以通过文件系统驱动的吞吐量和 IOPS 性能还取决于特定工作负载的特征。通常，您应预置足够的吞吐能力来支持工作负载的读取吞吐量以及两倍的工作负载写入吞吐量。您可以使用 CloudWatch 指标来确定要更改哪些维度以提高性能。有关更多信息，请参阅 the section called “在 Amazon FSx 控制台中进行监控”。

如何处理并发请求

对于第一代文件系统，您可以在 SSD 存储容量和预调配 IOPS 更新工作流程开始之前或进行中请求吞吐能力更新。Amazon FSx 处理这两个请求的顺序如下：

- 如果您同时提交 SSD/IOPS 更新和吞吐量容量更新，则两个请求都将被接受。 SSD/IOPS 更新优先级先于吞吐量容量更新。
- 如果您在更新过程中提交吞吐量容量 SSD/IOPS 更新，则吞吐量容量更新请求将被接受并排队等候在更新之后（有新值可用）和优化步骤期间进行。SSD/IOPS update. The throughput capacity update starts after SSD/IOPS这通常会在 10 分钟内完成。
- 如果您在吞吐量容量 SSD/IOPS 更新过程中提交更新，则 SSD/IOPS 存储更新请求将被接受并排队等待，等待吞吐量容量更新完成（新的吞吐量容量可用）后开始。这通常需要 20 分钟。

请求更新第二代文件系统的吞吐能力时，应考虑以下几点：

- 在更新第二代文件系统的吞吐能力之前，至少须等待六个小时。

- 吞吐容量冷却时间与 SSD/IOPS 扩展共享。
- 吞吐量容量 SSD/IOPS 扩展和扩展不能同时完成，也不能在两者进行时排队。
- 在吞吐量容量扩展或 SSD/IOPS 扩展过程中，您不能同时添加高可用性 (HA) 对。但是，添加 HA 对不会与 SSD/IOPS 扩展和吞吐量容量扩展共享冷却时间。有关更多信息，请参阅 添加高可用性（HA）对。

有关 SSD 存储和预调配 IOPS 更新的更多信息，请参阅管理存储容量。

更新吞吐能力

您可以使用亚马逊 FSx 控制台、 AWS Command Line Interface (AWS CLI) 或 Amazon FSx API 修改文件系统的吞吐容量。

> **Note**
>
> 在更新第二代文件系统的吞吐能力之前，至少须等待六个小时。

修改文件系统的吞吐能力（控制台）

1. 打开 Amazon FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 导航到文件系统，然后选择要增加其吞吐能力的 ONTAP 文件系统。
3. 在操作中，选择更新吞吐能力。或者，在摘要面板中，选择文件系统吞吐能力旁边的更新。
4. 从列表中选择吞吐能力的新值。
5. 选择更新，启动吞吐能力更新。
6. 您可以通过文件系统详细信息页面的更新选项卡来监控更新进度。

   您可以使用亚马逊 FSx 控制台、和 API 来监控更新进度。 AWS CLI有关更多信息，请参阅 监控吞吐能力更改。

修改文件系统的吞吐能力（CLI）

要修改文件系统的吞吐容量，请使用 AWS CLI 命令update-file-system。设置以下参数：

- 将 `--file-system-id` 设置为要更新的文件系统的 ID。

- 将 `ThroughputCapacity` 设置为要将文件系统更新到的所需值。

您可以使用亚马逊 FSx 控制台、和 API 来监控更新进度。 AWS CLI有关更多信息，请参阅 监控吞吐能力更改。

监控吞吐能力更改

您可以使用 Amazon FSx 控制台、API 和，监控吞吐容量修改的进度 AWS CLI。

在控制台中监控吞吐能力更改

通过文件系统详细信息窗口的更新选项卡，您可以查看每个更新操作类型的 10 个最新更新操作。

您可以查看关于吞吐能力更新操作的以下信息。

更新类型

支持的类型包括吞吐能力、存储容量和存储优化。

目标值

要将文件系统的吞吐能力更改为的所需值。

状态

当前更新状态。对于吞吐能力更新，可能出现如下值：

- 待处理 — Amazon FSx 已收到更新请求，但尚未开始处理。
- 处理@@ 中 — Amazon FSx 正在处理更新请求。
- 已完成 – 吞吐能力更新已成功完成。
- 失败 – 吞吐能力更新失败。选择问号（？）可查看关于吞吐量更新失败原因的详细信息。

请求时间

Amazon FSx 收到更新请求的时间。

使用 AWS CLI 和 API 监控更改

您可以使用 describe-file-systemsCLI 命令和 DescribeFileSystemsAPI 操作查看和监控文件系统吞吐量容量修改请求。`AdministrativeActions` 数组列出每种管理操作类型的 10 个最近更新操作。修改文件系统的吞吐能力时，会生成 `FILE_SYSTEM_UPDATE` 管理操作。

以下示例显示了 CLI 命令 describe-file-systems 的响应摘录。文件系统的吞吐容量为 128 MBps，目标吞吐量为 256 MBps。

```
.
.
.
    "ThroughputCapacity": 128,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "PENDING",
        "TargetFileSystemValues": {
          "OntapConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

当 Amazon 成功 FSx 处理操作后，状态将更改为COMPLETED。文件系统即可使用新的吞吐能力，并在 ThroughputCapacity 属性中显示。如以下 CLI 命令 describe-file-systems 的响应摘录中所示。

```
.
.
.
    "ThroughputCapacity": 256,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "COMPLETED",
        "TargetFileSystemValues": {
          "OntapConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

如果吞吐能力修改失败，状态将更改为 FAILED 且 FailureDetails 属性中会显示关于失败的信息。

管理 SMB 共享

要管理 Amazon FSx 文件系统上的 SMB 文件共享，可以使用 Microsoft Windows 共享文件夹 GUI。共享文件夹 GUI 提供了一个集中管理存储虚拟机（SVM）中所有共享文件夹的位置。以下过程详细说明如何创建、更新和删除文件共享。

> **Note**
>
> 您也可以使用 NetApp 系统管理器管理 SMB 文件共享。有关更多信息，请参阅 将 NetApp Systems Manager 与 NetApp Console 配合使用。

将共享文件夹连接到 Amazon FSx 文件系统

1. 启动 Amazon EC2 实例，并将其连接到 Amazon FSx 文件系统加入的 Microsoft Active Directory。为此，请从《AWS Directory Service 管理指南》中选择以下过程：
   - 无缝加入 Windows EC2 实例
   - 手动加入 Windows 实例
2. 以文件系统管理员组成员的用户身份连接到实例。有关详细信息，请参阅《Amazon EC2 用户指南》中的 Connecting to Your Windows Instance。
3. 打开开始菜单，然后使用以管理员身份运行来运行 fsmgmt.msc。此操作将打开共享文件夹 GUI 工具。
4. 在操作中，选择连接到另一台计算机。
5. 对于另一台计算机，输入存储虚拟机（SVM）的 DNS 名称，例如 **`netbios_name.corp.example.com`**。

   要在 Amazon FSx 控制台上查找 SVM 的 DNS 名称，请依次选择存储虚拟机、SVM，然后向下滚动到端点，直到找到 SMB DNS 名称。您还可以在 DescribeStorageVirtualMachinesAPI 操作的响应中获取 DNS 名称。
6. 选择确定。随后，共享文件夹工具的列表中将显示 Amazon FSx 文件系统的条目。

现在，共享文件夹已连接到您的 Amazon FSx 文件系统，您可以通过以下操作管理文件系统上的 Windows 文件共享：

> **Note**
>
> 我们建议您将 SMB 共享放在根卷之外的其他卷上。

- 创建新文件共享 – 在共享文件夹工具中，选择左侧窗格中的共享，查看 Amazon FSx 文件系统的活动共享。显示卷已挂载在创建卷时选择的路径上。选择新建共享，然后完成“创建共享文件夹”向导。

  在创建新文件共享之前，必须先创建本地文件夹。您可以按如下步骤执行操作：

  - 使用共享文件夹工具：在指定本地文件夹路径时选择浏览，然后选择新建文件夹来创建本地文件夹。
  - 使用命令行：

    ```
    New-Item -Type Directory -Path \\netbios_name.corp.example.com\C
    $volume_path\MyNewFolder
    ```

- 修改文件共享 – 在共享文件夹工具的右侧窗格中，打开要修改的文件共享的上下文（右键单击）菜单，然后选择属性。修改属性并选择确定。
- 删除文件共享 – 在共享文件夹工具的右侧窗格中，打开要删除的文件共享的上下文（右键单击）菜单，然后选择停止共享。

> **Note**
>
> 只有使用 Amazon FSx 文件系统的 DNS 名称连接到 fsmgmt.msc 时，才能从 GUI 中删除文件共享。如果您使用文件系统的 IP 地址或 DNS 别名进行连接，则停止共享选项将不起作用，也不会删除文件共享。

使用 NetApp 应用程序管理 FSx for ONTAP 资源

除了 AWS 管理控制台、AWS CLI 和 AWS API 及 SDK 外，您还可以使用以下 NetApp 管理工具和应用程序来管理 FSx for ONTAP 资源：

主题

- 注册 NetApp 账户。
- 使用 NetApp Console
- 使用 NetApp ONTAP CLI

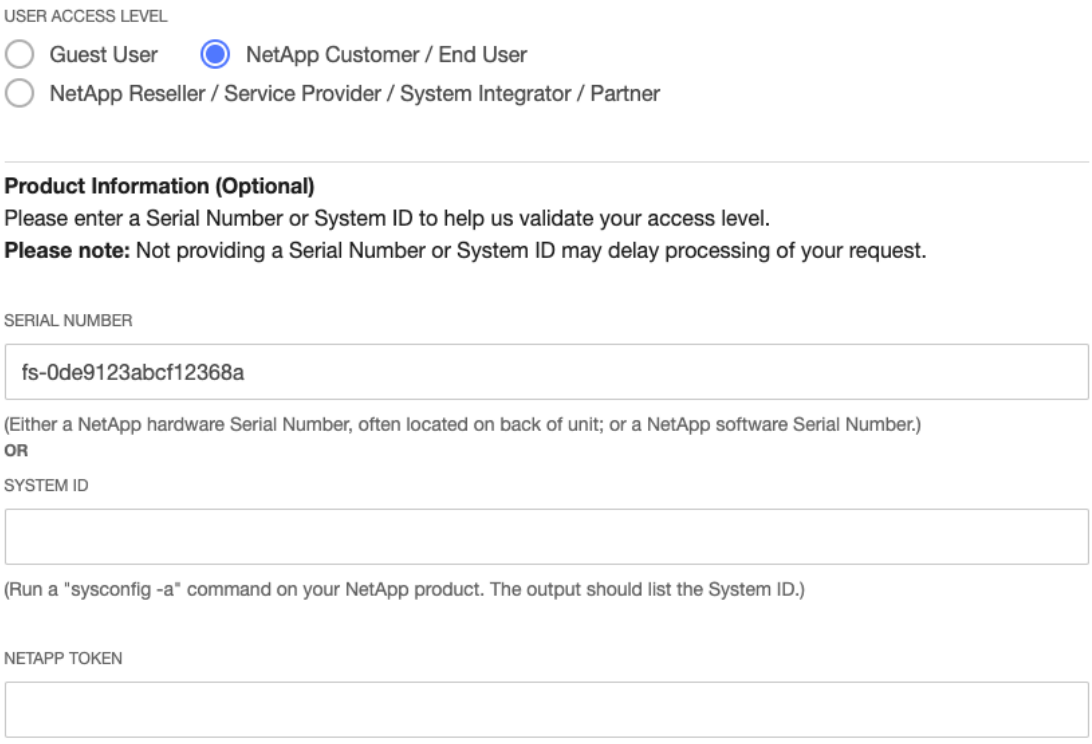
- 使用 ONTAP REST API

> **Important**
>
> 为了确保一致性，Amazon FSx 会定期与 ONTAP 同步。如果您使用 NetApp 应用程序创建或修改卷，这些更改可能需要几分钟时间才能反映在 AWS 管理控制台、AWS CLI、API 和 SDK 中。

注册 NetApp 账户。

要下载某些 NetApp 软件（例如 NetApp Console、SnapCenter 和 ONTAP 防病毒连接器），您需要具有一个 NetApp 账户。要注册 NetApp 账户，请执行以下步骤：

1. 前往 NetApp 用户注册页面，注册一个新的 NetApp 用户账户。
2. 在表格中填入您的信息 请务必选择 NetApp 客户/最终用户访问级别。在序列号字段中，复制并粘贴您的 FSx for ONTAP 文件系统的文件系统 ID。请参见以下示例：



注册后的权益

NetApp 产品的现有客户将在一个工作日内将其 NSS 账户升级为客户级别访问权限。NetApp 的新客户除了可以将其 NSS 账户升级为“客户级别”访问权限外，还可以使用标准业务实践进行登记。提供文件系统 ID 有助于加速此过程。您可以登录 mysupport.netapp.com 并导航到欢迎页面，来查看 NSS 账户的状态。您账户的访问权限级别应为客户访问。

使用 NetApp Console

NetApp 控制台（原为 NetApp BlueXP）是一个统一的控制面板，可简化本地和云环境中存储和数据服务的管理体验。NetApp 控制台提供集中式用户界面，用于管理、监控和自动化实施 AWS 和本地的 ONTAP 部署。有关更多信息，请参阅适用于 NetApp ONTAP 的 Amazon FSx 管理文档中的 NetApp 控制台文档。

> **Note**
>
> NetApp Console具有多个高可用性（HA）对的第二代文件系统不支持 。

将 NetApp Systems Manager 与 NetApp Console 配合使用

您可以直接从中使用 System Manager 来管理适用于 NetApp ONTAP 的 Amazon FSx 文件系统。使用 NetApp Console NetApp Console，您可以使用惯用的同一 System Manager 界面，这样就可以从一个控制面板中管理混合多云基础设施。您还可以访问 NetApp 控制台的其他功能。有关更多信息，请参阅 NetApp ONTAP 文档中的 Integrate ONTAP System Manager with NetApp Console 主题。

> **Note**
>
> 具有多个 HA 对的第二代文件系统不支持 NetApp System Manager。

使用 NetApp ONTAP CLI

您可以使用 NetApp ONTAP CLI 管理适用于 NetApp ONTAP 的 Amazon FSx 资源。您可以在文件系统（类似于 NetApp ONTAP 集群）级别和 SVM 级别管理资源。

使用 ONTAP CLI 管理文件系统

您可以在 FSx for ONTAP 文件系统上运行 ONTAP CLI 命令，这类似于在 NetApp ONTAP 集群上运行这些命令。您可以通过与文件系统管理端点建立 Secure Shell（SSH）连接并使用 `fsxadmin` 用户

名和密码来访问文件系统上的 ONTAP CLI。使用自定义创建流程或使用 AWS CLI 创建文件系统时，可以选择设置 fsxadmin 密码。如果使用“快速创建”选项创建文件系统，则说明未设置 fsxadmin 密码，因此您需要设置一个密码才能登录 ONTAP CLI。有关设置文件系统 fsxadmin 密码的更多信息，请参阅 更新文件系统。您可以在 Amazon FSx 控制台中找到文件系统的管理端点 DNS 名称和 IP 地址，位于 FSx for ONTAP 文件系统详细信息页面的管理选项卡下。

要通过 SSH 连接到文件系统的管理端点，请先登录到与 FSx for ONTAP 文件系统位于同一 VPC 的 EC2 实例。登录到 EC2 实例后，使用 fsxadmin 用户名和密码通过 SSH 连接到文件系统管理端点的 IP 地址或 DNS 名称，如下例所示。

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

带有示例值的 SSH 命令：

```
ec2user $ ssh fsxadmin@198.51.100.0
```

使用管理端点 DNS 名称的 SSH 命令：

```
ec2user $ ssh fsxadmin@file-system-management-endpoint-dns-name
```

使用示例 DNS 名称的 SSH 命令：

```
ec2user $ ssh fsxadmin@management.fs-0abcdef123456789.fsx.us-east-2.aws.com
  Password: fsxadmin_password

This is your first recorded login.
FsxId0abcdef123456789::>
```

fsxadmin 可用 ONTAP CLI 命令的范围

fsxadmin 的管理视图为文件系统级视图，其中包括文件系统中的所有 SVM 和卷。fsxadmin 角色发挥的是 ONTAP 集群管理员的作用。由于适用于 NetApp ONTAP 的 Amazon FSx 文件系统是完全托管的，因此 fsxadmin 角色可以运行一部分可用 ONTAP CLI 命令。

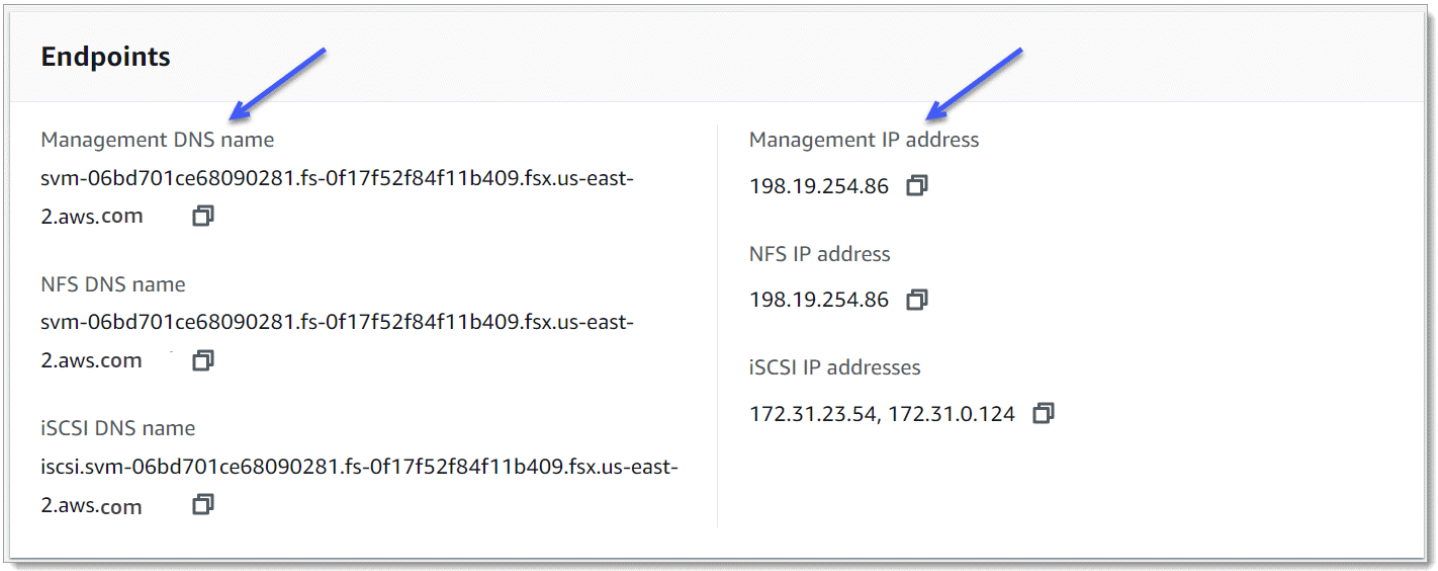
要查看 fsxadmin 可运行的命令列表，请使用以下 security login role show ONTAP CLI 命令：

```
FsxId0abc123def456::> security login role show -role fsxadmin -access !none
```

```
           Role          Command/                                    Access
Vserver    Name          Directory                             Query Level
---------- ------------- --------- ----------------------------------- --------
FsxId0abcdef123456789
           fsxadmin      application                                   all
                         cluster application-record                    all
                         cluster date show                             readonly
                         cluster ha modify                             readonly
                         cluster ha show                               readonly
                         cluster identity modify                       readonly
                         cluster identity show                         readonly
                         cluster log-forwarding           -port !55555 all
                         cluster modify                                readonly
                         cluster peer                                  all
                         cluster show                                  readonly
                         cluster statistics show                       readonly
                         cluster time-service ntp server create        readonly
                         cluster time-service ntp server delete        readonly
                         cluster time-service ntp server modify        readonly
                         cluster time-service ntp server show          readonly
                         debug network tcpdump       -ipspace !Cluster all
                         debug san lun                                 all
                         df         -vserver !FsxId* -vserver !Cluster readonly
                         echo                                          all
                         event catalog show                            readonly
                         event config                                  all
.
.
.
378 entries were displayed.
```

使用 ONTAP CLI 管理 SVM

您可以通过使用 `vsadmin` 用户名和密码建立 SVM 管理端点的 Secure Shell（SSH）连接来访问 SVM 上的 ONTAP CLI。您可以在 Amazon FSx 控制台中找到 SVM 的管理端点 DNS 名称和 IP 地址，位于存储虚拟机详细信息页面的端点面板下，如下图所示。



要通过 SSH 连接到 SVM 的管理端点，可使用 vsadmin 用户名和密码。如果在创建 SVM 时没有为 vsadmin 用户设置密码，您可以随时设置 vsadmin 密码。有关更多信息，请参阅 更新存储虚拟机（SVM）。您可以使用管理端点 IP 地址或 DNS 名称，从与文件系统位于同一 VPC 的客户端通过 SSH 连接到 SVM。

```
ssh vsadmin@svm-management-endpoint-ip-address
```

带有示例值的命令：

```
ssh vsadmin@198.51.100.10
```

使用管理端点 DNS 名称的 SSH 命令：

```
ssh vsadmin@svm-management-endpoint-dns-name
```

使用示例 DNS 名称的 SSH 命令：

```
ssh vsadmin@management.svm-abcdef01234567892fs-0abcdef123456789.fsx.us-east-2.aws.com
```

```
Password: vsadmin-password

This is your first recorded login.
FsxId0abcdef123456789::>
```

适用于 NetApp ONTAP 的 Amazon FSx 支持 NetApp ONTAP CLI 命令。

有关 NetApp ONTAP ONTAP CLI 命令的完整参考，请参阅 ONTAP 命令：手册页面参考。

使用 ONTAP REST API

使用 ONTAP REST API 通过 `fsxadmin` 凭证访问 FSx for ONTAP 文件系统时，请执行下列操作之一：

- 禁用 TLS 验证。

  或

- 信任 AWS 证书颁发机构（CA）– 可在以下 URL 中找到每个区域中 CA 的证书捆绑包：
  - 公共 AWS 区域：https://fsx-aws-certificates.s3.amazonaws.com/bundle-*aws-region*.pem
  - AWS GovCloud 区域：https://fsx-aws-us-gov-certificates.s3.us-gov-west-1.amazonaws.com/bundle-*aws-region*.pem
  - AWS 中国区域：https://fsx-aws-cn-certificates.s3.cn-north-1.amazonaws.com.cn/bundle-*aws-region*.pem

有关 NetApp ONTAP REST API 命令的完整参考，请参阅 NetApp ONTAP REST API 在线参考。

为 Amazon FSx 资源贴标签

为帮助您管理文件系统和其他 Amazon FSx 资源，您可以通过标签的形式为每个资源分配您自己的元数据。借助标签，您可以按照不同的方式（例如，按用途、所有者或环境）对 AWS 资源进行分类。当您具有很多相同类型的资源时，这种分类会很有用 – 您可以根据分配的标签快速识别特定的资源。本主题介绍标签并演示如何创建标签。

主题

- 有关标签的基本知识
- 标记您的资源
- 将标签复制到备份
- 标签限制
- 权限和标记

有关标签的基本知识

标签是为 AWS 资源分配的标记。每个标签由您定义的两个部分组成：

- 标签键（例如，CostCenter、Environment 或 Project）。标签键区分大小写。
- 标签值（例如，111122223333 或 Production）。与标签键一样，标签值区分大小写。标签值可选。

您可以使用标签按照不同的方式（例如，按用途、所有者或环境）对 AWS 资源进行分类。例如，您可以为账户中的 Amazon FSx 文件系统定义一组标签，以跟踪每个实例的所有者和堆栈级别。

我们建议您针对每类资源设计一组标签，以满足您的需要。使用一组连续的标签键，管理资源时会更加轻松。您可以根据添加的标签搜索和筛选资源。有关如何实施有效资源标记策略的更多信息，请参阅 AWS 一般参考 中的标记 AWS 资源。

需要记住的一些标记行为：

- 标签对 Amazon FSx 没有任何语义意义，应严格按字符串进行解析。
- 标签不会自动分配至资源。
- 您可以修改标签的键和值，还可以随时删除资源的标签。
- 您可以将标签的值设为空的字符串，但是不能将其设为 null。
- 如果您添加的标签的值与该实例上现有标签的值相同，新的值就会覆盖旧值。
- 如果删除资源，资源的所有标签也会被删除。
- 如果您使用的是 Amazon FSx API、AWS Command Line Interface（AWS CLI）或 AWS SDK，您可以执行以下操作：
  - 您还可以使用 TagResource API 操作，以便将标签应用于现有资源。
  - 对于某些资源创建操作，您可以在创建资源时为其指定标签。通过在创建时标记资源，您不需要在资源创建后运行自定义标记脚本。

    如果无法在资源创建期间应用标签，Amazon FSx 会回滚资源创建流程。该行为有助于确保要么创建带有标签的资源，要么根本不创建资源，即任何时候都不会创建出未标记的资源。

    > **Note**
    >
    > 用户需要具有某些 AWS Identity and Access Management（IAM）权限才能在创建时标记资源。有关更多信息，请参阅 在创建过程中授予标记资源的权限。

标记您的资源

您可以标记账户中已存在的 Amazon FSx 资源。如果您使用的是 Amazon FSx 控制台，您可以使用相关资源屏幕上的标签选项卡向资源应用标签。创建资源时，您可以应用带有值的名称键，也可以在创建新文件系统时应用您选择的标签。但是，即使控制台根据名称键对资源进行组织，但此键对 Amazon FSx 服务没有任何语义意义。

要对可在创建时标记资源的用户和组实施精细控制，对于支持在创建时进行标记的 Amazon FSx API 操作，您可以在 IAM 策略中应用基于标签的资源级权限。通过在策略中使用此类权限，您可以获得以下优势：

- 资源从创建开始会受到适当的保护。
- 标签会立即用于资源，因此控制资源使用的任何基于标签的资源级权限都会立即生效。
- 可以更准确地对您的资源进行跟踪和报告。
- 您可以强制对新资源使用标记，可以控制对资源设置哪些标签键和值。

要控制对现有资源设置哪些标签键和值，您可以在 IAM 策略中对 `TagResource` 和 `UntagResource` Amazon FSx API 操作应用资源级权限。

有关在创建时标记 Amazon FSx 资源所需权限的更多信息，请参阅在创建过程中授予标记资源的权限。

有关如何在 IAM 策略中使用标签限制对 Amazon FSx 资源的访问权限的更多信息，请参阅使用标签控制对 Amazon FSx 资源的访问权限。

有关标记资源以便于计费的信息，请参阅《AWS Billing 用户指南》中的使用成本分配标签。

将标签复制到备份

当您在 Amazon FSx API 或 AWS CLI 中创建或更新卷时，您可以启用 `CopyTagsToBackups` 以自动将卷中的标签复制到备份中。

> **Note**
>
> 如果您在创建用户启动备份时指定标签（包括使用 Amazon FSx 控制台创建备份时的名称标签），即使您已启用 `CopyTagsToBackups`，也不会从卷中复制标签。

有关备份的更多信息，请参阅使用卷备份保护数据。有关启用 CopyTagsToBackups 的更多信息，请参阅《适用于 NetApp ONTAP 的 Amazon FSx 用户指南》中的 创建卷（CLI） 和 更新卷配置（CLI），或者《适用于 NetApp ONTAP 的 Amazon FSx API 参考》中的 CreateVolume 和 UpdateVolume。

标签限制

下面是适用于标签的基本限制：

- 每个资源的最大标签数是 50。
- 最大键长度为 128 个 Unicode 字符（采用 UTF-8 格式）。
- 最大值长度为 256 个 Unicode 字符（采用 UTF-8 格式）。
- 允许使用的字符是可以使用 UTF-8 表示的字母、数字和空格，以及以下字符：+ - （连字符）= . _（下划线）：/ @。
- 对于每个资源，每个标签键都必须是唯一的，每个标签键只能有一个值。
- 标签键和值区分大小写。
- aws：前缀专门预留供 AWS 使用。如果某个标签具有带此前缀的标签键，您无法编辑或删除该标签的键或值。具有 aws：前缀的标签不计入每个资源的标签数限制。

您不能仅依据标签删除资源，而必须指定资源标识符。例如，要删除您使用 DeleteMe 标签键标记的文件系统，您必须将 DeleteFileSystem 操作与文件系统的资源标识符（例如 fs-1234567890abcdef0）结合使用。

当您为公有或共享资源添加标签时，您分配的标签仅对您的 AWS 账户 可用；其他 AWS 账户 无权访问这些标签。为了对共享资源进行基于标签的访问控制，每个 AWS 账户 必须分配自己的一组标签来控制对资源的访问。

权限和标记

有关在创建时标记 Amazon FSx 资源所需权限的更多信息，请参阅在创建过程中授予标记资源的权限。

有关如何在 IAM 策略中使用标签限制对 Amazon FSx 资源的访问权限的更多信息，请参阅使用标签控制对 Amazon FSx 资源的访问权限。

保护您的数据

除通过自动复制文件系统数据确保高持久性以外，Amazon FSx 还为您提供以下选项，用于进一步保护您的数据：

- 原生 Amazon FSx 卷备份能够满足您在 Amazon FSx 中的备份保留和合规需求。
- 使用 AWS Backup，跨多个 AWS 服务 实施集中式管理的自动备份和保留策略。
- 快照通过将文件恢复到早期版本，使用户可以轻松撤消不想要的文件更改。
- 使用 SnapLock，创建“一次写入，多次读取”（WORM）存储卷，从而在指定的保留期内防止文件在提交后被修改或删除
- FlexCache 卷为读取密集型工作负载提供存储高效、经济实惠的高性能数据复制，而且数据基本保持不变。
- 使用 SnapMirror，创建到第二个文件系统的定时自动文件系统复制，以实现数据保护和灾难恢复。

主题

使用卷备份保护数据

借助 FSx for ONTAP，您可以对文件系统上的卷进行每日自动备份和用户启动备份来保护数据。为卷创建定期备份是一种最佳实践，有助于满足您的数据留存和合规需求。您可以将卷备份还原到您有权访问的任何现有 FSx for ONTAP 文件系统，该文件系统位于存储备份 AWS 区域 的位置。使用 Amazon FSx 备份可以轻松创建、查看、还原和删除卷的备份。

Amazon FSx 支持使用读写（RW）模式 `OntapVolumeType`来备份 ONTAP 卷。

> **Note**
>
> Amazon FSx 目前不支持备份数据保护（DP）卷、负载共享镜像（LSM）卷或 FlexCache 和 SnapMirror 目标卷。

主题

备份的工作方式

所有 Amazon FSx 备份（每日自动备份和用户启动备份）均为增量备份，这意味着这些备份仅存储自上次备份完成以来的数据更改。这样可以最大程度地减少创建备份所需的时间和每次备份使用的存储量。增量备份不存储重复数据，从而优化了存储成本。FSx for ONTAP 备份是按卷进行备份的，每个备份仅包含一个特定卷的数据。Amazon FSx 备份以冗余方式存储于多个可用区，以实现高持久性。

Amazon FSx 备份使用快照（卷的时间点和只读映像）来保持两次备份之间的增量。每次进行备份时，Amazon FSx 首先会拍摄卷的快照。备份快照存储在卷中，会占用卷上的存储空间。然后，Amazon FSx 将此快照与之前的备份快照（如果存在）进行比较，并仅将更改后的数据复制到您的备份中。

如果不存在之前的备份快照，则会将最新备份快照的全部内容复制到您的备份中。成功拍摄最新备份快照后，Amazon FSx 会删除之前的备份快照。用于最新备份的快照将保留在您的卷中，直到进行下一次备份，该过程将重复进行。为了优化备份存储成本，ONTAP 在备份中保留了卷节省的存储效率。

删除备份时，仅会删除该备份特有的数据。每个 Amazon FSx 备份都包含从备份创建新卷所需的所有信息，从而有效地还原卷的时间点快照。

每个卷 AWS 账户 和每个卷可以存储的备份数量有限制。有关更多信息，请参阅您可以提高的配额和每个文件系统的资源限额。

> **Note**
>
> 如果您使用 NDMP 进行备份，则 ONTAP 不允许在NDMP传输过程中继续执行诸如修补程序操作之类的维护活动。为避免延迟补丁，在文件系统的维护时段内应用补丁操作时，Amazon FSx 将中止所有NDMP活动的传输会话。修补完成后，您需要从客户端手动重启NDMP传输会话，因为 Amazon FSx 无法自动恢复这些会话。为避免备份中断，我们建议使用支持并行备份和补丁操作的 Amazon FSx 备份 AWS Backup或。

存储需求

您的卷和文件系统都必须有足够的可用 SSD 存储容量来存储备份快照。在拍摄备份快照时，快照消耗的其他存储容量不能致使卷的 SSD 存储利用率超过 98%。如果发生这种情况，备份将失败。您可以随时增加卷或文件系统的 SSD 存储空间，以确保备份不会中断。

每日自动备份

在创建文件系统时，默认为文件系统的卷启用每日自动备份。您可以随时为现有文件系统启用或禁用每日自动备份。所有卷的每日自动备份是在文件系统的每日备份窗口内进行的，每日备份窗口是在创建文件系统时自动设置的。您可以随时修改每日备份窗口。为获得最佳备份性能，我们建议您在客户端和应用程序访问卷上的数据时，选择一个在正常运行时间以外的每日备份窗口。我们还建议您选择与文件系统的维护时段不重叠的备份窗口。如果窗口重叠，则优先执行维护活动，并在维护完成后进行自动备份。已在进行的备份将在维护期间继续进行，但是，在维护完成之前，可能不会创建新的备份。如果在整个窗口期间都进行维护，则在该窗口期间可能不会进行自动备份。

您可以使用控制台，在创建文件系统时或随时将每日自动备份的保留期设置为 1 到 90 天的值。每日自动备份的默认保留期为 30 天。Amazon FSx 将在保留期到期后删除每日自动备份。使用 AWS CLI 和 API，您可以将保留期设置为 0 到 90 天之间的值；将其设置为 0 将禁用自动备份，并删除文件系统卷的所有现有自动备份。

每日自动备份、每日备份时段和备份保留期为文件系统设置，适用于文件系统上的所有卷。您可以使用 Amazon FSx 控制台 AWS CLI、或 API 来更改这些设置。有关更多信息，请参阅 更新文件系统。

卷处于离线状态时无法创建卷备份（每日自动备份或用户启动的备份）。有关更多信息，请参阅 查看离线卷。

> **Note**
>
> 每日自动备份的最长保留期为 90 天，但是您创建的用户启动的备份（包括使用创建的备份）将永久保留 AWS Backup，除非您或将其 AWS Backup 删除。

可以使用 Amazon FSx 控制台、CLI 和 API 手动删除每日自动备份。删除卷时，也会删除该卷的每日自动备份。Amazon FSx 提供了在删除卷之前为卷创建最终备份的选项。最终备份将永久保存，除非将其删除。

User-initiated 备份

借助 Amazon FSx，您可以随时使用 AWS 管理控制台 AWS CLI、和 API 手动备份文件系统的卷。与可能为某个卷创建的其他备份相比，用户启动的备份是增量备份，除非您将其删除，否则这些备份将永久保留。 User-initiated 即使您删除了创建备份的卷或文件系统，备份也会保留。您只能使用 Amazon FSx 控制台、API 或 CLI 删除用户启动备份。Amazon FSx 永远不会自动删除这些备份。

有关如何创建用户启动的备份的说明，请参阅 创建用户启动备份。

将标签复制到备份

当使用 CLI 或 API 创建或更新卷时，您可以启用 CopyTagsToBackups 以自动将卷中的标签复制到其备份中。但是，如果在创建用户启动的备份时添加了任何标签，包括在使用控制台时为备份命名，Amazon FSx 不会从卷中复制标签，即使已启用 CopyTagsToBackups。

使用 AWS Backup 使用亚马逊 FSx

AWS Backup 是通过为 NetApp ONTAP 卷备份您的 Amazon FSx 来保护您的数据的简单且经济实惠的方法。 AWS Backup 是一项统一的备份服务，旨在简化备份的创建、恢复和删除，同时提供改进的报告和审计。使用 AWS Backup 可以更轻松地为法律法规和专业合规性制定集中式备份策略。它还提供了一个可以执行以下操作的中心位置，从而简化了对 AWS 存储卷、数据库和文件系统的保护：

- 配置和审核要备份的 AWS 资源。
- 计划自动备份。

- 设置保留策略。
- 监控所有最近的备份、复制和还原活动。

AWS Backup 使用 Amazon FSx 的内置备份功能。使用 AWS Backup 控制台创建的备份具有相同级别的文件系统一致性和性能，与用户启动的对您的卷进行的任何其他 Amazon FSx 备份相比是增量的，并且提供的还原选项与使用 Amazon FSx 控制台进行的备份相同。使用 AWS Backup 来管理这些备份提供了其他功能，包括能够像每小时一样频繁地创建定时备份。您可以通过将备份存储在备份库中来增加一道防护层，保护备份免遭意外或恶意删除。

由创建的备份 AWS Backup 被视为用户启动的备份，它们计入 Amazon FSx 用户启动的备份配额。有关更多信息，请参阅 您可以提高的配额。您可以查看和恢复 AWS Backup 使用 Amazon FSx 控制台、CLI 和 API 创建的备份。但是，您无法删除 AWS Backup 在 Amazon FSx 控制台、CLI 或 API 中创建的备份。有关更多信息，请参阅《 AWS Backup 开发人员指南》 AWS Backup中的入门。

AWS Backup 无法备份处于离线状态的卷。

您可以使用标签以选择在备份计划中保护哪些 FSx for ONTAP 资源。这些标签必须应用于卷级别，而非整个文件系统级别。有关更多信息，请参阅《 AWS Backup 开发人员指南》中的为备份计划分配资源。

将备份还原至新卷

可以将卷备份还原至文件系统上的新卷，该文件系统与存储备份所在的位置同处于 AWS 区域 。您无法将备份还原到与备份 AWS 区域 不同的文件系统中。

在 FSx for ONTAP 第二代文件系统上还原备份时，客户端可以在还原卷的同时挂载和读取卷中的数据。在 Amazon FSx 将所有元数据加载到新卷并且该卷报告的生命周期状态为 CREATED 之后，客户端就可以挂载正在还原的卷并读取文件数据。可以在 Amazon FSx 控制台的卷详细信息页面和 describe-volumes CLI 命令的响应中查找卷的生命周期状态。

在从备份还原卷的同时从卷中读取数据时，如果数据尚未下载到卷上，则首次访问数据将产生长达数十毫秒的读取延迟。这些读取缓存在 SSD 层中，后续读取预计会有亚毫秒的读取延迟。

Amazon FSx 使卷可供只读访问用去的时间与备份中存储的文件元数据量成正比。文件元数据通常占总备份数据的 1-7%，具体比例取决于数据集中的平均文件大小（小文件数据集比大型文件数据集消耗更多的元数据）。

将 FlexGroup 卷备份还原到具有不同于原始文件系统的高可用性（HA）对数的文件系统时，Amazon FSx 会额外添加组成卷，以确保各组件均匀分布。

> **Note**
>
> Amazon FSx 不支持在从 SnapLock 卷或第一代文件系统上任何卷的备份中还原卷时读取访问数据。在还原这些备份的过程中，在还原过程完成且所有元数据和数据都加载到新卷上之后，卷就可用于挂载和访问数据。

还原备份时，所有数据最初写入 SSD 存储层。在还原过程中，根据正在还原的卷的分层策略将数据分层到容量池存储。由于数据首先写入的是 SSD 层，因此，如果文件系统的 SSD 存储空间用完，Amazon FSx 会暂停还原过程。一旦有足够的 SSD 空间可用来继续此过程，还原就会自动恢复。如果还原卷的分层策略为 `All`，则定期运行的后台进程会将数据分层到容量池。如果还原卷的分层策略为 `Snapshot Only` 或 `Auto`，则在文件系统的 SSD 利用率大于 50% 且冷却速率由分层策略的冷却期决定时将数据分层到容量池。

如果在第二代文件系统上将备份还原至新卷时，工作负载需要稳定的亚毫秒级读取延迟，我们建议在启动还原时将卷的分层策略设置为 `None`，然后等到所有数据都完全下载到卷后再进行访问。所有数据都将在您尝试访问之前加载到 SSD 存储中，从而为您提供一致的低延迟数据访问。

有关如何将备份还原至新卷的分步说明，请参阅 将备份还原至新卷。

在第二代文件系统上，您还可以仅从备份中还原部分数据，而不必等待整个还原操作完成。仅还原备份的部分数据可以使您在数据意外删除、篡改或损坏时更快地恢复操作。有关更多信息，请参阅 还原部分数据。

您可以在 AWS 管理控制台、 AWS CLI和 API 中监控在第二代文件系统上恢复备份时的进度。有关更多信息，请参阅 在还原备份时监控进度。

> **Note**
>
> - 从备份中恢复卷时，您无法创建卷快照或执行基于快照的操作，例如克隆、 SnapMirror 复制和创建卷的备份。
> - 还原后的卷始终与原始卷具有相同的卷风格。还原时无法更改卷风格。

备份与还原性能

影响备份和还原操作性能的因素有很多。备份和还原操作是后台进程，这意味着其优先级低于客户端 IO 操作。客户端 IO 操作包括 NFS、CIFS 和 iSCSI 数据及元数据的读取和写入。所有后台进程仅利用

文件系统吞吐能力中未使用的部分，可能需要几分钟到几小时来完成，具体取决于备份的大小和文件系统上未使用的吞吐能力。

影响备份和还原性能的其他因素包括存储数据的存储层和数据集配置文件。我们建议在大部分数据处于 SSD 存储上时创建卷的第一个备份。与主要包含大文件的类似大小的数据集相比，主要包含小文件的数据集通常具有较低的性能。这是因为处理大量小文件消耗的 CPU 周期和网络开销高于处理数量较少的大文件。

一般来说，在备份 SSD 存储层中存储的数据时，预计可达到以下备份速率：

- 750 MBps，跨多个主要包含大文件的并发备份。
- 100 MBps，跨多个主要包含小文件的并发备份。

通常，可以提供以下还原速率。

- 250 MBps，跨多个主要包含大文件的并发还原。
- 100 MBps，跨多个主要包含小文件的并发还原。

正在备份 SnapLock 卷

您可以备份 SnapLock 卷以获得额外的数据保护。恢复卷时，该 SnapLock 卷的原始设置（例如默认保留期、最短保留期和最长保留期）将保留。还会保留“一次写入，多次读取”（WORM）设置和依法保留。

> **Note**
>
> 无法备份 SnapLock FlexGroup 卷。

您可以将 SnapLock 卷的备份恢复为 SnapLock 卷或非 SnapLock 卷。但是，您不能将非 SnapLock 卷的备份恢复为 SnapLock 卷。

有关更多信息，请参阅 SnapLock 的工作原理。

创建用户启动备份

以下过程介绍了如何创建卷的用户启动备份。

卷处于离线状态时无法创建卷备份。有关更多信息，请参阅 查看离线卷。

创建用户启动的备份（控制台）

1. 打开 Amazon FSx 控制台，网址为。https://console.aws.amazon.com/fsx/
2. 导航到文件系统，然后选择要为其备份卷的 ONTAP 文件系统。
3. 选择卷选项卡。
4. 选择要备份的卷。
5. 在操作中，选择创建备份。
6. 在打开的创建备份对话框中，为备份提供一个名称。备份名称最多可以包含 256 个 Unicode 字符，以及字母、空格、数字和特殊字符 . + - = _ : /
7. 选择创建备份。

现在，您已经为文件系统的某个卷创建了备份。在左侧导航中选择备份，即可在 Amazon FSx 控制台中找到所有备份。您可以搜索您为备份提供的名称，通过表格筛选条件仅显示匹配的结果。

当您按照此过程所述创建用户启动备份时，它具有 `USER_INITIATED` 类型，并且在完全可用之前显示为 `CREATING` 状态。

将备份还原至新卷

以下过程介绍如何使用和将 FSx for ONTAP 备份还原到新卷。 AWS 管理控制台 AWS CLI将卷恢复到第二代文件系统时，可以使用 AWS 管理控制台 AWS CLI、和 API 监控进度。

将卷备份还原至新卷（控制台）

1. 打开 Amazon FSx 控制台，网址为。https://console.aws.amazon.com/fsx/
2. 在导航窗格中，选择备份，然后选择要还原的 FSx for ONTAP 卷备份。
3. 在右上角操作菜单中，选择还原备份。此时将出现从备份创建卷页面。
4. 从下拉菜单中选择要将备份还原到的 FSx for ONTAP 文件系统和存储虚拟机。
5. 在右上角操作菜单中，选择还原备份。此时将出现从备份创建卷页面。
6. 从下拉菜单中选择要将备份还原到的 FSx for ONTAP 文件系统和存储虚拟机。
7. 卷详细信息下有几个选项。首先，输入卷名。最多可以使用 203 个字母数字或下划线（_）字符。
8. 在卷大小中输入 20–314572800 之间的任意整数来指定卷大小，单位为兆字节（MiB）。
9. 对于卷类型，选择 Read-Write (RW) 创建可读写卷，或选择 “数据保护” (DP) 创建只读卷，可用作NetAppSnapMirror或SnapVault关系的目标。有关更多信息，请参阅 卷类型。

10. 在连接路径中，输入文件系统中用于挂载此卷的位置。该名称必须包含一个前导正斜杠，例如 `/vol3`。
11. 在存储效率中选择已启用来启用 ONTAP 存储效率功能（重复数据删除、压缩和紧凑处理）。有关更多信息，请参阅 存储效率。
12. 在卷安全风格中，选择 Unix（Linux）、NTFS 或混合。卷的安全风格将决定在进行多协议访问时优先选择 NTFS 还是 UNIX ACL。“混合”模式不是多协议访问的必要条件，仅推荐高级用户使用。
13. 在快照策略中选择用于此卷的快照策略。有关快照策略的更多信息，请参阅快照策略。

    如果选择自定义策略，则必须在 custom-policy 字段中指定策略名称。必须是已存在于 SVM 或文件系统中的自定义策略。您可以通过 ONTAP CLI 或 REST API 创建自定义快照策略。有关更多信息，请参阅《NetApp ONTAP 产品文档》中的创建快照策略。
14. 分层策略冷却周期的有效值为 2–183 天。卷的分层策略冷却周期定义了将未被访问的数据标记为“冷”并移动到容量池存储之前的天数。此设置仅会对 `Auto` 和 `Snapshot-only` 策略造成影响。
15. 在高级部分，对于 SnapLock 配置，您可以保留默认的禁用设置，也可以选择启用以配置 SnapLock 卷。有关配置 SnapLock Compliance 卷或 SnapLock Enterprise 卷的更多信息，请参阅 了解 SnapLock Compliance 和 了解 SnapLock Enterprise。有关 SnapLock的更多信息，请参阅使用 SnapLock 保护您的数据。
16. 选择确认即可创建卷。
17. 如果要将备份还原至第二代文件系统，则可以在卷页面的更新选项卡上监控备份还原进度。有关更多信息，请参阅 在还原备份时监控进度。

将备份还原到新卷（CLI）

使用 create-volume-frome-backup CLI 命令或 CreateVolumeFromBackup等效的 API 命令将卷备份恢复到新卷。

- ```
  $ aws fsx create-volume-from-backup --backup-id backup-08e6fc1133fff3532 \
        --name demo --ontap-configuration JunctionPath=/demo,SizeInMegabytes=100000,\
        StorageVirtualMachineId=svm-0f04a9c7c27e1908b,TieringPolicy={Name=ALL}
  ```

  成功请求将备份还原至第二代文件系统的系统响应如下所示。响应包括提供请求相关状态和进度信息的 `"AdministrativeActions"` 对象。

  ```
  {
        "Volume": {
            "CreationTime": 1692721488.428,
  ```
  ```

```
          "FileSystemId": "fs-07ab735385276ed60",
          "Lifecycle": "CREATING",
          "Name": "demo",
          "OntapConfiguration": {
              "FlexCacheEndpointType": "NONE",
              "JunctionPath": "/demo",
              "SizeInMegabytes": 100000,
              "StorageEfficiencyEnabled": true,
              "StorageVirtualMachineId": "svm-0f04a9c7c27e1908b",
              "StorageVirtualMachineRoot": false,
              "TieringPolicy": {
                  "Name": "ALL"
              },
              "OntapVolumeType": "DP",
              "SnapshotPolicy": "default",
              "CopyTagsToBackups": false,
          },
          "ResourceARN": "arn:aws:fsx:us-east-1:752825163408:volume/
fs-07ab735385276ed60/fsvol-0b6ec764c9c5f654a",
          "VolumeId": "fsvol-0b6ec764c9c5f654a",
          "VolumeType": "ONTAP",
  --->    "AdministrativeActions": [
              {
                  "AdministrativeActionType": "DOWNLOAD_DATA_FROM_BACKUP",
                  "RequestTime": 1685729972.069,
                  "Status": "PENDING"
              }
          ]                 <----
      }
  }
```

成功请求将备份还原至第一代文件系统的系统响应如下所示。

```
{
      "Volume": {
          "CreationTime": 1692721488.428,
          "FileSystemId": "fs-07ab735385276ed60",
          "Lifecycle": "CREATING",
          "Name": "demo",
          "OntapConfiguration": {
              "FlexCacheEndpointType": "NONE",
              "JunctionPath": "/demo",
              "SizeInMegabytes": 100000,
```

```
                "StorageEfficiencyEnabled": true,
                "StorageVirtualMachineId": "svm-0f04a9c7c27e1908b",
                "StorageVirtualMachineRoot": false,
                "TieringPolicy": {
                    "Name": "ALL"
                },
                "OntapVolumeType": "DP",
                "SnapshotPolicy": "default",
                "CopyTagsToBackups": false,
            },
            "ResourceARN": "arn:aws:fsx:us-east-1:752825163408:volume/
fs-07ab735385276ed60/fsvol-0b6ec764c9c5f654a",
            "VolumeId": "fsvol-0b6ec764c9c5f654a",
            "VolumeType": "ONTAP",
        }
    }
```

将卷恢复到第二代文件系统时，可以使用 AWS 管理控制台 AWS CLI、和 API 监控进度。

还原部分数据

在将备份还原至第二代文件系统上的新卷时，可以从备份中还原部分数据，而不必等到整个备份数据集完成全部还原。

以下过程列出了您在还原备份但又无法等待整个还原完成时进行部分数据恢复需要采取的步骤：

在还原备份时还原部分数据

1. 打开 Amazon FSx 控制台，网址为。https://console.aws.amazon.com/fsx/
2. 在备份页面中，找到含有要还原的数据版本的备份。
3. 在右上角操作菜单中，选择还原备份。此时将出现从备份创建卷页面。
4. 从下拉菜单中选择要将备份还原到的 FSx for ONTAP 文件系统和存储虚拟机。
5. 在卷详细信息下，配置卷以满足要求。
6. 选择确认即可创建卷。
7. 监控备份还原的进度。
8. 当卷报告生命周期状态为 CREATED 时，挂载正在还原的卷。
9. 在卷上找到要复制的部分数据。
10. 将数据复制到应用程序使用的现有卷中。

11. 一旦将备份中的所需数据复制到目标位置后，就可以在还原完成前删除正在还原的卷，以优化文件系统资源的利用率。

在还原备份时监控进度

您可以在 AWS 管理控制台、 AWS CLI和 API 中监控将卷备份恢复到第二代文件系统时的进度。与所有 Amazon FSx 管理操作一样，在操作完成后 30 天内，控制台、CLI 和 API 中都会提供备份还原的状态。

在还原备份时监控进度（控制台）

打开 Amazon FSx 控制台，网址为。https://console.aws.amazon.com/fsx/

1. 在左侧导航菜单中，选择卷。
2. 选择备份要还原到的卷。
3. 选择更新选项卡。
4. 备份还原更新类型提供了以下信息：

   - 待处理表示正在将文件元数据下载到卷上。卷的生命周期状态为正在创建。
   - 进行中表示卷可用，客户端可以通过只读访问数据来挂载卷。进度百分比显示已下载到卷的数据的百分比。
   - 已完成表示所有数据都已下载到卷中，且备份还原已完成。客户端现在拥有读写访问权限。对于 RW 卷，此时卷类型从 DP 变为 RW。

在还原备份时监控进度（CLI）

- 在第二代 FSx for ONTAP 文件系统上将备份还原至新卷时，可以使用 `describe-volumes` CLI 命令监控还原进度。

  将备份还原至第二代文件系统时，响应包括 AdministrativeActions 对象，其中提供了有关数据下载过程的状态信息。这些区域有：

```
$ aws fsx describe-volumes
{
    “Volumes”: [
        {
            “CreationTime”: 1691686114.674,
            “FileSystemId”: fs-029ff92192bd4d375,
```

```
            “LifeCycle”: “CREATING”,
            “Name”: vol1,
            “OntapConfiguration”: {
                   “FlexCacheEndpointType”: “NONE”,
                   “JunctionPath”: “/vol1”,
                   “SizeInMegabytes”: 100000,
                   “StorageEfficiencyEnabled”: true,
                   “StorageVirtualMachineId”: “svm-0ed1d714019426ca9”,
                   “StorageVirtualMachineRoot”: false,
                   “TieringPolicy”: {
                    “Name”: “ALL”
                   },
                   “OntapVolumeType”: “DP”,
                   “SnapshotPolicy”: “default”,
                   “CopyTagsToBackups”: false,
                  },
                  “ResourceARN”: “arn:aws:fsx:us-east-1:630831496844:volume/
fs-08ac75f715c6aec76/fsvol-094c015af930790fa”,
                  “VolumeId”: “fsvol-094c015af930790fa”,
                  “VolumeType”: “ONTAP”,
                  “AdministrativeActions”: [
                         {
                          “AdministrativeActionType”: “DOWNLOAD_DATA_FROM_BACKUP”,
                          “RequestTime”: 1685729972.069,
                          “Status”: “PENDING”
                         }
                  ]
    }
```

Amazon FSx 将所有文件元数据加载到还原卷后，这些字段将具有以下值：

- `"LifeCycle": "CREATED"` - 表示卷已准备挂载。
- `"OntapVolumeType": "DP"` - 表示下载文件数据时卷处于只读状态。
- `"ProgressPercent` - 显示已加载到卷的文件数据的百分比。
- `"Status": "IN_PROGRESS"` - 正在将文件数据下载到卷中。

在还原过程的这一阶段，可以通过只读访问要还原的备份中的所有数据来挂载卷。

当 Amazon FSx 将所有文件数据下载到新卷后，如果这是 RW 卷，客户端将拥有完全的读写访问权限。这些指标具有以下值：

- `"LifeCycle": "CREATED"` - 不变
- `"OntapVolumeType": "RW"` - 表示客户端具有完全的读写访问权限。
- `"Status": "COMPLETED"` - 表示还原已完成。

如果还原过程失败，则 `AdminstrativeAction > Status` 的值将为 `FAILED`。`FailureDetails` 对象中提供了错误消息。有关更多信息，请参阅亚马逊 FSx API 参考AdministrativeActionFailureDetails中的

删除备份

可以使用 Amazon FSx 控制台、Amazon FSx API 或 AWS Command Line Interface （ AWS CLI ）删除卷的每日自动备份和用户启动备份。删除备份是一项永久性且不可恢复的操作。删除的备份中的所有数据也会被删除。除非您确定将来不再需要该备份，否则不要删除该备份。当源卷离线时，就无法删除备份。

在所有 FSx for ONTAP 文件系统上，可以在从备份还原卷的过程中将卷删除。在还原期间删除卷可有效地取消正在进行的还原操作。

> **Note**
>
> 除非已删除 ONTAP 卷的其他所有备份，否则 Amazon FSx 不支持删除卷的最新 `AVAILABLE` 备份。

要删除使用创建的备份 AWS Backup，请参阅《 AWS Backup 开发人员指南》中的删除备份。

删除备份（控制台）

1. 打开 Amazon FSx 控制台，网址为。https://console.aws.amazon.com/fsx/
2. 在控制台控制面板的左侧导航窗格中选择备份。
3. 选择备份表中您要删除的备份，然后选择删除备份。
4. 在打开的删除备份对话框中，确认所示备份 ID 与要删除的备份一致。
5. 确认已选中要删除的备份对应的复选框。
6. 选择删除备份。

您的备份和所有包含的数据现已永久删除且不可恢复。

删除备份（CLI）

- 使用 delete-backup CLI 命令或等效 DeleteBackup 的 API 操作删除用于 ONTAP 卷备份的 FSx，如以下示例所示。

```
$ aws fsx delete-backup --backup-id backup-a0123456789abcdef
```

系统响应包括当前所删除备份的 ID 及生命周期状态，其值为 DELETED，表示请求已成功。

```
{
    "BackupId": "backup-a0123456789abcdef",
    "Lifecycle": "DELETED"
}
```

使用快照保护您的数据

快照是 Amazon FSx for NetApp ONTAP 卷在某个时间点的只读映像。快照可防止卷中的文件被意外删除或修改。用户可通过快照轻松查看和还原早期快照中的单个文件或文件夹，以撤销更改、恢复删除的内容以及比较文件版本。

快照包含自上次快照以来发生更改的数据，这些数据会消耗文件系统的 SSD 存储容量。任何卷备份中均不含快照。默认情况下，使用 `default` 快照策略在卷上启用快照。快照存储于卷根的 `.snapshot` 目录中。不论何时，每个卷最多可存储 1,023 张快照。达到此限制后，必须先删除现有快照，然后才能创建卷的新快照。

主题

- 快照策略
- 从快照恢复文件
- 查看常见快照
- 更新卷的快照预留空间
- 禁用自动快照
- 删除快照
- 删除快照
- 快照预留

快照策略

快照策略定义系统为卷创建快照的方式。该策略指定何时创建快照、保留多少副本以及如何命名快照。ONTAP 有三种内置快 FSx 照策略：

- `default`
- `default-1weekly`
- `none`

默认情况下，每个卷都与文件系统的 `default` 快照策略相关联。建议在大多数工作负载中使用此策略。

`default` 策略会按照以下计划自动创建快照，并删除最旧的快照副本，以为较新的副本腾出空间：

- 每小时过五分钟后最多拍摄六张每小时快照。
- 周一至周六午夜过 10 分钟后最多拍摄两张每日快照。
- 每周日午夜过 15 分钟后最多拍摄两张每周快照。

> **Note**
>
> 快照时间基于文件系统的时区，默认为协调世界时（UTC）。您可以使用 `timezone -timezone` *`time_zone`* ONTAP CLI 命令 FSx 为 ONTAP 文件系统设置时区。有关访问 ONTAP CLI 的更多信息，请参阅 使用 NetApp ONTAP CLI。

`default-1weekly` 策略的工作原理与 `default` 策略相同，只是它仅保留每周计划中的一张快照。

`none` 策略不拍摄任何快照。您可将此策略分配给卷，以防止拍摄自动快照。

您还可以使用 ONTAP CLI 或 REST API 创建自定义快照策略。有关更多信息，请参阅 NetApp ONTAP 产品文档中的创建快照策略。在亚马逊 FSx 控制台、或 Amazon FSx API 中创建或更新卷时 AWS CLI，您可以选择快照策略。有关更多信息，请参阅创建卷和更新卷。

从快照恢复文件

使用 Amazon FSx 文件系统上的快照，您可以快速恢复单个文件或文件夹的先前版本。

如果使用 Linux 和 macOS 客户端，您可以在卷根的 `.snapshot` 目录中查看快照。如果使用 Windows 客户端，您可以在 Windows 资源管理器的 `Previous Versions` 选项卡（右键单击文件或文件夹时）中查看快照。

使用快照还原文件（Linux 和 macOS 客户端）

1. 如果原始文件仍然存在，并且您不希望它被快照中的文件覆盖，那么请使用 Linux 或 macOS 客户端重命名原始文件或将其移至其他目录中。
2. 在 `.snapshot` 目录中，找到包含要还原的文件版本的快照。
3. 将文件从 `.snapshot` 目录复制到文件最初存在的目录中。

使用快照还原文件（Windows 客户端）

Windows 客户端的用户可使用常用的 Windows 文件资源管理器界面将文件还原到以前的版本。

1. 若要还原文件，用户需选择要还原的文件，然后从上下文（右键单击）菜单中选择还原先前版本。
2. 然后，用户就可以从先前版本列表中查看和还原以前的版本。

快照中的数据是只读的。如要修改先前版本选项卡中列出的文件和文件夹，则必须将要修改的文件和文件夹的副本保存到可写入的位置，然后对副本进行修改。

查看常见快照

常见快照用于在两次备份之间实现增量备份。此过程介绍了如何识别卷上的常见快照。

查看卷的常见快照

- 要确定哪个快照是卷的常见快照，可使用 volume snapshot show ONTAP CLI 命令。

  ```
  volume snapshot show -volume volume-name
  ```

  在输出中，公用快照的名称的格式为`backup-id`，其中`id`是 17 位字母数字字符串，如以下示例所示：

  ```
  FsxIdabc12345::> volume snapshot show -volume test_vol
                                    ---Blocks---
  Vserver Volume    Snapshot                    Size     Total% Used%
  -------- -------- --------------------------- -------- ------ -----
  dest-svm test_vol
  ```

```
                    snap1                          144KB     0%      3%
                    snap2                          832KB     0%     16%
          --->      backup-abcdef0123456789a      4.87MB     0%     53% <---
                    weekly.2024-05-26_0015        5.02MB     0%     54%
                    weekly.2024-06-02_0015        2.22MB     0%     34%
                    daily.2024-06-04_0010          284KB     0%      6%
                    daily.2024-06-05_0010         4.29MB     0%     50%
                    hourly.2024-06-05_0705         168KB     0%      4%
8 entries were displayed.
```

Important

请勿删除卷上的常见快照，因为这种快照用于在两次备份之间实现增量备份。删除卷的常见快照会导致下次备份时对卷进行完全备份，而不是增量备份。

更新卷的快照预留空间

您可以按照以下过程所述，使用 NetApp ONTAP CLI 或 API 更改卷上的快照预留空间。

1. 要访问 ONTAP CLI，请运行以下命令在 Amazon FSx for NetApp ONTAP 文件系统或 SVM 的管理端口上建立 SSH 会话。将 *management_endpoint_ip* 替换为文件系统管理端口的 IP 地址。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   有关更多信息，请参阅 使用 ONTAP CLI 管理文件系统。

2. 使用 volume modify ONTAP CLI 命令更改快照副本预留磁盘空间的百分比。将以下占位符值替换为您自己的数据：

   - *svm_name* - 使用 SVM 的名字。
   - *vol_name* - 使用卷名。
   - *percent* - 要为快照副本预留的磁盘空间百分比。

   ```
   ::> volume modify -vserver svm_name -volume vol_name -percent-snapshot-
   space percent
   ```

   以下示例将卷 1 的快照预留空间更改为卷存储容量的 25%。

```
::> volume modify -vserver vs0 -volume vol1 -percent-snapshot-space 25
```

禁用自动快照

自动快照由您的 for ONTAP 文件系统中的卷 FSx 的默认快照策略启用。如果您不需要数据快照（例如，如果您使用的是测试数据），则可以通过将卷的快照策略设置为none使用 AWS 管理控制台、AWS CLI 和 API 以及 ONTAP CLI 来禁用快照，如以下过程所述。

禁用自动快照（AWS 控制台）

1. 打开亚马逊 FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 导航到文件系统，然后选择要为其更新卷的 ONTAP 文件系统。
3. 选择卷选项卡。
4. 选择要更新的卷。
5. 在操作中，选择更新卷。

   系统将显示更新卷对话框，其中包含该卷的当前设置。
6. 对于快照策略，选择无。
7. 选择更新即可更新卷。

禁用自动快照 (AWS CLI)

- 使用 update- AWS vol ume CLI 命令（或UpdateVolume等效的 API 命令）将设置none为SnapshotPolicy，如以下示例所示。

```
aws fsx update-volume \
    --volume-id fsvol-1234567890abcdefa \
    --name new_vol \
    --ontap-configuration CopyTagsToBackups=true,JunctionPath=/new_vol, \
           SizeInMegabytes=2048,SnapshotPolicy=none, \
           StorageEfficiencyEnabled=true, \
           TieringPolicy=all
```

禁用自动快照（ONTAP CLI）

设置卷的快照策略，使用 none 默认策略来关闭自动快照。

1. 使用 volume snapshot policy show ONTAP CLI 命令可显示 none 策略。

```
::> snapshot policy show -policy none

Vserver: FsxIdabcdef01234567892
                         Number of Is
Policy Name              Schedules Enabled Comment
------------------------ --------- ------- ----------------------------------
none                             0 false   Policy for no automatic snapshots.
    Schedule               Count     Prefix                 SnapMirror Label
    ---------------------- -----     ---------------------- -------------------
    -                          -     -                      -
```

2. 使用 volume modify ONTAP CLI 命令将卷的快照策略设置为 none 以禁用自动快照。将以下占位符值替换为您自己的数据：

   - *svm_name* - 使用 SVM 的名字。
   - *vol_name* - 使用卷名。

   当系统提示继续操作时，请输入 **y**。

```
::> volume modify -vserver svm_name -volume vol_name -snapshot-policy none

Warning: You are changing the Snapshot policy on volume "vol_name" to "none".
 Snapshot copies on this volume
        that do not match any of the prefixes of the new Snapshot policy will not
 be deleted. However, when
        the new Snapshot policy takes effect, depending on the new retention
 count, any existing Snapshot copies
        that continue to use the same prefixes might be deleted. See the 'volume
 modify' man page for more information.
Do you want to continue? {y|n}: y
Volume modify successful on volume vol_name of Vserver svm_name.
```

删除快照

快照仅占用自上次快照后发生变化的卷数据的存储容量。因此，如果您的工作负载快速写入数据，则旧数据的快照可能会占用卷的大部分容量。

例如，volume show-space ONTAP CLI 命令输出显示有 140 KB 的 User Data。然而，在删除用户数据前，该卷内有 9.8 GB 的 User Data。即使删除了卷中的文件，但快照仍可能引用旧的用户数据。因此，尽管卷上几乎没有用户数据，但上例中的 Snapshot Reserve 和 Snapshot Spill 总共占用了 9.8 GB 的空间。

若要释放卷上的空间，可删除不再需要的旧快照。由于快照是增量快照，因此删除快照时回收的存储量不会等于快照的大小。您可以使用卷快照 com pute-reclaimable-vserver ONTAP cli 命令查看删除快照时可以回收的存储量，使用您的数据来替换、和。*svm_name vol_name snapshot_name*

```
fsid8970abc52::> volume snapshot compute-reclaimable -vserver svm_name -volume vol_name
 -snapshot snapshot_name
A total of 667648 bytes can be reclaimed.
```

您可通过创建快照自动删除策略或手动删除快照来删除快照。删除快照会删除快照中存储的已更改数据。

删除快照

使用 volume snapshot delete ONTAP CLI 命令手动删除快照，用您的数据替换以下占位符值：

- 将 *svm_name* 替换为卷创建时所用 SVM 的名称。
- 将 *vol_name* 替换为卷的名称。
- 将 *snapshot_name* 替换为快照的名称。该命令支持 *snapshot_name* 的通配符（*）。因此，您可以删除所有的每小时快照，例如，使用 hourly*。

> **Important**
>
> 如果您启用了亚马逊 FSx 备份，Amazon FSx 会保留每个卷的最新亚马逊 FSx 备份的快照。这些快照用于在两次备份之间实现增量备份，不得使用此方法将其删除。有关更多信息，请参阅 查看常见快照。

```
FsxIdabcdef01234567892::> volume snapshot delete -vserver svm_name -volume vol_name -
snapshot snapshot_name
```

创建快照自动删除策略

您可以创建一个策略，以便在卷可用空间不足时自动删除快照。使用 volume snapshot autodelete modify ONTAP CLI 命令为卷建立自动删除策略。

使用此命令时，应使用您的数据替换以下占位符值：

- 将 *svm_name* 替换为卷创建时所用 SVM 的名称。
- 将 *vol_name* 替换为卷的名称。

请为 `-trigger` 指定以下其中一个值：

- `volume` – 如果您希望删除快照的阈值与已用卷总容量阈值相对应，请使用 `volume`。触发快照删除的已用卷容量阈值由卷的大小决定，阈值从已用容量的 85% 到 98% 不等。容量越小，阈值越小，容量越大，阈值越大。
- `snap_reserve` – 如果您希望根据快照储备中可保存的内容来删除快照，请使用 `snap_reserve`。

```
::> volume snapshot autodelete modify -vserver svm_name -volume vol_name -enabled true
 -trigger [volume|snap_reserve]
```

有关更多信息，请参阅 NetApp ONTAP 文档中心中的卷快照自动删除修改命令。

快照预留

快照副本预留设置一个特定的卷存储容量百分比来存储快照副本，默认值为 5%。快照副本预留必须为快照副本（包括卷备份）分配足够的空间。如果快照副本超过快照预留空间，则必须从活动文件系统中删除现有快照副本，以恢复存储容量供文件系统使用。您还可以修改分配给快照副本的磁盘空间百分比。

每当快照消耗量超过 100% 的快照预留空间时，快照会开始占用主要 SSD 存储空间。此过程称为“快照溢出”。当快照继续占用活动文件系统空间时，文件系统就有被占满的风险。如果文件系统由于快照溢出而占满，则只有在删除足够的快照后才能创建文件。

当快照预留中有足够的磁盘空间供快照使用时，从主要 SSD 层中删除文件可以为新文件腾出磁盘空间，而引用这些文件的快照副本仅占用快照副本预留中的空间。

由于无法阻止快照占用磁盘空间超过为其预留的容量（快照预留），因此必须为快照预留足够的磁盘空间，以便主要 SSD 层始终有可用空间来创建新文件或修改现有文件。

如果快照是在磁盘已满的情况下创建的，则从主要 SSD 层中删除文件不会产生任何可用空间，因为所有这些数据也会被新创建的快照引用。要创建或更新任何文件，必须删除快照释放存储空间。

您可以使用 NetApp ONTAP CLI 修改卷上的快照预留量。有关更多信息，请参阅 更新卷的快照预留空间。

使用自主勒索软件防护保护您的数据

自主勒索软件防护（ARP）是一项 NetApp ONTAP 人工智能驱动的功能，可在您的 Windows 或 Linux 客户端遭到入侵时监控和保护您的数据免受勒索软件和恶意软件攻击。使用机器学习，ARP 可熟悉您的 FSx for ONTAP 文件系统，从而主动检测异常活动。在适用于 NetApp ONTAP 的 Amazon FSx 可用的所有 AWS 区域 中，ARP 均适用于所有全新和现有的 FSx for ONTAP 文件系统。

ARP 工作原理

您可以使用 ONTAP CLI 或 REST API，在 SVM 中按卷启用 ARP，也可以默认启用所有新卷的 ARP。有关启用 ARP 的更多信息，请参阅 启用自主勒索软件防护。

由于 ARP 的 AI 在全面的数据集上进行训练，因此 ARP 无需经过一段时间的学习期即可在 FlexVol 卷上运行，因此可立即以主动模式启动。ARP AI 还具有自动更新功能，确保可抵御最新威胁的持续保护和弹性。主动模式下，ARP 会监控卷上的传入数据和活动，以识别潜在的勒索软件和恶意软件攻击。有关更多信息，请参阅 ARP 查找的内容。如果 ARP 检测到任何异常活动，ONTAP 会自动创建快照，助您将数据恢复至尽可能接近潜在攻击发生的时间点。快照以 `Anti_ransomware_backup` 为前缀，因此易于识别。如果确定攻击概率为中等，ONTAP 会生成事件管理系统（EMS）消息供您审核。有关更多信息，请参阅 如何通过 ARP 响应可疑攻击 和 了解自主勒索软件防护的 EMS 警报。

对于大多数工作负载，ARP 的性能开销不足挂齿。如果您的卷存在读取密集型工作负载，NetApp 建议每个文件系统保护的此类卷不超过 150 个。如果超过此数量，该工作负载的 IOPS 最多可能降低 4%。如果您的卷存在写入密集型工作负载，NetApp 建议每个文件系统保护的此类卷不超过 60 个。否则，该工作负载的 IOPS 最多可能降低 10%。有关性能的更多信息，请参阅 适用于 ONTAP 性能的 Amazon FS NetApp x。

在 FSx for ONTAP 文件系统上启用 ARP 不会产生额外费用。

ARP 查找的内容

ARP 会查找 Windows 或 Linux 客户端是否遭到入侵的迹象。特别是，ARP 会在卷上查找以下类型的活动：

- 熵的变化，即文件中数据随机性的差异。

- 文件扩展名类型的变化，即新的扩展名与通常使用的扩展名类型不一致。默认情况下为 20 个文件，其文件扩展名未出现在卷中。
- 文件 IOPS 的变化，即加密数据的异常卷活动激增。

如有必要，可修改卷的勒索软件检测参数。例如，如果卷托管多种类型的文件扩展名。有关更多信息，请参阅 NetApp 文档中心中的管理 ONTAP 自主勒索软件防护攻击检测参数。

> **Note**
>
> ARP 不会阻止使用凭证的恶意管理员访问 FSx for ONTAP 文件系统。AWS 建议采用分层安全方法，包括 AWS Backup、ONTAP 快照和 SnapLock。

如何通过 ARP 响应可疑攻击

如果 ARP 检测到攻击，将生成可用作恢复点的快照。快照已锁定，无法通过常规方式删除。根据攻击的严重程度，还将生成 EMS 警报，显示受影响的卷、攻击概率以及攻击时间线。如需接收卷上新建快照或检测到新文件扩展名的警报，可配置 ARP 以发送此类警报。有关更多信息，请参阅 NetApp 文档中心中的配置 ARP 警报。

您可以生成报告，以查看有关可疑攻击的详细信息。查看报告后，可帮助 ONTAP 判断警报是误报还是由可疑攻击所触发。如果将警报标记为可疑攻击，应确定攻击范围，然后从 ARP 创建的快照中恢复数据。如果将攻击标记为误报，则会自动删除 ARP 创建的快照。有关更多信息，请参阅 响应自主勒索软件防护警报。

我们建议在 ONTAP CLI 和 REST API 中监控文件系统的 EMS 消息以及卷的状态。有关 ARP 的 EMS 消息的更多信息，请参阅 了解自主勒索软件防护的 EMS 警报。

主题

- 启用自主勒索软件防护
- 响应自主勒索软件防护警报
- 了解自主勒索软件防护的 EMS 警报

启用自主勒索软件防护

以下过程说明如何使用 ONTAP CLI 启用自主勒索软件防护（ARP）主动模式以及如何验证 ARP 是否已启用。有关 ARP 的更多信息，请参阅 ARP 工作原理。

在主动模式下启用 ARP

使用 ONTAP CLI，在现有卷上以主动模式启用 ARP

- 运行以下命令。将 *vol_name* 和 *svm_name* 替换为您自己的信息。

```
security anti-ransomware volume enable -volume vol_name -vserver svm_name
```

有关此命令的更多信息，请参阅 NetApp 文档中心中的 security anti-ransomware volume enable。

默认启用 SVM 级别的 ARP

使用 ONTAP CLI，在现有 SVM 上默认启用 ARP

- 运行以下命令。将 *svm_name* 替换为您自己的信息。

```
vserver modify -vserver svm_name -anti-ransomware-default-volume-state dry-run
```

有关此命令的更多信息，请参阅 NetApp 文档中心中的 vserver modify。

验证 ARP 的状态

使用 ONTAP CLI 验证 ARP 的状态

- 运行以下命令。

```
security anti-ransomware volume show
```

有关此命令的更多信息，请参阅 NetApp 文档中心中的 security anti-ransomware volume show。

如果预见到工作负载激增的情况，可暂时暂停（随后恢复）ARP 功能。有关更多信息，请参阅 NetApp 文档中心中的暂停 ONTAP 自主勒索软件防护以将工作负载事件排除在分析之外。

响应自主勒索软件防护警报

以下过程说明如何使用 ONTAP CLI 查看自主勒索软件防护（ARP）警报、生成攻击报告，以及对报告采取措施。有关 ARP 如何检测和响应攻击的更多信息，请参阅 ARP 查找的内容 和 如何通过 ARP 响应可疑攻击。

查看 ARP 警报

使用 ONTAP CLI 查看卷上的 ARP 警报

- 运行以下命令。将 *svm_name* 和 *vol_name* 替换为您自己的信息。

  ```
  security anti-ransomware volume show -vserver svm_name -volume vol_name
  ```

  运行命令后，您将看到类似于以下示例的输出：

  ```
  Vserver Name: fsx
  Volume Name: vol1
  State: enabled
  Attack Probability: moderate
  Attack Timeline: 9/14/2021 01:03:23
  Number of Attacks: 1
  ```

  有关此命令的更多信息，请参阅 NetApp 文档中心中的 security anti-ransomware volume show。

生成 ARP 报告

使用 ONTAP CLI 生成 ARP 报告

- 运行以下命令。将 *vol_name* 和 */file_location/* 替换为您自己的信息。生成报告后，可在客户端系统上进行查看。

  ```
  security anti-ransomware volume attack generate-report -volume vol_name -dest-
  path /file_location/
  ```

  有关此命令的更多信息，请参阅 NetApp 文档中心中的 security anti-ransomware volume attack generate-report。

对 ARP 报告采取措施

使用 ONTAP CLI，对 ARP 报告的误报攻击采取措施

- 运行以下命令。将 *svm_name*、*vol_name* 和 *[extension identifiers]* 替换为您自己的信息。

```
security anti-ransomware volume attack clear-suspect -vserver svm_name -
volume vol_name [extension identifiers] -false-positive true
```

有关此命令的更多信息，请参阅 NetApp 文档中心中的 security anti-ransomware volume attack clear-suspect。

> **Note**
>
> 如果将警报标记为误报，则会更新勒索软件配置文件。执行此操作后，您将不会再收到有关该特定场景的警报。

使用 ONTAP CLI，对 ARP 报告的潜在攻击采取措施

- 运行以下命令。将 *svm_name*、*vol_name* 和 *[extension identifiers]* 替换为您自己的信息。

```
security anti-ransomware volume attack clear-suspect -vserver svm_name -
volume vol_name [extension identifiers] -false-positive false
```

有关此命令的更多信息，请参阅 NetApp 文档中心中的 security anti-ransomware volume attack clear-suspect。

了解自主勒索软件防护的 EMS 警报

您可以使用 NetApp ONTAP's 事件管理系统（EMS），监控与 ARP 相关的事件，包括潜在攻击。有关 ARP 及其如何检测攻击的更多信息，请参阅 ARP 工作原理 和 ARP 查找的内容。

下表包含与 ARP 相关的所有警报。有关 EMS 的更多信息，请参阅 监控 FSx for ONTAP EMS 事件。

EMS 消息名称	EMS 消息描述
arw.analytics.ext.report	当反勒索软件分析生成或更新卷的可疑文件扩展名报告时，就会出现此消息。
arw.analytics.high.entropy	当高熵数据日志消息（涉及勒索软件检测与分析）的数量超过卷的预定义阈值时，就会出现此消息。
arw.analytics.probability	当卷上的反勒索软件攻击概率从 low 变为 high 时，就会出现此消息。
arw.analytics.report	当生成或更新卷的反勒索软件分析报告时，就会出现此消息。
arw.analytics.suspects	当反勒索软件分析生成的嫌疑对象列表规模扩大到需要进一步调查的程度时，就会出现此消息。
arw.new.file.extn.seen	当在已启用反勒索软件的卷中发现新的文件扩展名时，就会出现此消息。其目的是及时通知用户已检测到的扩展名，以便及时进行调查。
arw.snapshot.created	当在已启用反勒索软件的卷中创建新的 ARP 快照时，就会出现此消息。此外，此消息还提供有关创建快照原因的信息。
arw.volume.state	当卷的反勒索软件状态发生变化时，就会出现此消息。
arw.vserver.state	当 SVM 的反勒索软件状态发生变化时，就会出现此消息。

使用 SnapLock 保护您的数据

SnapLock 是一项功能，允许您通过将文件转换为“一次写入，多次读取”（WORM）状态来保护文件，从而在指定的保留期内防止文件修改或删除 您可以使用 SnapLock 来满足监管合规性要求，保护关键业务数据免受勒索软件攻击，并为您的数据提供额外的保护层，使其免遭更改或删除。

Amazon FSx for NetApp ONTAP 支持合规和企业保留模式。SnapLock有关更多信息，请参阅了解 SnapLock Compliance和了解 SnapLock Enterprise。

您可以 FSx 为在 2023 年 7 月 13 日当天或之后创建的 ONTAP 文件系统创建SnapLock卷。现有文件系统将在即将到来的每周维护时段内获得 SnapLock 支持。

主题

SnapLock 的工作原理

SnapLock 可以防止您的文件被删除、更改或重命名，从而帮助您满足治理和监管目的。创建 SnapLock 卷时，将文件提交为“一次写入，多次读取”（WORM）存储，并为数据设置保留期。您的文件可以在指定时间内以不可擦除、不可写入的状态存储，也可以无限期存储。

> **Important**
>
> 您必须在创建卷时指定卷是否使用 SnapLock 设置。非 SnapLock 卷在创建后无法转换为 SnapLock 卷。

保留模式

SnapLock 有两种保留模式：Compliance 模式和 Enterprise 模式。Amazon FSx f NetApp or ONTAP 支持这两者。它们有不同的用例，有些功能也不同，但它们都使用 WORM 模型保护您的数据免遭修改或删除。下表说明了这些保留模式之间的一些相似之处和不同之处。

SnapLock 功能	了解 SnapLock Compliance	了解 SnapLock Enterprise
说明	在 Compliance 卷上转换为 WORM 的文件在保留期到期之前无法删除。	在 Enterprise 卷上转换为 WORM 的文件可以由授权用户在保留期到期之前使用特权删除功能删除。

SnapLock 功能	了解 SnapLock Compliance	了解 SnapLock Enterprise
使用案例	• 满足政府或行业特定要求，例如美国证券交易委员会（SEC）第 17a-4（f）条、金融业管理局（FINRA）第 4511 条和商品期货交易委员会（CFTC）第 1.31 条。 • 防范勒索软件攻击。	• 提高组织的数据完整性和内部合规性。 • 在使用 SnapLock Compliance 模式之前测试保留设置。
自动提交	支持	是
基于事件的保留（EBR）[1]	是	是
依法保留[1]	是	否
使用特权删除	否	是
卷附加模式	是	是
SnapLock 审计日志卷	是	是

Note

[1] ONTAP CLI 和 REST API 支持 EBR 和依法保留操作。

Note

FSx for ONTAP 支持将数据分层到所有SnapLock卷上的容量池，无论其类型如何。SnapLock 有关更多信息，请参阅 卷数据分层。

SnapLock 管理员

您必须具有 SnapLock 管理员权限才能对 SnapLock 卷执行某些操作。SnapLock 管理员权限在 ONTAP CLI 中的 `vsadmin-snaplock` 角色中定义。只有集群管理员才能创建具有 SnapLock 管理员角色的存储虚拟机（SVM）管理员账户。

您可以在 ONTAP CLI 中使用该 `vsadmin-snaplock` 角色执行以下操作：

- 管理自己的用户账户、本地密码和密钥信息
- 管理卷，但移动卷除外
- 管理配额、qtree、快照副本和文件
- 执行 SnapLock 操作，包括特权删除和依法保留
- 配置网络文件系统（NFS）和服务器消息块（SMB）协议
- 配置域名系统（DNS）、轻型目录访问协议（LDAP）和网络信息服务（NIS）服务
- 监控作业

以下过程详细介绍了如何在 ONTAP CLI 中创建 SnapLock 管理员。要执行此任务，您必须以集群管理员的身份通过安全外壳协议（SSH）等安全连接登录。

要在 ONTAP CLI 中创建具有 vsadmin-snaplock 角色的 SVM 管理员账户，请执行以下操作

- 运行如下命令。将 *SVM_name* 和 *SnapLockAdmin* 替换为您自己的信息。

```
cluster1::> security login create -vserver SVM_name -user-or-group-
name SnapLockAdmin -application ssh -authentication-method password -role vsadmin-
snaplock
```

有关更多信息，请参阅 ONTAP 角色和用户。

SnapLock 审计日志卷

SnapLock 审计日志卷包含 SnapLock 审计日志，其中包含事件的时间戳，例如何时创建 SnapLock 管理员、何时执行特权删除操作或何时对文件进行依法保留。SnapLock 审计日志卷是不可擦除的事件记录。

您必须在与 SnapLock 卷相同的 SVM 中创建 SnapLock 审计日志卷才能执行以下操作：

- 要在 SnapLock Enterprise 卷上开启或关闭特权删除，请执行以下操作。
- 对 SnapLock Compliance 卷中的文件应用依法保留。

Warning

- SnapLock 审计日志卷的最短保留期为六个月。在此保留期到期之前，即使 SnapLock 审计日志卷是在 SnapLock Enterprise 模式下创建的，也无法删除与之关联的 SVM 和文件系统。
- 如果使用特权删除功能删除文件，并且文件保留期长于该卷的保留期，则审计日志卷将继承该文件的保留期。例如，如果使用特权删除功能删除了保留期为 10 个月的文件，而审计日志卷的保留期为六个月，则审计日志卷的保留期将延长至 10 个月。

一个 SVM 中只能有一个活动的 SnapLock 审计日志卷，但可以由 SVM 中的多个 SnapLock 卷共享。要成功装入 SnapLock 审计日志卷，请将连接路径设置为 `/snaplock_audit_log`。任何其他卷都不能使用此连接路径，包括不是审计日志卷的卷。

您可以在审计日志卷根目录下的 `/snaplock_log` 目录中找到 SnapLock 审计日志。特权删除操作记录在 `privdel_log` 子目录中。依法保留开始和结束操作记录在 `/snaplock_log/legal_hold_logs/` 中。所有其他日志都存储在 `system_log` 子目录中。

您可以使用亚马逊 FSx 控制台、、亚马逊 API 以及 ONTAP CLI 和 REST FSx API 创建SnapLock审核日志卷。 AWS CLI

Note

数据保护（DP）卷不能用作 SnapLock 审计日志卷。

要使用 Amazon FSx API 打开SnapLock审核日志卷，请在`AuditLogVolume`中使用`CreateSnaplockConfiguration`。在 Amazon FSx 控制台中，对于 “审核日志量”，选择 “启用”。确保将连接路径设置为 `/snaplock_audit_log`。

访问 SnapLock 卷中的数据

您可以使用 NFS 和 SMB 等开放文件协议来访问 SnapLock 卷中的数据。向 SnapLock 卷写入数据或读取受 WORM 保护的数据不会对性能产生影响。

您可以使用 NFS 和 SMB 跨 SnapLock 卷复制文件，但它们不会在目标 SnapLock 卷上保留其 WORM 属性。您必须将复制的文件重新提交到 WORM，以防止它们被修改或删除。有关更多信息，请参阅 将文件提交到 WORM 状态。

您也可以使用 SnapMirror 复制 SnapLock 数据，但源卷和目标卷必须是相同保留模式的 SnapLock 卷（例如，两者都必须是 Compliance 卷或 Enterprise 卷）。

SnapLock 和 SSD 容量缩减操作

创建 SnapLock 卷之前，请考虑以下关于 SSD 容量减少的注意事项：

- Amazon FSx 将拒绝对包含SnapLock卷的文件系统提出的减少固态硬盘容量的请求。
- 在 SSD 容量缩减操作期间，无法创建 SnapLock 卷。

这些限制存在的原因在于 ONTAP 强制要求 SnapLock 审计日志卷最少保留 6 个月，如果在 SSD 缩减操作中移动了 SnapLock 卷，这将阻止在该期间内删除文件系统。

如果需缩减带 SnapLock 卷文件系统中的 SSD 容量，则需将数据迁移至 SSD 容量较小的新文件系统。有关 SSD 容量缩减操作的更多信息，包括限制和注意事项，请参阅 更新文件系统 SSD 存储和 IOPS。

了解 SnapLock Compliance

本节介绍 SnapLock Compliance 保留模式的使用案例和注意事项。

您可以为以下用例选择 Compliance 保留模式。

- 您可以使用 SnapLock Compliance 模式满足政府或行业特定要求，例如美国证券交易委员会（SEC）第 17a-4（f）条、金融业管理局（FINRA）第 4511 条和商品期货交易委员会（CFTC）第 1.31 条。SnapLockAmazon FSx fo NetApp r ONTAP 的合规性由Cohasset Associates以下机构进行了评估。有关更多信息，请参阅适用于 NetApp ONTAP 的 Amazon FSx 合规评估报告。
- 您可以使用 SnapLock Compliance 模式来补充或增强全面的数据保护策略，以抵御勒索软件攻击。

以下是有关 SnapLock Compliance 保留模式的一些重要考虑事项。

- 在 SnapLock Compliance 卷上将文件转换为“一次写入，多次读取”（WORM）状态后，任何用户都无法在其保留期到期之前将其删除。
- 只有当 SnapLock Compliance 卷上所有 WORM 文件的保留期均已到期，并且 WORM 文件已从卷中删除时，才能将其删除。
- Compliance 卷创建后无法重命名 SnapLock Compliance 卷。
- 您可以使用 SnapMirror 复制 WORM 文件，但源卷和目标卷必须具有相同的保留模式（例如，两者都必须为合规性）。

- SnapLock Compliance 卷无法转换为 SnapLock Enterprise 卷，反之亦然。

了解 SnapLock Enterprise

本节介绍 SnapLock Enterprise 保留模式的使用案例和注意事项。

您可以为以下使用案例选择 SnapLock Enterprise 保留模式。

- 您可以使用 SnapLock Enterprise 模式仅授权特定用户删除文件。
- 您可以使用 SnapLock Enterprise 模式来提高组织的数据完整性和内部合规性。
- 在使用 SnapLock Enterprise 模式之前先使用 SnapLock Compliance 模式测试保留设置。

以下是有关 SnapLock Enterprise 保留模式的一些重要考虑事项。

- 您也可以使用 SnapMirror 复制 WORM 文件，但源卷和目标卷必须是相同保留模式的卷（例如，两者都必须是 Enterprise 卷）。
- SnapLock 卷不能从 Enterprise 模式转换为 Compliance 模式，也无法从 Compliance 模式转换为 Enterprise 模式。
- SnapLock Enterprise 模式不支持依法保留功能。

使用特权删除

SnapLock Enterprise 模式和 SnapLock Compliance 模式之间的主要区别之一是，SnapLock 管理员可以在 SnapLock Enterprise 卷上启用特权删除，以允许在文件的保留期到期之前删除文件。SnapLock 管理员是唯一可以从具有有效保留策略的 SnapLock Enterprise 卷中删除文件的用户。有关更多信息，请参阅 SnapLock 管理员。

您可以使用亚马逊 FSx 控制台、亚马逊 API 以及 ONTAP CLI 和 REST FSx API 开启或关闭特权删除。 AWS CLI要启用特权删除，必须先在与 SnapLock 卷相同的 SVM 中创建 SnapLock 审计日志卷。有关更多信息，请参阅 SnapLock 审计日志卷。

要使用 Amazon FSx API 开启特权删除功能，`PrivilegedDelete`请在中使用`CreateSnaplockConfiguration`。在 Amazon FSx 控制台中，对于 “特权删除”，选择 “启用”。

> **Note**
>
> 您无法发出特权删除命令来删除保留期过期的“一次写入、多次读取”（WORM）文件。保留期到期后，您可以执行正常的删除操作。

您可以选择永久关闭特权删除功能，但此操作是不可逆的。如果永久关闭了特权删除功能，则无需将 SnapLock 审计日志卷与 SnapLock Enterprise 卷相关联。

要使用 Amazon FSx API 永久关闭特权删除功能，`PrivilegedDelete`请在中使用`CreateSnaplockConfiguration`。在 Amazon FSx 控制台中，对于 “特权删除”，选择 “永久禁用”。

绕过 SnapLock Enterprise 模式

如果您使用的是亚马逊 FSx 控制台或亚马逊 FSx API，则必须拥有 IAM `fsx:BypassSnapLockEnterpriseRetention` 权限才能删除包含具有有效保留策略的 WORM 文件的SnapLock企业卷。

有关更多信息，请参阅 删除 SnapLock 卷。

了解 SnapLock 保留期

创建 SnapLock 卷时，可以为该卷设置默认保留期，也可以明确设置“一次写入，多次读取”（WORM）文件的保留期。在保留期内，您无法删除或修改受 WORM 保护的文件。保留期用于计算保留时间。例如，如果您在 2023 年 7 月 14 日午夜将文件转换为 WORM，并将保留期设置为五年，则保留时间将持续到 2028 年 7 月 14 日午夜。

有关 WORM 的更多信息，请参阅：将文件提交到 WORM 状态。

保留期政策

保留期由您分配给以下参数的值决定：

- 默认保留期 – 如果您没有明确为 WORM 文件提供保留期，则系统会为其分配的默认保留期。
- 最短保留期 – 可以分配给 WORM 文件的最短保留期。
- 最长保留期 – 可以分配给 WORM 文件的最长保留期。

> **Note**
>
> 即使在保留期到期之后，您也无法修改 WORM 文件。您只能将其删除或设置新的保留期以再次启用 WORM 保护。

您可以使用几个不同的时间单位来指定保留期。下表列出了受支持的特定范围。

Type	值	注意
秒	0 - 65,535	
Minutes	0 - 65,535	
Hours	0 - 24	
天	0 - 365	
月份	0 -12	
年	0 - 100	
无限	-	永久保留文件。 适用于默认保留期、最长保留期和最短保留期。
未指定[1]	-	保留文件，直到您设置保留期。 仅适用于默认保留期。

> **Note**
>
> [1]当您将保留期未指定的文件转换到 WORM 时，系统会为这些文件提供为该 SnapLock 卷配置的最短保留期。当您将受 WORM 保护的文件转换为绝对保留时间时，新的保留期必须大于您之前为这些文件设置的最短保留期。

保留期已过期

WORM 文件的保留期到期后，您可以删除该文件或设置新的保留期以重新开启 WORM 保护。WORM 文件在保留期到期后不会自动删除。即使在保留期到期之后，您也无法修改 WORM 文件的内容。

设置 SnapLock 卷的保留期

您可以使用亚马逊 FSx 控制台、亚马逊 API 以及 ONTAP CLI 和 REST FSx API 来设置SnapLock卷的保留期。 AWS CLI

要使用 Amazon FSx API 设置保留期，请使用`SnaplockRetentionPeriod`配置。在 Amazon FSx 控制台的 “保留期” 中，输入默认保留期、最小保留期和最大保留期的值。然后为每个保留期选择一个对应的单位。

将文件提交到 WORM 状态

本节介绍如何将文件转换为“一次写入，多次读取”（WORM）状态。它还讨论了卷附加模式，这是一种将数据以增量方式写入受 WORM 保护的文件的方法。

自动提交

如果文件在您指定的时间段内未修改，则可以使用自动提交将文件转换为 WORM。您可以使用亚马逊 FSx控制台、亚马逊 API 以及 ONTAP CLI 和 REST FSx API 开启自动提交。 AWS CLI

您可以指定一个介于 5 分钟到 10 年之间的自动提交期限。下表列出了受支持的特定范围。

单位	值
Minutes	5 - 65,535
Hours	1 - 65,535
天	1 - 3,650
月份	1 - 120
年	1 - 10

要使用 Amazon FSx API 开启自动提交，请在`AutocommitPeriod`中`CreateSnaplockConfiguration`使用。在 Amazon FSx 控制台中，对于 “自动提交”，选择 “启用”。然后，在自动提交时段中输入一个值并选择相应的自动提交单位。

您可以指定 5 分钟到 10 年之间的值。

卷附加模式

您无法修改受 WORM 保护的文件中的现有数据。但是，SnapLock 允许您使用可附加 WORM 的文件来保护现有数据。例如，您可以生成日志文件或保留音频或视频流数据，同时以增量方式向它们写入数据。您可以使用亚马逊 FSx 控制台、亚马逊 API 以及 C ONTAP LI 和 R FSx EST API 开启或关闭卷追加模式。 AWS CLI

更新卷追加模式的要求

- 必须卸载该 SnapLock 卷。
- 该 SnapLock 卷中必须没有快照副本和用户数据。

要使用 Amazon FSx API 开启卷追加模式，请在中使用`VolumeAppendModeEnabled`。`CreateSnaplockConfiguration`在 Amazon FSx 控制台中，对于卷追加模式，选择启用。

基于事件的保留（EBR）

您可以使用基于事件的保留（EBR）来创建具有相关保留期的自定义策略。例如，您可以将指定路径中的所有文件转换为 WORM，并使用 `snaplock event-retention policy create` 和 `snaplock event-retention apply` 命令将保留期设置为一年。使用 EBR 时，必须指定卷、目录或文件。您在创建 EBR 策略时选择的保留期将应用于指定路径中的所有文件。

ONTAP CLI 和 REST API 支持 EBR。

> **Note**
>
> ONTAP不支持带 FlexGroup 卷的 EBR。

以下步骤介绍如何创建、应用、修改和删除 EBR 策略。您必须是 SnapLock 管理员（具有 `vsadmin-snaplock` 角色）才能在 ONTAP CLI 中完成这些任务。有关更多信息，请参阅 SnapLock 管理员。

在 ONTAP CLI 中创建 EBR 策略

在 CLI 中创建 EBR 策略 ONTAP

- 运行如下命令。将 *p1* 和 *"10 years"* 替换为您自己的信息。

```
vs1::> snaplock event-retention policy create -name p1 -retention-period "10 years"
```

在 ONTAP CLI 中应用 EBR 策略

在 CLI 中应用 EBR 策略 ONTAP

- 运行如下命令。将 *p1* 和 *slc* 替换为您自己的信息。如果要为 EBR 策略指定特定路径，则可以在正斜杠（/）之后添加路径。否则，此命令会将 EBR 策略应用于卷上的所有文件。

```
vs1::> snaplock event-retention apply -policy-name p1 -volume slc -path /
```

在 ONTAP CLI 中修改 EBR 策略

在 CLI 中修改 EBR 策略 ONTAP

- 运行如下命令。将 *p1* 和 *"5 years"* 替换为您自己的信息。

```
vs1::> snaplock event-retention policy modify -name p1 -retention-period "5 years"
```

在 ONTAP CLI 中删除 EBR 策略

在 CLI 中删除 EBR 策略 ONTAP

- 运行如下命令。*p1*用您自己的信息替换。

```
vs1::> snaplock event-retention policy delete -name p1
```

NetApp 文档中心中的相关命令：

- snaplock event-retention abort
- snaplock event-retention show-vservers
- snaplock event-retention show
- snaplock event-retention policy show

依法保留

您可以使用依法保留功能无限期保留 WORM 文件。依法保留通常用于诉讼目的。在解除依法保留之前，无法删除处于依法保留状态的 WORM 文件。

ONTAP CLI 和 REST API 支持依法保留。

> **Note**
>
> ONTAP不支持对 FlexGroup 卷进行合法保留。

以下步骤介绍如何启动和终止依法保留。您必须是 SnapLock 管理员（具有 `vsadmin-snaplock` 角色）才能在 ONTAP CLI 中完成这些任务。有关更多信息，请参阅 SnapLock 管理员。

使用 ONTAP CLI 对 SnapLock Compliance 卷中的文件启动依法保留

使用 ONTAP CLI 对 SnapLock Compliance 卷中的文件启动依法保留

- 运行如下命令。用您自己的信息替换*litigation1*、*slc_vol1*、和*file1*。

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_vol1 -
path /file1
```

使用 ONTAP CLI 对 SnapLock Compliance 卷中的所有文件启动依法保留

使用 ONTAP CLI 对 SnapLock Compliance 卷中的所有文件启动依法保留

- 运行如下命令。将 *litigation1* 和 *slc_vol1* 替换为您自己的信息。

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_vol1 -
path /
```

使用 ONTAP CLI 对 SnapLock Compliance 卷中的文件结束依法保留

使用 ONTAP CLI 对 SnapLock Compliance 卷中的文件结束依法保留

- 运行如下命令。用您自己的信息替换*litigation1*、*slc_vol1*、和*file1*。

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume slc_vol1 -
path /file1
```

> **Note**
>
> 我们建议您在使用依法保留时使用 `snaplock legal-hold show` 命令监控 `-operation-status`，以确保它不会失败。

使用 ONTAP CLI 对 SnapLock Compliance 卷中的所有文件结束依法保留

使用 ONTAP CLI 对 SnapLock Compliance 卷中的所有文件结束依法保留

- 运行如下命令。将 *litigation1* 和 *slc_vol1* 替换为您自己的信息。

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume slc_vol1 -
path /
```

> **Note**
>
> 我们建议您在使用依法保留时使用 `snaplock legal-hold show` 命令监控 `-operation-status`，以确保它不会失败。

NetApp 文档中心中的相关命令：

- snaplock legal-hold abort
- snaplock legal-hold dump-files
- snaplock legal-hold dump-litigations
- snaplock legal-hold show

使用 FlexCache 复制您的数据

FlexCache 是一种 NetApp ONTAP's 远程缓存功能，让数据集更靠近客户端，从而提高访问性能并降低成本。该功能可简化文件分配并降低 WAN 成本。创建 FlexCache 卷时，初始阶段仅会从源文件系

统复制元数据。与完整数据副本相比，这种方法的速度更快且空间利用效率更高，且仅占用极小的存储容量。

FlexCache 的工作原理

FlexCache 卷是一种稀疏填充的缓存，用于访问存储在源卷中的数据。缓存可以位于不同的文件系统中，该文件系统可选为远程文件系统。与复制来源卷全部数据不同，FlexCache 仅按需复制数据。FlexCache 卷最适合读取密集型工作流程且数据变更频率较低的情境，因为源数据的任何变更都需要刷新缓存。

您可以在以下配置中将 FlexCache 与 FSx for ONTAP 配合使用：

来源卷	FlexCache volume
本地 NetApp ONTAP	FSx for ONTAP
FSx for ONTAP	本地 NetApp ONTAP
FSx for ONTAP	FSx for ONTAP

FlexCache 写入模式

FlexCache 卷支持两种写入操作模式：绕写模式和写回模式。

在绕写模式（即默认模式）下，写入从缓存转发到来源卷。写入操作只有在数据被提交到来源卷存储并由来源卷确认写回缓存后，才会向客户端发送确认。由于每次写入都必须穿越缓存和来源之间的网络，因此该模式的延迟高于写回模式。

在 ONTAP 9.15.1 中引入的写回模式下，写入操作会提交到缓存位置的存储中，并立即向客户端发送确认。数据随后以异步方式写入来源卷。此模式使写入操作能够以接近本地的速度运行，可显著提高分布式工作负载的性能。

对于需要低延迟缓存写入的写入密集型工作负载，请使用写回模式。对于对延迟不敏感的读取密集型工作负载，或者源文件系统包含超过 10 个 FlexCache 来源卷时，请使用绕写模式。

FlexCache 卷创建概述

创建 FlexCache 卷包含以下步骤：

1. 收集源和目标逻辑接口（LIF）
2. 在来源和缓存文件系统之间建立集群对等
3. 创建存储虚拟机（SVM）对等关系
4. 创建 FlexCache 卷，并选择写入模式
5. 在客户端上挂载 FlexCache 卷

有关详细说明，请参阅创建 FlexCache。

创建 FlexCache

按照以下步骤，您将在 Amazon FSx for NetApp ONTAP 文件系统上创建一个由本地NetApp ONTAP 集群中的原始卷支持的卷。FlexCache

使用 ONTAP CLI

您将使用 ONTAP CLI 在 for ONTAP 文件系统上创建和管理FlexCache配置。 FSx

这些过程中的命令使用以下集群、SVM 和卷的别名：

- `Cache_ID`— 缓存集群的 ID（格式为 FSx idabcdef1234567890a）
- `Origin_ID`：来源集群的 ID
- `CacheSVM`：缓存 SVM 名称
- `OriginSVM`：来源 SVM 名称
- `OriginVol`：来源卷名称
- `CacheVol`：FlexCache 卷名称。

本部分中的过程使用以下 NetApp ONTAP CLI 命令。

- `network interfaces show`
- `cluster peer` 命令
- `volume flexcache create`

先决条件

在您开始以下部分中的过程之前，请确保您已符合以下先决条件：

- 源文件系统和目标文件系统连接在同一 VPC 中，或者位于使用 Amazon VPC、 AWS Transit Gateway Direct Connect、或 Site-to-Site VPN对等连接的网络中。有关更多信息，请参阅《Amazon VPC 对等连接指南》中的 从内部访问数据 AWS Cloud 和什么是 VPC 对等连接？。
- 适用于 ONTAP 文件系统的 VPC 安全组具有入站和出站规则，允许集群间终端节点在端口 11104 和 11105 上使用 ICMP 和 TCP（ ）。 FSx LIFs
- 您已使用 SVM FSx 为 ONTAP 文件系统创建了目标，但尚未创建将用作的卷。 FlexCache有关更多信息，请参阅 创建文件系统。

记录集群间的源和目标 LIFs

1. 对于作为目标集群的 ONTAP 文件系统： FSx

   a. 打开亚马逊 FSx 控制台，网址为https://console.aws.amazon.com/fsx/。

   b. 选择 “文件系统”，然后选择 ONTAP 文件系统（目标集群）以打开文件系统详细信息页面。 FSx

   c. 在管理中，查找集群间端点 - IP 地址，然后记录该值。

   > **Note**
   >
   > 对于横向扩展的文件系统，每个高可用性（HA）对有两个集群间端点 IP 地址。

2. 对于本地源集群，使用以下 ONTAP CLI 命令检索集群间 LIF IP 地址：

```
Origin::> network interface show -role intercluster
Logical                         Network
Vserver     Interface  Status   Address/Mask
----------- ---------- -------  ------------
OriginSVM
            inter_1     up/up   10.0.0.36/24
            inter_2     up/up   10.0.1.69/24
```

3. 保存 `inter_1` 和 `inter_2` IP 地址。这些地址在 `OriginSVM` 中的别名为 `origin_inter_1` 和 `origin_inter_2`，在 `CacheSVM` 中的别名为 `cache_inter_1` 和 `cache_inter_2`。

在来源和缓存之间建立集群对等

使用 cluster peer create ONTAP CLI 命令在 Cache 和 Source 集群上建立集群对等关系。您将提供之前在 记录集群间的源和目标 LIFs 过程中保存的集群间 IP 地址。出现提示时，将要求您创建在 Origin 集群上建立集群对等时需要输入的 *cluster-peer-passphrase*。

1. 在集群上设置集Cache群对等互连（ FSx 适用于 ONTAP 文件系统）。

   a. 要访问 ONTAP CLI，请运行以下命令在 Amazon FSx for NetApp ONTAP 文件系统或 SVM 的管理端口上建立 SSH 会话。将 *management_endpoint_ip* 替换为文件系统管理端口的 IP 地址。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   有关更多信息，请参阅 使用 ONTAP CLI 管理文件系统。

   b. 使用以下命令，并记录您创建的密码。对于横向扩展的文件系统，请为每个 HA 对提供 `inter_1` 和 `inter_2` IP 地址。

   ```
   FSx-Cache::> cluster peer create -address-family ipv4 -peer-
   addrs origin_inter_1,origin_inter_2

   Enter the passphrase: cluster-peer-passphrase
   Confirm the passphrase: cluster-peer-passphrase
   Notice: Now use the same passphrase in the "cluster peer create" command in the
    other cluster.
   ```

2. 使用以下命令，在 `source`（本地）集群上设置集群对等。您需要输入在上述步骤中创建的密码才能进行身份验证。对于横向扩展的文件系统，需要为每个 HA 对提供集群间 IP 地址。

   ```
   Origin::> cluster peer create -address-family ipv4 -peer-
   addrs cache_inter_1,cache_inter_2

   Enter the passphrase: cluster-peer-passphrase
   Confirm the passphrase: cluster-peer-passphrase
   ```

3. 在 `source` 集群上，使用以下命令验证集群对等是否设置成功。在输出中，`Availability` 应设置为 `Available`。

   ```
   Origin::> cluster peer show
   ```

```
Peer Cluster Name     Availability    Authentication
-------------------   -------------   --------------
Cache_ID              Available       ok
```

如果输出未显示 `Available`，请对 `source` 和 `cache` 集群重复上述步骤。

配置存储虚拟机（SVM）对等

成功建立集群对等后，下一步是使用 vserver peer 命令在缓存集群（缓存）上创建 SVM 对等关系。以下流程中使用的其他别名如下：

- *`CacheLocalName`*：此名称用于在 `origin` SVM 上配置 SVM 对等时标识 `cache` SVM。
- *`OriginLocalName`*：此名称用于在 `cache` SVM 上配置 SVM 对等时标识 `origin` SVM。

1. 在 `cache` SVM 上，使用以下命令，以创建 SVM 对等关系。

```
FSx-Cache::> vserver peer create -vserver CacheSVM -peer-vserver OriginSVM -peer-
cluster Origin_ID -local-name OriginLocalName -application flexcache
```

2. 在源集群上，使用以下命令，以接受 SVM 对等关系。

```
Origin::> vserver peer accept -vserver OriginSVM -peer-vserver CacheSVM -local-
name CacheLocalName
```

3. 接受源集群上的对等关系。

```
Origin::> vserver peer accept -vserver OriginSVM -peer-vserver CacheSVM -local-
name CacheLocalName
```

4. 使用以下命令验证 SVM 对等连接是否成功；`Peer State` 在响应中应设置为 `peered`。

```
Origin::> vserver peer show

Vserver      Peer Vserver    Peer State    Peering Cluster    Remote Applications

------------ --------------- ------------- ------------------
 ------------------------
OriginSVM    CacheSVM        peered        FSx-Cache          flexcache
```

创建 FlexCache 卷

成功创建 SVM 对等关系后，下一步是在缓存 SVM 上创建 FlexCache 卷。FlexCache 卷必须为 FlexGroup。您还将为 FlexCache 卷选择操作模式。有关更多信息，请参阅 FlexCache 写入模式。

1. 在缓存集群上，使用以下 ONTAP CLI 命令创建 FlexCache 卷。该示例创建了一个名为 2 TB 的 FlexCache 卷*CacheVol*。

   - 要创建绕写 FlexCache 卷，请使用以下命令。

   ```
   FSx-Cache::> volume flexcache create -vserver CacheSVM -size 2t -volume CacheVol
    -origin-volume OriginVol -origin-vserver OriginSVM -junction-path /flexcache -
   aggr-list aggr1
   ```

   - 要创建写回 FlexCache 卷，请使用以下命令。

   ```
   FSx-Cache::> volume flexcache create -vserver CacheSVM -size 2t -volume CacheVol
    -origin-volume OriginVol -origin-vserver OriginSVM -junction-path /flexcache -
   aggr-list aggr1 -is-writeback-enabled true
   ```

   > **Note**
   >
   > 您可以使用 volume flexcache config modify -is-writeback-enabled {true|false} 命令修改写入模式。使用此命令之前，请确保使用 set -privilege advanced 命令进入 ONTAP CLI 高级模式。

2. 验证 FlexCache 卷和来源卷之间的 FlexCache 关系。

   - 对于 FlexCache 绕写卷，输出将类似于以下示例。

   ```
   FSx-Cache::> volume flexcache show

   Vserver   Volume      Size     Origin-Vserver  Origin-Volume  Origin-Cluster
   -------   ----------  -------  --------------  -------------  --------------
   CacheSVM  CacheVol    2TB      OriginSVM       OriginVol      Origin
   ```

   - 对于 FlexCache 写回卷，输出将类似于以下示例。

   ```
   FSx-Cache::> volume flexcache show
   ```

```
Vserver   Volume      Size     Origin-Vserver  Origin-Volume  Origin-Cluster
 Writeback
-------   ----------  -------  --------------  -------------  --------------
 ---------
CacheSVM  CacheVol    2TB      OriginSVM       OriginVol      Origin
 true
```

挂载 FlexCache 卷

一旦该FlexCache卷变为可用， NFSv3 NFSv4、和 SMB 客户端就可以将其挂载。挂载 FlexCache 后，客户端即可访问本地来源卷上的整个数据集。

- 要创建装载点并装载 FlexCache，请在客户机上运行以下命令：

```
$ sudo mkdir -p /fsx/CacheVol
$ sudo mount -t nfs management.fs-01d2f606463087f6d.fsx.us-east-1.amazonaws.com:/
CacheVol /fsx/CacheVol
```

使用 NetApp SnapMirror 复制您的数据

您可以使用 NetApp SnapMirror 计划定期在 FSx for ONTAP 文件系统与辅助文件系统之间的复制。此功能适用于区域内和跨区域部署。

NetApp SnapMirror 以高速复制数据，能够在整个 ONTAP 系统中提供高数据可用性和快速的数据复制，无论是在 AWS 中进行两个 Amazon FSx 文件系统之间的复制，还是从本地到 AWS 之间的复制。您可以将复制频率设置为每 5 分钟一次，但也应该根据 RPO（恢复点目标）、RTO（恢复时间目标）和性能注意事项来谨慎选择时间间隔。

如果将数据复制到 NetApp 存储系统并持续更新辅助数据，您的数据就会保持为最新且随时可用的状态。而不需要外部复制服务器。有关使用 NetApp SnapMirror 复制数据的更多信息，请参阅 NetApp Console 文档中的了解 NetApp 复制。

除 NetApp ONTAP CLI 和 REST API 之外，您还可以使用 Amazon FSx 控制台、AWS CLI 和 Amazon FSx API，以创建 NetApp SnapMirror 的数据保护（DP）目标卷。有关使用 Amazon FSx 控制台和 AWS CLI 创建目标卷的信息，请参阅创建卷。

您可以使用 NetApp Console 或 ONTAP CLI 来计划文件系统复制。

> **Note**
>
> SnapMirror 复制有两种类型：卷级 SnapMirror 和 SVM 灾难恢复（SVMDR）。FSx for ONTAP 仅支持卷级 SnapMirror 复制。不支持 Synchronous SnapMirror，包括 StrictSync。

使用 NetApp Console 计划复制

您可以使用 NetApp Console 在 FSx for ONTAP 文件系统上设置通过 SnapMirror 进行的复制。有关更多信息，请参阅 NetApp 控制台文档中的在 NetApp 复制中设置数据复制。

使用 ONTAP CLI 计划复制

您可以使用 ONTAP CLI 配置定时卷复制。有关信息，请参阅 NetApp ONTAP 文档中心中的管理 SnapMirror 卷复制。

FSx for ONTAP 的 AWS 账单和使用情况报告

AWS 为 FSx for ONTAP 提供两份使用情况报告：

- AWS 账单报告从宏观层面显示了您所用 AWS 服务 的所有活动（包括 FSx for ONTAP）。
- AWS 使用情况报告概括了特定服务按小时、天或月汇总的活动情况。该报告还包括提供了 FSx for ONTAP 使用情况图示的使用情况图表。

> **Note**
>
> 与其他 AWS 服务 一样，FSx for ONTAP 只对您使用的部分收费。有关更多信息，请参阅适用于 NetApp ONTAP 的 Amazon FSx 定价。

查看 FSx for ONTAP 的 AWS 账单报告

您可在AWS 账单与成本管理控制台的账单页面上，查看您的AWS使用情况和费用摘要。

查看AWS账单报告

1. 登录 AWS 管理控制台，然后通过以下网址打开 AWS 账单与成本管理 控制台：https://console.aws.amazon.com/costmanagement/。
2. 在导航窗格上，选择账单。
3. 选择一个账单周期（例如，2024 年 8 月）。
4. 要查看 Amazon FSx 费用，请在按服务计费选项卡上，在“按服务筛选”文本字段中输入 FSx，然后展开 FSx 以查看按 AWS 区域 计费。

   FSx for ONTAP 文件系统的费用显示在报告中的 Amazon FSx CreateFileSystem:ONTAP 条目下。
5. 要以 CSV 格式下载详细账单报告，请在账单页面的顶部选择全部下载为 CSV。

有关 AWS 账单的更多信息，请参阅《AWS Billing 用户指南》中的查看您的账单。

账单报告包含适用于 FSx for ONTAP 文件系统的以下使用类型：

First generation FSx for ONTAP file systems

费用类型	单位	描述	
ONTAP 单可用区 SSD 存储	GB-月	第一代单可用区 ONTAP 文件系统上预置的 SSD 存储量	
ONTAP 多可用区 SSD 存储	GB-月	第一代多可用区 FSx for ONTAP 文件系统上预置的 SSD 存储量	
ONTAP 单可用区吞吐能力	MBps-月	第一代单可用区 FSx for ONTAP 文件系统上预置的吞吐能力	
ONTAP 多可用区吞吐能力	MBps-月	第一代多可用区 FSx for ONTAP 文件系统上预置的吞吐能力	
预置的 ONTAP 单可用区 SSD IOPS	IOPS-月	第一代单可用区 FSx for ONTAP 文件系统上预置的 SSD IOPS 量	
预置的 ONTAP 多可用区 SSD IOPS	IOPS-月	第一代多可用区 FSx for ONTAP 文件系统上预置的 SSD IOPS 量	

Second generation FSx for ONTAP file systems

费用类型	单位	描述	
ONTAP 单可用区 2 SSD 存储	GB-月	第二代单可用区 FSx for ONTAP 文件系统上预置的 SSD 存储量	
ONTAP 多可用区 2 SSD 存储	GB-月	第二代多可用区 FSx for ONTAP 文件系统上预置的 SSD 存储量	

费用类型	单位	描述	
ONTAP 单可用区 2 吞吐能力	MBps-月	第二代单可用区 FSx for ONTAP 文件系统上预置的吞吐能力	
ONTAP 多可用区 2 吞吐能力	MBps-月	第二代多可用区 FSx for ONTAP 文件系统上预置的吞吐能力	
预置的 ONTAP 单可用区 2 SSD IOPS	IOPS-月	第二代单可用区 FSx for ONTAP 文件系统上预置的 SSD IOPS 量	
预置的 ONTAP 多可用区 2 SSD IOPS	IOPS-月	第二代多可用区 FSx for ONTAP 文件系统上预置的 SSD IOPS 量	

All FSx for ONTAP filesystems

费用类型	单位	描述	
ONTAP 标准容量池存储	GB-月	FSx for ONTAP 文件系统使用的容量池存储量。	
ONTAP 备份存储	GB-月	用于备份的存储容量	
SnapLock 使用量	GB-月	SnapLock 卷使用的存储容量	
向 ONTAP 标准容量池存储发出的读取请求	操作	向 FSx for ONTAP 文件系统上标准容量池存储发出的读取请求数	
向 ONTAP 标准容量池存储发出的写入请求	操作	向 FSx for ONTAP 文件系统上标准容量池存储发出的写入请求数	

查看 FSx for ONTAP AWS 使用情况报告

AWS 提供比账单报告更详细的 FSx 使用情况报告。该使用情况报告提供按小时、天或月汇总的使用数据；并按区域和使用类型列出相关操作。

查看AWS使用情况报告

1. 登录 AWS 管理控制台，然后通过以下网址打开 AWS 账单与成本管理 控制台：https://console.aws.amazon.com/costmanagement/。
2. 在导航窗格中，选择 Cost Explorer。
3. 在报告参数部分下，选择报告的日期范围及粒度。
4. 将分组依据 > 维度设置为服务。
5. 在筛选条件 > 服务下，选择 FSx
6. 选择使用类型。有关 FSx for ONTAP 使用类型的列表，请参阅此流程后随附的表格。
7. 为报告选择任何其他筛选条件。
8. 要将报告详细信息下载到文件中，选择下载为 CSV。

下表列出 FSx for ONTAP 使用类型，您可以使用这些类型筛选报告，以查看 ONTAP 文件系统的使用情况数据。有关使用成本资源管理器的更多信息，请参阅《AWS Cost Management 用户指南》中的使用 AWS Cost Explorer 分析成本和使用情况。

First generation FSx for ONTAP file systems

使用类型	单位	描述
region-Storage.SAZ_2N:SSD	GB-月	第一代单可用区 FSx for ONTAP 文件系统上预置的 SSD 存储量。
region-Storage.MAZ:SSD	GB-月	第一代多可用区 FSx for ONTAP 文件系统上预置的 SSD 存储量。
region-ThroughputCapacity.SAZ_2N	MiBps-月	第一代单可用区 FSx for ONTAP 文件系统上预置的吞吐能力。
region-ThroughputCapacity.MAZ	MiBps-月	第一代多可用区 FSx for ONTAP 文件系统上预置的吞吐能力。

使用类型	单位	描述
region-ProvisionedSSDIOPS.SAZ_2N	IOPS-月	第一代单可用区 FSx for ONTAP 文件系统上预置的每 GiB SSD 存储超过 3IOPS 的 SSD IOPS 量。
region-ProvisionedSSDIOPS.MAZ	IOPS-月	第一代多可用区 FSx for ONTAP 文件系统上预置的每 GiB SSD 存储超过 3IOPS 的 SSD IOPS 量。

Second generation FSx for ONTAP file systems

使用类型	单位	描述
region-Storage.SAZ_2N2:SSD	GB-月	第二代单可用区 FSx for ONTAP 文件系统上预置的 SSD 存储量。
region-Storage.MAZ2:SSD	GB-月	第二代多可用区 FSx for ONTAP 文件系统上预置的 SSD 存储量。
region-ThroughputCapacity.SAZ_2N2	MiBps-月	第二代单可用区 FSx for ONTAP 文件系统上预置的吞吐能力。
region-ThroughputCapacity.MAZ2	MiBps-月	第二代多可用区 FSx for ONTAP 文件系统上预置的吞吐能力。
region-ProvisionedSSDIOPS.SAZ_2N2	IOPS-月	第二代单可用区 FSx for ONTAP 文件系统上预置的每 GiB SSD 存储超过 3IOPS 的 SSD IOPS 量。
region-ProvisionedSSDIOPS.MAZ2	IOPS-月	第二代多可用区 FSx for ONTAP 文件系统上预置的每 GiB SSD 存储超过 3IOPS 的 SSD IOPS 量。

All FSx for ONTAP file systems

使用类型	单位	描述
region-Storage.SAZ_2N:CPoolStd	GB-月	第一代或第二代单可用区 FSx for ONTAP 文件系统上使用的标准容量池存储量。
region-Storage.MAZ:CPoolStd	GB-月	第一代或第二代多可用区 FSx for ONTAP 文件系统上使用的标准容量池存储量。
region-BackupUsage	GB-月	用于备份的存储容量。
region-SnaplockUsage	GB-月	SnapLock 卷使用的存储容量。
region-Requests.SAZ_2N:CPoolStdRd	操作	向单可用区 FSx for ONTAP 文件系统上标准容量池存储发出的读取请求数。
region-Requests.SAZ_2N:CPoolStdWr	操作	向单可用区 FSx for ONTAP 文件系统上标准容量池存储发出的写入请求数。
region-Requests.MAZ:CPoolStdRd	操作	向多可用区 FSx for ONTAP 文件系统上标准容量池存储发出的读取请求数。
region-Requests.MAZ:CPoolStdWr	操作	向多可用区 FSx for ONTAP 文件系统上标准容量池存储发出的写入请求数。

监控亚马逊 FSx 的 NetApp ONTAP

您可以使用以下服务和工具来监控 Amazon FSx 的 NetApp ONTAP 使用情况和活动：

- 亚马逊 CloudWatch — 您可以使用亚马逊监控文件系统 CloudWatch，亚马逊会自动收集来自 ONTAP 的原始数据并将其处理 FSx 为可读的指标。这些统计数据的保留期限为 15 个月，以便您可以访问历史信息，了解文件系统的运行状况。您还可以根据特定时间段中的指标设置警报，并根据相对于您指定的阈值的指标值执行一项或多项操作。
- ONTAP EMS 事件 — 您可以使用 ONTAP 的事件管理系统 (EMS) 生成的事件来监控您 FSx 的 ONTAP 文件系统。EMS 事件是文件系统中发生事件的通知，例如 iSCSI LUN 创建或自动调整卷大小。
- NetApp 数据基础设施见解 — 您可以使用 NetApp 数据基础设施见解服务监控 ONTAP 文件系统的配置、容量和性能指标。 FSx 您也可以根据指标条件创建警报。
- NetApp Harvest 和 NetApp Grafan a — 你可以使用 NetApp Harvest 和 Grafana 监控 FSx 你的 ONTAP 文件系统。 NetApp NetApp Harvest 通过收集 ONTAP 文件系统的性能、容量和硬件指标来 FSx 监控 ONTAP 文件系统。Grafana 配备的控制面板中会显示收集的 Harvest 指标。
- AWS CloudTrail— 您可以使用 AWS CloudTrail 将所有 Amazon 的 API 调用捕获 FSx 为事件。这些事件记录了用户、角色或 AWS 服务在 Amazon 中采取的操作 FSx。

主题

使用 Amazon 进行监控 CloudWatch

您可以使用 Amazon 监控文件系统 CloudWatch，亚马逊会收集来自 Amazon for NetApp ONTAP 的原始数据，并将其处理 FSx 为可读的近乎实时的指标。这些统计数据会保留 15 个月，因此您可以访问历史信息来确定文件系统的运行情况。 FSx 对于 ONTAP，默认情况下，指标数据以 1 CloudWatch 分钟为周期自动发送到。有关的更多信息 CloudWatch，请参阅 Amazon 是什么 CloudWatch？ 在《亚马逊 CloudWatch 用户指南》中。

> **Note**
>
> 默认情况下，ONTAP 以 1 分钟 FSx 为周期向发送指标数据，但以下指标以 5 分钟为间隔发送除外： CloudWatch
>
> - `FileServerDiskThroughputBalance`
> - `FileServerDiskIopsBalance`

CloudWatch ONTAP FSx 的指标分为四个类别，这些类别由用于查询每个指标的维度定义。有关尺寸的更多信息，请参阅 Amazon CloudWatch 用户指南中的尺寸。

- 文件系统指标： File-system-level性能和存储容量指标。
- 文件服务器指标： File-server-level指标。
- 详细的文件系统聚合指标：每个聚合的详细文件系统指标。
- 详细的文件系统指标：每个 File-system-level存储层（ SSD 和容量池）的存储指标。
- 卷指标：各卷的性能和存储容量指标。
- 详细的卷指标：按存储层或数据类型（用户、快照或其他）划分的各卷的存储容量指标。

ONTAP 的所有 CloudWatch FSx 指标都将发布到中的`AWS/FSx`命名空间。 CloudWatch

主题

访问 CloudWatch 指标

您可以通过以下方式查看亚马逊 FSx 的亚马逊 CloudWatch 指标：

- Amazon FSx 控制台
- Amazon CloudWatch 控制台
- 的 AWS Command Line Interface (AWS CLI) for CloudWatch

- 这个 CloudWatch API

以下过程说明了如何使用 Amazon FSx 控制台查看文件系统的 CloudWatch 指标。

使用 Amazon FSx 控制台查看文件系统的 CloudWatch 指标

1. 打开 Amazon FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 在左侧导航窗格中，选择文件系统，然后选择要查看其指标的文件系统。
3. 在摘要页面上，从第二个面板中选择监控和性能，查看文件系统指标的图表。

监控和性能面板上有四个选项卡。

- 选择 “摘要”（默认选项卡）以显示文件系统活动的所有活动 CloudWatch 警告、警报和图表。
- 选择存储可查看存储容量和利用率指标。
- 选择性能，查看文件服务器和存储性能指标。
- 选择CloudWatch 警报以查看为文件系统配置的所有警报的图表。

以下过程说明了如何使用 Amazon FSx 控制台查看您的交易量 CloudWatch 指标

使用 Amazon FSx 控制台查看您的交易量 CloudWatch 指标

1. 打开 Amazon FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 在左侧导航窗格中，选择卷，然后选择要查看其指标的卷。
3. 在摘要页面上，从第二个面板中选择监控（默认选项卡），查看卷的指标图表。

以下过程说明了如何使用 Amazon CloudWatch 控制台查看文件系统的 CloudWatch 指标。

使用 Amazon CloudWatch 控制台查看指标

1. 在文件系统的摘要页面上，从第二个面板中选择监控和性能，查看文件系统指标的图表。
2. 从要在 Amazon CloudWatch 控制台中查看的图表右上角的操作菜单中选择在指标中查看。这将在 Amazon CloudWatch 控制台中打开 “指标” 页面。

以下过程说明了如何将 ONTAP 文件系统 FSx 指标添加到 Amazon CloudWatch 控制台中的控制面板。

向 Amazon CloudWatch 控制台添加指标

1. 在 Amazon FSx 控制台的 “监控和性能” 面板中选择一组指标（摘要、存储或性能）。
2. 选择面板右上角的添加到控制面板。这将打开 Amazon CloudWatch 控制台。
3. 从列表中选择一个现有 CloudWatch 仪表板，或者创建一个新的仪表板。有关更多信息，请参阅亚马逊 CloudWatch 用户指南中的使用亚马逊 CloudWatch 控制面板。

下述步骤介绍的是如何使用 AWS CLI访问文件系统的指标。

要访问来自的指标 AWS CLI

- 使用带参数的 CloudWatch list-Metrics CLI 命令。`--namespace "AWS/FSx"`有关更多信息，请参阅 AWS CLI 命令参考。

以下过程说明了如何使用 CloudWatch API 访问文件系统的指标。

从 CloudWatch API 访问指标

- 调用 GetMetricStatistics API 操作 。有关更多信息，请参阅 Amazon CloudWatch API 参考。

在 Amazon FSx 控制台中进行监控

Amazon 报告的 CloudWatch 指标 FSx 提供了有关您的 for ONTAP 文件系统和卷 FSx 的宝贵信息。

主题

- 在 Amazon FSx 控制台中监控文件系统指标
- 在 Amazon FSx 控制台中监控交易量指标
- 性能警告和建议
- 创建亚马逊 CloudWatch 警报以监控亚马逊 FSx

在 Amazon FSx 控制台中监控文件系统指标

您可以使用 Amazon FSx 控制台中文件系统控制面板上的 “监控和性能” 面板来查看下表中描述的指标。有关更多信息，请参阅 访问 CloudWatch 指标。

监控和性能	如何...	图表	相关指标
Summary	...确定文件系统上的可用存储容量大小？	可用的主存储容量（字节）	StorageCapacity {SSD} - StorageUsed {SSD}
	...确定我的文件系统的客户端总吞吐量？	客户端总吞吐量（字节/秒）	总和（DataReadBytes + DataWriteBytes ）/周期（以秒为单位）
	...确定我的文件系统的客户端 IOPS 总数？	客户端 IOPS 总数（操作/秒）	总和（DataReadOperations + DataWriteOperations + MetadataOperations ）/周期（以秒为单位）
	...确定我的文件系统在进行读取、写入和元数据操作时的平均延迟？	平均延迟（毫秒/操作）	平均读取延迟：DataReadOperationTime * 1000/DataReadOperations 平均写入延迟：DataWriteOperationTime * 1000/DataWriteOperations 平均元数据延迟：MetadataOperationTime * 1000/MetadataOperations
	...确定我的文件系统上已使用的和可用存储容量的分配情况？	存储分配	可用的主要层：StorageCapacity {SSD} – StorageUsed {SSD}

监控和性能	如何...	图表	相关指标
			已使用的主要层：StorageUsed {SSD} 已使用的容量池：StorageUsed {StandardCapacityPool }
	...确定存储效率带来的节省（压缩、重复数据删除和紧凑处理）？	存储效率节省	StorageEfficiencySavings
存储	...确定可用的主存储容量？	可用的主存储容量（字节）	StorageCapacity {SSD} - StorageUsed {SSD}
	...确定我的文件系统中已使用的主存储的百分比？	主存储容量利用率（百分比）	StorageUsed {SSD} * 100/StorageCapacity {SSD}
文件服务器性能	...确定我的文件系统是否即将达到其网络吞吐量限制？	网络吞吐量 – 利用率（百分比）	NetworkThroughputUtilization
	...确定我的文件系统是否即将达到其磁盘吞吐量限制？	磁盘吞吐量 – 利用率（百分比）	FileServerDiskThroughputUtilization
	...确定我的文件系统是否已用尽其允许的磁盘吞吐量突增点数？	磁盘吞吐量 – 突增平衡（百分比）	FileServerDiskThroughputBalance

监控和性能	如何...	图表	相关指标
	...确定我的文件系统是否即将达到其文件服务器的 SSD IOPS 数限制？	磁盘 IOPS – 利用率（百分比）	`FileServerDiskIopsUtilization`
	...确定我的文件系统是否已用尽其文件服务器允许的磁盘 SSD IOPS 突增点数？	磁盘 IOPS – 突增平衡（百分比）	`FileServerDiskIopsBalance`
	...确定文件系统 CPU 的平均利用率？	CPU 利用率（百分比）	`CPUUtilization`
	... 确定我的工作负载是否有效利用了文件系统的 RAM 和 NVMe 读取缓存？	缓存命中率（百分比）	`FileServerCacheHitRatio`
磁盘性能	...确定我的文件系统是否即将达到其当前预置的 SSD IOPS 容量？	磁盘 IOPS – 利用率（SSD）（百分比）	`DiskIopsUtilization`

> **Note**
>
> 我们建议您将任何与性能相关的维度（例如网络利用率、CPU 利用率和 SSD IOPS 利用率）的吞吐能力平均利用率保持在 50% 以下。这样可以确保您有足够的备用吞吐能力来应对工作负载中的意外峰值以及任何后台存储操作（例如存储同步、数据分层或备份）。

在 Amazon FSx 控制台中监控交易量指标

您可以在 Amazon FSx 控制台中查看卷控制面板上的 “监控” 面板，以查看其他性能指标。有关更多信息，请参阅 访问 CloudWatch 指标。

监控	如何...	图表	相关指标
	...确定卷的可用存储容量？	可用存储容量	StorageCapacity
	...确定卷的客户端总吞吐量？	客户端总吞吐量（字节/秒）	总和（DataReadBytes + DataWriteBytes）/周期（以秒为单位）
	...确定卷的客户端 IOPS 总数？	客户端 IOPS 总数（操作/秒）	总和（DataReadOperations + DataWriteOperations + MetadataOperations）/周期（以秒为单位）
	...确定有多少读取和写入操作来自或流向容量池层？	容量池 IOPS（操作/秒）	读取操作：CapacityPoolReadOperations 写入操作：CapacityPoolWriteOperations
	...确定卷在进行读取、写入和元数据操作时的平均延迟？	平均延迟（毫秒/操作）	平均读取延迟：DataReadOperationTime * 1000/DataReadOperations 平均写入延迟：DataWriteOperationTime * 1000/DataWriteOperations 平均元数据延迟：MetadataO

监控	如何...	图表	相关指标
			perationTime * 1000/Metadata0perations
	...确定卷上的可用文件或可用索引节点数？	可用文件（索引节点）	FilesCapacity - FilesUsed
	...确定卷上已使用和可用存储容量的分配情况？	存储分配	StorageCapacity - StorageUsed

性能警告和建议

FSx for ONTAP 每当其中一个 CloudWatch 指标接近或超过多个连续数据点的预定阈值时，就会显示针对这些指标的警告。这些警告会为您提供切实可行的建议，您可以使用这些建议来优化文件系统的性能。

可以在监控和性能控制面板的多个区域内访问警告。所有活动或最近的 Amazon FSx 性能警告以及为文件系统配置的处于 CloudWatch 警报状态的所有警报都将显示在 “监控和性能” 面板的 “摘要” 部分中。仪表板中显示指标图表的部分也会显示警告。

您可以为任何 Amazon FSx 指标创建 CloudWatch 警报。有关更多信息，请参阅 创建亚马逊 CloudWatch 警报以监控亚马逊 FSx。

使用性能警告提高文件系统的性能

Amazon FSx 提供切实可行的建议，您可以使用这些建议来优化文件系统的性能。这些建议介绍了如何解决潜在的性能瓶颈。如果您希望继续进行活动，或者该活动对文件系统的性能造成了影响，您可以采取建议的操作。根据触发警告的指标，您可以通过增加文件系统的吞吐能力或存储容量来解决警告，如下表所述。

控制面板部分	如果有针对此指标的警告	请执行该操作
仓储服务	主存储容量利用率	如果文件系统尚未达到最大的 SSD 存储容量，则增加文件系统的主存储容量。有关更多信息，请参阅 更新 SSD 存储容量和预调配 IOPS。

控制面板部分	如果有针对此指标的警告	请执行该操作
		如果文件系统有多个 HA 对，且只有一部分文件系统聚合（构成主存储层的存储池）的主存储容量利用率较高，您还可以重新平衡工作负载，以便主存储容量利用率更均匀地分布在文件系统中。有关重新平衡工作负载的更多信息，请参阅 跨 HA 对平衡工作负载。 如果您当前正在执行 SSD 缩减操作，且新磁盘组的利用率超过 80%，可采取以下任一措施：将数据分层迁移至容量池、从已重定向至新磁盘的卷中删除数据，或在缩减操作期间提交增加 SSD 容量的请求。在恢复降价操作之前，Amazon FSx 将优先考虑提高请求的优先级。有关更多信息，请参阅 减少文件系统的 SSD 存储容量（控制台）。
文件服务器性能	网络吞吐量 磁盘吞吐量 磁盘 IOPS CPU 使用率	如果文件系统尚未达到最大吞吐能力，请增加文件系统的吞吐能力。有关更新吞吐能力的更多信息，请参阅 更新吞吐能力。 如果文件系统有多个 HA 对，且只有一部分文件服务器的利用率很高，您还可以重新平衡工作负载，以便工作负载更均匀地利用文件系统每个 HA 对的性能。有关重新平衡工作负载的更多信息，请参阅 跨 HA 对平衡工作负载。
磁盘性能	磁盘 IOPS	如果文件系统尚未达到当前其吞吐能力的最大 SSD IOPS，请增加 SSD IOPS。有关更新文件系统预置 IOPS 的更多信息，请参阅 更新 SSD 存储容量和预调配 IOPS。 如果文件系统有多个 HA 对，且只有一部分文件系统聚合（构成主存储层的存储池）的磁盘 IOPS 利用率较高，您还可以重新平衡工作负载，以便在文件系统中更均匀地利用磁盘 IOPS。有关重新平衡工作负载的更多信息，请参阅 跨 HA 对平衡工作负载。

> **Note**
>
> 在 SSD 缩减操作期间，由于该操作会消耗磁盘和网络资源，写入密集型工作负载可能会出现暂时的性能下降。为最大限度降低对性能的影响，在执行 SSD 缩减操作之前，应保持足够的余量，具体要求为：持续性工作负载不得长期占用超过 50% 的 CPU、50% 的磁盘吞吐量或 50% 的 SSD IOPS。
>
> I/O 当客户端访问被重定向到新的磁盘组时，每个卷可能会出现最多 60 秒的短暂停顿。在操作的切换阶段出现这些暂停实属预期且正常。

有关文件系统的更多信息，请参阅适用于 ONTAP 性能的 Amazon FS NetApp x。

创建亚马逊 CloudWatch 警报以监控亚马逊 FSx

您可以创建一个 CloudWatch 警报，在警报状态发生变化时发送亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 消息。警报会在指定时间段内监控某个指标。根据需要，警报接下来会根据相对于给定阈值的指标的值在很多个时间段内执行一项或多项操作。操作是一个发送到 Amazon SNS 主题或 Auto Scaling 策略的通知。

警报仅针对持续的状态变化调用操作。 CloudWatch 警报不会仅仅因为它们处于特定状态而调用操作；该状态必须已更改并保持了指定的时间段。您可以从亚马逊 FSx 控制台或亚马逊控制台创建警报。CloudWatch

以下过程介绍如何使用 Amazon FSx 控制台、 AWS Command Line Interface (AWS CLI) 和 API 创建警报。

使用 Amazon FSx 控制台设置警报

1. 打开 Amazon FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 在左侧导航窗格中，选择文件系统，然后选择要创建警报的文件系统。
3. 在摘要页面上，从第二个面板中选择监控和性能。
4. 选择 “CloudWatch 警报” 选项卡。
5. 选择创建 CloudWatch 警报。随后您将被重定向至 CloudWatch 控制台。
6. 选择选择指标。
7. 在 “指标” 部分中，选择FSx。
8. 选择一个指标类别：
   - 文件系统指标

- 详细的文件系统指标
- 卷指标
- 详细的卷指标

9. 选中您要为其创建警报的指标，然后选择选择指标。
10. 在条件部分中，选择您希望用于该警报的条件，然后选择下一步。

> **Note**
>
> 在文件系统维护期间，可能不会发布指标。为防止不必要和误导性的警报条件更改，并配置警报使其能够应对丢失的数据点，请参阅 Amazon CloudWatch 用户指南中的配置 CloudWatch 警报如何处理丢失的数据。

11. 如果您 CloudWatch 想在警报状态启动操作时向您发送电子邮件或 Amazon SNS 通知，请为警报状态触发选择警报状态。

    为向以下 SNS 主题发送通知选择一个选项。如果您选择创建主题，则可以为新电子邮件订阅列表设置名称和电子邮件地址。此列表将保存下来并会在将来的警报字段中显示出来。选择下一步。

> **Note**
>
> 如果您使用创建主题 创建了一个新的 Amazon SNS 主题，那么电子邮件地址在接收通知之前必须通过验证。当报警器进入报警状态时，才发送电子邮件。如果在验证电子邮件地址之前此警报状态发生了变化，那么它们不会接收到通知。

12. 填写警报名称和警报描述字段，然后选择下一步。
13. 在预览和创建页面上，查看您即将创建的警报，然后选择创建警报。

使用 CloudWatch 控制台设置警报

1. 打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
2. 选择创建警报以启动创建警报向导。
3. 从步骤 6 开始，按照使用 Amazon FSx 控制台设置警报中的步骤进行操作。

要使用设置警报 AWS CLI

- 调用 C put-metric-alarmLI 命令。有关更多信息，请参阅 AWS CLI 命令参考。

使用 CloudWatch API 设置警报

- 调用 PutMetricAlarm API 操作 。有关更多信息，请参阅 Amazon CloudWatch API 参考。

文件系统指标

您 FSx 的 Amazon for NetApp ONTAP 文件系统指标分为文件系统指标或详细文件系统指标。

- 文件系统指标是单个文件系统的聚合性能和存储指标，采用单一维度，即 FileSystemId。这些指标会衡量文件系统的网络性能和存储容量使用情况。
- 详细的文件系统指标会衡量文件系统的存储容量以及各个存储层（例如，SSD 存储和容量池存储）中已使用的存储量。每个指标中都包含 FileSystemId、StorageTier 和 DataType 维度。

请注意以下有关亚马逊何时向其 FSx 发布这些指标的数据点的信息 CloudWatch：

- 对于利用率指标（名称以利用率结尾的任何指标，例如 NetworkThroughputUtilization），每个活动文件服务器或聚合的每个周期都会发出一个数据点。例如，A FSx mazon 为每个活动文件服务器发布一个分钟指标FileServerDiskIopsUtilization，为每个聚合发布一个分钟指标。DiskIopsUtilization
- 对于其他所有指标，每个周期发出一个数据点，这与所有活动文件服务器中的指标（例如文件服务器指标为 DataReadBytes）或所有聚合中的指标（例如存储指标为 DiskReadBytes）的总值相对应。

主题

- 网络 I/O 指标
- 文件服务器指标
- 磁盘 I/O 指标
- 存储容量指标
- 详细的文件系统指标

网络 I/O 指标

以上所有指标均采用同一维度，即 FileSystemId。

指标	说明
NetworkThroughputUtilization	文件系统的网络吞吐量利用率百分比。请注意，此指标反映了流量较高的方向，即入站或出站。要查看每个方向的单独指标，请参阅 NetworkReceivedBytes 和 NetworkSentBytes 指标。 Average 统计数据是指定时间段内文件系统的网络吞吐量的平均利用率。 Minimum 统计数据是指定时间段内文件系统的网络吞吐量的最低利用率。 Maximum 统计数据是指定时间段内文件系统的网络吞吐量的最高利用率。 单位：百分比 有效统计数据：Average、Minimum 和 Maximum
NetworkSentBytes	文件系统发送的字节数（网络 I/O）。 Sum 统计数据是指定时间段内文件系统发送的字节总数。 要计算指定时段内的任意统计数据的发送吞吐量（每秒字节数），请将统计数据除以该时段的秒数。 单位：字节 有效统计数据：Sum
NetworkReceivedBytes	文件系统收到的字节数（网络 I/O）。 Sum 统计数据是指定时间段内文件系统收到的字节总数。

指标	说明
	要计算指定时段内的任意统计数据的接收吞吐量（每秒字节数），请将统计数据除以该时段的秒数。 单位：字节 有效统计数据：Sum
DataReadBytes	从客户端读取到文件系统的字节数（网络 I/O）。 Sum 统计数据是指定时间段内与读取操作相关的总字节数。要计算指定时段内的平均吞吐量（每秒字节数），请将 Sum 统计数据除以该时段的秒数。 单位：字节 有效统计数据：Sum
DataWriteBytes	从客户端写入文件系统的字节数（网络 I/O）。 Sum 统计数据是指定时间段内与写入操作相关的总字节数。要计算指定时段内的平均吞吐量（每秒字节数），请将 Sum 统计数据除以该时段的秒数。 单位：字节 有效统计数据：Sum

指标	说明
DataReadOperations	从客户端读取到文件系统的读取操作（网络 I/O）次数。 Sum统计数据是在指定时间段内发生的 I/O 操作总数。要计算指定时段内的每秒平均读取操作数，请将 Sum 统计数据除以该时段的秒数。 单位：计数 有效统计数据：Sum
DataWriteOperations	从客户端写入到文件系统的写入操作（网络 I/O）次数。 Sum统计数据是在指定时间段内发生的 I/O 操作总数。要计算指定时段内的每秒平均写入操作数，请将 Sum 统计数据除以该时段的秒数。 单位：计数 有效统计数据：Sum
MetadataOperations	从客户端到文件系统的元数据操作（网络 I/O）次数。 Sum统计数据是在指定时间段内发生的 I/O 操作总数。要计算指定时段内的每秒平均元数据操作数，请将 Sum 统计数据除以该时段的秒数。 单位：计数 有效统计数据：Sum

指标	说明
DataReadOperationTime	因客户端访问文件系统内数据而在文件系统内进行读取操作（网络 I/O）所花费的总时间。 Sum 统计数据是指定时间段内进行读取操作所花费的总秒数。要计算某个时间段内的平均读取延迟，请将 Sum 统计数据除以同一时间段内的 DataReadOperations 指标的 Sum。 单位：秒 有效统计数据：Sum
DataWriteOperationTime	因客户端访问文件系统内数据而在文件系统内完成写入操作（网络 I/O）所花费的总时间。 Sum 统计数据是指定时间段内进行写入操作所花费的总秒数。要计算某个时间段内的平均写入延迟，请将 Sum 统计数据除以同一时间段内的 DataWriteOperations 指标的 Sum。 单位：秒 有效统计数据：Sum
CapacityPoolReadBytes	从文件系统的容量池层读取（网络 I/O）的字节数。 为确保数据完整性，ONTAP 会在执行写入操作后立即对容量池执行读取操作。 Sum 统计数据是指定时间段内从文件系统的容量池层读取的字节总数。要计算容量池的每秒字节数，请将 Sum 统计数据除以指定时间段内的秒数。 单位：字节 有效统计数据：Sum

指标	说明
CapacityPoolReadOperations	从文件系统的容量池层执行读取操作（网络 I/O）的次数。这将转化为容量池读取请求。 为确保数据完整性，ONTAP 会在执行写入操作后立即对容量池执行读取操作。 Sum 统计数据是指定时间段内从文件系统的容量池层执行读取操作的总次数。要计算容量池的每秒请求次数，请将 Sum 统计数据除以指定时间段内的秒数。 单位：计数 有效统计数据：Sum
CapacityPoolWriteBytes	向文件系统的容量池层写入（网络 I/O）的字节数。 为确保数据完整性，ONTAP 会在执行写入操作后立即对容量池执行读取操作。 Sum 统计数据是指定时间段内向文件系统的容量池层写入的字节总数。要计算容量池的每秒字节数，请将 Sum 统计数据除以指定时间段内的秒数。 单位：字节 有效统计数据：Sum

指标	说明
CapacityPoolWriteOperations	向文件系统的容量池层执行写入操作（网络 I/O）的次数。这将转化为写入请求。 为确保数据完整性，ONTAP 会在执行写入操作后立即对容量池执行读取操作。 Sum 统计数据是指定时间段内向文件系统的容量池层执行写入操作的总次数。要计算容量池的每秒请求次数，请将 Sum 统计数据除以指定时间段内的秒数。 单位：计数 有效统计数据：Sum

文件服务器指标

以上所有指标均采用同一维度，即 FileSystemId。

指标	说明
CPUUtilization	文件系统 CPU 资源的利用率百分比。 Average 统计数据是指定时间段内文件系统的平均 CPU 利用率。 Minimum 统计数据是指定时间段内文件系统的最低 CPU 利用率。 Maximum 统计数据是指定时间段内文件系统的最高 CPU 利用率。 单位：百分比 有效统计数据：Average、Minimum 和 Maximum

指标	说明
FileServerDiskThroughputUtilization	您的文件服务器和主要层之间的磁盘吞吐量，占由吞吐能力决定的预配置限制的百分比。 Average 统计数据是指定时间段内文件服务器的磁盘吞吐量的平均利用率。 Minimum 统计数据是指定时间段内文件服务器的磁盘吞吐量的最低利用率。 Maximum 统计数据是指定时间段内文件服务器的磁盘吞吐量的最高利用率。 单位：百分比 有效统计数据：Average、Minimum 和 Maximum
FileServerDiskThroughputBalance	文件服务器和主要层之间磁盘吞吐量的可用突增点数百分比。这对于预配置的吞吐容量小于 512 MBps 的文件系统有效。 Average 统计数据是指定时间段内的平均可用突增平衡。 Minimum 统计数据是指定时间段内的最小可用突增平衡。 Maximum 统计数据是指定时间段内的最大可用突增平衡。 单位：百分比 有效统计数据：Average、Minimum 和 Maximum

指标	说明
FileServerDiskIopsBalance	您的文件服务器和主要层之间可用磁盘 IOPS 突增点数的百分比。这对于预配置的吞吐容量小于 512 MBps 的文件系统有效。 Average 统计数据是指定时间段内的平均可用突增平衡。 Minimum 统计数据是指定时间段内的最小可用突增平衡。 Maximum 统计数据是指定时间段内的最大可用突增平衡。 单位：百分比 有效统计数据：Average、Minimum 和 Maximum
FileServerDiskIopsUtilization	文件服务器的可用磁盘 IOPS 容量的 IOPS 利用率百分比。 Average 统计数据是指定时间段内文件系统的平均磁盘 IOPS 利用率。 Minimum 统计数据是指定时间段内文件系统的最小磁盘 IOPS 利用率。 Maximum 统计数据是指定时间段内文件系统的最大磁盘 IOPS 利用率。 单位：百分比 有效统计数据：Average、Minimum 和 Maximum

指标	说明
FileServerCacheHitRatio	由文件系统 RAM 和 NVMe 缓存中的数据处理的所有读取请求的百分比。百分比越高意味着文件系统的读取缓存所提供的读取越多。 单位：百分比 Average 统计数据是指定时间段内文件系统的平均缓存命中率百分比。 Minimum 统计数据是指定时间段内文件系统的最低缓存命中率百分比。 Maximum 统计数据是指定时间段内文件系统的最高缓存命中率百分比。 有效统计数据：Average、Minimum 和 Maximum

磁盘 I/O 指标

以上所有指标均采用同一维度，即 FileSystemId。

指标	说明
DiskReadBytes	从任何磁盘读取到文件系统的主要层的字节数（磁盘 I/O）。 Sum 统计数据是指定时间段内从文件系统读取的字节总数。 要计算指定时段内的任意统计数据的读取磁盘吞吐量（每秒字节数），请将 Sum 统计数据除以该时段的秒数。 单位：字节 有效统计数据：Sum

指标	说明
DiskWriteBytes	从任何磁盘写入到文件系统的主要层的字节数（磁盘 I/O）。 Sum 统计数据是指定时间段内从文件系统写入的字节总数。 要计算指定时段内的任意统计数据的写入磁盘吞吐量（每秒字节数），请将 Sum 统计数据除以该时段的秒数。 单位：字节 有效统计数据：Sum
DiskIopsUtilization	您的文件服务器和存储卷之间的磁盘 IOPS，占由主要层预配置的磁盘 IOPS 限制的百分比。 Average 统计数据是指定时间段内文件系统的平均磁盘 IOPS 利用率。 Minimum 统计数据是指定时间段内文件系统的最小磁盘 IOPS 利用率。 Maximum 统计数据是指定时间段内文件系统的最大磁盘 IOPS 利用率。 单位：百分比 有效统计数据：Average、Minimum 和 Maximum

指标	说明
DiskReadOperations	从文件系统的主要层执行读取操作（网络 I/O）的次数。 Sum 统计数据是指定时间段内从主要层执行读取操作的总次数。 单位：计数 有效统计数据：Sum
DiskWriteOperations	向文件系统的主要层执行写入操作（网络 I/O）的次数。 Sum 统计数据是指定时间段内向主要层执行写入操作的总次数。 单位：计数 有效统计数据：Sum

存储容量指标

以上所有指标均采用同一维度，即 FileSystemId。

指标	说明
StorageEfficiencySavings	通过存储效率功能（压缩、重复数据删除和压缩）节省的字节。 Average 统计数据是指定时间段内的存储效率带来的平均节省量。要计算存储效率节省在一分钟内占所有数据存储的百分比，请使用 StorageEfficiencySavings 除以 StorageEfficiencySavings 和 StorageUsed 文件系统指标（使用 StorageUsed 的统计数据 Sum）之和。

指标	说明
	Minimum 统计数据是指定时间段内的存储效率带来的最小节省量。 Maximum 统计数据是指定时间段内的存储效率带来的最大节省量。 单位：字节 有效统计数据：Average、Minimum 和 Maximum
StorageUsed	存储在文件系统上的物理数据总量，包括主要（SSD）层和容量池层。该指标包括存储效率功能（例如数据压缩和重复数据删除）带来的节省。 单位：字节 有效统计数据：Average、Minimum 和 Maximum

指标	说明
LogicalDataStored	存储在文件系统上的逻辑数据总量，包括 SSD 层和容量池层。该指标包括快照的总逻辑大小 FlexClones，但不包括通过压缩、压缩和重复数据删除实现的存储效率节约。 要计算存储效率带来的节省（以字节为单位），请取某个给定时间段内的 StorageUsed 的 Average，然后从同一时间段的 LogicalDataStored 的 Average 中减去此值。 要计算存储效率带来的节省占逻辑数据总大小的百分比，请取某个给定时间段内的 StorageUsed 的 Average，然后从同一时间段的 LogicalDataStored 的 Average 中减去此值。然后使用差值除以同一时间段内的 LogicalDataStored 的 Average。 单位：字节 有效统计数据：Average、Minimum 和 Maximum

详细的文件系统指标

详细的文件系统指标是每个存储层的详细存储利用率指标。详细的文件系统指标均包含维度 FileSystemId、StorageTier 和 DataType。

- StorageTier 维度指示的是该指标衡量的存储层，可能的值为 SSD 和 StandardCapacityPool。
- DataType 维度指示的是该指标衡量的数据的类型，可能的值为 All。

给定指标和维度键值对的每个唯一组合都占有一行，其中描述该组合的衡量内容。

指标	说明
StorageCapacityUtilization	文件系统的每个聚合的存储容量利用率。对于文件系统的每个聚合，每分钟都会发出一个指标。 Average 统计数据是指定时间段内文件系统性能层的平均存储容量利用率。 Minimum 统计数据是指定时间段内文件系统性能层的最低存储容量利用率。 Maximum 统计数据是指定时间段内文件系统性能层的最高存储容量利用率。 单位：百分比 有效统计数据：Average、Minimum 和 Maximum
StorageCapacity	主要（SSD）层的总存储容量。 单位：字节 有效统计数据：Maximum
StorageUsed	特定于存储层的已使用的物理存储容量（以字节为单位）。该值包括存储效率功能（例如数据压缩和重复数据删除）带来的节省。StorageTier 的有效维度值为 SSD 和 StandardCapacityPool ，对应该指标衡量的存储层。此指标还需要带有 All 值的维度 DataType。 Average、Minimum 和 Maximum 统计数据是给定时间段内各层的存储消耗（以字节为单位）。 要计算主要（SSD）存储层的存储容量利用率，请使用同一时间段内的 Maximum StorageCapacity 除以这些统计数据中的任意值，并且 StorageTier 维度等于 SSD。

指标	说明
	要计算主要（SSD）存储层的免费存储容量（以字节为单位），请使用同一时间段内的 Maximum StorageCapacity 除以这些统计数据中的任意值，并且 StorageTier 维度等于 SSD。 单位：字节 有效统计数据：Average、Minimum 和 Maximum

第二代文件系统指标

为 ONTAP 第二代文件系统 FSx 提供了以下指标。对于指标，每个 HA 对和每个聚合（存储利用率指标）都会发出一个数据点。

> **Note**
>
> 如果文件系统具有多个 HA 对，还可以使用单 HA 对文件系统指标和卷指标。

主题

- 网络 I/O 指标
- 文件服务器指标
- 磁盘 I/O 指标
- 详细的文件系统指标

网络 I/O 指标

以上所有指标均使用 FileSystemId 和 FileServer 两个维度。

- FileSystemId— 您的文件系统的 AWS 资源 ID。
- FileServer - ONTAP 中文件服务器（或节点）的名称（例如 FsxId01234567890abcdef-01）。奇数文件服务器为首选文件服务器（也就是说，除非文件系统已失效转移至辅助文件服务器，否则将由这些服务器提供流量），而偶数文件服务器为辅助文件服务

器（也就是说，它们仅在伙伴服务器不可用时提供流量）。因此，辅助文件服务器的利用率通常低于首选文件服务器。

指标	说明
NetworkThroughputUtilization	网络吞吐量利用率，用文件系统可用网络吞吐量的百分比表示。该指标等于 NetworkSentBytes 与 NetworkReceivedBytes 的最大值，表示为文件系统中一个 HA 对的网络吞吐能力的百分比。此指标将考虑所有流量，包括后台任务（例如 SnapMirror分层和备份）。对于文件系统的每个文件服务器，每分钟都会发出一个指标。 Average 统计数据是给定文件服务器在指定时间段内的平均网络吞吐量利用率。 Minimum 统计数据是给定文件服务器在指定时间段内一分钟的最低网络吞吐量利用率。 Maximum 统计数据是给定文件服务器在指定时间段内一分钟的最高网络吞吐量利用率。 单位：百分比 有效统计数据：Average、Minimum 和 Maximum
NetworkSentBytes	文件系统发送的字节数（网络 I/O）。此指标将考虑所有流量，包括后台任务（例如 SnapMirror分层和备份）。对于文件系统的每个文件服务器，每分钟都会发出一个指标。 Sum 统计数据是给定文件服务器在指定时间段内通过网络发送的字节总数。 Average 统计数据是给定文件服务器在指定时间段内通过网络发送的平均字节数。

指标	说明
	Minimum 统计数据是给定文件服务器在指定时间段内通过网络发送的最低字节数。 Maximum 统计数据是给定文件服务器在指定时间段内通过网络发送的最高字节数。 要计算指定时段内的任意统计数据的发送吞吐量（每秒字节数），请将统计数据除以该时段的秒数。 单位：字节 有效统计数据：Sum、Average、Minimum 和 Maximum

指标	说明
NetworkReceivedBytes	文件系统收到的字节数（网络 I/O）。此指标将考虑所有流量，包括后台任务（例如 SnapMirror分层和备份）。对于文件系统的每个文件服务器，每分钟都会发出一个指标。 Sum 统计数据是给定文件服务器在指定时间段内通过网络接收的字节总数。 Average 统计数据是给定文件服务器在指定时间段内每分钟通过网络接收的平均字节数。 Minimum 统计数据是给定文件服务器在指定时间段内每分钟通过网络接收的最低字节数。 Maximum 统计数据是给定文件服务器在指定时间段内每分钟通过网络接收的最高字节数。 要计算此时段内的任意统计数据的接收吞吐量（每秒字节数），请将统计数据除以该时段的秒数。 单位：字节 有效统计数据：Sum、Average、Minimum 和 Maximum

文件服务器指标

以上所有指标均使用 FileSystemId 和 FileServer 两个维度。

指标	说明
CPUUtilization	文件系统 CPU 资源的利用率百分比。对于文件系统的每个文件服务器，每分钟都会发出一个指标。

指标	说明
	Average 统计数据是指定时间段内文件系统的平均 CPU 利用率。 Minimum 统计数据是给定文件服务器在指定时间段内的最低 CPU 利用率。 Maximum 统计数据是给定文件服务器在指定时间段内的最高 CPU 利用率。 单位：百分比 有效统计数据：Average、Minimum 和 Maximum
FileServerDiskThroughputUtilization	文件服务器与聚合之间的磁盘吞吐量，表示为由吞吐能力决定的预调配限制的百分比。此指标将考虑所有流量，包括后台任务（例如 SnapMirror分层和备份）。该指标等于 DiskReadBytes 与 DiskWriteBytes 之和，表示为文件系统中一个 HA 对的文件服务器磁盘吞吐能力的百分比。对于文件系统的每个文件服务器，每分钟都会发出一个指标。 Average 统计数据是给定文件服务器在指定时间段内的平均文件服务器磁盘吞吐量利用率。 Minimum 统计数据是给定文件服务器在指定时间段内的最低文件服务器磁盘吞吐量利用率。 Maximum 统计数据是给定文件服务器在指定时间段内的最高文件服务器磁盘吞吐量利用率。 单位：百分比 有效统计数据：Average、Minimum 和 Maximum

指标	说明
FileServerDiskIopsUtilization	文件服务器的可用磁盘 IOPS 容量的 IOPS 利用率，表示为磁盘 IOPS 限制的百分比。这与 DiskIopsUtilization 区别在于，磁盘 IOPS 利用率超出了文件服务器可以处理的最大值，而不是预置的磁盘 IOPS。此指标将考虑所有流量，包括后台任务（例如 SnapMirror分层和备份）。对于文件系统的每个文件服务器，每分钟都会发出一个指标。 Average 统计数据是指定时间段内给定文件服务器的平均磁盘 IOPS 利用率。 Minimum 统计数据是指定时间段内给定文件服务器的最低磁盘 IOPS 利用率。 Maximum 统计数据是指定时间段内给定文件服务器的最高磁盘 IOPS 利用率。 单位：百分比 有效统计数据：Average、Minimum 和 Maximum

指标	说明
FileServerCacheHitRatio	由驻留在文件系统 RAM 中的数据或每个 HA 对（例如 HA 对中的活动文件服务器）的 NVMe 缓存中的数据处理的所有读取请求的百分比。百分比越高表示缓存读取量占总读取量的比例越高。所有任务 I/O 都考虑在内，包括后台任务（例如 SnapMirror分层和备份）。对于文件系统的每个文件服务器，每分钟都会发出一个指标。 单位：百分比 Average 统计数据是指定时间段内文件系统的一个 HA 对的平均缓存命中率。 Minimum 统计数据是指定时间段内文件系统的一个 HA 对的最低缓存命中率。 Maximum 统计数据是指定时间段内文件系统的一个 HA 对的最高缓存命中率。 有效统计数据：Average、Minimum 和 Maximum

磁盘 I/O 指标

以上所有指标均使用 FileSystemId 和 Aggregate 两个维度。

- FileSystemId— 您的文件系统的 AWS 资源 ID。
- Aggregate - 文件系统的性能层由称为聚合的多个存储池组成。每个 HA 对都有一个聚合。例如，在一个 HA 对中，聚合 aggr1 映射到文件服务器 FsxId01234567890abcdef-01（活动文件服务器）和文件服务器 FsxId01234567890abcdef-02（辅助文件服务器）。

指标	说明
DiskReadBytes	从此聚合中进行任何磁盘读取的字节数（磁盘 IO）。此指标将考虑所有流量，包括后台任务（例如 SnapMirror分层和备份）。对于文件系统的每个聚合，每分钟都会发出一个指标。 在 SSD 容量缩减操作期间，该指标将同时针对原始聚合（aggr1_old ）和新的较小聚合（aggr1）进行报告。 Sum 统计数据是指定时间段内每分钟从给定聚合读取的字节总数。 Average 统计数据是指定时间段内每分钟从给定聚合读取的平均字节数。 Minimum 统计数据是指定时间段内每分钟从给定聚合读取的最低字节数。 Maximum 统计数据是指定时间段内每分钟从给定聚合读取的最高字节数。 要计算此时段内的任意统计数据的读取磁盘吞吐量（每秒字节数），请将统计数据除以该时段的秒数。 单位：字节 有效统计数据：Sum、Average、Minimum 和 Maximum
DiskWriteBytes	向此聚合进行任何磁盘写入的字节数（磁盘 IO）。此指标将考虑所有流量，包括后台任务（例如 SnapMirror分层和备份）。对于文件系统的每个聚合，每分钟都会发出一个指标。

指标	说明
	在 SSD 容量缩减操作期间，该指标将同时针对原始聚合（aggr1_old ）和新的较小聚合（aggr1）进行报告。 Sum 统计数据是指定时间段内从给定聚合写入的字节总数。 Average 统计数据是指定时间段内每分钟向给定聚合写入的平均字节数。 Minimum 统计数据是指定时间段内每分钟向给定聚合写入的最低字节数。 Maximum 统计数据是指定时间段内每分钟向给定聚合写入的最高字节数。 要计算指定时段内的任意统计数据的写入磁盘吞吐量（每秒字节数），请将统计数据除以该时段的秒数。 单位：字节 有效统计数据：Sum、Average、Minimum 和 Maximum

指标	说明
DiskIopsUtilization	一个聚合的磁盘 IOPS 利用率，表示为聚合的磁盘 IOPS 限制的百分比（即文件系统的总 IOPS 除以文件系统的 HA 对数）。这与 FileServerDiskIopsUtilization 的区别在于，它是预置磁盘 IOPS 相对于预置 IOPS 限制的利用率，而不是文件服务器支持的最大磁盘 IOPS（即由每个 HA 对配置的吞吐能力决定的值）。此指标将考虑所有流量，包括后台任务（例如 SnapMirror分层和备份）。对于文件系统的每个聚合，每分钟都会发出一个指标。 在 SSD 容量缩减操作期间，该指标将同时针对原始聚合（aggr1_old ）和新的较小聚合（aggr1）进行报告。 Average 统计数据是指定时间段内给定聚合的平均磁盘 IOPS 利用率。 Minimum 统计数据是指定时间段内给定聚合的最低磁盘 IOPS 利用率。 Maximum 统计数据是指定时间段内给定聚合的最高磁盘 IOPS 利用率。 单位：百分比 有效统计数据：Average、Minimum 和 Maximum

指标	说明
DiskReadOperations	对此聚合执行读取操作（磁盘 IO）的次数。此指标将考虑所有流量，包括后台任务（例如SnapMirror分层和备份）。对于文件系统的每个聚合，每分钟都会发出一个指标。 在 SSD 容量缩减操作期间，该指标将同时针对原始聚合（aggr1_old ）和新的较小聚合（aggr1）进行报告。 Sum 统计数据是给定聚合在指定时间段内执行读取操作的总次数。 Average 统计数据是指定时间段内每分钟由给定聚合执行的平均读取操作次数。 Minimum 统计数据是指定时间段内每分钟由给定聚合执行的最低读取操作次数。 Maximum 统计数据是指定时间段内每分钟由给定聚合执行的最高读取操作次数。 要计算一段时间内的平均磁盘 IOPS，可使用 Average 统计数据并将结果除以 60（秒）。 单位：计数 有效统计数据：Sum、Average、Minimum 和 Maximum

指标	说明
DiskWriteOperations	对此聚合执行写入操作（磁盘 IO）的次数。此指标将考虑所有流量，包括后台任务（例如SnapMirror分层和备份）。对于文件系统的每个聚合，每分钟都会发出一个指标。 在 SSD 容量缩减操作期间，该指标将同时针对原始聚合（aggr1_old ）和新的较小聚合（aggr1）进行报告。 Sum 统计数据是给定聚合在指定时间段内执行写入操作的总次数。 Average 统计数据是指定时间段内每分钟由给定聚合执行的平均写入操作次数。 要计算一段时间内的平均磁盘 IOPS，可使用 Average 统计数据并将结果除以 60（秒）。 单位：计数 有效统计数据：Sum 和 Average

详细的文件系统指标

详细的文件系统指标是每个存储层的详细存储利用率指标。详细的文件系统指标有 FileSystemId、StorageTier 和 DataType 维度，或 FileSystemId、StorageTier、DataType 和 Aggregate 维度。

- 未提供 Aggregate 维度时，指标适用于整个文件系统。StorageUsed 和 StorageCapacity 指标每分钟都有一个数据点，对应于文件系统的总存储使用量（每个存储层）和总存储容量（SSD 层）。同时，StorageCapacityUtilization 指标每分钟为每个聚合发出一个指标。
- 提供 Aggregate 维度时，指标适用于各个聚合。

维度的含义如下：

- FileSystemId— 您的文件系统的 AWS 资源 ID。

- Aggregate - 文件系统的性能层由称为聚合的多个存储池组成。每个 HA 对都有一个聚合。例如，在一个 HA 对中，聚合 aggr1 映射到文件服务器 FsxId01234567890abcdef-01（活动文件服务器）和文件服务器 FsxId01234567890abcdef-02（辅助文件服务器）。
- StorageTier - 指示该指标衡量的存储层，可能的值为 SSD 和 StandardCapacityPool。
- DataType - 指示该指标衡量的数据的类型，可能的值为 All。

给定指标和维度键值对的每个唯一组合都占有一行，其中描述该组合的衡量内容。

指标	说明
StorageCapacityUtilization	给定文件系统聚合的存储容量利用率。对于文件系统的每个聚合，每分钟都会发出一个指标。 Average 统计数据是指定时间段内给定聚合的平均存储容量利用率。 Minimum 统计数据是指定时间段内给定聚合的最小存储容量利用率。 Maximum 统计数据是指定时间段内给定聚合的最大存储容量利用率。 在 SSD 容量缩减操作期间，该指标将同时针对原始聚合（aggr1_old ）和新的较小聚合（aggr1）进行报告。 单位：百分比 有效统计数据：Average、Minimum 和 Maximum
StorageCapacity	给定文件系统聚合的存储容量。对于文件系统的每个聚合，每分钟都会发出一个指标。 Average 统计数据是指定时间段内给定聚合的平均存储容量。 Minimum 统计数据是指定时间段内给定聚合的最小存储容量。

指标	说明
	Maximum 统计数据是指定时间段内给定聚合的最大存储容量。 在 SSD 容量缩减操作期间，该指标将同时针对原始聚合（aggr1_old ）和新的较小聚合（aggr1）进行报告。 单位：字节 有效统计数据：Average、Minimum 和 Maximum
StorageUsed	特定于存储层的已使用的物理存储容量（以字节为单位）。该值包括存储效率功能（例如数据压缩和重复数据删除）带来的节省。StorageTier 的有效维度值为 SSD 和 StandardCapacityPool ，对应该指标衡量的存储层。对于文件系统的每个聚合，每分钟都会发出一个指标。 Average 统计数据是给定聚合在指定时间内在给定存储层上消耗的平均物理存储容量。 Minimum 统计数据是给定聚合在指定时间内在给定存储层上消耗的最小物理存储容量。 Maximum 统计数据是给定聚合在指定时间内在给定存储层上消耗的最大物理存储容量。 在 SSD 容量缩减操作期间，该指标将同时针对原始聚合（aggr1_old ）和新的较小聚合（aggr1）进行报告。 单位：字节 有效统计数据：Average、Minimum 和 Maximum

卷指标

您 FSx 的 Amazon for NetApp ONTAP 文件系统可以有一个或多个卷来存储您的数据。这些卷中的每一个都有一组 CloudWatch 指标，分为交易量指标或详细交易量指标。

- 卷指标是每个卷的性能和存储指标，分为 FileSystemId 和 VolumeId 两个维度。FileSystemId 会映射到该卷所属的文件系统。
- 详细的容量 per-storage-tier指标是使用维度（可能的值为和）和使用StorageTier维度（可能的值为、SSD和StandardCapacityPool）来衡量每DataType层数据类型的存储消耗量的指标（可能的值为UserSnapshot、和Other）。这些指标使用 FileSystemId、VolumeId、StorageTier 和 DataType 维度。

主题

网络 I/O 指标

以上所有指标均使用 FileSystemId 和 VolumeId 两个维度。

指标	说明
DataReadBytes	客户端从卷读取的字节数（网络 I/O）。 Sum 统计数据是指定时间段内与读取操作相关的总字节数。要计算指定时段内的平均吞吐量（每秒字节数），请将 Sum 统计数据除以该时段的秒数。 单位：字节 有效统计数据：Sum
DataWriteBytes	客户端写入卷的字节数（网络 I/O）。

指标	说明
	Sum 统计数据是指定时间段内与写入操作相关的总字节数。要计算指定时段内的平均吞吐量（每秒字节数），请将 Sum 统计数据除以该时段的秒数。 单位：字节 有效统计数据：Sum
DataReadOperations	客户端在卷上执行读取操作（网络 I/O）的次数。 Sum 统计数据是指定时间段内执行读取操作的总次数。要计算指定时段内的每秒平均读取操作数，请将 Sum 统计数据除以该时段的秒数。 单位：计数 有效统计数据：Sum
DataWriteOperations	客户端在卷上执行写入操作（网络 I/O）的次数。 Sum 统计数据是指定时间段内执行写入操作的总次数。要计算指定时段内的每秒平均写入操作数，请将 Sum 统计数据除以该时段的秒数。 单位：计数 有效统计数据：Sum

指标	说明
MetadataOperations	从客户端的元数据活动到卷的 I/O 操作（网络 I/O）数量。 Sum 统计数据是指定时间段内执行元数据操作的总次数。要计算指定时段内的每秒平均元数据操作数，请将 Sum 统计数据除以该时段的秒数。 单位：计数 有效统计数据：Sum
DataReadOperationTime	因客户端访问卷内数据而在卷内进行读取操作（网络 I/O）所花费的总时间。 Sum 统计数据是指定时间段内进行读取操作所花费的总秒数。要计算某个时间段内的平均读取延迟，请将 Sum 统计数据除以同一时间段内的 DataReadOperations 指标的 Sum。 单位：秒 有效统计数据：Sum
DataWriteOperationTime	因客户端访问卷内数据而在卷内完成写入操作（网络 I/O）所花费的总时间。 Sum 统计数据是指定时间段内进行写入操作所花费的总秒数。要计算某个时间段内的平均写入延迟，请将 Sum 统计数据除以同一时间段内的 DataWriteOperations 指标的 Sum。 单位：秒 有效统计数据：Sum

指标	说明
MetadataOperationTime	因客户端访问卷内数据而在卷内完成元数据操作（网络 I/O）所花费的总时间。 Sum 统计数据是指定时间段内进行读取操作所花费的总秒数。要计算某个时间段内的平均延迟，请将 Sum 统计数据除以同一时间段内的 MetadataOperations 的 Sum。 单位：秒 有效统计数据：Sum
CapacityPoolReadBytes	从卷的容量池层读取（网络 I/O）的字节数。 为确保数据完整性，ONTAP 会在执行写入操作后立即对容量池执行读取操作。 Sum 统计数据是指定时间段内从卷的容量池层读取的字节总数。要计算容量池的每秒字节数，请将 Sum 统计数据除以指定时间段内的秒数。 单位：字节 有效统计数据：Sum

指标	说明
CapacityPoolReadOperations	从卷的容量池层进行读取操作（网络 I/O）的次数。这将转化为容量池读取请求。 为确保数据完整性，ONTAP 会在执行写入操作后立即对容量池执行读取操作。 Sum 统计数据是指定时间段内从卷的容量池层执行读取操作的总次数。要计算容量池的每秒请求次数，请将 Sum 统计数据除以指定时间段内的秒数。 单位：计数 有效统计数据：Sum
CapacityPoolWriteBytes	向卷的容量池层写入（网络 I/O）的字节数。 为确保数据完整性，ONTAP 会在执行写入操作后立即对容量池执行读取操作。 Sum 统计数据是指定时间段内向卷的容量池层写入的字节总数。要计算容量池的每秒字节数，请将 Sum 统计数据除以指定时间段内的秒数。 单位：字节 有效统计数据：Sum

指标	说明
CapacityPoolWriteOperations	向卷的容量池层执行写入操作（网络 I/O）的次数。这将转化为写入请求。 为确保数据完整性，ONTAP 会在执行写入操作后立即对容量池执行读取操作。 Sum 统计数据是指定时间段内向卷的容量池层执行写入操作的总次数。要计算容量池的每秒请求次数，请将 Sum 统计数据除以指定时间段内的秒数。 单位：计数 有效统计数据：Sum

存储容量指标

以上所有指标均使用 FileSystemId 和 VolumeId 两个维度。

指标	说明
StorageCapacity	卷的大小（以字节计算）。 单位：字节 有效统计数据：Maximum
StorageUsed	卷中已使用逻辑存储容量。 单位：字节 有效统计数据：Average
StorageCapacityUtilization	卷的存储容量利用率。 单位：百分比 有效统计数据：Average

指标	说明
FilesUsed	卷中已使用的文件（文件数或索引节点数）。 单位：计数 有效统计数据：Average
FilesCapacity	可在卷上创建的索引节点总数。 单位：计数 有效统计数据：Maximum

详细的卷指标

相较于卷指标，详细的卷指标使用的维度更多，因此可以更为精细地衡量数据。详细的卷指标包含维度 FileSystemId、VolumeId、StorageTier 和 DataType。

- StorageTier 维度指示的是该指标衡量的存储层，可能的值为 All、SSD 和 StandardCapacityPool。
- DataType 维度指示的是该指标衡量的数据的类型，可能的值为 All、User、Snapshot 和 Other。

下表定义了所列维度的 StorageUsed 指标的衡量内容。

指标	说明
StorageUsed	已使用的逻辑空间量（以字节为单位）。该指标根据与其共同使用的维度来衡量不同类型的空间消耗。当将 StorageTier 设置为 SSD 或 StandardCapacityPool ，且将 DataType 设置为 All 时，此指标将分别衡量该卷在 SSD 和容量池层中的逻辑空间使用情况。将 DataType 维度设置为 User、Snapshot 或 Other，且将 StorageTier 设置为 All 时，此指标会衡量每种相应的数据类型的逻辑空间使用情况。

指标	说明
	Snapshot 数据消耗包括快照储备，默认为卷大小的 5%。 单位：字节 有效统计数据：Average、Minimum 和 Maximum
StorageCapacityUtilization	卷中已使用物理磁盘空间的百分比。 单位：百分比 有效统计数据：Maximum

监控 FSx for ONTAP EMS 事件

您可以使用 NetAPP ONTAP 的本机事件管理系统（EMS）监控 FSx for ONTAP 文件系统事件。您可以使用 NetApp ONTAP CLI 查看这些事件。

主题

- EMS 事件概述
- 查看 EMS 事件
- EMS 事件转发到 Syslog 服务器

EMS 事件概述

EMS 事件是自动生成的通知，当 FSx for ONTAP 文件系统中出现预定义的情况时，会提醒您。这些通知可让您随时了解情况，以便预防或纠正问题，避免导致更大问题，例如存储虚拟机（SVM）身份验证问题或卷已满。

默认情况下，事件会记录在事件管理系统日志中。使用 EMS 可以监控诸如用户密码更改、FlexGroup 中接近满容量的部分、逻辑单元号（LUN）手动联机或脱机或自动调整卷大小之类的事件。

有关 ONTAP EMS 事件的更多信息，请参阅 NetApp ONTAP 文档中心中的 ONTAP EMS 参考。要显示事件类别，请使用文档的左侧导航窗格。

> **Note**
>
> 仅部分 ONTAP EMS 消息适用于 FSx for ONTAP 文件系统。要查看可用 ONTAP EMS 消息的列表，请使用 NetApp ONTAP CLI 中的 event catalog show 命令。

EMS 事件描述包含事件名称、严重性、可能的原因、日志消息和纠正措施，可帮助您决定如何响应。例如，当自动调整卷大小失败时即会发生 wafl.vol.autoSize.fail 事件。根据事件描述，纠正措施是在设置自动调整大小的同时增加最大卷的大小。

查看 EMS 事件

使用 NetApp ONTAP CLI 中的 event log show 命令显示事件日志的内容。如果您在文件系统上具有 `fsxadmin` 角色，则此命令适用。命令语法如下所示：

```
event log show [event_options]
```

最近的事件列在最前面。默认情况下，此命令会显示 EMERGENCY、ALERT、和 ERROR 严重性等级事件，其中包含以下信息：

- 时间 – 事件的时间。
- 节点 –发生事件的节点。
- 严重性 –事件的严重性等级。要显示 NOTICE、INFORMATIONAL、或 DEBUG 严重性等级事件，请使用 `-severity` 选项。
- 事件 –事件名称和消息。

要显示有关事件的详细信息，请使用下表中列出的一个或多个事件选项。

事件选项	描述
`-detail`	显示其他事件信息。
`-detailtime`	按反向时间顺序显示详细事件信息。
`-instance`	显示有关所有字段的详细信息。

事件选项	描述
-node *nodename*|local	显示您指定的节点的事件列表。使用此选项和 -seqnum 显示详细信息。
-seqnum *sequence_number*	选择序列中与该数字匹配的事件。与 -node 一起使用可显示详细信息。

-time *MM/DD/YYYY HH:MM:SS*	选择在此特定时间发生的事件。使用格式：MM/DD/YYYY HH:MM:SS [+- HH:MM]。您可以通过在两个时间语句之间使用 .. 运算符来指定时间范围。
	`event log show -time "04/17/2023 05:55:00".."04/17/2023 06:10:00"`
	比较时间值是相对于运行命令时的当前时间而言的。以下示例说明了如何仅显示最近一分钟内发生的事件：
	`event log show -time >1m`
	此选项的月份和日期字段不使用零填充。这些字段可以是个位数；例如，4/1/2023 06:45:00。

事件选项	描述
-severity *sev_level*	选择与 *sev_level* 值匹配的事件，该值必须为以下类型之一： • EMERGENCY – 中断 • ALERT – 单点故障 • ERROR – 降级 • NOTICE – 信息 • INFORMATIONAL – 信息 • DEBUG – 调试信息 要显示所有事件，请按如下方式指定严重性： `event log show -severity <=DEBUG`

事件选项	描述
-ems-severity *ems_sev_level*	选择与 *ems_sev_level* 值匹配的事件，该值必须为以下类型之一： • NODE_FAULT – 检测到数据损坏或节点无法提供客户端服务。 • SVC_FAULT – 检测到服务暂时中断，通常是软件瞬时故障。 • NODE_ERROR – 检测到非致命性硬件错误。 • SVC_ERROR – 检测到非致命性软件错误。 • WARNING – 不指示故障的高优先级消息。 • NOTICE – 不指示故障的普通优先级消息。 • INFO – 不指示故障的低优先级消息。 • DEBUG – 调试消息。 • VAR – 在运行时系统选择的严重性可变的信息。 要显示所有事件，请按如下方式指定严重性： `event log show -ems-severity <=DEBUG`
-source *text*	选择与##值匹配的事件。源代码通常是软件模块。

事件选项	描述
-message-name *message_name*	选择与 *message_name* 值匹配的事件。消息名称是描述性的，因此按消息名称筛选输出会显示特定类型的消息。
-event *text*	选择与##值匹配的事件。event 字段包含事件全文，包括任何参数。
-kernel-generation-num *integer*	选择与##值匹配的事件。仅来自内核的事件具有内核生成号。
-kernel-sequence-num *integer*	选择与##值匹配的事件。仅来自内核的事件具有内核序列号。
-action *text*	选择与##值匹配的事件。action 字段描述了您必须采取哪些纠正措施（如果有）来纠正这种情况。
-description *text*	选择与##值匹配的事件。description 字段描述了事件发生的原因及其含义。
-filter-name *filter_name*	选择与 *filter_name* 值匹配的事件。只有与该值匹配的现有筛选条件所包含的事件才会显示。
-fields *fieldname* ,...	表示命令输出中还包括指定的一个或多个字段。您可以使用 -fields ？选择想要指定的字段。

查看 EMS 事件

1. 要通过 SSH 进入文件系统的 NetApp ONTAP CLI，请按照《适用于 NetApp ONTAP 的 Amazon FSx 用户指南》中 使用 NetApp ONTAP CLI 部分中记录的步骤进行操作。

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. 使用 `event log show` 命令显示事件日志的内容。

   ```
   ::> event log show
   Time                 Node          Severity      Event
   ------------------- ------------ ------------ ------------------------
   6/30/2023 13:54:19  node1         NOTICE        vifmgr.portup: A link up event was
    received on node node1, port e0a.
   6/30/2023 13:54:19  node1         NOTICE        vifmgr.portup: A link up event was
    received on node node1, port e0d.
   ```

有关 `event log show` 命令返回的 EMS 事件的信息，请参阅 NetApp ONTAP 文档中心的 ONTAP EMS 参考。

EMS 事件转发到 Syslog 服务器

您可以将 EMS 事件配置为转发通知至 Syslog 服务器。EMS 事件转发用于实时监控文件系统，以确定和隔离各种问题的根本原因。如果您的环境还没有用于处理事件通知的 Syslog 服务器，必须先创建一个。必须在文件系统上配置 DNS 才能解析 Syslog 服务器名称。

> **Note**
>
> Syslog 目的地必须位于文件系统使用的主子网中。

将 EMS 事件配置为转发通知至 Syslog 服务器。

1. 要通过 SSH 进入文件系统的 NetApp ONTAP CLI，请按照《适用于 NetApp ONTAP 的 Amazon FSx 用户指南》中 使用 NetApp ONTAP CLI 部分中记录的步骤进行操作。

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. 使用 event notification destination create 命令，创建类型为 `syslog` 的事件通知目的地，并指定以下属性：

- *dest_name* - 要创建的通知目的地的名称（例如，syslog-ems）。事件通知目的地名称必须有 2 到 64 个字符。有效字符为以下 ASCII 字符：A-Z、a-z、0-9、“_” 和“-”。名称必须以 A-Z、a-z 或 0-9 开头和结尾。
- *syslog_name* - Syslog 消息发送到的 Syslog 服务器主机名称或 IP 地址。
- *transport_protocol* - 用于发送事件的协议：
  - udp-unencrypted - 非安全用户数据报协议。此为默认协议。
  - tcp-unencrypted - 非安全传输控制协议。
  - tcp-encrypted - 采用传输层安全性协议（TLS）的传输控制协议。指定此选项后，FSx for ONTAP 将通过验证目的地主机的证书来验证其身份。
- *port_number* - Syslog 消息发送到的 Syslog 服务器端口。syslog-port 参数默认值取决于 syslog-transport 参数的设置。如果 syslog-transport 设置为 tcp-encrypted，syslog-port 默认值为 6514。如果 syslog-transport 设置为 tcp-unencrypted，syslog-port 默认值为 601。否则，默认端口设置为 514。

```
::> event notification destination create -name dest_name -syslog syslog_name -
syslog-transport transport_protocol -syslog-port port_number
```

3. 使用 event notification create 命令创建新的通知，将事件过滤器定义的一组事件转发到在上一步中创建的通知目的地，并指定以下属性：

- *node_name* – 事件筛选器的名称。事件过滤器中包含的事件会被转发到 -destinations 参数中指定的目的地。
- *dest_name* - 事件通知发送到的现有通知目的地的名称。

```
::> event notification create -filter-name filter_name -destinations dest_name
```

4. 如果选择 TCP 作为 *transport_protocol*，则可以使用 event notification destination check 命令生成测试消息并验证设置是否有效。用该命令指定以下属性：

- *node_name* - 节点的名称（例如，FsxId07353f551e6b557b4-01）。
- *dest_name* - 事件通知发送到的现有通知目的地的名称。

```
::> set diag
```

```
::*> event notification destination check -node node_name -destination-
name dest_name
```

使用 Data Infrastructure Insights 进行监控

NetApp 数据基础设施见解（前身为 Cloud Insights）是一项 NetApp 服务，可用于监控 Amazon FSx for NetApp ONTAP 文件系统以及其他 NetApp 存储解决方案。借助 Data Infrastructure Insights，您可以监控某段时间内的配置、容量和性能指标，了解工作负载的趋势，规划未来的性能和存储容量需求。您还可以依据指标条件来创建可以与现有的工作流程和生产力工具集成的警报。

> **Note**
>
> 具有多个 HA 对的第二代文件系统不支持 Data Infrastructure Insights。

Data Infrastructure Insights 提供以下功能：

- 各项指标和日志 – 收集配置、容量和性能指标。通过预定义的控制面板、警报和报告了解工作负载的趋势。
- 用户分析和勒索软件防护 – 您可以使用 Cloud Secure 和 ONTAP 快照来审计、检测、阻止和修复用户错误事件和勒索软件。
- SnapMirror 报告-了解您的 SnapMirror 关系并设置复制问题警报。
- 容量规划 — 了解本地工作负载的资源需求，以帮助您将工作负载迁移到更高效 FSx 的 ONTAP 配置。您还可以利用这些见解来规划何时需要更高的性能或容量来部署 fo FSx r ONTAP。

有关更多信息，请参阅 NetApp ONTAP 产品文档中的数据基础设施见解文档。

使用 Harvest 和 Grafana 监控 FSx for ONTAP 文件系统

NetApp Harvest 是一款用于从 ONTAP 系统收集性能和容量指标的开源工具，与 FSx for ONTAP 兼容。可以结合使用 Harvest 与 Grafana 来获得开源监控解决方案。

开始使用 Harvest 和 Grafana

以下部分详细介绍了如何设置和配置 Harvest 和 Grafana，以测算 FSx for ONTAP 文件系统的性能和存储容量利用率。

您可以使用 Harvest 和 Grafana 监控适用于 NetApp ONTAP 的 Amazon FSx 文件系统。NetApp Harvest 通过从 FSx for ONTAP 文件系统收集性能、容量和硬件指标来监控 ONTAP 数据中心。Grafana 提供可显示所收集 Harvest 指标的控制面板。

支持的 Harvest 控制面板

适用于 NetApp ONTAP 的 Amazon FSx 公开的指标集与本地 NetApp ONTAP 不同。因此，目前仅支持以下带有 `fsx` 标签的开箱即用 Harvest 控制面板与 FSx for ONTAP 配合使用。这些控制面板中的某些面板可能缺少不支持的信息。

- Harvest：元数据
- ONTAP：聚合
- ONTAP：cDOT
- ONTAP：集群
- ONTAP：合规性
- ONTAP：数据中心
- ONTAP：数据保护
- ONTAP：LUN
- ONTAP：网络
- ONTAP：节点
- ONTAP：Qtree
- ONTAP：安全性
- ONTAP：SnapMirror
- ONTAP：SnapMirror 目标
- ONTAP：SnapMirror 源
- ONTAP：SVM
- ONTAP：卷
- ONTAP：按 SVM 划分的卷
- ONTAP：卷深入研究

FSx for ONTAP 支持以下 Harvest 控制面板，但这些控制面板默认情况下未在 Harvest 中启用。

- ONTAP：FlexCache

- ONTAP：FlexGroup
- ONTAP：NFS 客户端
- ONTAP：NFSv4 存储池显示器
- ONTAP：NFS 故障排除
- ONTAP：NVMe 命名空间
- ONTAP：SMB
- ONTAP：工作负载

不支持的 Harvest 控制面板

FSx for ONTAP 不支持以下 Harvest 控制面板。

- ONTAP：磁盘
- ONTAP：外部服务操作
- ONTAP：文件系统分析（FSA）
- ONTAP：余量
- ONTAP：运行状况
- ONTAP：MAV 请求
- ONTAP：MetroCluster
- ONTAP：功率
- ONTAP：Shelf
- ONTAP：S3 对象存储

CloudFormation 模板

首先，您可以部署一个 CloudFormation 模板来自动启动运行 Harvest 和 Grafana 的 Amazon EC2 实例。作为 CloudFormation 模板的输入，您可以为将在此部署中添加的文件系统指定 `fsxadmin` 用户和 Amazon FSx 管理端点。部署完成后，您可以登录 Grafana 控制面板来监控您的文件系统。

此解决方案采用 CloudFormation 自动部署 Harvest 和 Grafana 解决方案。该模板创建了一个 Amazon EC2 Linux 实例并安装 Harvest 和 Grafana 软件。要使用此解决方案，请下载 fsx-ontap-harvest-grafana.template CloudFormation 模板。

> **Note**
>
> 实施此解决方案会产生相关 AWS 服务的账单。有关更多信息，请参阅有关这些服务的定价详细信息页面。

Amazon EC2 实例类型

在配置模板时，您需要提供 Amazon EC2 实例类型。NetApp 对实例大小的建议取决于您监控的文件系统的数量以及您选择收集的指标数量。使用默认配置时，对于您监控的每 10 个文件系统，NetApp 建议：

- CPU：2 个核心
- 内存：1 GB
- 磁盘：500 MB（主要用于日志文件）

以下是一些示例配置和您可以选择的 `t3` 实例类型。

文件系统	CPU	磁盘	实例类型
10 以下	2 个核心	500 MB	`t3.micro`
10–40	4 个核心	1000 MB	`t3.xlarge`
40+	8 个核心	2000 MB	`t3.2xlarge`

有关 Amazon EC2 实例类型的更多信息，请参阅《Amazon EC2 用户指南》中的通用实例。

实例端口规则

在设置 Amazon EC2 实例时，请确保端口 3000 和 9090 接受 Amazon EC2 Harvest 和 Grafana 实例所在安全组的入站流量。由于启动的实例通过 HTTPS 连接到端点，因此它需要解析该端点，这需要使用端口 53 的 TCP/UDP 进行 DNS。此外，要访问该端点，需要使用端口 443 的 TCP 进行 HTTPS 和互联网访问。

部署程序

以下程序配置和部署 Harvest/Grafana 解决方案。部署大约需要五分钟。在开始之前，您的 AWS 账户中必须有一个运行于 Amazon Virtual Private Cloud（Amazon VPC）之中的 FSx for Lustre 文件系统，以及下面列出的模板参数信息。有关创建文件系统的更多信息，请参阅创建文件系统。

启动 Harvest/Grafana 解决方案堆栈

1. 下载 fsx-ontap-harvest-grafana.template CloudFormation 模板。有关创建 CloudFormation 堆栈的更多信息，请参阅《AWS CloudFormation 用户指南》中的在 AWS CloudFormation 控制台上创建堆栈。

   > **Note**
   >
   > 默认情况下，该模板在美国东部（弗吉尼亚州北部）AWS 区域发布。您必须在可以使用 Amazon FSx 的 AWS 区域 启动此解决方案。有关更多信息，请参阅 AWS 一般参考 中的 Amazon FSx 端点和配额。

2. 对于参数，请查看模板的参数并根据文件系统的需求对其进行修改。该解决方案使用以下默认值。

参数	默认值	描述
InstanceType	`t3.micro`	Amazon EC2 实例类型。以下是 `t3` 实例类型。 • `t3.micro` • `t3.small` • `t3.medium` • `t3.large` • `t3.xlarge` • `t3.2xlarge` 有关此参数允许使用的 Amazon EC2 实例类型值的完整列表，请参阅 fsx-ontap-harvest-grafana.template。

参数	默认值	描述
KeyPair	无默认值	用于访问 Amazon EC2 实例的键对。
SecurityGroup	无默认值	Harvest/Grafana 实例的安全组 ID。除了端口 53 和 443，确保您希望用于访问 Grafana 控制面板的客户端已打开入站端口 3000 和 9090。
子网类型	无默认值	指定子网类型 `public` 或 `private`。对必须连接互联网的资源使用 `public` 子网，而对不会连接到互联网的资源使用私有子网。有关更多信息，请参阅《Amazon VPC 用户指南》中的子网类型。
子网	无默认值	指定与适用于 NetApp ONTAP 的 Amazon FSx 文件系统首选子网相同的子网。您可以在 Amazon FSx 控制台的 FSx for ONTAP 文件系统详细信息页面的网络和安全选项卡中找到文件系统的首选子网 ID
LatestLinuxAmiId	`/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2`	给定 AWS 区域 中最新版本的 Amazon Linux 2 AMI

参数	默认值	描述
FSxEndPoint	无默认值	文件系统的管理端点 IP 地址。您可以在 Amazon FSx 控制台的 FSx for ONTAP 文件系统详细信息页面的管理选项卡中找到文件系统的管理端点 IP 地址。
SecretName	无默认值	包含文件系统 `fsxadmin` 用户密码的 AWS Secrets Manager 密钥名称。这是您在创建文件系统时提供的密码。

3. 选择下一步。
4. 在选项中，选择下一步。
5. 在审核中，审核并确认设置。必须选择复选框，以确认模板将创建 IAM 资源。
6. 选择创建以部署堆栈。

您可以在 CloudFormation 控制台的状态列中查看堆栈的状态。您应该在大约五（5）分钟内看到 CREATE_COMPLETE 状态。

登录 Grafana

部署完成后，使用浏览器登录到 Amazon EC2 实例的 IP 和端口 3000 上的 Grafana 控制面板：

```
http://EC2_instance_IP:3000
```

出现提示时，使用 Grafana 默认用户名（`admin`）和密码（`pass`）。我们建议您登录后立即更改密码。

有关更多信息，请参阅 GitHub 上的 NetApp Harvest 页面。

排查 Harvest 和 Grafana 故障

如果遇到 Harvest 和 Grafana 控制面板中提及的任何数据缺失问题，或者难以通过 FSx for ONTAP 设置 Harvest 和 Grafana，请查看以下主题获取潜在的解决方案。

主题

SVM 和卷控制面板为空白

如果 CloudFormation 堆栈已成功部署并且可以联系到 Grafana，但 SVM 和卷控制面板为空白，请使用以下过程排查环境中的故障。您需要通过 SSH 访问部署有 Harvest 和 Grafana 的 Amazon EC2 实例。

1. 通过 SSH 访问当前运行有 Harvest 和 Grafana 客户端的 Amazon EC2 实例。

```
[~]$ ssh ec2-user@ec2_ip_address
```

2. 使用以下命令打开 `harvest.yml` 文件并且：

   - 验证是否为 FSx for ONTAP 实例创建了一个条目 `Cluster-2`。
   - 验证输入的用户名和密码是否与 `fsxadmin` 凭证相符。

```
[ec2-user@ip-ec2_ip_address ~]$ sudo cat /home/ec2-user/harvest_install/harvest/
harvest.yml
```

3. 如果密码字段为空，请在编辑器中打开文件并使用 `fsxadmin` 密码进行更新，如下所示：

```
[ec2-user@ip-ec2_ip_address ~]$ sudo vi /home/ec2-user/harvest_install/harvest/
harvest.yml
```

4. 确保 `fsxadmin` 用户凭证以如下格式存储在 Secrets Manager 中，以备将来部署时使用，并将 *fsxadmin_password* 替换为您的密码。

```
{"username" : "fsxadmin", "password" : "fsxadmin_password"}
```

CloudFormation 堆栈在超时后回滚

如果无法成功部署 CloudFormation 堆栈，并且堆栈出错回滚，请使用以下过程来解决此问题。您需要通过 SSH 访问通过 CloudFormation 堆栈部署的 EC2 实例。

1. 重新部署 CloudFormation 堆栈，确保自动回滚已禁用。
2. 通过 SSH 访问当前运行有 Harvest 和 Grafana 客户端的 Amazon EC2 实例。

```
[~]$ ssh ec2-user@ec2_ip_address
```

3. 使用以下命令验证 Docker 容器是否已成功启动。

```
[ec2-user@ip-ec2_ip_address ~]$ sudo docker ps
```

在响应中，您应该会看到以下五个容器：

```
CONTAINER ID   IMAGE                    COMMAND                  CREATED
 STATUS                          PORTS                    NAMES
6b9b3f2085ef   rahulguptajss/harvest   "bin/poller --config…"   8 minutes ago
 Restarting (1) 20 seconds ago                            harvest_cluster-2
3cf3e3623fde   rahulguptajss/harvest   "bin/poller --config…"   8 minutes ago   Up
 About a minute                                           harvest_cluster-1
708f3b7ef6f8   grafana/grafana         "/run.sh"                8 minutes ago   Up
 8 minutes                   0.0.0.0:3000->3000/tcp   harvest_grafana
0febee61cab7   prom/alertmanager       "/bin/alertmanager -…"   8
 minutes ago   Up 8 minutes                    0.0.0.0:9093->9093/tcp
 harvest_prometheus_alertmanager
1706d8cd5a0c   prom/prometheus         "/bin/prometheus --c…"   8 minutes ago   Up
 8 minutes                   0.0.0.0:9090->9090/tcp   harvest_prometheus
```

4. 如果 Docker 容器未运行，按如下步骤检查 `/var/log/cloud-init-output.log` 文件中的故障。

```
[ec2-user@ip-ec2_ip_address ~]$ sudo cat /var/log/cloud-init-output.log
     PLAY [Manage Harvest]
 ************************************************************

TASK [Gathering Facts] *************************************************************
ok: [localhost]

TASK [Verify images] ***************************************************************
failed: [localhost] (item=prom/prometheus) => {"ansible_loop_var": "item",
 "changed": false, "item": "prom/prometheus",
"msg": "Error connecting: Error while fetching server API version: ('Connection
 aborted.', ConnectionResetError(104, 'Co
nnection reset by peer'))"}
```

```
failed: [localhost] (item=prom/alertmanager) => {"ansible_loop_var": "item",
 "changed": false, "item": "prom/alertmanage
r", "msg": "Error connecting: Error while fetching server API version: ('Connection
 aborted.', ConnectionResetError(104,
'Connection reset by peer'))"}
failed: [localhost] (item=rahulguptajss/harvest) => {"ansible_loop_var": "item",
 "changed": false, "item": "rahulguptajs
s/harvest", "msg": "Error connecting: Error while fetching server API version:
 ('Connection aborted.', ConnectionResetEr
ror(104, 'Connection reset by peer'))"}
failed: [localhost] (item=grafana/grafana) => {"ansible_loop_var": "item",
 "changed": false, "item": "grafana/grafana",
"msg": "Error connecting: Error while fetching server API version: ('Connection
 aborted.', ConnectionResetError(104, 'Co
nnection reset by peer'))"}

PLAY RECAP *********************************************************************
localhost                  : ok=1    changed=0    unreachable=0    failed=1
 skipped=0    rescued=0    ignored=0
```

5. 如果出现故障，请执行以下命令部署 Harvest 和 Grafana 容器。

```
[ec2-user@ip-ec2_ip_address ~]$ sudo su
     [ec2-user@ip-ec2_ip_address ~]$ cd /home/ec2-user/harvest_install
     [ec2-user@ip-ec2_ip_address ~]$ /usr/local/bin/ansible-playbook
 manage_harvest.yml
     [ec2-user@ip-ec2_ip_address ~]$ /usr/local/bin/ansible-playbook
 manage_harvest.yml --tags api
```

6. 通过运行 sudo docker ps 并连接至 Harvest 和 Grafana 网址来验证容器是否已成功启动。

FSx 使用监控 ONTAP API 调用 AWS CloudTrail

FSx Amazon 与 AWS CloudTrail一项服务集成，该服务可记录用户、角色或 AWS 服务在亚马逊中执行的操作 FSx。 CloudTrail 将所有亚马逊 FSx API 调用的 Amazon f NetApp o FSx r ONTAP 捕获为事件。捕获的调用包括来自亚马逊 FSx 控制台的调用以及对亚马逊 FSx API 操作的代码调用。

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，包括针对亚马逊的事件 FSx。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 Amazon 提出的请求 FSx。还可以确定发出请求的源 IP 地址、请求方、请求时间以及其他详细信息。

要了解更多信息 CloudTrail，请参阅AWS CloudTrail 用户指南。

中的亚马逊 FSx 信息 CloudTrail

CloudTrail 在您创建 AWS 账户时已在您的账户上启用。当 API 活动发生在 Amazon 中时 FSx，该活动会与其他 AWS 服务 CloudTrail 事件一起记录在事件历史记录中。您可以在自己的 AWS 账户中查看、搜索和下载最近发生的事件。有关更多信息，请参阅使用事件历史记录查看 CloudTrail 事件。

要持续记录您的 AWS 账户中的事件，包括亚马逊的事件 FSx，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。默认情况下，当您在控制台中创建跟踪时，该跟踪将应用于所有 AWS 区域。跟踪记录 AWS 分区中所有 AWS 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 AWS 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《AWS CloudTrail 用户指南》中的以下主题：

- 为您创建路线 AWS 账户
- AWS 与日志的服务集成 CloudTrail
- 配置 Amazon SNS 通知 CloudTrail
- 接收来自多个地区的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail日志文件

所有亚马逊 FSx API 调用都由记录 CloudTrail。例如，对`CreateFileSystem`和`TagResource`操作的调用会在 CloudTrail 日志文件中生成条目。

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：

- 请求是使用根证书还是 AWS Identity and Access Management (IAM) 用户凭证发出。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务发出。

有关更多信息，请参阅《CloudTrail 用户指南》中的 “用户身份”AWS CloudTrail 元素。

了解 Amazon FSx 日志文件条目

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 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 调用的有序堆栈跟踪，因此它们不会按任何特定的顺序出现。

以下示例显示了一个 CloudTrail 日志条目，该条目演示了从控制台为文件系统创建标签时的TagResource操作。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
        "principalId": “111122223333”,
        "arn": "arn:aws:sts::111122223333:root”,
        "accountId": “111122223333”,
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE”,
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-14T22:36:07Z"
            }
        }
    },
    "eventTime": "2018-11-14T22:36:07Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "TagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": “192.0.2.0”,
    "userAgent": “console.amazonaws.com”,
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789”
    },
    "responseElements": null,
    "requestID": “aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51”,
    "eventID": “bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p”,
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": “111122223333”
}
```

以下示例显示了一个 CloudTrail 日志条目，该条目演示了从控制台中删除文件系统的标签时的UntagResource操作。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
```

```
        "principalId": "111122223333",
        "arn": "arn:aws:sts::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-14T23:40:54Z"
            }
        }
    },
    "eventTime": "2018-11-14T23:40:54Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "UntagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789"
    },
    "responseElements": null,
    "requestID": "aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51",
    "eventID": "bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p",
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": "111122223333"
}
```

在 FSx ONTAP 中使用微软 Active Directory

亚马逊 FSx 与微软 Active Directory 合作，与您的现有环境集成。Active Directory 是 Microsoft 目录服务，用于存储有关网络上对象的信息，并帮助管理员和用户查找和使用这些信息。这些对象通常包括共享资源，例如文件服务器以及网络用户和计算机账户。

您可以选择将 FSx 适用于 ONTAP 的存储虚拟机 (SVMs) 加入您的 Active Directory 域，以提供用户身份验证以及文件和文件夹级别的访问控制。然后，服务器消息块（SMB）客户端可以使用其在 Active Directory 中的现有用户身份自行进行身份验证并访问 SVM 卷。您的用户可以使用其现有身份来控制对单个文件和文件夹的访问。此外，您 FSx 无需进行任何修改即可将现有文件和文件夹及其安全访问控制列表 (ACL) 配置迁移到 Amazon。

如果 Microsoft Active Directory 域基础设施不可用，则可在 SVM 的工作组中配置服务器消息块（SMB）服务器，作为将 SVM 加入 Microsoft Active Directory 的替代方案。有关更多信息，请参阅在工作组中设置 SMB 服务器。

当你将 Amazon FSx for NetApp ONTAP 加入活动目录时，即独立地 SVMs 将文件系统加入活动目录。这意味着您可以拥有一个文件系统，其中一些已加入活动目录 SVMs ，而另 SVMs 一些则未加入 Active Directory。

将 SVM 加入 Active Directory 后，您可以更新以下 Active Directory 配置属性：

- DNS 服务器的 IP 地址
- 自行管理的 Active Directory 服务账户用户名和密码

主题

- 将 SVM 加入自行管理的 Microsoft AD 的先决条件
- 使用 Active Directory 的最佳实践
- 如何加入微软 Ac SVMs tive Directory
- 管理 SVM Active Directory 配置

将 SVM 加入自行管理的 Microsoft AD 的先决条件

在将 for FSx ONTAP SVM 加入自我管理的 Microsoft AD 域之前，请确保您的活动目录和网络符合以下各节中描述的要求。

主题

本地 Active Directory 要求

确保您已经有一个本地或其他自行管理的 Microsoft AD，可以在其中加入 SVM。此 Active Directory 应具有以下配置：

- Active Directory 域控制器的域功能级别为 Windows Server 2000 或更高版本。
- Active Directory 使用的域名不是单标签域（SLD）格式。Amazon FSx 不支持 SLD 域名。
- 如果您定义了 Active Directory 站点，请确保在 VPC 中与您的 for ONTAP 文件系统关联的子网是在相同的 Active Directory 站点中定义的，并且您 FSx 的 VPC 子网与 Active Directory 站点上的子网之间不存在冲突。

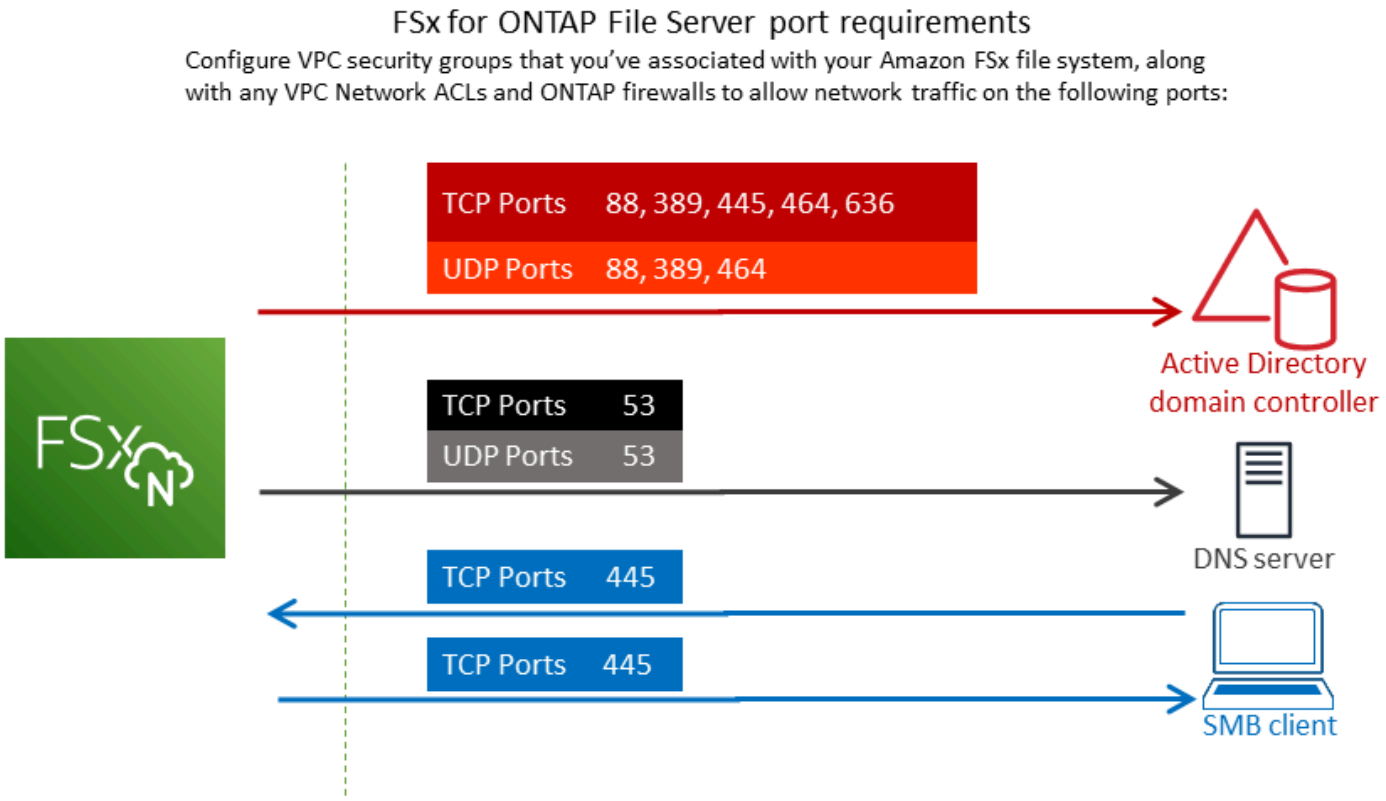
> **Note**
>
> 如果您使用的是 Directory Service，f FSx or ONTAP 不支持 SVMs 加入简单活动目录。

网络配置要求

确保您进行了以下网络配置并具有相关信息。

> **Important**
>
> 要让 SVM 加入 Active Directory，你需要确保本主题中记录的端口允许所有 Active Directory 域控制器与 SVM 上的两个 iSCSI IP 地址（iscsi_1 和 iscsi_2 逻辑接口 ()）之间的流量。LIFs

- DNS 服务器和 Active Directory 域控制器的 IP 地址。
- 使用 Direct Connect、Site-to-Site VPN 或 AWS Transit Gateway 在创建文件系统的 Amazon VPC 与自行管理的 Active Directory 之间建立了连接。
- 您要在其上创建文件系统的子网的安全组和 VPC 网络 ACLs 必须允许端口上的流量，其方向如下图所示。



下表说明了每个端口的作用。

协议	端口	角色
TCP/UDP	53	域名系统（DNS）
TCP/UDP	88	Kerberos 身份验证
TCP/UDP	389	轻型目录访问协议（LDAP）
TCP	445	目录服务 SMB 文件共享
TCP/UDP	464	更改/设置密码
TCP	636	轻量级目录访问协议 TLS/SSL (LDAPS)

- 这些流量规则还应镜像到适用于每个 Active Directory 域控制器、DNS 服务器、 FSx 客户端和管理员的防火墙上。 FSx

> **Important**
>
> 虽然 Amazon VPC 安全组要求仅在网络流量启动的方向上打开端口，但大多数 Windows 防火墙和 VPC 网络都 ACLs 要求双向打开端口。

Active Directory 服务账户要求

确保您在自行管理的 Microsoft AD 中有一个服务账户，该账户具有将计算机加入该域的委派权限。服务账户是自行管理的 Active Directory 中的一个用户账户，该账户已被委派某些任务。

在要加入 SVM 的 OU 中，必须至少为服务账户委派了以下权限：

- 能够重置密码
- 能够限制账户读取和写入数据
- 能够在计算机对象上设置 `msDS-SupportedEncryptionTypes` 属性
- 验证写入 DNS 主机名的能力
- 验证写入服务主体名称的能力
- 能够创建和删除计算机对象
- 经过验证的读取和写入账户限制的能力

这些权限代表将计算机对象加入到您的 Active Directory 至少需要具备的一组权限。有关更多信息，请参阅 Windows Server 文档主题 Error: Access is denied when non-administrator users who have been delegated control try to join computers to a domain controller。

您可以将您的 Active Directory 服务账户凭证存储在 AWS Secrets Manager （推荐）中，并向亚马逊 FSx 提供加入 Active Directory 的秘密 ARN，也可以提供纯文本凭证。

要了解有关创建具有正确权限的服务账户的更多信息，请参阅向您的 Amazon FSx 服务账户委派权限。

> **Important**
>
> 亚马逊 FSx 要求在您的亚马逊 FSx 文件系统的整个生命周期内都有一个有效的服务账户。Amazon FSx 必须能够全面管理文件系统并执行要求其取消加入并重新加入您的 Active Directory 域的资源。这些任务包括更换出现故障的文件系统或 SVM，或者修补 NetApp

ONTAP 软件。在 Amazon 上更新您的 Active Directory 配置信息 FSx，包括服务账户凭证。要了解更多信息，请参阅使用 Amazon 更新您的活动目录配置 FSx。

如果这是您首次使用 AWS 和 FSx ONTAP，请确保在开始 Active Directory 集成之前完成初始设置步骤。有关更多信息，请参阅 设置 FSx for ONTAP。

Important

请勿在 FSx 创建组织单位后移动 Amazon 在 OU 中创建的计算机对象， SVMs 也不要在您的 SVM 已加入 Active Directory 时将其删除。这样做会 SVMs 导致您的配置错误。

使用 Active Directory 的最佳实践

以下是加入 Amazon FSx for NetApp ONTAP SVMs 加入自我管理的 Microsoft Active Directory 时应考虑的一些建议和指南。请注意，这些建议和指南是最佳实践，不是硬性要求。

主题

- 向您的 Amazon FSx 服务账户委派权限
- 使用 Amazon 更新您的活动目录配置 FSx
- 使用安全组限制 VPC 内的流量
- 为文件系统的网络接口创建出站安全组规则
- 使用存储活动目录凭证 AWS Secrets Manager

向您的 Amazon FSx 服务账户委派权限

请务必将您提供给 Amazon 的服务账户配置 FSx 为所需的最低权限。此外，将组织单元（OU）与其他域控制器问题分开。

要将 Amazon FSx SVMs 加入您的域名，请确保服务账户拥有委托权限。域管理员组的成员有足够的权限来执行此任务。但是，作为最佳实践，请使用仅具有此任务的最低执行权限的服务账户。以下过程演示如何仅将加入 FSx ONTAP 所需的权限委托 SVMs 给您的域。

您必须在已加入目录且已安装 Active Directory User and Computers MMC 管理单元的计算机上执行此过程。

为 Microsoft Active Directory 域创建服务账户

1. 确保您以 Microsoft Active Directory 域的域管理员身份登录。
2. 打开 Active Directory User and Computers MMC 管理单元。
3. 在任务窗格中，展开域节点。
4. 找到并打开您要修改的 OU 的上下文（右键单击）菜单，然后选择委派控制。
5. 在委派控制向导页面上，选择下一步。
6. 选择添加，在选定的用户和组中添加特定用户或特定组，然后选择下一步。
7. 在要委派的任务页面上，选择创建要委派的自定义任务，然后选择下一步。
8. 选择仅文件夹中的以下对象，然后选择计算机对象。
9. 选择在此文件夹中创建选定对象和删除此文件夹中的选定对象。然后选择下一步。
10. 在显示这些权限 下，确保选中常规和特定于属性。
11. 在权限中，请选择以下选项：
    - 重置密码
    - 读取和写入账户限制
    - 已验证写入 DNS 主机名
    - 已验证写入服务主体名称
    - 写下 MSD-SupportedEncryptionTypes
12. 选择下一步，然后选择完成。
13. 关闭 Active Directory User and Computers MMC 管理单元。

> **Important**
>
> FSx 创建计算机对象后，请勿移动 Amazon 在 OU 中创建 SVMs 的计算机对象。这样做会 SVMs 导致您的配置错误。

使用 Amazon 更新您的活动目录配置 FSx

要使您的 Amazon 不间断地使用 FSx SVMs，请在更改自我管理 AD 设置时更新 SVM 的自我管理活动目录 (AD) 配置。

例如，假设您的 AD 使用基于时间的密码重置策略。在这种情况下，密码重置后，请务必使用Amazon 更新服务账户密码 FSx。为此，请使用亚马逊 FSx 控制台、亚马逊 FSx API 或 AWS CLI。同样，如果您的 Active Directory 域的 DNS 服务器 IP 地址发生变化，则一旦发生更改，请立即使用 Amazon 更新 DNS 服务器 IP 地址 FSx。

如果更新的自行管理 AD 配置存在问题，则 SVM 状态会切换为错误配置。在此状态下，控制台、API 和 CLI 中的 SVM 描述旁边会显示错误消息和推荐操作。如果您的 SVM 的 AD 配置存在问题，请务必对配置属性采取推荐的纠正操作。如果问题得到解决，请验证 SVM 的状态是否更改为已创建。

有关更多信息，请参阅使用 AWS 管理控制台、 AWS CLI和 API 更新现有 SVM Active Directory 配置和使用 ONTAP CLI 修改 Active Directory 配置。

使用安全组限制 VPC 内的流量

要限制虚拟私有云（VPC）内的网络流量，您可以在 VPC 中实施最低权限原则。换言之，您可以将权限限制为所需的最低权限。为此，请使用安全组规则。要了解更多信息，请参阅Amazon VPC 安全组。

为文件系统的网络接口创建出站安全组规则

为提高安全性，请考虑使用出站流量规则来配置安全组。这些规则应仅允许出站流量流向自行管理的 AD 域控制器或子网或安全组内部。将此安全组应用于与您的亚马逊 FSx 文件系统的 elastic network interface 关联的 VPC。要了解更多信息，请参阅使用 Amazon VPC 进行文件系统访问控制。

使用存储活动目录凭证 AWS Secrets Manager

你可以使用 AWS Secrets Manager 安全地存储和管理你的 Microsoft Active Directory 域加入服务帐户凭据。此方法无需在应用程序代码或配置文件中以明文形式存储敏感凭证，从而增强您的安全状况。

您还可以配置 IAM 策略，以管理对密钥的访问权限，并为密码设置自动轮换策略。

将活动目录凭据存储在 AWS Secrets Manager （控制台）

步骤 1：创建 KMS 密钥

创建 KMS 密钥，以在 Secrets Manager 中对 Active Directory 凭证进行加密和解密。

创建密钥

> **Note**
>
> 对于加密密钥，请创建新密钥，不要使用 AWS 默认 KMS 密钥。请务必 AWS KMS key 在包含要加入 Active Directory 的 SVM 的同一个区域中创建。

1. 在 https://console.aws.amazon.com /km AWS KMS s 处打开控制台
2. 选择创建密钥。
3. 对于密钥类型，选择对称。
4. 对于密钥用法，选择加密和解密。
5. 对于高级选项，执行以下操作：
   a. 对于密钥材料源，选择 KMS。
   b. 对于区域性，选择单区域密钥，然后选择下一步。
6. 选择下一步。
7. 对于别名，提供 KMS 密钥的名称。
8. （可选）对于描述，提供 KMS 密钥的描述。
9. （可选）对于标签，提供 KMS 密钥的标签，然后选择下一步。
10. （可选）对于密钥管理员，提供获授权管理此密钥的 IAM 用户和角色。
11. 对于密钥删除，确保选中允许密钥管理员删除此密钥复选框，然后选择下一步。
12. （可选）对于密钥用户，提供获授权在加密操作中使用此密钥的 IAM 用户和角色。选择下一步。
13. 对于密钥策略，选择编辑并在政策声明中包含以下内容以允许 Amazon FSx 使用 KMS 密钥，然后选择下一步。请务必将替换*us-west-2*为文件系统的部署 AWS 区域 位置和您*123456789012*的 AWS 账户 ID。

```
{
    "Sid": "Allow FSx to use the KMS key",
    "Version": "2012-10-17",
    "Effect": "Allow",
    "Principal": {
        "Service": "fsx.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
```

```
            "kms:DescribeKey"
        ],
        "Resource": "arn:aws:kms:us-west-2:123456789012:key/*",
        "Condition": {
            "StringEquals": {
                "kms:ViaService": "secretsmanager.us-west-2.amazonaws.com",
                "aws:SourceAccount": "123456789012"
            },
            "ArnLike": {
                "aws:SourceArn": [
                    "arn:aws:fsx:us-west-2:123456789012:file-system/*",
                    "arn:aws:fsx:us-west-2:123456789012:storage-virtual-machine/fs-*/
svm-*"
                ]
            }
        }
}
```

14. 选择结束。

> **Note**
>
> 通过修改 Resource 和 aws:SourceArn 字段，您可以设置更精细的访问控制，以针对特定的密钥和文件系统。

第 2 步：创建 AWS Secrets Manager 密钥

创建密钥

1. 打开 Secrets Manager 控制台，网址为https://console.aws.amazon.com/secretsmanager/。
2. 选择存储新密钥。
3. 对于密钥类型，请选择其他密钥类型。
4. 对于键/值对，请执行以下操作以添加您的两个密钥：
   a. 对于第一个密钥，请输入 CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME。
   b. 对于第一个密钥的值，请仅输入 AD 用户的用户名（不带域前缀）。
   c. 对于第二个密钥，请输入 CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD。
   d. 对于第二个密钥的值，请输入您在域中为 AD 用户创建的密码。

5. 对于加密密钥，输入上一步所创建 KMS 密钥的 ARN，然后选择下一步。
6. 在密钥名称中，输入一个描述性名称，以便您稍后查找自己的密钥。
7. （可选）对于描述，输入密钥名称的描述。
8. 对于资源权限，选择编辑。

   在权限策略中添加以下策略以允许 Amazon FSx 使用该密钥，然后选择 Next。请务必将替换*us-west-2*为文件系统的部署 AWS 区域 位置和您*123456789012*的 AWS 账户 ID。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "fsx.amazonaws.com"
            },
            "Action": [
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret"
            ],
            "Resource": "arn:aws:secretsmanager:us-west-2:123456789012:secret:*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012"
                },
                "ArnLike": {
                    "aws:SourceArn": [
                        "arn:aws:fsx:us-west-2:123456789012:file-system/*",
                        "arn:aws:fsx:us-west-2:123456789012:storage-virtual-
machine/fs-*/svm-*"
                    ]
                }
            }
        }
    ]
}
```

9. （可选）您可以将 Secrets Manager 配置为自动轮换凭证。选择下一步。
10. 选择结束。

将活动目录凭据存储在 AWS Secrets Manager (CLI)

步骤 1：创建 KMS 密钥

创建 KMS 密钥，以在 Secrets Manager 中对 Active Directory 凭证进行加密和解密。

要创建 KMS 密钥，请使用 AWS CLI 命令创建密钥。

在此命令中，设置 `--policy` 参数，以指定定义 KMS 密钥权限的密钥策略。该策略必须包含以下内容：

- Amazon 的服务主体 FSx，即`fsx.amazonaws.com`。
- 所需的 KMS 操作：`kms:Decrypt` 和 `kms:DescribeKey`。
- 您的 AWS 区域 和账户的资源 ARN 模式。
- 限制密钥使用的条件键：
  - `kms:ViaService`，以确保请求通过 Secrets Manager 发出。
  - `aws:SourceAccount`，以限制您的账户。
  - `aws:SourceArn`仅限于特定的 Amazon FSx 文件系统。

以下示例创建了一个对称加密 KMS 密钥，其策略允许 Amazon FSx 使用该密钥进行解密和密钥描述操作。该命令会自动检索您的 AWS 账户 ID 和区域，然后使用这些值配置密钥策略，以确保亚马逊 FSx、Secrets Manager 和 KMS 密钥之间进行适当的访问控制。确保您的 AWS CLI 环境与将加入 Active Directory 的 SVM 位于同一区域。

```
# Set region and get Account ID
REGION=${AWS_REGION:-$(aws configure get region)}
ACCOUNT_ID=$(aws sts get-caller-identity --query 'Account' --output text)

# Create Key
KMS_KEY_ARN=$(aws kms create-key --policy "{
  \"Version\": \"2012-10-17\",
  \"Statement\": [
    {
      \"Sid\": \"Enable IAM User Permissions\",
      \"Effect\": \"Allow\",
      \"Principal\": {
        \"AWS\": \"arn:aws:iam::$ACCOUNT_ID:root\"
      },
      \"Action\": \"kms:*\",
      \"Resource\": \"*\"
```

```
    },
    {
      \"Sid\": \"Allow FSx to use the KMS key\",
      \"Effect\": \"Allow\",
      \"Principal\": {
        \"Service\": \"fsx.amazonaws.com\"
      },
      \"Action\": [
        \"kms:Decrypt\",
        \"kms:DescribeKey\"
      ],
      \"Resource\": \"*\",
      \"Condition\": {
        \"StringEquals\": {
          \"kms:ViaService\": \"secretsmanager.$REGION.amazonaws.com\",
          \"aws:SourceAccount\": \"$ACCOUNT_ID\"
        },
        \"ArnLike\": {
          \"aws:SourceArn\": [
            \"arn:aws:fsx:$REGION:$ACCOUNT_ID:file-system/*\",
            \"arn:aws:fsx:$REGION:$ACCOUNT_ID:storage-virtual-machine/fs-*/svm-*\"]
        }
      }
    }
  ]
}" --query 'KeyMetadata.Arn' --output text)

echo "KMS Key ARN: $KMS_KEY_ARN"
```

> **Note**
>
> 通过修改 Resource 和 aws:SourceArn 字段，您可以设置更精细的访问控制，以针对特定的密钥和文件系统。

第 2 步：创建 AWS Secrets Manager 密钥

要为亚马逊 FSx 创建用于访问您的活动目录的密钥，请使用 c reate-secre AWS CLI t 命令并设置以下参数：

- --name：密钥的标识符。
- --description：密钥用途的描述。

- `--kms-key-id`：您在步骤 1 中创建的 KMS 密钥 ARN，用于加密静态密钥。
- `--secret-string`：包含 AD 凭证的 JSON 字符串，格式如下：
  - `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME`：不带域前缀的 AD 服务账户用户名，例如 `svc-fsx`。请勿提供域前缀，例如 `CORP\svc-fsx`。
  - `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD`：AD 服务账户密码
- `--region`：您的 SVM 将在 AWS 区域 何处创建。如果 `AWS_REGION`未设置，则默认为您配置的区域。

创建密钥后，使用put-resource-policy命令附加资源策略，并设置以下参数：

- `--secret-id`：要附加策略的密钥的名称或 ARN。以下示例使用 **`FSxSecret`** 作为 `--secret-id`。
- `--region`: 和你的秘密 AWS 区域 一样。
- `--resource-policy`：授予亚马逊访问密钥 FSx 权限的 JSON 政策文档。该策略必须包含以下内容：
  - Amazon 的服务主体 FSx，即**`fsx.amazonaws.com`**。
  - 所需的 Secrets Manager 操作：`secretsmanager:GetSecretValue` 和 `secretsmanager:DescribeSecret`。
  - 您的 AWS 区域 和账户的资源 ARN 模式。
  - 以下限制访问的条件键：
    - `aws:SourceAccount`，以限制您的账户。
    - `aws:SourceArn`仅限于特定的 Amazon FSx 文件系统。

以下示例创建了一个具有所需格式的密钥，并附加了允许 Amazon FSx 使用该密钥的资源策略。此示例会自动检索您的 AWS 账户 ID 和区域，然后使用这些值配置资源策略，以确保在 Amazon FSx 和密钥之间进行适当的访问控制。

确保使用您在步骤 1 中所创建密钥的 ARN 替换 `KMS_KEY_ARN`，并使用 Active Directory 服务账户凭证替换 `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME` 和 `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD`。此外，请验证您的 AWS CLI 环境是否配置为与将加入 Active Directory 的 SVM 相同的区域。

```
# Set region and get account ID
REGION=${AWS_REGION:-$(aws configure get region)}
ACCOUNT_ID=$(aws sts get-caller-identity --query 'Account' --output text)
```

```
# Replace with your KMS key ARN from Step 1
KMS_KEY_ARN="arn:aws:kms:us-east-2:123456789012:key/1234542f-d114-555b-9ade-
fec3c9200d8e"

# Replace with your Active Directory credentials
AD_USERNAME="Your_Username"
AD_PASSWORD="Your_Password"

# Create the secret
SECRET_ARN=$(aws secretsmanager create-secret \
  --name "FSxSecret" \
  --description "Secret for FSx access" \
  --kms-key-id "$KMS_KEY_ARN" \
  --secret-string "{\"CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME\":\"$AD_USERNAME\",
\"CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD\":\"$AD_PASSWORD\"}" \
  --region "$REGION" \
  --query 'ARN' \
  --output text)

echo "Secret created with ARN: $SECRET_ARN"

# Attach the resource policy with proper formatting
aws secretsmanager put-resource-policy \
  --secret-id "FSxSecret" \
  --region "$REGION" \
  --resource-policy "{
    \"Version\": \"2012-10-17\",
    \"Statement\": [
      {
        \"Effect\": \"Allow\",
        \"Principal\": {
          \"Service\": \"fsx.amazonaws.com\"
        },
        \"Action\": [
          \"secretsmanager:GetSecretValue\",
          \"secretsmanager:DescribeSecret\"
        ],
        \"Resource\": \"$SECRET_ARN\",
        \"Condition\": {
          \"StringEquals\": {
            \"aws:SourceAccount\": \"$ACCOUNT_ID\"
          },
          \"ArnLike\": {
```

```
            \"aws:SourceArn\": [
              \"arn:aws:fsx:$REGION:$ACCOUNT_ID:file-system/*\",
              \"arn:aws:fsx:$REGION:$ACCOUNT_ID:storage-virtual-machine/fs-*/svm-*\"]
          }
        }
      }
    ]
  }"

echo "Resource policy attached successfully"
```

> **Note**
>
> 通过修改 `Resource` 和 `aws:SourceArn` 字段，您可以设置更精细的访问控制，以针对特定的密钥和文件系统。

如何加入微软 Ac SVMs tive Directory

您的组织可能会使用 Active Directory 管理身份和设备，而无论是在本地还是在云中。使用 f FSx or ONTAP，您可以通过以下方式 SVMs 直接加入现有的 Active Directory 域：

- 新用户 SVMs 在创建活动目录时加入活动目录：
  - 使用亚马逊 FSx 控制台中的标准创建选项为 ONTAP 文件系统创建新 FSx 的，您可以将默认 SVM 加入自我管理的 Active Directory。有关更多信息，请参阅 创建文件系统（控制台）。
  - 使用亚马逊 FSx 控制台或 Amazon FSx API 在现有的 ONTAP 文件系统上创建新 FSx 的 SVM。AWS CLI有关更多信息，请参阅 创建存储虚拟机（SVM）。
- SVMs 加入现有活动目录：
  - 使用 AWS 管理控制台 AWS CLI、和 API 将 SVM 加入 Active Directory，如果首次尝试加入失败，则使用、和 API 重新尝试将 SVM 加入 Active Directory。您还可以更新已加入活动目录 SVMs 的某些活动目录配置属性。有关更多信息，请参阅 管理 SVM Active Directory 配置。
  - 使用 NetApp ONTAP CLI 或 REST API 加入、重新尝试加入和取消加入 SVM Active Directory 配置。有关更多信息，请参阅 使用 CLI 更新 SVM 活动目录配置 NetApp。

> **Important**
>
> - FSx 只有当你使用微软 DNS 作为默认 DNS 服务时，亚马逊才会为 SVM 注册 DNS 记录。如果您使用第三方 DNS，则必须在创建 Amazon FSx SVMs 之后手动设置 DNS 条目。
> - 如果使用 AWS Managed Microsoft AD，则必须指定一个群组，例如 AWS 委派 FSx 管理员、 AWS 委派管理员或对 OU 具有委派权限的自定义群组。

当您将 FSx 适用于 ONTAP 的 SVM 直接加入自我管理的 Active Directory 时，SVM 与您的用户和现有资源（包括现有文件服务器）位于同一 Active Directory 林（包含域、用户和计算机的 Active Directory 配置中最顶层的逻辑容器）中，并且位于同一个 Active Directory 域中。

将 SVM 加入 Active Directory 时所需的信息

无论选择哪种 API 操作，在将 SVM 加入 Active Directory 时，您都必须提供有关 Active Directory 的以下信息：

- 为 SVM 创建的 Active Directory 计算机对象的 NetBIOS 名称。这是 Active Directory 中 SVM 的名称，其在 Active Directory 中必须唯一。不要使用主域的 NetBIOS 名称。NetBIOS 名称不能超过 15 个字符。
- Active Directory 域的完全限定域名（FQDN）。FQDN 不能超过 255 个字符。

  > **Note**
  >
  > FQDN 不能采用单标签域（SLD）格式。Amazon FSx 不支持 SLD 域名。

- 域的 DNS 服务器或域主机的 IP 地址（最多三个）。

  DNS 服务器 IP 地址和 Active Directory 域控制器 IP 地址可以在任何 IP 地址范围内，但以下地址除外：

  - 与相应 AWS 区域中 Amazon Web Services 拥有的 IP 地址冲突的 IP 地址。有关按地区划分 AWS 的 IP 地址列表，请参阅 AWS IP 地址范围。
  - 以下 CIDR 数据块范围内的 IP 地址：198.19.0.0/16
- Amazon 用于将 SVM 加入您的域的 A FSx ctive Directory 服务账户的证书。可通过以下任一方式提供这些凭证：
  - 选项 1： AWS Secrets Manager 秘密 ARN-包含您的 Active Directory 域上服务帐户的用户名和密码的密钥。有关更多信息，请参阅 使用存储活动目录凭证 AWS Secrets Manager。

- 选项 2：纯文本凭证
  - 服务账户用户名：现有 Microsoft Active Directory 中服务账户的用户名。请勿包含域前缀或后缀。例如，对于 `EXAMPLE\ADMIN`，仅使用 `ADMIN`。
  - 服务账户密码 – 服务账户的密码。
- （可选）域中 SVM 所加入的组织单元（OU）。

> **Note**
>
> 如果您将 SVM 加入 Act AWS Directory Service ive Directory，则必须提供一个 OU，该组织单元位于为相关的目录对象 Directory Service 创建的默认 OU 中。 AWS这是因为 Directory Service 不提供对您的 Active Directory 默认 `Computers` OU 的访问权限。例如，如果您的 Active Directory 域是 `example.com`，则可以指定以下 OU：`OU=Computers,OU=example,DC=example,DC=com`。

- （可选）您要将授权委派给的域组，使其对文件系统执行管理操作。例如，此域组可以管理 Windows SMB 文件共享、获取文件和文件夹的所有权等。如果您未指定此组，则默认情况下，亚马逊 FSx 会将此权限委托给您的 Active Directory 域中的域管理员组。

管理 SVM Active Directory 配置

本节介绍如何使用 AWS 管理控制台、 AWS CLI、 FSx API 和 ONTAP CLI 来执行以下操作：

- 将现有 SVM 加入 Active Directory
- 修改现有的 SVM 活动目录配置
- SVMs 从活动目录中删除

要从 Active Directory 中删除 SVM，必须使用 NetApp ONTAP CLI。

主题

使用 AWS 管理控制台、 AWS CLI 和 API 加入 SVMs 活动目录

可以使用以下过程将现有 SVM 加入 Active Directory。在此过程中，SVM 还没有加入 Active Directory。

将 SVM 加入 Active Directory（AWS 管理控制台）

1. 打开亚马逊 FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 选择要加入活动目录的 SVM：
   - 在左侧导航窗格中，选择文件系统，然后选择包含要更新的 SVM 的 ONTAP 文件系统。
   - 选择存储虚拟机选项卡。

     –或–
   - 要显示所有可用虚拟机的列表 SVMs，请在左侧导航窗格中展开 ONTAP，然后选择存储虚拟机。中将显示您的账户 SVMs 中所有内容 AWS 区域 的列表。

   从列表中选择要加入 Active Directory 的 SVM。
3. 在 SVM 摘要面板的右上角，选择操作 > 加入/更新 Active Directory。此时显示将 SVM 加入 Active Directory 窗口。
4. 输入要将 SVM 加入其中的 Active Directory 的以下信息：
   - 为 SVM 创建的 Active Directory 计算机对象的 NetBIOS 名称。这是 Active Directory 中 SVM 的名称，其在 Active Directory 中必须唯一。不要使用主域的 NetBIOS 名称。NetBIOS 名称不能超过 15 个字符。
   - Active Directory 域的完全限定域名（FQDN）。域名不能超过 255 个字符。
   - DNS 服务器 IP 地址-您的域名的 DNS 服务器的 IPv4 或 IPv6 地址。
   - 服务账户凭证：选择如何提供服务账户凭证：
     - 选项 1： AWS Secrets Manager 秘密 ARN-包含您的 Active Directory 域上服务帐户的用户名和密码的密钥。有关更多信息，请参阅 使用存储活动目录凭证 AWS Secrets Manager。
     - 选项 2：纯文本凭证
       - 服务账户用户名：现有 Microsoft Active Directory 中服务账户的用户名。请勿包含域前缀或后缀。例如，对于 `EXAMPLE\ADMIN`，仅使用 `ADMIN`。
       - 服务账户密码 – 服务账户的密码。
       - 确认密码 – 服务账户的密码。

- 在 Secrets Manager 中管理（默认）：提供包含服务账户凭证的 Secrets Manager 密钥的 ARN。密钥必须包含键值对 CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME 和 CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD。
- （可选）组织单元（OU）：要将 SVM 加入到的组织单元的可分辨路径名称。
- 委托文件系统管理员组 – Active Directory 中可以管理您的文件系统的组的名称。

  如果您正在使用 AWS Managed Microsoft AD，则必须指定一个群组，例如 AWS 委派 FSx管理员、 AWS 授权管理员或具有向 OU 委派权限的自定义群组。

  如果您要加入自行管理的活动目录，请在活动目录中使用该组的名称。默认组为 Domain Admins。

5. 选择加入 Active Directory，使用您提供的配置将 SVM 加入 Active Directory。

将 SVM 加入活动目录 (AWS CLI)

- 要将 fo FSx r ONTAP SVM 加入活动目录，请使用 CL update-storage-virtual-machineI 命令（或等效UpdateStorageVirtualMachine的 API 操作），如以下示例所示。

```
aws fsx update-storage-virtual-machine \
  --storage-virtual-machine-id svm-abcdef0123456789a\
  --active-directory-configuration
 SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
    OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",
\
    FileSystemAdministratorsGroup="FSxAdmins",UserName="FSxService",\
    Password="password", \
    DnsIps=["10.0.1.18"]}',NetBiosName=amznfsx12345
```

成功创建存储虚拟机后，Amazon 以 JSON 格式 FSx 返回其描述，如以下示例所示。

```
{
  "StorageVirtualMachine": {
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
```

```
        ],
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.7", "198.19.0.8"]
      }
    },
    "FileSystemId": "fs-0123456789abcdef0",
    "Lifecycle": "CREATED",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/
fs-0123456789abcdef0/svm-abcdef0123456789a",
    "StorageVirtualMachineId": "svm-abcdef0123456789a",
    "Subtype": "default",
    "Tags": [],

  }
}
```

使用 AWS 管理控制台、 AWS CLI和 API 更新现有 SVM Active Directory 配置

可以使用以下过程更新已加入 Active Directory 的 SVM 的 Active Directory 配置。

更新 SVM Active Directory 配置（AWS 管理控制台）

1. 打开亚马逊 FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 按如下所示方法选择要更新的 SVM：

   - 在左侧导航窗格中，选择文件系统，然后选择包含要更新的 SVM 的 ONTAP 文件系统。
   - 选择存储虚拟机选项卡。

   –或–

   - 要显示所有 SVMs 可用虚拟机的列表，请在左侧导航窗格中展开 ONTAP，然后选择存储虚拟机。

   从列表中选择要更新的 SVM。
3. 在 SVM 摘要面板上，选择操作 > 加入/更新 Active Directory。此时将显示更新 SVM Active Directory 配置窗口。
4. 可以在此窗口中更新以下 Active Directory 配置属性。

   - DNS 服务器 IP 地址-您的域名的 DNS 服务器的 IPv4 或 IPv6 地址。
   - 服务账户凭证：选择如何提供服务账户凭证：
     - 选项 1： AWS Secrets Manager 秘密 ARN-包含您的 Active Directory 域上服务帐户的用户名和密码的密钥。有关更多信息，请参阅 使用存储活动目录凭证 AWS Secrets Manager。
     - 选项 2：纯文本凭证
       - 服务账户用户名：现有 Microsoft Active Directory 中服务账户的用户名。请勿包含域前缀或后缀。例如，对于 `EXAMPLE\ADMIN`，仅使用 `ADMIN`。
       - 服务账户密码 – 服务账户的密码。
       - 确认密码 – 服务账户的密码。
5. 输入更新后，选择更新 Active Directory 进行更改。

可以使用以下过程更新已加入 Active Directory 的 SVM 的 Active Directory 配置。

更新 SVM Active Directory 配置（AWS CLI）

- 要使用 AWS CLI 或 API 更新 SVM 的 Active Directory 配置，请使用 update-storage-virtual-machineCLI 命令（或等效UpdateStorageVirtualMachine的 API 操作），如以下示例所示。

```
aws fsx update-storage-virtual-machine \
    --storage-virtual-machine-id svm-abcdef0123456789a\
    --active-directory-configuration \
    SelfManagedActiveDirectoryConfiguration='{UserName="FSxService",\
    Password="password", \
    DnsIps=["10.0.1.18"]}'
```

使用 CLI 更新 SVM 活动目录配置 NetApp

您可以使用 NetApp ONTAP CLI 将您的 SVM 加入和取消加入活动目录，也可以修改现有 SVM 活动目录配置。

使用 ONTAP API 将 SVM 加入 Active Directory

您可以使用 ONTAP CLI SVMs 将现有目录加入活动目录，如以下过程所述。即使 SVM 已经加入 Active Directory，也可以执行此过程。

1. 要访问 ONTAP CLI，请运行以下命令在 Amazon FSx for NetApp ONTAP 文件系统或 SVM 的管理端口上建立 SSH 会话。将 *management_endpoint_ip* 替换为文件系统管理端口的 IP 地址。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   有关更多信息，请参阅 使用 ONTAP CLI 管理文件系统。
2. 通过提供完整的目录 DNS 名称（`corp.example.com`）和至少一个 DNS 服务器 IP 地址，为 Active Directory 创建 DNS 条目。

   ```
   ::>vserver services name-service dns create -vserver svm_name -
   domains corp.example.com -name-servers dns_ip_1, dns_ip_2
   ```

   要验证与 DNS 服务器的连接，请运行以下命令。*svm_name*用您自己的信息替换。

   ```
   FsxId0ae30e5b7f1a50b6a::>vserver services name-service dns check -vserver svm_name

                                Name Server
   ```

```
Vserver       Name Server     Status       Status Details
------------- --------------- ------------ --------------------------
svm_name      172.31.14.245   up           Response time (msec): 0
svm_name      172.31.25.207   up           Response time (msec): 1
2 entries were displayed.
```

3. 要将 SVM 加入 Active Directory，请运行以下命令。请注意，必须指定 Active Directory 中尚不存在的 computer_name，并为 -domain 提供目录 DNS 名称。对于-OU，输入您希望 SVM 加入的，以及 DC 格式的完整 DNS 名称。 OUs

```
::>vserver cifs create -vserver svm_name -cifs-server computer_name -
domain corp.example.com -OU OU=Computers,OU=example,DC=corp,DC=example,DC=com
```

要验证 Active Directory 连接的状态，请运行以下命令：

```
::>vserver cifs check -vserver svm_name

              Vserver : svm_name
                    Cifs NetBIOS Name : svm_netBIOS_name
                          Cifs Status : Running
                                 Site : Default-First-Site-Name
Node Name       DC Server Name  DC Server IP    Status   Status Details
--------------- --------------  --------------- ------   --------------
FsxId0ae30e5b7f1a50b6a-01
                corp.example.com
                                172.31.14.245   up       Response time (msec): 5
FsxId0ae30e5b7f1a50b6a-02
                corp.example.com
                                172.31.14.245   up       Response time (msec): 20
2 entries were displayed.
```

4. 如果此次加入后无法访问共享，请确定用于访问共享的账户是否具有权限。例如，如果您在托管 Active Directory 中使用默认Admin帐户（委 AWS 托管理员），则必须在 ONTAP 中运行以下命令。netbios_domain 与您的 Active Directory 的域名相对应（对于 corp.example.com，此处使用的 netbios_domain 是 example）。

```
FsxId0123456789a::>vserver cifs users-and-groups local-group add-members -vserver
 svm_name -group-name BUILTIN\Administrators -member-names netbios_domain\admin
```

使用 ONTAP CLI 修改 Active Directory 配置

可以使用 ONTAP CLI 修改现有 Active Directory 配置。

1. 要访问 ONTAP CLI，请运行以下命令在 Amazon FSx for NetApp ONTAP 文件系统或 SVM 的管理端口上建立 SSH 会话。将 *management_endpoint_ip* 替换为文件系统管理端口的 IP 地址。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   有关更多信息，请参阅 使用 ONTAP CLI 管理文件系统。
2. 运行以下命令，暂时关闭 SVM 的 CIFS 服务器：

   ```
   FsxId0123456789a::>vserver cifs modify -vserver svm_name -status-admin down
   ```
3. 如果需要修改 Active Directory 的 DNS 条目，请运行以下命令：

   ```
   ::>vserver services name-service dns modify -vserver svm_name -
   domains corp.example.com -name-servers dns_ip_1,dns_ip_2
   ```

   可以使用 `vserver services name-service dns check -vserver svm_name` 命令验证与 Active Directory 的 DNS 服务器的连接状态。

   ```
   ::>vserver services name-service dns check -vserver svm_name
                                Name Server
   Vserver       Name Server    Status       Status Details
   ------------- -------------- ------------ --------------------------
   svmciad       dns_ip_1       up           Response time (msec): 1
   svmciad       dns_ip_2       up           Response time (msec): 1
   2 entries were displayed.
   ```
4. 如果需要修改 Active Directory 配置本身，则可以使用以下命令更改现有字段，并替换以下项：

   - *computer_name*，如果你想修改 SVM 的 NetBIOS（计算机帐户）名称。
   - *domain_name*，如果你想修改域的名称。这应与本部分步骤 3 中所述的 DNS 域条目相对应（`corp.example.com`）。
   - `organizational_unit`，如果要修改 OU（`OU=Computers,OU=example,DC=corp,DC=example,DC=com`）。

   您需要重新输入用于将此设备加入 Active Directory 的 Active Directory 凭证。

```
::>vserver cifs modify -vserver svm_name -cifs-server computer_name -
domain domain_name -OU organizational_unit
```

可以使用 `vserver cifs check -vserver svm_name` 命令验证 Active Directory 连接的连接状态。

5. 完成 Active Directory 和 DNS 配置修改后，运行以下命令，恢复 CIFS 服务器：

```
::>vserver cifs modify -vserver svm_name -status-admin up
```

使用 ONTAP CLI 从 SVM 取消加入活动目录 NetApp

也可以按照以下步骤使用 NetApp ONTAP CLI 取消您的 SVM 与 Active Directory 的加入：

1. 要访问 ONTAP CLI，请运行以下命令在 Amazon FSx for NetApp ONTAP 文件系统或 SVM 的管理端口上建立 SSH 会话。将 *management_endpoint_ip* 替换为文件系统管理端口的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

有关更多信息，请参阅 使用 ONTAP CLI 管理文件系统。

2. 运行以下命令，删除将您的设备从 Active Directory 取消加入的 CIFS 服务器。要使 ONTAP 删除 SVM 的计算机账户，请提供最初用于将 SVM 加入 Active Directory 的凭证。

```
FsxId0123456789a::>vserver cifs modify -vserver svm_name -status-admin down
```

3. 如果需要修改 Active Directory 的 DNS 条目，请运行以下命令：

```
FsxId0123456789a::vserver cifs delete -vserver svm_name

In order to delete an Active Directory machine account for the CIFS server, you
 must supply the name and password of a Windows account with
sufficient privileges to remove computers from the "CORP.ADEXAMPLE.COM" domain.

Enter the user name: user_name

Enter the password:

Warning: There are one or more shares associated with this CIFS server
```

```
          Do you really want to delete this CIFS server and all its shares? {y|n}: y
```

4. 运行以下命令，删除 Active Directory 的 DNS 服务器：

```
::vserver services name-service dns delete -vserver svm_name
```

如果显示类似以下内容的警告（指明应将 dns 作为 ns-switch 删除），并且您不打算将此设备重新加入 Active Directory，则可以删除 ns-switch 条目。

```
Warning: "DNS" is present as one of the sources in one or more ns-switch databases
 but no valid DNS configuration was found for Vserver
         "svm_name". Remove "DNS" from ns-switch using the "vserver services name-
service ns-switch" command. Configuring "DNS" as a source
         in the ns-switch setting when there is no valid configuration can cause
 protocol access issues.
```

5. （可选）运行以下命令，删除 dns 的 ns-switch 条目。验证源顺序，然后删除 hosts 数据库的 dns 条目，即修改 sources，使其仅包含列出的其他源。在此示例中，唯一的其他源是 files。

```
::>vserver services name-service ns-switch show -vserver svm_name -database hosts

                    Vserver: svm_name
Name Service Switch Database: hosts
   Name Service Source Order: files, dns
```

```
::>vserver services name-service ns-switch modify -vserver svm_name -database hosts
 -sources files
```

6. （可选）删除 dns 条目，即修改数据库主机的 sources 以仅包含 files。

```
::>vserver services name-service ns-switch modify -vserver svm_name -database hosts
 -sources files
```

迁移到 Amazon f NetApp o FSx r ONTAP

以下各节提供有关如何将现有 NetApp ONTAP 文件系统迁移到 Amazon FSx for NetApp ONTAP 的信息。

> **Note**
>
> 如果您计划使用 `All` 分层策略将数据迁移至容量池层，请记住，文件元数据始终存储在 SSD 层上，且所有新用户数据都首先写入 SSD 层。当数据写入 SSD 层时，后台分层进程将开始将您的数据分层到容量池存储，但是分层进程非即时，并且会消耗网络资源。考虑到文件元数据（占用户数据大小的 3-7%），您需要调整 SSD 层的大小，作为用户数据的缓冲区，然后再将其分层到容量池存储。建议 SSD 层利用率不要超过 80%。
> 迁移数据时，请务必使用CloudWatch 文件系统指标监控您的固态硬盘层，以确保其填充速度不会超过分层过程将数据移动到容量池存储所能达到的速度。

主题

- 使用 FSx 迁移到 ONTAP NetApp SnapMirror
- 使用 FSx 迁移到 ONTAP AWS DataSync

使用 FSx 迁移到 ONTAP NetApp SnapMirror

您可以使用将您的 NetApp ONTAP 文件系统迁移到亚马逊 FSx NetApp ONTAP 版。 NetApp SnapMirror

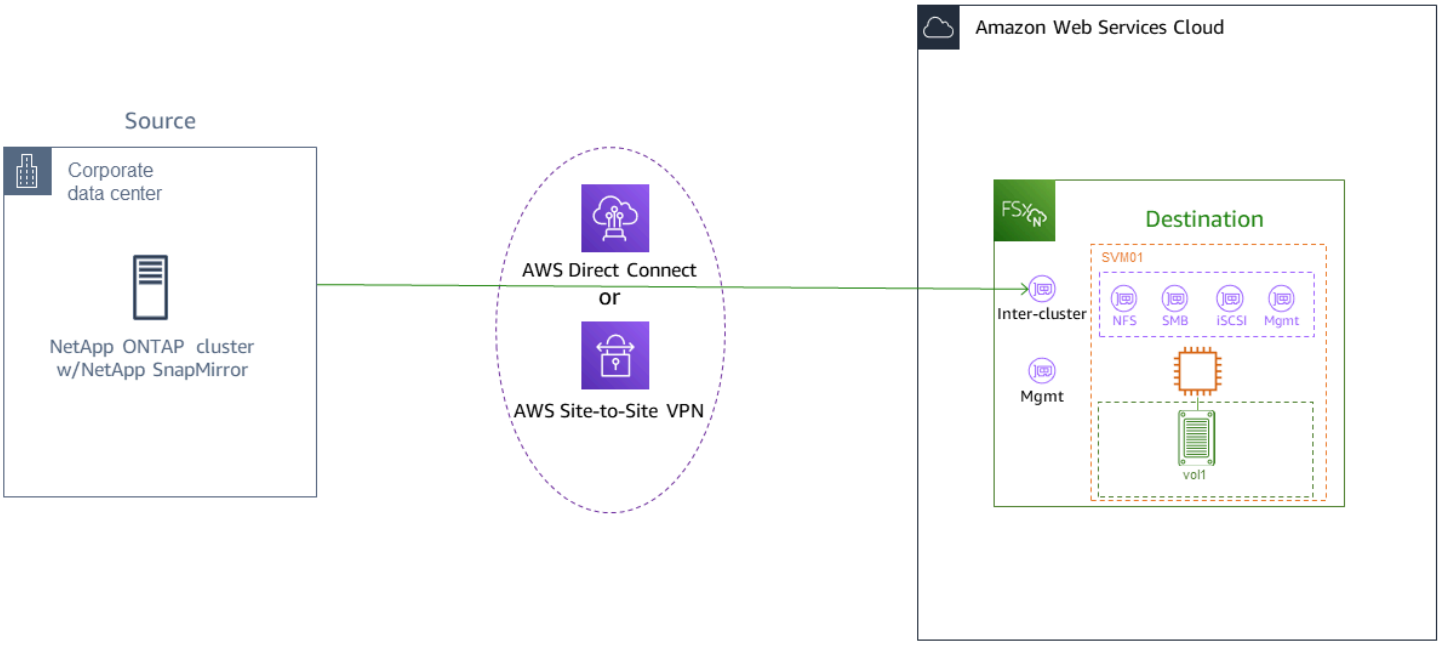
NetApp SnapMirror 在两个 ONTAP 文件系统之间使用块级复制，将数据从指定的源卷复制到目标卷。我们建议使用将本地 NetApp ONTAP 文件系统迁移 SnapMirror 到 FSx 适用于 ONTAP。 NetApp SnapMirror的块级复制既快速又高效，即使对于具有以下特性的文件系统也是如此：

- 复杂的目录结构
- 超过 5000 万个文件
- 文件大小非常小（以千字节为单位）

当您使用迁移 SnapMirror 到 FSx for ONTAP 时，经过重复数据删除和压缩的数据将保持这些状态，从而缩短了传输时间并减少了迁移所需的带宽量。迁移至目标卷时，源 ONTAP 卷上存在的快照会被保留。将本地 NetApp ONTAP 文件系统迁移到 FSx ONTAP 文件系统涉及以下高级任务：

1. 在 Amazon 中创建目标卷 FSx。
2. 收集源和目标逻辑接口 (LIFs)。
3. 在源文件系统和目标文件系统之间建立集群对等。
4. 创建 SVM 对等关系。
5. 建立 SnapMirror 关系。
6. 维护更新的目标集群。
7. 切换到你的 fo FSx r ONTAP 文件系统。

下图阐明了本节中描述的迁移方案。



主题

- 开始前的准备工作
- 创建目标卷
- 记录集群间的源和目标 LIFs
- 在源和目标之间建立集群对等
- 创建 SVM 对等关系
- 建立 SnapMirror 关系
- 将数据传输到您的 fo FSx r ONTAP 文件系统
- 切换到 Amazon FSx

开始前的准备工作

在您开始以下部分所述的过程之前，请确保您已符合以下先决条件：

- FSx for ONTAP 将客户端流量优先于后台任务，包括数据分层、存储效率和备份。迁移数据时，作为一般最佳实践，我们建议您监控 SSD 层的容量，以确保其利用率不超过 80%。您可以使用CloudWatch 文件系统指标监控固态硬盘层的利用率。有关更多信息，请参阅 卷指标。
- 如果您在迁移数据时将目标卷的数据分层策略设置为 `All`，则所有文件元数据都存储在主 SSD 存储层上。无论卷的数据分层策略如何，文件元数据始终存储在基于 SSD 的主要层上。主要层与容量池层存储容量的比例建议假定为 1:10。
- 源文件系统和目标文件系统连接在同一 VPC 中，或者位于使用 Amazon VPC 对等互连、Transit Gateway 或进行对等连接的网络中。 AWS Direct Connect Site-to-Site VPN有关更多信息，请参阅《Amazon VPC 对等连接指南》中的 从内部访问数据 AWS Cloud 和什么是 VPC 对等连接？。
- 适用于 ONTAP 文件系统的 VPC 安全组具有入站和出站规则，允许您的集群间终端节点在端口 443、10000、11104 和 11105 上使用 ICMP 和 TCP（ ）。 FSx LIFs
- 在创建 SnapMirror 数据保护关系之前，请验证源卷和目标卷是否运行兼容的 NetApp ONTAP 版本。有关更多信息，请参阅 ONTAP 用户文档中的兼容 NetApp的 ONTAP 版本以了解 SnapMirror 关系。此处介绍的过程使用本地 NetApp ONTAP 文件系统作为源。
- 您的本地（源） NetApp ONTAP 文件系统包含 SnapMirror 许可证。
- 您已使用 SVM FSx 为 ONTAP 文件系统创建了目标，但尚未创建目标卷。有关更多信息，请参阅 创建文件系统。

这些过程中的命令使用以下集群、SVM 和卷别名：

- *`FSx-Dest`*— 目标 (FSx) 集群的 ID（格式为 FSx idabcdef1234567890a ）。
- *`OnPrem-Source`* – 源集群的 ID。
- *`DestSVM`* – 目标 SVM 名称。
- *`SourceSVM`* – 源 SVM 名称。
- 源卷和目标卷的名称均为 `vol1`。

> **Note**
>
> 在所有 ONTAP CLI 命令中， FSx 适用于 ONTAP 的文件系统都被称为集群。

本节中的过程使用以下 NetApp ONTAP CLI 命令。

- volume create 命令
- cluster 命令
- vserver peer 命令
- snapmirror 命令

您将使用 NetApp ONTAP CLI 在 FSx 适用于 ONTAP 的文件 SnapMirror 系统上创建和管理配置。有关更多信息，请参阅 使用 NetApp ONTAP CLI。

创建目标卷

除了 NetApp ONTAP CLI 和 REST API 之外，您还可以使用亚马逊 FSx 控制台 AWS CLI、和亚马逊 FSx API 创建数据保护 (DP) 目标卷。有关使用 Amazon FSx 控制台和创建目标卷的信息 AWS CLI，请参阅创建卷。

> **Note**
>
> 当目标卷的分层策略为 `All` 时，ONTAP 不会保留在目标 DP 卷源位置实现的后处理压缩节省。要保留处理后压缩节省的费用，应将目标卷分层策略设置为目标文件系统`Auto`并在目标文件系统 inactive-data-compression上启用，以便在目标文件系统上重新应用后处理后的压缩节省。

在以下步骤中，您将使用 NetApp ONTAP CLI 在 for ONTAP 文件系统 FSx 上创建目标卷。您将需要 `fsxadmin` 密码以及文件系统管理端口的 IP 地址或 DNS 名称。

1. 使用您在创建文件系统时设置的用户 `fsxadmin` 和密码与目标文件系统建立 SSH 会话。

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. 在目标集群上创建一个存储容量至少等于源卷存储容量的卷。用于`-type DP`将其指定为 SnapMirror 关系的目的地。

   如果您计划使用数据分层，我们建议您将 `-tiering-policy` 设置为 `all`。这样可以确保您的数据立即传输到容量池存储，并防止 SSD 层上的容量耗尽。迁移后，您可以将 `-tiering-policy` 切换到 `auto`。

> **Note**
>
> 无论卷的数据分层策略如何，文件元数据始终存储在基于 SSD 的主要层上。

```
FSx-Dest::> vol create -vserver DestSVM -volume vol1 -aggregate aggr1 -size 1g -
type DP -tiering-policy all
```

记录集群间的源和目标 LIFs

SnapMirror 使用集群间逻辑接口 (LIFs)，每个接口都有唯一的 IP 地址，以促进源集群和目标集群之间的数据传输。

1. 对 FSx 于 ONTAP 文件系统的目标，您可以导航到文件系统详细信息页面上的 “管理” 选项卡，从 Amazon FSx 控制台检索集群间终端节点-IP 地址。
2. 对于源 NetApp ONTAP 集群，使用 ONTAP CLI 检索集群间 LIF IP 地址。运行如下命令：

```
OnPrem-Source::> network interface show -role intercluster

Logical                         Network
Vserver     Interface  Status  Address/Mask
----------- ---------- ------- ------------
FSx-Dest
             inter_1    up/up  10.0.0.36/24
             inter_2    up/up  10.0.1.69/24
```

> **Note**
>
> 对于第二代单可用区文件系统，每个高可用性（HA）对有两个集群间 IP 地址。保存这些值供稍后使用。

保存 `inter_1` 和 `inter_2` IP 地址。它们在 `FSx-Dest` 中称为 `dest_inter_1` 和 `dest_inter_2`，在 `OnPrem-Source` 中为 `source_inter_1` 和 `source_inter_2`。

在源和目标之间建立集群对等

通过提供集群间 IP 地址，在目标集群上建立集群对等关系。您还需要创建一个密码，当您在源集群上建立集群对等关系时，需要输入该密码。

1. 使用以下命令在目标集群上设置对等关系。对于第二代单可用区文件系统，需要提供各个集群间 IP 地址。

```
FSx-Dest::> cluster peer create -address-family ipv4 -peer-
addrs source_inter_1,source_inter_2

Enter the passphrase:
Confirm the passphrase:
Notice: Now use the same passphrase in the "cluster peer create" command in the
 other cluster.
```

2. 接下来，在源集群上建立集群对等关系。您需要输入上面创建的密码才能进行身份验证。对于第二代单可用区文件系统，需要提供各个集群间 IP 地址。

```
OnPrem-Source::> cluster peer create -address-family ipv4 -peer-
addrs dest_inter_1,dest_inter_2

Enter the passphrase:
Confirm the passphrase:
```

3. 在源集群上使用以下命令验证对等连接是否成功。在输出中，`Availability` 应设置为 `Available`。

```
OnPrem-Source::> cluster peer show

Peer Cluster Name  Availability   Authentication
-----------------  -------------- --------------
FSx-Dest           Available      ok
```

创建 SVM 对等关系

建立集群对等关系后，下一步是对等。 SVMs使用命令在目标集群 (FSx-Dest) 上创建 SVM 对等关系。`vserver peer`以下命令中使用的其他别名如下：

- `DestLocalName` – 此名称用于在源 SVM 上配置 SVM 对等关系时标识目标 SVM。

- SourceLocalName – 此名称用于在源 SVM 上配置 SVM 对等关系时标识源 SVM。

1. 使用以下命令在源和目标之间创建 SVM 对等关系。 SVMs

```
FSx-Dest::> vserver peer create -vserver DestSVM -peer-vserver SourceSVM -peer-
cluster OnPrem-Source -applications snapmirror -local-name SourceLocalName

 Info: [Job 207] 'vserver peer create' job queued
```

2. 接受源集群上的对等关系：

```
OnPrem-Source::> vserver peer accept -vserver SourceSVM -peer-vserver DestSVM -
local-name DestLocalName

 Info: [Job 211] 'vserver peer accept' job queued
```

3. 使用以下命令验证 SVM 对等关系连接状态；Peer State 在响应中应设置为 peered。

```
OnPrem-Source::> vserver peer show

        Peer     Peer   Peer     Peering       Remote
Vserver Vserver  State  Cluster  Applications  Vserver
------- -------- ------ -------- ------------- ---------
svm01   destsvm1 peered FSx-Dest snapmirror    svm01
```

建立 SnapMirror 关系

现在，您已经对源和目标进行了对 SVMs等，接下来的步骤是在目标集群上创建和初始化 SnapMirror 关系。

> **Note**
>
> 创建并初始化 SnapMirror 关系后，目标卷将处于只读状态，直到关系破裂。

- 使用snapmirror create命令在目标集群上创建 SnapMirror 关系。snapmirror create 命令必须通过目标 SVM 使用。

  您可以选择使用-throttle来设置关系的最大带宽（以 KB/sec 为单位）。 SnapMirror

```
FSx-Dest::> snapmirror create -source-path SourceLocalName:vol1 -destination-
path DestSVM:vol1 -vserver DestSVM -throttle unlimited

 Operation succeeded: snapmirror create for the relationship with destination
 "DestSVM:vol1".
```

将数据传输到您的 fo FSx r ONTAP 文件系统

既然您已经创建了 SnapMirror 关系，就可以将数据传输到目标文件系统了。

1. 通过在目标文件系统上运行以下命令，可以将数据传输到目标文件系统。

> **Note**
>
> 运行此命令后， SnapMirror 开始将数据快照从源卷传输到目标卷。

```
FSx-Dest::> snapmirror initialize -destination-path DestSVM:vol1 -source-
path SourceLocalName:vol1
```

2. 如果要迁移正在使用的数据，则需要更新目标集群，使其与源集群保持同步。要对目标集群执行一次性更新，请运行以下命令。

```
FSx-Dest::> snapmirror update -destination-path DestSVM:vol1
```

3. 在完成迁移并将客户端迁移到 ONTAP 之前，您还可以安排每小时或每天 FSx 的更新。您可以使用snapmirror modify命令建立 SnapMirror 更新计划。

```
FSx-Dest::> snapmirror modify -destination-path DestSVM:vol1 -schedule hourly
```

切换到 Amazon FSx

要为切换到 for ONTAP 文件系统做准备，请执行以下操作： FSx

- 断开所有写入源集群的客户端。
- 执行最后一次 SnapMirror 传输，以确保切换时不会丢失数据。

- 打破 SnapMirror 关系。
- 将所有客户端连接到您的 fo FSx r ONTAP 文件系统。

1. 要确保源集群中的所有数据都传输到 FSx ONTAP 文件系统，请执行最后一次 Snapmirror 传输。

```
FSx-Dest::> snapmirror update -destination-path DestSVM:vol1
```

2. 验证 `Mirror State` 设置为 `Snapmirrored`，且 `Relationship Status` 设置为 `Idle`，确保数据迁移已完成。您还应确保 `Last Transfer End Timestamp` 日期符合预期，因为它表示上次向目标卷传输的时间。
3. 运行以下命令以显示 SnapMirror 状态。

```
FSx-Dest::> snapmirror show -fields state,status,last-transfer-end-timestamp

Source     Destination   Mirror        Relationship Last Transfer End
Path       Path          State         Status       Timestamp
---------- -----------   ----------    -------      ---------------
Svm01:vol1 svm02:DestVol Snapmirrored  Idle         09/02 09:02:21
```

4. 使用`snapmirror quiesce`命令禁用任何 future SnapMirror 传输。

```
FSx-Dest::> snapmirror quiesce -destination-path DestSVM:vol1
```

5. 验证是否已使用 `snapmirror show` 将 `Relationship Status` 更改为 `Quiesced`。

```
FSx-Dest::> snapmirror show

Source            Destination   Mirror        Relationship
Path              Path          State         Status
-----------       ------------  ------------ --------
sourcesvm1:vol1   svm01:DestVol Snapmirrored  Quiesced
```

6. 在迁移过程中，目标卷为只读状态。要启用读/写，您需要中断 SnapMirror 关系并切换到您 FSx 的 for ONTAP 文件系统。使用以下命令中断 SnapMirror 关系。

```
FSx-Dest::> snapmirror break -destination-path DestSVM:vol1

Operation succeeded: snapmirror break for destination "DestSVM:vol1".
```

7. SnapMirror 复制完成且 SnapMirror关系中断后，您可以装载该卷以使数据可用。

```
FSx-Dest::> vol mount -vserver fsx -volume vol1 -junction-path /vol1
```

现在，该卷已可用，源卷中的数据已完全迁移到目标卷。该卷还可供客户读取和写入。如果您之前将此卷的 `tiering-policy` 设置为 `all`，则可以将其更改为 `auto` 或 `snapshot-only`，您的数据将根据访问模式自动在存储层之间传输。要使客户端和应用程序可以访问这些数据，请参阅访问您的 fo FSx r ONTAP 数据。

使用 FSx 迁移到 ONTAP AWS DataSync

我们建议使用 AWS DataSync 在 ONTAP 文件系统和非 ONTap 文件系统之间 FSx 传输数据，包括 FSx Lustre、OpenZFS、 FSx Windows 文件服务器、 FSx Amazon EFS、Amazon S3 和本地文件管理器。如果您要在 ONTAP 和 NetApp ONTAP 之间 FSx 传输文件，我们建议使用。NetApp SnapMirror AWS DataSync 是一项数据传输服务，可简化、自动化和加速通过 Internet 或在自我管理的存储系统和 AWS 存储服务之间移动和复制数据。 Direct Connect DataSync 可以传输您的文件系统数据和元数据，例如所有权、时间戳和访问权限。

您可以使用 DataSync 在 ONTAP 文件系统的两个 FSx 文件系统之间传输文件，也可以使用将数据移动到其他 AWS 区域 或 AWS 帐户中的文件系统。您也可以将 DataSync 与 ONTAP 文件系统配合 FSx 使用以执行其他任务。例如，您可以执行一次性数据迁移、定期摄取分布式工作负载的数据以及按计划复制以实现数据保护与恢复。

在中 DataSync，位置是适用于 ONTAP 的文件系统的终端节点。 FSx 有关特定传输场景的信息，请参阅《AWS DataSync 用户指南》中的使用位置。

> **Note**
>
> 如果您计划使用 `All` 分层策略将数据迁移至容量池层，请记住，文件元数据始终存储在 SSD 层上，且所有新用户数据都首先写入 SSD 层。当数据写入 SSD 层时，后台分层进程将开始将您的数据分层到容量池存储，但是分层进程非即时，并且会消耗网络资源。考虑到文件元数据（占用户数据大小的 3-7%），您需要调整 SSD 层的大小，作为用户数据的缓冲区，然后再将其分层到容量池存储。建议 SSD 利用率不要超过 80%。
>
> 迁移数据时，请务必使用CloudWatch 文件系统指标监控您的固态硬盘层，以确保其填充速度不会超过分层过程将数据移动到容量池存储所能达到的速度。您还可以将 DataSync 传输限制为低于分层速率的速率，以确保您的固态硬盘层使用率不超过 80%。例如，对于吞吐量至少为 512 的文件系统 MBps，200 的 MBps 限制通常会平衡数据传输和数据分层速率。

先决条件

要将数据迁移到 FSx for ONTAP 设置中，您需要符合 DataSync 要求的服务器和网络。要了解更多信息，请参阅《AWS DataSync 用户指南》 DataSync中的要求。

使用迁移文件的基本步骤 DataSync

使用将文件从源传输到目标 DataSync 包括以下基本步骤：

- 在您的环境中下载并部署代理并激活它（如果在两者之间传输，则不需要 AWS 服务）。
- 创建源和目标位置。
- 创建 任务。
- 运行任务，将文件从源传输到目标。

有关更多信息，请参阅《AWS DataSync 用户指南》中的以下主题：

- 在自管存储和自管存储之间传输数据 AWS
- 为 AMAZON for NetApp ONTA FSx P 创建营业地点

适用于 ONTAP 的 Amazon FSx 中的安全 NetApp

云安全 AWS 是重中之重。作为 AWS 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 AWS 的责任。责任共担模式将其描述为云的安全性和云中的安全性：

- 云安全 — AWS 负责保护在云中运行 AWS 服务的基础架构 AWS Cloud。 AWS 还为您提供可以安全使用的服务。 Third-party 作为AWS 合规计划合规计划合规计划合的一部分，审计师定期测试和验证我们安全的有效性。要了解适用于 Amazon FSx for NetApp ONTAP 的合规计划，请参阅按合规计划划分的范围内AWS 服务按合规计划划。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

该文档帮助您了解如何在使用 Amazon FSx 时应用责任共担模式。以下主题说明如何配置 Amazon FSx 以实现您的安全性和合规性目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 Amazon FSx 资源。

主题

适用于 ONTAP 的 Amazon FSx 中的数据保护 NetApp

AWS 分担责任模型分适用于适用于 ONTAP 的 Amazon FSx 中的数据保护。 NetApp 如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础结构上的内

容的控制。您还负责您所使用的 AWS 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解答AWS条款。 有关欧洲数据保护的信息，请参阅通用数据保护条例（GDPR）中心。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证（MFA）。
- 用于 SSL/TLS 与 AWS 资源通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。有关使用 CloudTrail 跟踪捕获 AWS 活动的信息，请参阅AWS CloudTrail 用户指南中的使用跟 CloudTrail 踪。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-3 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-3 版》https://aws.amazon.com/compliance/fips/。

强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括您使用控制台、API 或软件开发工具包 AWS 服务 使用 Amazon FSx 或其他软件开发工具包 AWS CLI的情况。 AWS 在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供 URL，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

FSx for ONTAP 中的数据加密

适用于 NetApp ONTAP 的 Amazon FSx 支持对静态数据进行加密和对传输中的数据进行加密。创建 Amazon FSx 文件系统时，系统会自动启用静态数据加密。如果您使用 NetApp 轻量级目录访问协议 (LDAP) 访问已加入活动目录或域的存储虚拟机 (SVM) 中的数据，则适用于 ONTAP 的 Amazon FSx 支持通过 NFS 和 SMB 协议传输的加 Kerberos-based 密。

何时使用加密

如果您的组织受到要求对数据和元数据进行静态加密的公司或监管政策的约束，则您的数据会自动进行静态加密。我们还建议您通过对传输中数据进行加密来挂载文件系统，从而对传输中数据进行加密。

有关使用适用于 NetApp ONTAP 的 Amazon FSx 进行数据加密的更多信息，请参阅和。静态数据加密 加密传输中数据

静态数据加密

所有适用于 NetApp ONTAP 文件系统的 Amazon FSx 和备份都使用使用 AWS Key Management Service () 管理的密钥进行静态加密。AWS KMS数据在写入文件系统前会自动加密，并在读取时自动解密。所有备份都会在创建时自动加密，并在备份恢复到新卷时自动解密。这些过程由 Amazon FSx 透明地处理，因此，您不必修改您的应用程序。

Amazon FSx 使用行业标准的 AES-256 加密算法对静态的 Amazon FSx 数据和元数据进行加密。有关更多信息，请参阅《AWS Key Management Service 开发人员指南》中的加密基础知识。

> **Note**
>
> AWS 密钥管理基础设施使用经联邦信息处理标准 (FIPS) 140-2 批准的加密算法。该基础设施符合美国国家标准与技术研究院（NIST）800-57 建议。

亚马逊 FSx 是如何使用的 AWS KMS

Amazon FSx 与之集成， AWS KMS 用于密钥管理。Amazon FSx 使用 KMS 密钥来加密您的文件系统和任何卷备份。您可以选择用于加密和解密文件系统及卷备份（包括数据和元数据）的 KMS 密钥。您可以启用、禁用或撤销对该 KMS 密钥的授权。该 KMS 密钥可以是以下两种类型之一：

- AWS托管 KMS 密钥 – 这是默认 KMS 密钥，可以免费使用。
- Customer-managed KMS 密钥 — 这是最灵活的 KMS 密钥，因为您可以为多个用户或服务配置其密钥策略和授权。有关创建 KMS 密钥的更多信息，请参阅 AWS Key Management Service 开发人员指南中的创建密钥。

> **Important**
>
> Amazon FSx 仅接受对称加密 KMS 密钥。您不能在 Amazon FSx 上使用非对称 KMS 密钥。

如果将客户托管式密钥作为您的 KMS 密钥进行文件数据加密和解密，您可以启用密钥轮换。在启用密钥轮换时， AWS KMS 自动每年轮换一次您的密钥。此外，对于客户托管式 KMS 密钥，您可以随时

选择何时禁用、重新启用、删除或撤销您的 KMS 密钥访问权限。有关更多信息，请参阅《AWS Key Management Service 开发人员指南》中的轮换 AWS KMS keys以及启用和禁用密钥。

Amazon FSx 的关键政策 AWS KMS

密钥政策是控制对 KMS 密钥访问的主要方法。有关密钥政策的更多信息，请参阅《AWS Key Management Service 开发人员指南》中的使用 AWS KMS中的密钥政策。以下列表描述了 Amazon FSx 为静态加密文件系统和备份支持的所有 AWS KMS相关权限：

- kms:Encrypt –（可选）将明文加密为加密文字。该权限包含在默认密钥策略中。
- kms:Decrypt –（必需）解密加密文字。加密文字是以前加密的明文。该权限包含在默认密钥策略中。
- kms: ReEncrypt —（可选）使用新的加密服务器端的数据 AWS KMS key，而不会在客户端暴露数据的纯文本。将先解密数据，然后重新加密。该权限包含在默认密钥策略中。
- kms: GenerateDataKeyWithoutPlaintext —（必填）返回使用 KMS 密钥加密的数据加密密钥。此权限包含在 k ms: GenerateDataKey * 下的默认密钥策略中。
- km CreateGrant s: —（必填）向密钥添加授权，以指定谁可以在什么条件下使用该密钥。授权是密钥政策的替代权限机制。有关授权的更多信息，请参阅《AWS Key Management Service 开发人员指南》中的使用授权。该权限包含在默认密钥策略中。
- kms: DescribeKey —（必填）提供有关指定 KMS 密钥的详细信息。该权限包含在默认密钥策略中。
- km ListAliases s: —（可选）列出账户中的所有密钥别名。在使用控制台创建加密的文件系统时，该权限将填充 KMS 密钥列表。我们建议您使用该权限以提供最佳的用户体验。该权限包含在默认密钥策略中。

加密传输中数据

本主题说明了可用于对 FSx for ONTAP 文件系统和连接客户端间的传输中文件数据进行加密的不同选项。它还提供指导帮助您选择最适合工作流程的加密方法。

流经 AWS 全球 AWS 区域 网络的所有数据在离开 AWS 安全设施之前，都会在物理层自动加密。可用区之间的所有流量都是加密的。其他加密层（包括本节中列出的加密层）会提供额外保护。有关如何为流经可用区域和实例的数据 AWS 提供保护的更多信息 AWS 区域，请参阅《适用于 Linux 实例的 Amazon Elastic Compute Cloud 用户指南》中的传输中加密。

适用于 NetApp ONTAP 的 Amazon FSx 支持以下方法来加密在 FSx for ONTAP 文件系统和连接的客户端之间传输的数据：

- 对在支持的 Amazon EC2 Linux 和 Windows 实例类型上运行的所有支持的协议和客户端进行自动 Nitro-based 加密。
- Kerberos-based 通过 NFS 和 SMB 协议进行加密。
- IPsec-based 通过 NFS、iSCSI 和 SMB 协议进行加密

所有支持的传输中数据加密方法都使用行业标准的加密算法，这些算法可提供企业级 AES-256 加密功能。

主题

选择加密传输中数据的方法

本节提供的信息可以帮助您确定哪种支持的传输中加密方法最适合您的工作流程。您可以在探索以下各节中详细介绍的支持选项时重新参阅本节。

在选择如何加密 FSx for ONTAP 文件系统和连接客户端间的传输中数据时，需要考虑几个因素。这些因素包括：

- 你 AWS 区域 的 FSx for ONTAP 文件系统正在其中运行。
- 客户端运行的实例类型。
- 客户端访问文件系统的位置。
- 网络性能要求。
- 您要加密的数据协议。
- 如果您使用的是 Microsoft Active Directory。

AWS 区域

您的文件系统的运行状态决定了您是否可以使用 Amazon Nitro-based 加密。 AWS 区域 有关更多信息，请参阅 使用对传输中的数据进行加密 AWS Nitro System。

客户端实例类型

如果访问您的文件系统的客户端运行在任何支持的 Amaz Nitro-based on EC2 Mac、Linux 或 Windows 实例类型上，并且您的工作流程满足使用Nitro-based 加密的所有其他要求，则可以使用亚马逊加密。使用 Kerberos 或 IPsec 加密没有任何客户端实例类型要求。

客户端位置

客户端访问数据的位置相对于文件系统的位置会影响可以使用的传输中加密方法。如果客户端和文件系统位于同一 VPC 中，则可以使用任何支持的加密方法。如果客户端和文件系统位于对等 VPC 中，则情况也是如此，前提是流量不通过虚拟网络设备或服务，例如传输网关。 Nitro-based 如果客户端不在同一个或对等的 VPC 中，或者流量通过虚拟网络设备或服务，则加密不是一个可用的选项。

网络性能

使用 Amazon Nitro-based 加密不会对网络性能产生任何影响。这是因为支持的 Amazon EC2 实例利用底层 Nitro 系统硬件的分载功能，自动加密实例间的传输中流量。

使用 Kerberos 或 IPsec 加密会影响网络性能。这是因为这两种加密方法都是基于软件的加密，需要客户端和服务器使用计算资源来加密和解密传输中的流量。

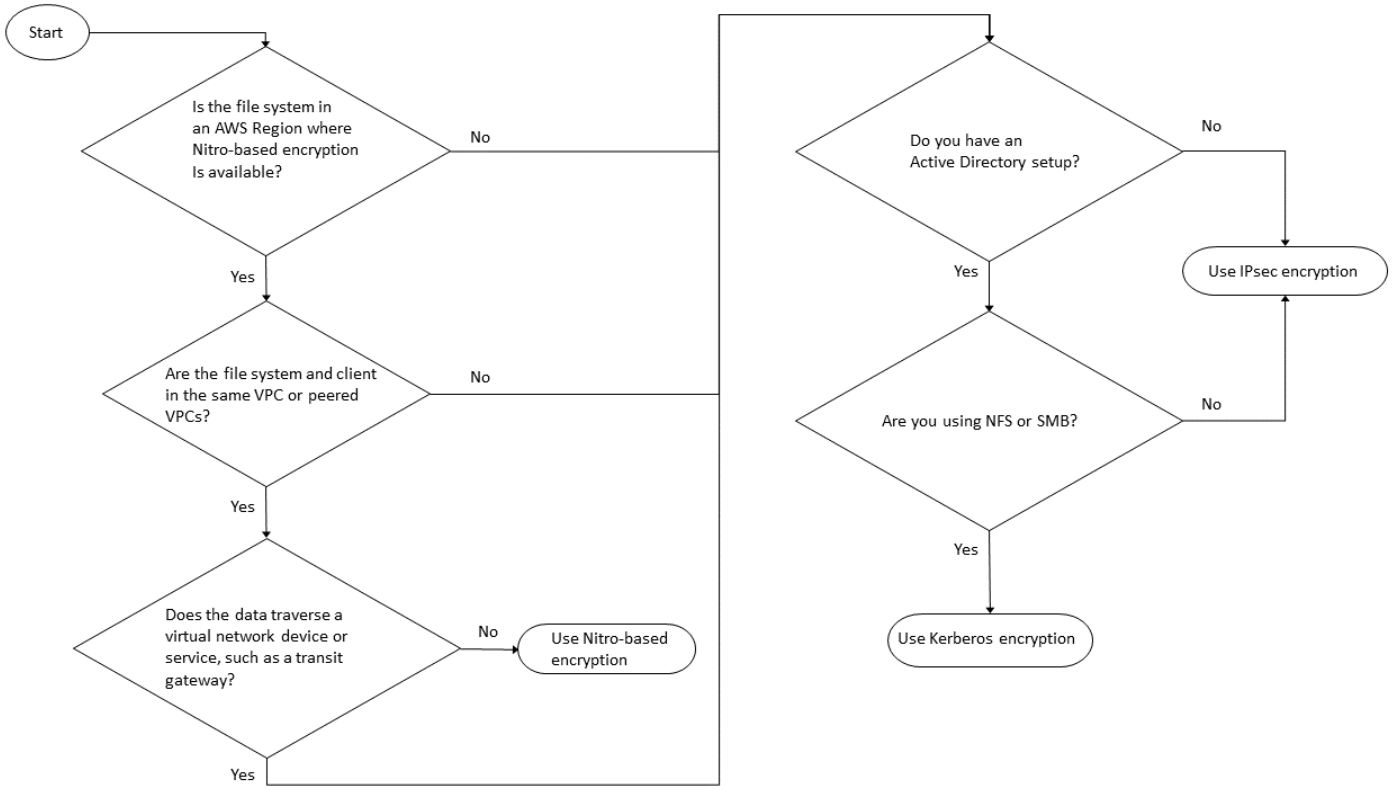
数据协议

您可以将 Amazon Nitro-based 加密和 IPsec 加密与所有支持的协议（NFS、SMB 和 iSCSI）一起使用。Kerberos 加密与 NFS 和 SMB 协议（使用 Active Directory）可以一起使用。

Active Directory

如果您使用的是 Microsoft Active Directory，则可以通过 NFS 和 SMB 协议使用 Kerberos 加密。

利用下图来帮助您决定使用哪种传输中加密方法。



如果以下所有条件都适用于您的工作流程，则 IPsec 加密是唯一可用选项：

- 您使用的是 NFS、SMB 或 iSCSI 协议。
- 您的工作流程不支持使用 Amazon Nitro-based 加密。
- 您使用的不是 Microsoft Active Directory 域。

使用对传输中的数据进行加密 AWS Nitro System

通过 Nitro-based 加密，当访问您的文件系统的客户端在支持的 Amazon EC2 Linux 或 Windows 实例类型上运行时，传输中的 AWS 区域 数据会自动加密，FSx for ONTAP 上有这些实例类型。

使用 Amazon Nitro-based 加密不会对网络性能产生任何影响。这是因为支持的 Amazon EC2 实例利用底层 Nitro 系统硬件的分载功能，自动加密实例间的传输中流量。

Nitro-based 当支持的客户端实例类型位于相同的 VPC 中，或者位于 AWS 区域 与文件系统的 VPC 对等的 VPC 中时，会自动启用加密。此外，如果客户端位于对等 VPC 中，则数据无法通过虚拟网络设备或服务（例如传输网关），从而自动 Nitro-based 启用加密。有关 Nitro-based 加密的更多信息，请参阅《适用于 Linux 或 Windows 实例类型的 Amazon EC2 用户指南》的 “传输中的加密” 部分。

下表详细说明了 AWS 区域 可用的 Nitro-based 加密功能。

Support 支持 Nitro-based 加密

生成	部署类型	AWS 区域
First-generation 文件系统 [1]	Single-AZ 1 Multi-AZ 1	美国东部（弗吉尼亚州北部）、美国东部（俄亥俄州）、美国西部（俄勒冈州）、欧洲地区（爱尔兰）
Second-generation 文件系统	Single-AZ 2 Multi-AZ 2	美国东部（弗吉尼亚州北部）、美国东部（俄亥俄州）、美国西部（北加利福尼亚）、美国西部（俄勒冈州）、欧洲地区（法兰克福）、欧洲地区（爱尔兰）、亚太地区（悉尼）

[1] 在 2022 年 11 月 28 日当天或之后创建 First-generation 的文件系统支持所列 AWS 区域内容中的 Nitro-based 传输中加密。

有关适用于 ONTAP 的 FSx AWS 区域 在何处可用的更多信息，请参阅适用于 ONTAP 的 Amazon FSx 定价。 NetApp

有关 FSx for ONTAP 文件系统性能规格的更多信息，请参阅吞吐能力对性能的影响。

使用加密对传输中的数据进行加密 Kerberos-based

如果您使用的是 Act Microsoft ive Directory，则可以通过 NFS 和 SMB 协议使用 Kerberos-based 加密来加密已加入 M icrosoft Active Directory 的 SVM 子卷的传输数据。

通过 NFS 使用 Kerberos 进行传输中数据加密

NFSv3 和 NFSv4 协议支持使用 Kerberos 对传输中数据进行加密。要针对 NFS 协议使用 Kerberos 启用传输中加密，请参阅 NetApp ONTAP 文档中心中的使用 Kerberos 与 NFS 获得强大的安全性。

通过 SMB 使用 Kerberos 进行传输中数据加密

在支持 SMB 协议 3.0 或更高版本的计算实例上映射的文件共享支持通过 SMB 协议进行传输中数据加密。这包括 Microsoft Server 2012 及更高版本以及 Microsoft Windows 8 及更高版本的所有 Microsoft

Windows 版本。启用后，FSx for ONTAP 会在您访问文件系统时使用 SMB 加密自动加密传输中数据，而无需修改应用程序。

FSx for ONTAP SMB 支持 128 位和 256 位加密，具体取决于客户端会话请求。有关不同加密级别的描述，请参阅 NetApp ONTAP 文档中心中使用 CLI 管理 SMB 的设置 SMB 服务器最低身份验证安全级别部分。

> **Note**
>
> 客户端决定加密算法。NTLM 和 Kerberos 身份验证支持 128 位和 256 位加密。FSx for ONTAP SMB 服务器接受所有标准 Windows 客户端请求，精细控制由 Microsoft 组策略或注册表设置处理。

您可以使用 ONTAP CLI 管理 FSx for ONTAP SVM 和卷的传输中加密设置。要访问 NetApp ONTAP CLI，请在要进行传输中加密设置的 SVM 上建立 SSH 会话，如 使用 ONTAP CLI 管理 SVM 中所述。

有关如何在 SVM 或卷上启用 SMB 加密的说明，请参阅 启用传输中数据的 SMB 加密。

使用 IPsec 加密进行传输中数据加密

FSx for ONTAP 支持在传输模式下使用 IPsec 协议，确保数据在传输过程中持续保持安全和加密。IPsec 针对所有支持的 IP 流量（NFS、iSCSI 和 SMB 协议）为客户端和 FSx for ONTAP 文件系统之间的传输中数据提供端到端加密。借助 IPsec 加密，您可以在配置为启用 IPsec 的 FSx for ONTAP SVM 与在访问数据的连接客户端上运行的 IPsec 客户端之间建立 IPsec 隧道。

当从不支持加密的客户端访问数据时，以及如果您的客户端和 SVM 未加入加密所必需的 Active Directory，我们建议您使用 IPsec 对通过 NFS、SMB 和 iSCSI 协议Nitro-based 传输的数据进行加密。 Kerberos-based 当您的 iSCSI 客户端不支持加密时，IPsec 加密是唯一可用于对 iSCSI 流量传输的数据进行加密的选项。 Nitro-based

对于 IPsec 身份验证，您可以使用预共享密钥（PSK）或证书。如果您使用的是 PSK，则您使用的 IPsec 客户端必须支持带 PSK 的互联网密钥交换版本 2（IKEv2）。在 FSx for ONTAP 和客户端上配置 IPsec 加密的概括步骤如下：

1. 在您的文件系统上启用和配置 IPsec。
2. 在您的客户端上安装和配置 IPsec
3. 配置 IPsec 以实现多客户端访问

有关如何使用 PSK 配置 IPsec 的详细信息，请参阅 NetApp ONTAP 文档中心中的通过在线加密配置 IP 安全（IPsec）。

有关如何使用证书配置 IPsec 的更多信息，请参阅 使用证书身份验证配置 IPsec。

启用传输中数据的 SMB 加密

默认情况下，创建 SVM 时，SMB 加密处于关闭状态。您可以对单个共享或 SVM 启用需要 SMB 加密，后者会为该 SVM 上的所有共享启用 SMB 加密。

> **Note**
>
> 在 SVM 或共享上启用“需要 SMB 加密”时，不支持加密的 SMB 客户端将无法连接到该 SVM 或共享。

要求对 SVM 上传入的 SMB 流量进行 SMB 加密

按照以下步骤使用 NetApp ONTAP CLI 要求对 SVM 进行 SMB 加密。

1. 要通过 SSH 连接到 SVM 管理端点，请使用创建 SVM 时设置的用户名 `vsadmin` 和 vsadmin 密码。如果您没有设置 vsadmin 密码，请使用用户名 `fsxadmin` 和 fsxadmin 密码。您可以使用管理端点 IP 地址或 DNS 名称，从与文件系统位于同一 VPC 的客户端通过 SSH 连接到 SVM。

   ```
   ssh vsadmin@svm-management-endpoint-ip-address
   ```

   带有示例值的命令：

   ```
   ssh vsadmin@198.51.100.10
   ```

   使用管理端点 DNS 名称的 SSH 命令：

   ```
   ssh vsadmin@svm-management-endpoint-dns-name
   ```

   使用示例 DNS 名称的 SSH 命令：

   ```
   ssh vsadmin@management.svm-abcdef01234567892fs-08fc3405e03933af0.fsx.us-east-2.aws.com
   ```

```
Password: vsadmin-password

This is your first recorded login.
FsxIdabcdef01234567892::>
```

2. 使用以下 vserver cifs security modify NetApp ONTAP CLI 命令要求对传入 SVM 的 SMB 流量进行 SMB 加密。

```
vserver cifs security modify -vserver vserver_name -is-smb-encryption-required true
```

3. 使用以下命令，停止对传入 SMB 流量进行 SMB 加密。

```
vserver cifs security modify -vserver vserver_name -is-smb-encryption-required
 false
```

4. 要查看 SVM 上的当前 is-smb-encryption-required 设置，请使用以下 vserver cifs security show NetApp ONTAP CLI 命令：

```
vserver cifs security show -vserver vs1 -fields is-smb-encryption-required

vserver  is-smb-encryption-required
-------- -------------------------
vs1      true
```

有关在 SVM 上管理 SMB 加密的更多信息，请参阅 NetApp ONTAP 文档中心中的在 SMB 服务器上为 SMB 数据传输配置需要 SMB 加密。

在卷上启用 SMB 加密

按照以下步骤使用 NetApp ONTAP CLI 对共享启用 SMB 加密。

1. 按照 使用 ONTAP CLI 管理 SVM 中所述，建立与 SVM 管理端点的 Secure Shell（SSH）连接。
2. 使用以下 NetApp ONTAP CLI 命令创建新的 SMB 共享，并要求在访问此共享时进行 SMB 加密。

```
vserver cifs share create -vserver vserver_name -share-name share_name -
path share_path -share-properties encrypt-data
```

有关更多信息，请参阅《NetApp ONTAP CLI 命令手册》中的 vserver cifs share create。

3. 如需要求对现有 SMB 共享进行 SMB 加密，请使用以下命令。

```
vserver cifs share properties add -vserver vserver_name -share-name share_name -
share-properties encrypt-data
```

有关更多信息，请参阅《NetApp ONTAP CLI 命令手册》中的 vserver cifs share create。

4. 如需关闭对现有 SMB 共享进行 SMB 加密，请使用以下命令。

```
vserver cifs share properties remove -vserver vserver_name -share-name share_name -
share-properties encrypt-data
```

有关更多信息，请参阅《NetApp ONTAP CLI 命令手册》中的 vserver cifs share properties remove。

5. 要查看 SMB 共享上的当前 `is-smb-encryption-required` 设置，请使用以下 NetApp ONTAP CLI 命令：

```
vserver cifs share properties show -vserver vserver_name -share-name share_name -
fields share-properties
```

如果命令返回的属性之一是 `encrypt-data` 属性，则该属性指定访问此共享时必须使用 SMB 加密。

有关更多信息，请参阅《NetApp ONTAP CLI 命令手册》中的 vserver cifs share properties show。

使用 PSK 身份验证配置 IPsec

如果您使用 PSK 进行身份验证，则在 FSx for ONTAP 和客户端上配置 IPsec 加密的步骤如下：

1. 在您的文件系统上启用和配置 IPsec。
2. 在您的客户端上安装和配置 IPsec
3. 配置 IPsec 以实现多客户端访问

有关使用 PSK 配置 IPsec 的详细信息，请参阅 NetApp ONTAP 文档中心中的通过在线加密配置 IP 安全（IPsec）。

使用证书身份验证配置 IPsec

以下主题对在 FSx for ONTAP 文件系统和运行 Libreswan IPsec 的客户端上使用证书身份验证配置 IPsec 加密进行了说明。此解决方案使用 AWS Certificate Manager 和 AWS 私有证书颁发机构 来创建私有证书颁发机构并生成证书。

在 FSx for ONTAP 文件系统和连接的客户端上使用证书身份验证配置 IPsec 加密的概括步骤如下：

1. 设立证书颁发机构来颁发证书。
2. 为文件系统和客户端生成和导出 CA 证书。
3. 在客户端实例上安装证书并配置 IPsec。
4. 在您的文件系统上安装证书并配置 IPsec。
5. 定义安全策略数据库（SPD）。
6. 配置 IPsec 以实现多客户端访问。

创建和安装 CA 证书

要进行证书身份验证，您需要在 FSx for ONTAP 文件系统和将访问文件系统上数据的客户端上生成并安装来自证书颁发机构的证书。以下示例 AWS 私有证书颁发机构 用于设置私有证书颁发机构，并生成要安装在文件系统和客户端上的证书。使用 AWS 私有证书颁发机构，您可以创建完全 AWS 托管的根证书颁发机构和从属证书颁发机构 (CA) 层次结构，供组织内部使用。此过程分为五个步骤：

1. 使用创建私有证书颁发机构 (CA) AWS 私有 CA
2. 在私有 CA 上颁发并安装根证书
3. 从 AWS Certificate Manager 为您的文件系统和客户端申请私有证书
4. 为文件系统和客户端导出证书。

有关更多信息，请参阅《 AWS 私有证书颁发机构 用户指南》中的私有 CA 管理。

创建根私有 CA

1. 创建 CA 时，必须在提供的文件中指定 CA 配置。以下命令使用 Nano 文本编辑器创建 `ca_config.txt` 文件，指定以下信息：

   - 算法的名称
   - CA 用来签名的签名算法
   - X.500 主题信息

```
$ > nano ca_config.txt
```

随即显示文本编辑器。

2. 编辑 CA 规范文件。

```
{
   "KeyAlgorithm":"RSA_2048",
   "SigningAlgorithm":"SHA256WITHRSA",
   "Subject":{
      "Country":"US",
      "Organization":"Example Corp",
      "OrganizationalUnit":"Sales",
      "State":"WA",
      "Locality":"Seattle",
      "CommonName":"*.ec2.internal"
   }
}
```

3. 保存并关闭文件，退出文本编辑器。有关更多信息，请参阅《 AWS 私有证书颁发机构 用户指南》中的创建 CA 的步骤。

4. 使用 create-certificate-authority AWS 私有 CA CLI 命令创建私有 CA。

```
~/home > aws acm-pca create-certificate-authority \
     --certificate-authority-configuration file://ca_config.txt \
     --certificate-authority-type "ROOT" \
     --idempotency-token 01234567 --region aws-region
```

如果成功，此命令将输出 CA 的 Amazon 资源名称（ ARN ）。

```
{
   "CertificateAuthorityArn": "arn:aws:acm-pca:aws-region:111122223333:certificate-
authority/12345678-1234-1234-1234-123456789012"
}
```

为您的私有根 CA 创建和安装证书 (AWS CLI)

1. 使用 get-certificate-authority-csr AWS CLI 命令生成证书签名请求 (CSR)。

```
$ aws acm-pca get-certificate-authority-csr \
     --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
     --output text \
     --endpoint https://acm-pca.aws-region.amazonaws.com \
     --region eu-west-1 > ca.csr
```

生成的文件 `ca.csr` 是以 base64 格式编码的 PEM 文件，其内容显示如下。

```
-----BEGIN CERTIFICATE-----
 MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
 VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
 b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
 BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
 MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
 VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
 b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
 YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
 21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
 rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
 Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
 nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
 FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
 NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=
 -----END CERTIFICATE-----
```

有关更多信息，请参阅《 AWS 私有证书颁发机构 用户指南》中的安装根 CA 证书。

2. 使用issue-certificate AWS CLI 命令在您的私有 CA 上颁发和安装根证书。

```
$ aws acm-pca issue-certificate \
     --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
     --csr file://ca.csr \
     --signing-algorithm SHA256WITHRSA \
     --template-arn arn:aws:acm-pca:::template/RootCACertificate/V1 \
     --validity Value=3650,Type=DAYS --region aws-region
```

3. 使用get-certificate AWS CLI 命令下载根证书。

```
$ aws acm-pca get-certificate \
```

```
    --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
    --certificate-arn arn:aws:acm-pca:aws-region:486768734100:certificate-
authority/12345678-1234-1234-1234-123456789012/certificate/
abcdef0123456789abcdef0123456789 \
    --output text --region aws-region > rootCA.pem
```

4. 使用import-certificate-authority-certificate AWS CLI 命令在您的私有 CA 上安装根证书。

```
$ aws acm-pca import-certificate-authority-certificate \
     --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
     --certificate file://rootCA.pem --region aws-region
```

生成并导出文件系统和客户端证书

1. 使用request-certificate AWS CLI 命令请求 AWS Certificate Manager 证书以在您的文件系统和客户机上使用。

```
$ aws acm request-certificate \
    --domain-name *.ec2.internal \
    --idempotency-token 12345 \
    --region aws-region \
    --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012
```

   如果请求成功，则返回颁发证书的 ARN。

2. 为了安全起见，您必须在导出私钥时为其分配密码。创建密码并将其存储在名为 `passphrase.txt` 的文件中

3. 使用export-certificate AWS CLI 命令导出先前颁发的私有证书。导出的文件包含证书、证书链以及与证书中嵌入的公钥关联的加密私有 2048 位 RSA 密钥。为了安全起见，您必须在导出私钥时为其分配密码。以下示例是 Linux EC2 实例。

```
$ aws acm export-certificate \
     --certificate-arn arn:aws:acm:aws-
region:111122223333:certificate/12345678-1234-1234-1234-123456789012 \
     --passphrase $(cat passphrase.txt | base64) --region aws-region >
 exported_cert.json
```

4. 使用以下 `jq` 命令从 JSON 响应中提取私钥和证书。

```
$ passphrase=$(cat passphrase.txt | base64)
cat exported_cert.json | jq -r .PrivateKey > prv.key

cat exported_cert.json | jq -r .Certificate > cert.pem
```

5. 使用以下 `openssl` 命令从 JSON 响应中解密私钥。输入命令后，系统会提示您输入密码。

```
$ openssl rsa -in prv.key -passin pass:$passphrase -out decrypted.key
```

在 Amazon Linux 2 客户端上安装和配置 Libreswan IPsec

以下各节提供了在运行 Amazon Linux 2 的 Amazon EC2 实例上安装和配置 Libreswan IPsec 的说明。

安装和配置 Libreswan

1. 使用 SSH 连接到 EC2 实例。有关如何执行此操作的具体说明，请参阅《适用于 Linux 实例的 Amazon Elastic Compute Cloud 用户指南》中的使用 SSH 客户端连接到 Linux 实例。
2. 运行以下命令安装 `libreswan`：

```
$ sudo yum install libreswan
```

3. （可选）在后续步骤中验证 IPsec 时，如果没有这些设置，可能会标记这些属性。我们建议在没有这些设置的情况下先测试您的设置。如果连接出现问题，请返回此步骤并进行以下更改。

   安装完成后，使用您的首选文本编辑器将以下条目添加到 `/etc/sysctl.conf` 文件中。

```
net.ipv4.ip_forward=1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.send_redirects = 0
net.ipv4.conf.lo.accept_redirects = 0
net.ipv4.conf.lo.send_redirects = 0
net.ipv4.conf.all.rp_filter = 0
net.ipv4.conf.default.rp_filter = 0
net.ipv4.conf.eth0.rp_filter = 0
```

保存更改，退出文本编辑器。

4. 应用更改。

```
$ sudo sysctl -p
```

5. 验证 IPsec 配置。

```
$ sudo ipsec verify
```

验证您安装的 Libreswan 版本是否正常运行。

6. 初始化 IPsec NSS 数据库。

```
$ sudo ipsec checknss
```

在客户端上安装证书

1. 将您为客户端生成的证书复制到 EC2 实例上的工作目录中。You
2. 将之前生成的证书导出为与 libreswan 兼容的格式。

```
$ openssl pkcs12 -export -in cert.pem -inkey decrypted.key \
    -certfile rootCA.pem -out certkey.p12 -name fsx
```

3. 导入重新格式化的密钥，并在系统提示时提供密码。

```
$ sudo ipsec import certkey.p12
```

4. 使用首选文本编辑器创建 IPsec 配置文件。

```
$ sudo cat /etc/ipsec.d/nfs.conf
```

将以下条目添加到配置文件：

```
conn fsxn
    authby=rsasig
    left=172.31.77.6
    right=198.19.254.13
    auto=start
    type=transport
```

```
    ikev2=insist
    keyexchange=ike
    ike=aes256-sha2_384;dh20
    esp=aes_gcm_c256
    leftcert=fsx
    leftrsasigkey=%cert
    leftid=%fromcert
    rightid=%fromcert
    rightrsasigkey=%cert
```

在文件系统上配置 IPsec 后，您将在客户端上启动 IPsec。

在文件系统上配置 IPsec

本节提供有关在 FSx for ONTAP 文件系统上安装证书以及配置 IPsec 的说明。

在文件系统上安装证书

1. 将根证书（`rootCA.pem`））、客户端证书（`cert.pem`）和解密的密钥（`decrypted.key`）文件复制到您的文件系统。您需要知道证书的密码。
2. 要访问 ONTAP CLI，请运行以下命令，在适用于 NetApp ONTAP 文件系统的 Amazon FSx 或 SVM 的管理端口上建立 SSH 会话。将 *`management_endpoint_ip`* 替换为文件系统管理端口的 IP 地址。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   有关更多信息，请参阅 使用 ONTAP CLI 管理文件系统。
3. 在客户端（而不是在您的文件系统）上使用 cat 列出 `rootCA.pem`、`cert.pem` 和 `decrypted.key` 文件的内容，以便复制每个文件的输出并在系统提示时粘贴到以下步骤中。

   ```
   $ > cat cert.pem
   ```

   复制证书内容。
4. 除非已经安装（例如 ONTAP 自签名 root-CA），否则必须将双向身份验证期间使用的所有 CA ONTAP 证书（包括两者 ONTAP-side 以及客户端 CA）安装到证书管理中。

   按如下方式使用 `security certificate install` NetApp CLI 命令安装客户证书：

```
FSxID123:: > security certificate install -vserver dr -type client -cert-name
 ipsec-client-cert
```

```
Please enter Certificate: Press <Enter> when done
```

粘贴您之前复制的 `cert.pem` 文件的内容，然后按 Enter。

```
Please enter Private Key: Press <Enter> when done
```

粘贴 `decrypted.key` 文件的内容，然后按 Enter。

```
Do you want to continue entering root and/or intermediate certificates {y|n}:
```

输入 n 以完成客户端证书的输入。

5. 创建并安装证书以供 SVM 使用。此证书的颁发者 CA 必须已安装到 ONTAP 并已添加到 IPsec 中。

   使用以下命令来安装根证书：

```
FSxID123:: > security certificate install -vserver dr -type server-ca -cert-name
 ipsec-ca-cert
```

```
Please enter Certificate: Press <Enter> when done
```

   粘贴 `rootCA.pem` 文件的内容，然后按 Enter。

6. 要确保身份验证期间安装的 CA 位于 IPsec CA 搜索路径中，请使用“security ipsec ca-certificate add”命令将 ONTAP 证书管理 CA 添加到 IPsec 模块。

   输入以下命令来添加根证书。

```
FSxID123:: > security ipsec ca-certificate add -vserver dr -ca-certs ipsec-ca-cert
```

7. 输入以下命令，在安全策略数据库（SPD）中创建所需的 IPsec 策略。

```
security ipsec policy create -vserver dr -name policy-name -local-ip-
subnets 198.19.254.13/32 -remote-ip-subnets 172.31.0.0/16 -auth-method PKI -action
```

```
ESP_TRA -cipher-suite SUITEB_GCM256 -cert-name ipsec-client-cert -local-identity
"CN=*.ec2.internal" -remote-identity "CN=*.ec2.internal"
```

8. 使用以下命令显示 IPsec 策略，以便文件系统确认。

```
FSxID123:: > security ipsec policy show -vserver dr -instance

                                  Vserver: dr
                              Policy Name: promise
                           Local IP Subnets: 198.19.254.13/32
                          Remote IP Subnets: 172.31.0.0/16
                                Local Ports: 0-0
                               Remote Ports: 0-0
                                  Protocols: any
                                     Action: ESP_TRA
                                Cipher Suite: SUITEB_GCM256
          IKE Security Association Lifetime: 86400
        IPsec Security Association Lifetime: 28800
IPsec Security Association Lifetime (bytes): 0
                          Is Policy Enabled: true
                             Local Identity: CN=*.ec2.internal
                            Remote Identity: CN=*.ec2.internal
                     Authentication Method: PKI
             Certificate for Local Identity: ipsec-client-cert
```

在客户端上启动 IPsec

现在，FSx for ONTAP 文件系统和客户端上都配置了 IPsec，您可以在客户端上启动 IPsec。

1. 使用 SSH 连接到文件系统。
2. 启动 IPsec。

```
$ sudo ipsec start
```

3. 检查 IPsec 的状态。

```
$ sudo ipsec status
```

4. 在您的文件系统上挂载卷。

```
$ sudo mount -t nfs 198.19.254.13:/benchmark /home/ec2-user/acm/dr
```

5. 在 FSx for ONTAP 文件系统上显示加密连接，以验证 IPsec 设置。

```
FSxID123:: > security ipsec show-ikesa -node FsxId123
FsxId08ac16c7ec2781a58::> security ipsec show-ikesa -node FsxId08ac16c7ec2781a58-01
            Policy Local           Remote
Vserver     Name   Address         Address         Initator-SPI     State
----------- ------ --------------- --------------- ---------------- -----------
dr          policy-name
                   198.19.254.13   172.31.77.6     551c55de57fe8976 ESTABLISHED
fsx         policy-name
                   198.19.254.38   172.31.65.193   4fd3f22c993e60c5 ESTABLISHED
2 entries were displayed.
```

为多个客户端设置 IPsec

当少数客户端需要利用 IPsec 时，为每个客户端使用一个 SPD 条目就足够了。但是，如果成百上千个客户端需要利用 IPsec，我们建议您使用 IPsec 多客户端配置。

FSx for ONTAP 支持在启用 IPsec 的情况下将跨多个网络的多个客户端连接到单个 SVM IP 地址。您可以使用 `subnet` 配置或 `Allow all clients` 配置来完成此操作，详细过程如下：

使用子网配置为多个客户端配置 IPsec

允许特定子网上的所有客户端 (192.168.134. 0/24 例如）要使用单个 SPD 策略条目连接到单个 SVM IP 地址，则必须以子网`remote-ip-subnets`形式指定。此外，您必须使用正确的客户端标识来指定 `remote-identity` 字段。

> **Important**
>
> 使用证书身份验证时，每个客户端都可以使用其唯一证书或共享证书进行身份验证。FSx for ONTAP IPsec 会根据其本地信任存储上安装的 CA 来检查证书的有效性。FSx for ONTAP 还支持证书吊销列表（CRL）检查。

1. 要访问 ONTAP CLI，请运行以下命令，在适用于 NetApp ONTAP 文件系统的 Amazon FSx 或 SVM 的管理端口上建立 SSH 会话。将 *management_endpoint_ip* 替换为文件系统管理端口的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

有关更多信息，请参阅 使用 ONTAP CLI 管理文件系统。

2. 按如下方式使用 `security ipsec policy create` NetApp ONTAP CLI 命令，用您的特定*sample*值替换这些值。

```
FsxId123456::> security ipsec policy create -vserver svm_name -name policy_name \
  -local-ip-subnets 192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 \
  -local-ports 2049 -protocols tcp -auth-method PSK \
  -cert-name my_nfs_server_cert -local-identity ontap_side_identity \
  -remote-identity client_side_identity
```

使用允许所有客户端的配置为多个客户端配置 IPsec

要允许任何客户端（无论其源 IP 地址如何）连接到 SVM IPsec-enabled IP 地址，请在指定`remote-ip-subnets`字段时使用通`0.0.0.0/0`配符。

此外，您必须使用正确的客户端标识来指定 `remote-identity` 字段。对于证书身份验证，您可以输入 `ANYTHING`。

另外，在 0.0.0 的时候。 0/0 使用通配符，必须配置特定的本地或远程端口号才能使用。例如，NFS 端口 2049。

1. 要访问 ONTAP CLI，请运行以下命令，在适用于 NetApp ONTAP 文件系统的 Amazon FSx 或 SVM 的管理端口上建立 SSH 会话。将 *management_endpoint_ip* 替换为文件系统管理端口的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

有关更多信息，请参阅 使用 ONTAP CLI 管理文件系统。

2. 按如下方式使用 `security ipsec policy create` NetApp ONTAP CLI 命令，用您的特定*sample*值替换这些值。

```
FsxId123456::> security ipsec policy create -vserver svm_name -name policy_name \
  -local-ip-subnets 192.168.134.34/32 -remote-ip-subnets 0.0.0.0/0 \
  -local-ports 2049 -protocols tcp -auth-method PSK \
  -cert-name my_nfs_server_cert -local-identity ontap_side_identity \
  -local-ports 2049 -remote-identity client_side_identity
```

适用于 ONTAP 的 Amazon FSx 的身份和访问管理 NetApp

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制谁可以通过身份验证（登录）和获得授权（具有权限）来使用 Amazon FSx 资源。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题

受众

您的使用方式 AWS 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（请参阅针对 NetApp ONTAP 身份和访问权限的 Amazon FSx 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（请参阅适用于 NetApp ONTAP 的 Amazon FSx 如何与 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Identity-based 适用于 ONTAP 的 Amazon FSx 的策略示例 NetApp）

使用身份进行身份验证

身份验证是您 AWS 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 AWS 账户根用户，或者通过担任 IAM 角色进行身份验证。

您可以使用来自身份源的证书 AWS IAM Identity Center （例如（IAM Identity Center）、单点登录身份验证或 Google/Facebook 证书，以联合身份登录。有关登录的更多信息，请参阅《AWS 登录 用户指南》中的如何登录您的 AWS 账户。

对于编程访问， AWS 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AWS 签名版本 4。

AWS 账户 根用户

创建时 AWS 账户，首先会有一个名为 AWS 账户 root 用户的登录身份，该身份可以完全访问所有资源 AWS 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 AWS 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 Directory Service ，或者 AWS 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。

要集中管理访问权限，建议使用。 AWS IAM Identity Center有关更多信息，请参阅《AWS IAM Identity Center 用户指南》中的什么是 IAM Identity Center？。

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 AWS 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 AWS CLI 或 AWS 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 EC2 上运行的应用程序非常有用。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 AWS 通过创建策略并将其附加到 AWS 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。 AWS 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 AWS 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。

Identity-based 政策

Identity-based 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。

Identity-based 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。

Resource-based 政策

Resource-based 策略是您附加到资源的 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。

Resource-based 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 AWS 托管策略。

其他策略类型

AWS 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（SCP）– 指定 AWS Organizations中组织或组织单元的最大权限。有关更多信息，请参阅《AWS Organizations 用户指南》中的服务控制策略。

- 资源控制策略（RCP）– 设置对账户中资源的最大可用权限。有关更多信息，请参阅《AWS Organizations 用户指南》中的资源控制策略（RCP）。
- 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 AWS 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

适用于 NetApp ONTAP 的 Amazon FSx 如何与 IAM 配合使用

在使用 IAM 管理对 Amazon FSx 的访问之前，了解哪些 IAM 功能可与 Amazon FSx 配合使用。

你可以在适用于 ONTAP 的 Amazon FSx 上使用的 IAM 功能 NetApp

IAM 功能	Amazon FSx 支持
Identity-based 政策	是
Resource-based 政策	否
策略操作	是
策略资源	是
策略条件键	是
ACL	否
ABAC（策略中的标签）	是
临时凭证	是
转发访问会话（FAS）	是
服务角色	否
Service-linked 角色	是

要全面了解 Amazon FSx 和其他 AWS 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中与 IAM 配合使用的AWS 服务。

Identity-based 亚马逊 FSx 的政策

支持基于身份的策略：是

Identity-based 策略是您可以附加到身份（例如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户管理型策略定义自定义 IAM 权限。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

Identity-based 亚马逊 FSx 的政策示例

要查看 Amazon FSx 基于身份的策略示例，请参阅 Identity-based 适用于 ONTAP 的 Amazon FSx 的策略示例 NetApp。

Resource-based 亚马逊 FSx 内部的政策

支持基于资源的策略：否

Amazon FSx 的策略操作

支持策略操作：是

管理员可以使用 AWS 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。

要查看 Amazon FSx 操作的列表，请参阅《服务授权参考》中的 Actions defined by Amazon FSx。

Amazon FSx 中的策略操作在操作前面使用以下前缀：

```
fsx
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
```

```
      "fsx:action1",
      "fsx:action2"
         ]
```

要查看 Amazon FSx 基于身份的策略示例，请参阅 Identity-based 适用于 ONTAP 的 Amazon FSx 的策略示例 NetApp。

Amazon FSx 的策略资源

支持策略资源：是

管理员可以使用 AWS 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": "*"
```

要查看 Amazon FSx 资源类型及其 ARN 的列表，请参阅《服务授权参考》中的 Amazon FSx 定义的资源。要了解您可以在哪些操作中指定每个资源的 ARN，请参阅 Amazon FSx 定义的资源。

要查看 Amazon FSx 基于身份的策略示例，请参阅 Identity-based 适用于 ONTAP 的 Amazon FSx 的策略示例 NetApp。

Amazon FSx 的策略条件键

支持特定于服务的策略条件键：是

管理员可以使用 AWS 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 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

要查看 Amazon FSx 条件键的列表，请参阅《服务授权参考》中的 Amazon FSx 的条件键。要了解您可以对哪些操作和资源使用条件键，请参阅 Amazon FSx 定义的操作。

要查看 Amazon FSx 基于身份的策略示例，请参阅 Identity-based 适用于 ONTAP 的 Amazon FSx 的策略示例 NetApp。

Amazon FSx 中的访问控制列表（ACL）

支持 ACL：否

Attribute-based 使用 Amazon FSx 进行访问控制 (ABAC)

支持 ABAC（策略中的标签）：是

Attribute-based 访问控制 (ABAC) 是一种授权策略，它根据称为标签的属性来定义权限。您可以将标签附加到 IAM 实体和 AWS 资源，然后设计 ABAC 策略以允许在委托人的标签与资源上的标签匹配时进行操作。

要基于标签控制访问，您需要使用 `aws:ResourceTag/key-name`aws:RequestTag/*key-name* 或 `aws:TagKeys` 条件键在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为部分。

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权定义权限。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问权限控制（ABAC）。

有关标记 Amazon FSx 资源的更多信息，请参阅为 Amazon FSx 资源贴标签。

要查看基于身份的策略（用于根据资源上的标签来限制对该资源的访问）的示例，请参阅 使用标签控制对 Amazon FSx 资源的访问权限。

将临时凭证用于 Amazon FSx

支持临时凭证：是

临时证书提供对 AWS 资源的短期访问权限，并且是在您使用联合身份或切换角色时自动创建的。AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的临时安全凭证和使用 IAM 的。AWS 服务

Amazon FSx 的转发访问会话

支持转发访问会话（FAS）：是

转发访问会话 (FAS) 使用调用主体的权限 AWS 服务，再加上 AWS 服务 向下游服务发出请求的请求。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

Amazon FSx 的服务角色

支持服务角色：否

Service-linked 亚马逊 FSx 的角色

支持服务关联角色：是

服务相关角色是一种与服务相关联的 AWS 服务服务角色。该服务可以代替您执行操作。 Service-linked 角色出现在您的， AWS 账户 并且归服务所有。IAM 管理员可以查看但不能编辑服务关联角色的权限。

有关创建或管理 Amazon FSx 服务关联角色的详细信息，请参阅 使用 Amazon FSx 的服务关联角色。

Identity-based 适用于 ONTAP 的 Amazon FSx 的策略示例 NetApp

默认情况下，用户和角色没有创建或修改 Amazon FSx 资源的权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅《IAM 用户指南》中的创建 IAM 策略（控制台）。

有关 Amazon FSx 定义的操作和资源类型的详细信息，包括每种资源类型的 ARN 格式，请参阅《服务授权参考》中的 Amazon FSx 的操作、资源和条件键。

主题

- 策略最佳实践
- 使用 Amazon FSx 控制台
- 允许用户查看他们自己的权限

策略最佳实践

Identity-based 策略决定了是否有人可以在您的账户中创建、访问或删除 Amazon FSx 资源。这些操作可能会使 AWS 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 AWS 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AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 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AWS 托管策略或工作职能的AWS 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 AWS 服务，例如 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 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的使用 MFA 保护 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实践。

使用 Amazon FSx 控制台

要访问适用于 NetApp ONTAP 的 Amazon FSx 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的 Amazon FSx 资源的详细信息。 AWS 账户如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

为确保用户和角色仍然可以使用 Amazon FSx 控制台，还要将`AmazonFSxConsoleReadOnlyAccess` AWS 托管策略附加到实体。有关更多信息，请参阅《IAM 用户指南》中的为用户添加权限。

可以在AWS 适用于 ONTAP 的 Amazon FSx 的托管策略 NetApp中查看`AmazonFSxConsoleReadOnlyAccess` 和其他 Amazon FSx 托管式服务策略。

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 AWS CLI 或 AWS 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": "*"
        }
    ]
}
```

针对 NetApp ONTAP 身份和访问权限的 Amazon FSx 进行故障排除

使用以下信息可帮助您诊断和修复在使用 Amazon FSx 和 IAM 时可能遇到的常见问题。

主题

- 我无权在 Amazon FSx 中执行操作
- 我无权执行 iam：PassRole
- 我想允许我以外的人进入 AWS 账户 访问我的 Amazon FSx 资源

我无权在 Amazon FSx 中执行操作

如果您收到错误提示，指明您无权执行某个操作，则必须更新策略以允许执行该操作。

当 mateojackson IAM 用户尝试使用控制台查看有关虚构 *my-example-widget* 资源的详细信息，但不拥有虚构 fsx:*GetWidget* 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 fsx:GetWidget on resource: my-example-widget
```

在此情况下，必须更新 mateojackson 用户的策略，以允许使用 fsx:*GetWidget* 操作访问 *my-example-widget* 资源。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我无权执行 iam：PassRole

如果您收到一个错误，指明您无权执行 iam:PassRole 操作，则必须更新策略以允许您将角色传递给 Amazon FSx。

有些 AWS 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 FSx 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 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人进入 AWS 账户 访问我的 Amazon FSx 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以代入角色。对于支持基于资源的策略或访问控制列表（ACL）的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解 Amazon FSx 是否支持这些功能，请参阅 适用于 NetApp ONTAP 的 Amazon FSx 如何与 IAM 配合使用。
- 要了解如何提供对您拥有的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 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 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 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。

使用 Amazon FSx 的服务关联角色

Amazon FSx 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种独特的 IAM 角色，直接关联到 Amazon FSx。 Service-linked 角色由 Amazon FSx 预定义，包括该服务代表您调用其他 AWS 服务所需的所有权限。

服务关联角色可让您更轻松地设置 Amazon FSx，因为您不必手动添加必要的权限。Amazon FSx 定义其服务关联角色的权限，除非另外定义，否则只有 Amazon FSx 可以代入该角色。定义的权限包括信任策略和权限策略，以及不能附加到任何其他 IAM 实体的权限策略。

只有在首先删除相关资源后，您才能删除服务关联角色。这将保护您的 Amazon FSx 资源，因为您不会无意中删除对资源的访问权限。

有关支持服务相关角色的其它服务的信息，请参阅使用 IAM 的AWS 服务并查找Service-Linked 角色列中显示为是的服务。请选择是与查看该服务的服务关联角色文档的链接。

Service-linked 亚马逊 FSx 的角色权限

Amazon FSx 使用名为 AWSServiceRoleForAmazonFSx— 的服务相关角色在您的账户中执行某些操作，例如在 VPC 中为文件系统创建弹性网络接口，并在中发布文件系统和卷指标。 CloudWatch

有关此策略的更新，请参阅 AmazonFSxServiceRolePolicy。

权限详细信息

AWSServiceRoleForAmazonFSx 角色权限由 AmazonFSxServiceRolePolicy AWS 托管策略定义。AWSServiceRoleForAmazonFSx 具有以下权限：

> **Note**
>
> 所有 Amazon FSx 文件系统类型都使用；列出的某些权限不适用于适用于 ONTAP 的 FSx。
> AWSServiceRoleForAmazonFSx

- ds— 允许 Amazon FSx 查看、授权和取消对您目录中的应用程序的授权。 Directory Service
- ec2：允许 Amazon FSx 执行以下操作：
  - 查看、创建与 Amazon FSx 文件系统关联的网络接口以及取消关联。
  - 查看一个或多个与 Amazon FSx 文件系统关联的弹性 IP 地址。
  - 查看与 Amazon FSx 文件系统关联的 Amazon VPC、安全组和子网。
  - 为带有 AmazonFSx.FileSystemId 标签的客户网络接口分配 IPv6 地址。
  - 从带有 AmazonFSx.FileSystemId 标签的客户网络接口取消分配 IPv6 地址。
  - 为可以与 VPC 配合使用的所有安全组提供增强的安全组验证。
  - 为获得 AWS授权的用户创建在网络接口上执行某些操作的权限。
- cloudwatch— 允许 Amazon FSx 在 AWS/fsX 命名空间 CloudWatch 下发布指标数据点。
- route53 – 允许 Amazon FSx 将 Amazon VPC 与私有托管区关联。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CreateFileSystem",
            "Effect": "Allow",
            "Action": [
                "ds:AuthorizeApplication",
                "ds:GetAuthorizedApplicationDetails",
                "ds:UnauthorizeApplication",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeAddresses",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeNetworkInterfaces",
```

```
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVPCs",
                "ec2:DisassociateAddress",
                "ec2:GetSecurityGroupsForVpc",
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PutMetrics",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/FSx"
                }
            }
        },

        {
            "Sid": "TagResourceNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "AmazonFSx.FileSystemId"
                }
            }
        },
```

```
        {
            "Sid": "ManageNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonFSx.FileSystemId": "false"
                }
            }
        },
        {
            "Sid": "ManageRouteTable",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateRoute",
                "ec2:ReplaceRoute",
                "ec2:DeleteRoute"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/AmazonFSx": "ManagedByAmazonFSx"
                }
            }
        }
    ]
}
```

亚马逊 FSx 更新至 AWS 托管策略 中介绍了本政策的所有更新。

您必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务关联角色。有关更多信息，请参阅 IAM 用户指南中的Service-Linked 角色权限。

为 Amazon FSx 创建服务关联角色

您无需手动创建服务关联角色。当您在 AWS 管理控制台、IAM CLI 或 IAM API 中创建文件系统时，Amazon FSx 会为您创建服务相关角色。

> **Important**
>
> 如果您在其他使用此角色支持的功能的服务中完成某个操作，此服务关联角色可以出现在您的账户中。要了解更多信息，请参阅我的 IAM 账户中的新角色。

如果您删除该服务关联角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。当您创建文件系统时，Amazon FSx 会再次为您创建服务关联角色。

为 Amazon FSx 编辑服务关联角色

Amazon FSx 不允许您编辑 AWSServiceRoleForAmazonFSx 服务相关角色。创建服务关联角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。但是可以使用 IAM 编辑角色描述。有关更多信息，请参阅 IAM 用户指南中的编辑 Service-Linked 角色。

删除 Amazon FSx 的服务关联角色

如果不再需要使用某个需要服务关联角色的功能或服务，我们建议您删除该角色。这样就没有未被主动监控或维护的未使用实体。但是，您必须先删除所有文件系统和备份，然后才能手动删除服务关联角色。

> **Note**
>
> 如果当您试图删除资源时 Amazon FSx 服务正在使用该角色，则删除操作可能会失败。如果发生这种情况，请等待几分钟后重试。

使用 IAM 手动删除服务关联角色

使用 IAM 控制台、IAM CLI 或 IAM API 删除 AWSServiceRoleForAmazonFSx 服务相关角色。有关更多信息，请参阅 IAM 用户指南中的删除 Service-Linked 角色。

Amazon FSx 服务关联角色支持的区域

Amazon FSx 支持在该服务可用的所有区域中使用服务关联角色。有关更多信息，请参阅 AWS 区域和端点。

在 Amazon FSx 上使用标签

您可以使用标签来控制对 Amazon FSx 资源的访问权限并实现基于属性的访问权限控制（ABAC）。要在创建期间对 Amazon FSx 资源应用标签，用户必须具有某些 AWS Identity and Access Management（IAM）权限。

在创建过程中授予标记资源的权限

您通过一些资源创建 Amazon FSx API 操作在创建资源时指定标签。您可以使用这些资源标签来实现基于属性的访问权限控制（ABAC）。有关更多信息，请参阅 ABAC 有什么用 AWS？ 在 IAM 用户指南中。

为使用户在创建时为资源添加标签，他们必须具有使用创建该资源的操作（如 `fsx:CreateFileSystem`、`fsx:CreateStorageVirtualMachine` 或 `fsx:CreateVolume`）的权限。如果在资源创建操作中指定了标签，则 IAM 会对 `fsx:TagResource` 操作执行额外的授权，以验证用户是否具备创建标签的权限。因此，用户还必须具有使用 `fsx:TagResource` 操作的显式权限。

以下示例策略允许用户创建文件系统和存储虚拟机 (SVM)，并在特定 AWS 账户环境中创建期间对其应用标签。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateFileSystem",
         "fsx:CreateStorageVirtualMachine",
         "fsx:TagResource"
      ],
      "Resource": [
         "arn:aws:fsx:region:account-id:file-system/*",
         "arn:aws:fsx:region:account-id:file-system/*/storage-virtual-machine/*"
      ]
    }
  ]
}
```

同样，下面的策略允许用户在特定文件系统上创建备份，并在创建备份的过程中向备份应用任何标签。

```
{
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateBackup"
      ],
      "Resource": "arn:aws:fsx:region:account-id:file-system/file-system-id*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:region:account-id:backup/*"
    }
  ]
}
```

仅当用户在资源创建时应用了标签的情况下，系统才会评估 `fsx:TagResource` 操作。因此，如果未在此请求中指定任何标签，则拥有创建资源权限（假定没有标记条件）的用户无需具备使用 `fsx:TagResource` 操作的权限。但是，如果用户不具备使用 `fsx:TagResource` 操作的权限而又试图创建带标签的资源，则请求将失败。

有关标记 Amazon FSx 资源的更多信息，请参阅为 Amazon FSx 资源贴标签。有关如何使用标签控制对 Amazon FSx 资源的访问权限的更多信息，请参阅 使用标签控制对 Amazon FSx 资源的访问权限。

使用标签控制对 Amazon FSx 资源的访问权限

要控制对 Amazon FSx 资源和操作的访问权限，您可以根据标签使用 IAM 策略。您可以使用两种方法提供此类控制：

- 您可以根据这些资源上的标签控制对 Amazon FSx 资源的访问权限。
- 您可以控制在 IAM 请求条件中传递哪些标签。

有关如何使用标签控制 AWS 资源访问的信息，请参阅 IAM 用户指南中的使用标签控制访问权限。有关在创建时标记 Amazon FSx 资源的更多信息，请参阅在创建过程中授予标记资源的权限。有关标记资源的更多信息，请参阅为 Amazon FSx 资源贴标签。

根据资源上的标签控制访问权限

要控制用户或角色可以对 Amazon FSx 资源执行的操作，您可以使用资源上的标签。例如，您可能希望根据文件系统资源上的标签的键/值对允许或拒绝对该资源执行特定的 API 操作。

Example策略示例 – 仅在使用特定标签时创建文件系统

只有当用户使用特定标签键值对标记文件系统时，此策略才允许用户创建文件系统，在本示例中为 `key=Department`，`value=Finance`。

```
{
    "Effect": "Allow",
    "Action": [
        "fsx:CreateFileSystem",
        "fsx:TagResource"
    ],
    "Resource": "arn:aws:fsx:region:account-id:file-system/*",
    "Condition": {
        "StringEquals": {
            "aws:RequestTag/Department": "Finance"
        }
    }
}
```

Example策略示例 — 仅为带有特定标签的 NetApp ONTAP 卷创建 Amazon FSx 的备份

此策略仅允许用户为带有 `key=Department`, `value=Finance` 键值对标签的 FSx for ONTAP 卷创建备份。使用标签 `Department=Finance` 创建备份。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:volume/*",
            "Condition": {
                "StringEquals": {
```

```
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource",
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example策略示例 – 通过带有特定标签的备份创建带有特定标签的卷

此策略允许用户仅通过带有 Department=Finance 标签的备份创建带有 Department=Finance 标签的卷。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateVolumeFromBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateVolumeFromBackup"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example策略示例 – 删除带有特定标签的文件系统

此策略允许用户删除带有 Department=Finance 标签的文件系统。如果他们创建了最终备份，则必须使用 Department=Finance 标记。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteFileSystem"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource"
```

```
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example示例策略 – 删除带有特定标签的卷

此策略允许用户仅删除带有 Department=Finance 标签的卷。如果他们创建了最终备份，则必须使用 Department=Finance 标记。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteVolume"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
```

```
                }
            }
        }
    ]
}
```

AWS 适用于 ONTAP 的 Amazon FSx 的托管策略 NetApp

AWS 托管策略是由创建和管理的独立策略 AWS。 AWS 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住， AWS 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 AWS 客户使用。我们建议通过定义特定于使用案例的客户管理型策略来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。 AWS 最有可能在启动新的 API 或现有服务可以使用新 AWS 服务 的 API 操作时更新 AWS 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略。

AmazonFSxServiceRolePolicy

允许 Amazon FSx 代表您管理 AWS 资源。请参阅 使用 Amazon FSx 的服务关联角色，了解更多信息。

AWS 托管策略： AmazonFSxDeleteServiceLinkedRoleAccess

您不能将 AmazonFSxDeleteServiceLinkedRoleAccess 附加到自己的 IAM 实体。该策略关联到服务，仅用于该服务的服务关联角色。您不能附加、分离、修改或删除此策略。有关更多信息，请参阅使用 Amazon FSx 的服务关联角色。

该策略授予管理权限，允许 Amazon FSx 删除用于访问 Amazon S3 的服务关联角色，仅供适用于 Lustre 的 Amazon FSx 使用。

权限详细信息

此策略包括 iam 中的以下权限：允许 Amazon FSx 对用于访问 Amazon S3 的 FSx 服务关联角色进行查看、删除及查看其删除状态。

要查看此策略的权限，请参阅AmazonFSxDeleteServiceLinkedRoleAccess《 AWS 托管策略参考指南》。

AWS 托管策略： AmazonFSxFullAccess

您可以附加 AmazonFSxFullAccess 到您的 IAM 实体。Amazon FSx 还会将此策略附加到允许 Amazon FSx 代表您执行操作的服务角色。

提供对 Amazon FSx 的完全访问权限和对相关 AWS 服务的访问权限。

权限详细信息

该策略包含以下权限。

- `fsx`：允许主体完全访问，可执行所有 Amazon FSx 操作，但 `BypassSnaplockEnterpriseRetention` 除外。
- `ds`— 允许委托人查看有关 Directory Service 目录的信息。
- `ec2`
  - 允许主体在指定的条件下创建标签。
  - 为可以与 VPC 配合使用的所有安全组提供增强的安全组验证。
- `iam`：允许主体代表用户创建 Amazon FSx 服务关联角色。这是必需的，这样 Amazon FSx 才能代表用户管理 AWS 资源。
- `firehose`：允许主体将记录写入 Amazon Data Firehose。必须具有此权限，用户才能将审计访问日志发送到 Firehose，进而监控 FSx for Windows File Server 文件系统的访问情况。
- `logs`：允许主体创建日志组、日志流并将事件写入日志流。这是必需的，这样用户才能通过向日志发送审核访问日志 CloudWatch 来监控 FSx 的 Windows File Server 文件系统访问权限。

要查看此策略的权限，请参阅AmazonFSxFullAccess《 AWS 托管策略参考指南》。

AWS 托管策略： AmazonFSxConsoleFullAccess

您可以将 `AmazonFSxConsoleFullAccess` 策略附加到 IAM 身份。

此策略授予管理权限，允许对 Amazon FSx 进行完全访问和通过访问相关 AWS 服务。 AWS 管理控制台

权限详细信息

该策略包含以下权限。

- fsx：允许主体在 Amazon FSx 管理控制台中执行所有操作，但 BypassSnaplockEnterpriseRetention 除外。
- cloudwatch— 允许委托人在 Amazon FSx 管理控制台中查看 CloudWatch 警报和指标。
- ds— 允许委托人列出有关 Directory Service 目录的信息。
- ec2
  - 允许主体在路由表上创建标签，列出网络接口、路由表、安全组、子网和与 Amazon FSx 文件系统关联的 VPC。
  - 允许主体为可与 VPC 配合使用的所有安全组提供增强的安全组验证。
  - 允许主体查看与 Amazon FSx 文件系统关联的弹性网络接口。
- kms— 允许委托人列出密钥的别名。 AWS Key Management Service
- s3：允许主体列出 Amazon S3 桶中的部分或全部对象（最多 1000 个）。
- secretsmanager— 允许委托人列出 AWS Secrets Manager 用于选择域加入服务帐户凭据的密码。
- iam：授予创建服务关联角色的权限，允许 Amazon FSx 代表用户执行操作。

要查看此策略的权限，请参阅AmazonFSxConsoleFullAccess《 AWS 托管策略参考指南》。

AWS 托管策略： AmazonFSxConsoleReadOnlyAccess

您可以将 AmazonFSxConsoleReadOnlyAccess 策略附加到 IAM 身份。

此政策向 Amazon FSx 和相关 AWS 服务授予只读权限，以便用户可以在中查看有关这些服务的信息。 AWS 管理控制台

权限详细信息

该策略包含以下权限。

- fsx – 允许主体在 Amazon FSx 管理控制台中查看有关 Amazon FSx 文件系统的信息，包括所有标签。
- cloudwatch— 允许委托人在 Amazon FSx 管理控制台中查看 CloudWatch 警报和指标。
- ds— 允许委托人在 Amazon FSx Directory Service 管理控制台中查看有关目录的信息。
- ec2

  - 允许主体在 Amazon FSx 管理控制台中查看网络接口、安全组、子网以及与 Amazon FSx 文件系统关联的 VPC。
  - 允许主体为可与 VPC 配合使用的所有安全组提供增强的安全组验证。
  - 允许主体查看与 Amazon FSx 文件系统关联的弹性网络接口。
- kms— 允许委托人在 Amazon FSx 管理控制 AWS Key Management Service 台中查看密钥的别名。
- log— 允许委托人描述与提出请求的账户关联的 Amazon Logs CloudWatch 日志组。必须具有此权限，主体才能查看 FSx for Windows File Server 文件系统的现有文件访问审计配置。
- secretsmanager— 允许委托人列出 AWS Secrets Manager 用于选择域加入服务帐户凭据的密码。
- firehose：允许主体描述与发出请求的账户关联的 Amazon Data Firehose 传输流。必须具有此权限，主体才能查看 FSx for Windows File Server 文件系统的现有文件访问审计配置。

要查看此策略的权限，请参阅AmazonFSxConsoleReadOnlyAccess《 AWS 托管策略参考指南》。

AWS 托管策略： AmazonFSxReadOnlyAccess

您可以将 AmazonFSxReadOnlyAccess 策略附加到 IAM 身份。

- fsx：允许主体在 Amazon FSx 管理控制台中查看有关 Amazon FSx 文件系统的信息，包括所有标签。
- ec2：为可以与 VPC 配合使用的所有安全组提供增强的安全组验证。

要查看此策略的权限，请参阅AmazonFSxReadOnlyAccess《 AWS 托管策略参考指南》。

亚马逊 FSx 更新至 AWS 托管策略

查看自该服务开始跟踪这些更改以来对 Amazon FSx AWS 托管政策的更新的详细信息。要获得有关此页面更改的自动提示，请订阅 Amazon FSx 适用于 ONTAP 的 Amazon FSx 的文档历史记录NetApp页面上的 RSS 源。

更改	描述	日期
AmazonFSxConsoleFullAccess：对现有策略的更新	Amazon FSx 添加了一项新权限secretsmanager:ListSecrets ，允许委托人列出	2025 年 11 月 5 日

更改	描述	日期
	AWS Secrets Manager 用于选择域加入服务账户凭证的密码。	
AmazonFSxConsoleReadOnlyAccess：对现有策略的更新	Amazon FSx 添加了一项新权限`secretsmanager:ListSecrets`，允许委托人列出 AWS Secrets Manager 用于选择域加入服务账户凭证的密码。	2025 年 11 月 3 日
AmazonFSxServiceRolePolicy：对现有策略的更新	Amazon FSx 添加了新权限`ec2:AssignIpv6Addresses`，允许主体为带有`AmazonFSx.FileSystemId`标签的客户网络接口分配 IPv6 地址。	2025 年 7 月 22 日
AmazonFSxServiceRolePolicy：对现有策略的更新	Amazon FSx 添加了新权限`ec2:UnassignIpv6Addresses`，允许主体从带有`AmazonFSx.FileSystemId`标签的客户网络接口取消分配 IPv6 地址。	2025 年 7 月 22 日
AmazonFSxConsoleFullAccess：对现有策略的更新	Amazon FSx 添加了新权限`fsx:CreateAndAttachS3AccessPoint`，允许主体创建 S3 接入点并将其连接到 FSx 卷。	2025 年 6 月 25 日
AmazonFSxConsoleFullAccess：对现有策略的更新	Amazon FSx 添加了一项新权限`fsx:DescribeS3AccessPointAttachments`，允许委托人列出所有 S3 接入点。 AWS 账户 AWS 区域	2025 年 6 月 25 日

更改	描述	日期
AmazonFSxConsoleFullAccess：对现有策略的更新	Amazon FSx 添加了新权限 `fsx:DetachAndDeleteS3AccessPoint` ，允许主体删除 S3 接入点。	2025 年 6 月 25 日
AmazonFSxFullAccess：对现有策略的更新	Amazon FSx 添加了新权限 `fsx:CreateAndAttachS3AccessPoint` ，允许主体创建 S3 接入点并将其连接到 FSx 卷。	2025 年 6 月 25 日
AmazonFSxFullAccess：对现有策略的更新	Amazon FSx 添加了一项新权限`fsx:DescribeS3AccessPointAttachments` ，允许委托人列出所有 S3 接入 AWS 账户 点。 AWS 区域	2025 年 6 月 25 日
AmazonFSxFullAccess：对现有策略的更新	Amazon FSx 添加了新权限 `fsx:DetachAndDeleteS3AccessPoint` ，允许主体删除 S3 接入点。	2025 年 6 月 25 日
AmazonFSxConsoleReadOnlyAccess：对现有策略的更新	Amazon FSx 添加了新权限 `ec2:DescribeNetworkInterfaces` ，允许主体查看与其文件系统关联的弹性网络接口。	2025 年 2 月 25 日
AmazonFSxConsoleFullAccess：对现有策略的更新	Amazon FSx 添加了新权限 `ec2:DescribeNetworkInterfaces` ，允许主体查看与其文件系统关联的弹性网络接口。	2025 年 2 月 7 日

更改	描述	日期
AmazonFSxServiceRolePolicy：对现有策略的更新	Amazon FSx 添加了新的权限 `ec2:GetSecurityGroupsForVpc` ，允许主体为可以与 VPC 配合使用的所有安全组提供增强的安全组验证。	2024 年 1 月 9 日
AmazonFSxReadOnlyAccess：对现有策略的更新	Amazon FSx 添加了新的权限 `ec2:GetSecurityGroupsForVpc` ，允许主体为可以与 VPC 配合使用的所有安全组提供增强的安全组验证。	2024 年 1 月 9 日
AmazonFSxConsoleReadOnlyAccess：对现有策略的更新	Amazon FSx 添加了新的权限 `ec2:GetSecurityGroupsForVpc` ，允许主体为可以与 VPC 配合使用的所有安全组提供增强的安全组验证。	2024 年 1 月 9 日
AmazonFSxFullAccess：对现有策略的更新	Amazon FSx 添加了新的权限 `ec2:GetSecurityGroupsForVpc` ，允许主体为可以与 VPC 配合使用的所有安全组提供增强的安全组验证。	2024 年 1 月 9 日
AmazonFSxConsoleFullAccess：对现有策略的更新	Amazon FSx 添加了新的权限 `ec2:GetSecurityGroupsForVpc` ，允许主体为可以与 VPC 配合使用的所有安全组提供增强的安全组验证。	2024 年 1 月 9 日
AmazonFSxFullAccess：对现有策略的更新	Amazon FSx 添加了新的权限，可以使用户为 FSx for OpenZFS 文件系统执行跨区域和跨账户的数据复制。	2023 年 12 月 20 日

更改	描述	日期
AmazonFSxConsoleFullAccess：对现有策略的更新	Amazon FSx 添加了新的权限，可以使用户为 FSx for OpenZFS 文件系统执行跨区域和跨账户的数据复制。	2023 年 12 月 20 日
AmazonFSxFullAccess：对现有策略的更新	Amazon FSx 添加了新的权限，可以使用户按需复制适用于 FSx for OpenZFS 文件系统的卷。	2023 年 11 月 26 日
AmazonFSxConsoleFullAccess：对现有策略的更新	Amazon FSx 添加了新的权限，可以使用户按需复制适用于 FSx for OpenZFS 文件系统的卷。	2023 年 11 月 26 日
AmazonFSxFullAccess：对现有策略的更新	Amazon FSx 添加了新的权限，使用户能够查看、启用和禁用对 ONTAP 文件系统的 FSx 的共享 VPC 支持。 Multi-AZ	2023 年 11 月 14 日
AmazonFSxConsoleFullAccess：对现有策略的更新	Amazon FSx 添加了新的权限，使用户能够查看、启用和禁用对 ONTAP 文件系统的 FSx 的共享 VPC 支持。 Multi-AZ	2023 年 11 月 14 日
AmazonFSxFullAccess：对现有策略的更新	亚马逊 FSX 添加了新的权限，允许亚马逊 FSX 管理适用于 OpenZFS 文件系统的 FSX 的网络配置。 Multi-AZ	2023 年 8 月 9 日

更改	描述	日期
AWS 托管策略: AmazonFSx ServiceRolePolicy— 更新现有策略	Amazon FSx 修改了现有`cloudwatch:PutMetricData` 权限，以便亚马逊 FSx 将 CloudWatch 指标发布到命名空间。`AWS/FSx`	2023 年 7 月 24 日
AmazonFSxFullAccess：对现有策略的更新	Amazon FSx 更新了该策略，删除了 `fsx:*` 权限并添加了具体的 `fsx` 操作。	2023 年 7 月 13 日
AmazonFSxConsoleFullAccess：对现有策略的更新	Amazon FSx 更新了该策略，删除了 `fsx:*` 权限并添加了具体的 `fsx` 操作。	2023 年 7 月 13 日
AmazonFSxConsoleReadOnlyAccess：对现有策略的更新	Amazon FSx 增加了新的权限，用户能够在 Amazon FSx 控制台中查看 FSx for Windows File Server 文件系统的增强性能指标和建议的操作。	2022 年 9 月 21 日
AmazonFSxConsoleFullAccess：对现有策略的更新	Amazon FSx 增加了新的权限，用户能够在 Amazon FSx 控制台中查看 FSx for Windows File Server 文件系统的增强性能指标和建议的操作。	2022 年 9 月 21 日
AmazonFSxReadOnlyAccess— 已开始追踪政策	此策略授予对所有 Amazon FSx 资源及其相关标签的只读访问权限。	2022 年 2 月 4 日
AmazonFSxDeleteServiceLinkedRoleAccess— 已开始追踪政策	此策略授予管理权限，允许 Amazon FSx 删除用于访问 Amazon S3 的服务关联角色。	2022 年 1 月 7 日

更改	描述	日期
AmazonFSxServiceRolePolicy：对现有策略的更新	亚马逊 FSx 添加了新的权限，允许亚马逊 FSx 管理适用于 ONTAP 文件系统的亚马逊 FSx 的网络配置。 NetApp	2021 年 9 月 2 日
AmazonFSxFullAccess：对现有策略的更新	Amazon FSx 增加了新的权限，允许 Amazon FSx 在 EC2 路由表上创建标签，从而缩小了调用范围。	2021 年 9 月 2 日
AmazonFSxConsoleFullAccess：对现有策略的更新	亚马逊 FSx 添加了新的权限，允许亚马逊 FSx 为 ONTAP 文件系统创建亚马逊 FSx。 NetApp Multi-AZ	2021 年 9 月 2 日
AmazonFSxConsoleFullAccess：对现有策略的更新	Amazon FSx 增加了新的权限，允许 Amazon FSx 在 EC2 路由表上创建标签，从而缩小了调用范围。	2021 年 9 月 2 日
AmazonFSxServiceRolePolicy：对现有策略的更新	Amazon FSx 添加了新的权限，允许 Amazon FSx 描述和写入日志流。 CloudWatch 这是必需的，这样用户才能使用日志查看 FSx for Windows File Server 文件系统的 CloudWatch 文件访问审核日志。	2021 年 6 月 8 日

更改	描述	日期
AmazonFSxServiceRolePolicy：对现有策略的更新	Amazon FSx 添加了新的权限，允许 Amazon FSx 描述和写入 Amazon Data Firehose 传输流。 必须具有此权限，用户才能使用 Amazon Data Firehose 查看 FSx for Windows File Server 文件系统的文件访问审计日志。	2021 年 6 月 8 日
AmazonFSxFullAccess：对现有策略的更新	Amazon FSx 添加了新的权限，允许委托人描述和创建 CloudWatch 日志组、日志流以及将事件写入日志流。 这是必需的，这样委托人才能使用日志查看 FSx for Windows File Server 文件系统的 CloudWatch 文件访问审核日志。	2021 年 6 月 8 日
AmazonFSxFullAccess：对现有策略的更新	Amazon FSx 添加了新的权限，允许主体描述并将记录写入 Amazon Data Firehose。 必须具有此权限，用户才能使用 Amazon Data Firehose 查看 FSx for Windows File Server 文件系统的文件访问审计日志。	2021 年 6 月 8 日

更改	描述	日期
AmazonFSxConsoleFullAccess：对现有策略的更新	Amazon FSx 增加了新的权限，允许委托人描述与提出请求的账户关联的 Amazon Logs CloudWatch 日志组。 这是必需的，这样委托人才能在为 FSx for Windows File Server 文件系统配置文件访问审计时选择现有的 CloudWatch 日志日志组。	2021 年 6 月 8 日
AmazonFSxConsoleFullAccess：对现有策略的更新	Amazon FSx 添加了新的权限，允许主体描述与发出请求的账户关联的 Amazon Data Firehose 传输流。 必须具有此权限，主体才能在为 FSx for Windows File Server 文件系统配置文件访问审计时选择现有的 Firehose 传输流。	2021 年 6 月 8 日
AmazonFSxConsoleReadOnlyAccess：对现有策略的更新	Amazon FSx 增加了新的权限，允许委托人描述与提出请求的账户关联的 Amazon Logs CloudWatch 日志组。 必须具有此权限，主体才能查看 FSx for Windows File Server 文件系统的现有文件访问审计配置。	2021 年 6 月 8 日

更改	描述	日期
AmazonFSxConsoleReadOnlyAccess：对现有策略的更新	Amazon FSx 添加了新的权限，允许主体描述与发出请求的账户关联的 Amazon Data Firehose 传输流。 必须具有此权限，主体才能查看 FSx for Windows File Server 文件系统的现有文件访问审计配置。	2021 年 6 月 8 日
Amazon FSx 开启了跟踪更改	Amazon FSx 开始跟踪其 AWS 托管策略的变更。	2021 年 6 月 8 日

使用 Amazon VPC 进行文件系统访问控制

您可以使用其中一个终端节点的 DNS 名称或 IP 地址访问适用于 NetApp ONTAP 文件系统和 SVM 的 Amazon FSx，具体取决于访问类型。DNS 名称映射到文件系统的私有 IP 地址或您 VPC 中 SVM 的弹性网络接口。只有关联 VPC 中的资源，或者通过 Direct Connect 或 VPN 与关联 VPC 连接的资源，才能通过 NFS、SMB 或 iSCSI 协议访问文件系统中的数据。有关更多信息，请参阅《Amazon VPC 用户指南》中的什么是 Amazon VPC？。

> **Warning**
>
> 不得修改或删除与您的文件系统关联的弹性网络接口。修改或删除该网络接口可能会导致永久丢失您的 VPC 和文件系统之间的连接。

Amazon VPC 安全组

安全组充当 FSx for ONTAP 文件系统的虚拟防火墙，用于控制传入和传出流量。入站规则控制传入到文件系统的流量，出站规则控制从文件系统传出的流量。创建文件系统时，您需要指定要在其中创建文件系统的 VPC，并应用该 VPC 的默认安全组。您可以为每个安全组添加规则，规定流入或流出其关联文件系统的流量。您可以随时修改安全组的规则。新规则和修改后的规则将自动应用到与安全组相关联的所有资源。在 Amazon FSx 确定是否允许流量到达资源时，它会评估与资源关联的所有安全组中的所有规则。

要使用安全组控制对 Amazon FSx 文件系统的访问，请添加入站和出站规则。入站规则控制传入的流量，出站规则控制从文件系统传出的流量。确保您的安全组中有正确的网络流量规则，以便将 Amazon FSx 文件系统的文件共享映射到支持的计算实例上的文件夹。

有关安全组规则的更多信息，请参阅《Amazon EC2 用户指南》中的安全组规则。

创建 VPC 安全组

为 Amazon FSx 创建安全组

1. 打开位于 https://console.aws.amazon.com/ec2 的 Amazon EC2 控制台。
2. 在导航窗格中，选择 Security Groups（安全组）。
3. 选择创建安全组。
4. 为安全组指定名称和描述。
5. 对于 VPC，请选择与您的文件系统关联的 Amazon VPC 以在该 VPC 中创建安全组。
6. 对于出站规则，允许所有端口上的所有流量传输。
7. 将以下规则添加到安全组的入站端口。在源字段中，您应选择自定义，然后输入与需要访问 FSx for ONTAP 文件系统的实例关联的安全组或 IP 地址范围，包括：

   - 通过 NF and/or S、SMB 或 iSCSI 访问文件系统中数据的 Linux、Windows、macOS 客户端。
   - 您将与您的文件 systems/clusters 系统对等的任何 ONTAP 文件（例如，使用 SnapMirror SnapVault、或 FlexCache）。
   - 您将用于访问 ONTAP REST API、CLI 或 zAPI 的任何客户端（例如， Harvest/Grafana 实例、NetApp 连接器或 NetApp 控制台）。

协议	端口	角色
所有 ICMP	全部	对实例执行 ping 操作
SSH	22	通过 SSH 访问集群管理 LIF 或节点管理 LIF 的 IP 地址
TCP	111	NFS 的远程过程调用
TCP	135	CIFS 的远程过程调用
TCP	139	CIFS 的 NetBIOS 服务会话

协议	端口	角色
TCP	161-162	简单网络管理协议（SNMP）
TCP	443	通过 ONTAP REST API 访问集群管理 LIF 或 SVM 管理 LIF 的 IP 地址
TCP	445	微软 SMB/CIFS 在 TCP 上使用 NetBIOS 成帧
TCP	635	NFS 挂载
TCP	749	Kerberos
TCP	2049	NFS 服务器进程守护程序
TCP	3260	通过 iSCSI 数据 LIF 进行 iSCSI 访问
TCP	4045	NFS 锁定进程守护程序
TCP	4046	NFS 网络状态监控
TCP	10000	网络数据管理协议 (NDMP) 和集群 NetApp SnapMirror 间通信
TCP	11104	管理 NetApp SnapMirror 集群间通信
TCP	11105	SnapMirror 使用集群间 LIF 进行数据传输
UDP	111	NFS 的远程过程调用
UDP	135	CIFS 的远程过程调用
UDP	137	CIFS 的 NetBIOS 名称解析
UDP	139	CIFS 的 NetBIOS 服务会话
UDP	161-162	简单网络管理协议（SNMP）
UDP	635	NFS 挂载
UDP	2049	NFS 服务器进程守护程序

协议	端口	角色
UDP	4045	NFS 锁定进程守护程序
UDP	4046	NFS 网络状态监控
UDP	4049	NFS 配额协议

8. 将安全组添加到文件系统的弹性网络接口。

禁止访问文件系统

要暂时禁止所有客户端通过网络访问您的文件系统，您可以删除与文件系统的 elastic network interface 关联的所有安全组，然后将其替换为没有 inbound/outbound 规则的组。

适用于 ONTAP 的 Amazon FSx 的合规性验证 NetApp

要了解是否属于特定合规计划的范围，请参阅AWS 服务 “按合规计划划分的范围” ”，然后选择您感兴趣的合规计划。 AWS 服务 有关一般信息，请参阅AWS 合规计划AWS。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的 “下载报告” 中的 “ AWS Artifact。

您在使用 AWS 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 AWS 服务，请参阅AWS 安全文档。

适用于 NetApp ONTAP 的 Amazon FSx 和接口 VPC 终端节点 (AWS PrivateLink)

您可以将 Amazon FSx 配置为使用接口 VPC 端点以改善 VPC 的安全状况。接口 VPC 终端节点由一项技术提供支持，使您无需互联网网关AWS PrivateLink、NAT 设备、VPN 连接或 Direct Connect 连接即可私密访问 Amazon FSx API。VPC 中的实例即使没有公有 IP 地址也可与 Amazon FSx API 进行通信。您的 VPC 和 Amazon FSx 之间的流量不会离开网络。 AWS

每个接口 VPC 端点均由子网中的一个或多个弹性网络接口表示。网络接口提供一个私有 IP 地址，此地址可用作指向 Amazon FSx API 的流量的入口点。Amazon FSx 支持使用 IPv4 和双堆栈（IPv4 和 IPv6）IP 地址类型配置的 VPC 端点。有关更多信息，请参阅《Amazon VPC 用户指南》中的创建接口 VPC 端点。

Amazon FSx 接口 VPC 端点注意事项

请务必先查看《Amazon VPC 用户指南》中的接口 VPC 端点属性和限制，然后再为 Amazon FSx 设置接口 VPC 端点。

您可以从 VPC 调用任何 Amazon FSx API 操作。例如，您可以通过在您的 VPC 中调用 CreateFileSystem API 来为 ONTAP 文件系统创建 FSx。有关 Amazon FSx API 的完整列表，请参阅 Amazon FSx API 参考中的操作。

VPC 对等连接注意事项

可通过 VPC 对等连接，将其他 VPC 连接到有接口 VPC 端点的 VPC。VPC 对等连接是两个 VPC 之间的网络连接。您可以在自己的两个 VPC 之间建立 VPC 对等连接，或者与其他 AWS 账户中的 VPC 之间建立此连接。这些 VPC 也可以分为两个不同 AWS 区域的。

对等 VPC 之间的流量保留在 AWS 网络上，不会通过公共互联网。建立对等 VPC 连接后，两个 VPC 中的资源，如 Amazon Elastic Compute Cloud（Amazon EC2）实例，可以通过在其中一个 VPC 中创建的接口 VPC 端点访问 Amazon FSx API。

为 Amazon FSx API 创建接口 VPC 端点

您可以使用亚马逊 VPC 控制台或 AWS Command Line Interface ()AWS CLI为 Amazon FSx API 创建 VPC 终端节点。有关更多信息，请参阅《Amazon VPC 用户指南》中的创建接口 VPC 端点。

要为 Amazon FSx 创建接口 VPC 端点，请执行以下操作之一：

- **com.amazonaws.*region*.fsx** – 为 Amazon FSx API 操作创建端点。
- **com.amazonaws.*region*.fsx-fips** – 为 Amazon FSx API 创建符合美国联邦信息处理标准（FIPS）140-2 的端点。

要使用私有 DNS 选项，您必须设置 VPC 的 `enableDnsHostnames` 和 `enableDnsSupport` 属性。有关更多信息，请参阅《Amazon VPC 用户指南》中的查看和更新 VPC 的 DNS 支持。

中国除外 AWS 区域 ，如果您为终端节点启用私有 DNS，则可以使用 VPC 终端节点向 Amazon FSx 发出 API 请求， AWS 区域例如，`fsx.us-east-1.amazonaws.com`使用其默认 DNS 名称。对于中国（北京）和中国（宁夏 AWS 区域），您可以分别`fsx-api.cn-north-1.amazonaws.com.cn`使用`fsx-api.cn-northwest-1.amazonaws.com.cn`和向 VPC 终端节点发出 API 请求。

有关更多信息，请参阅《Amazon VPC 用户指南》中的通过接口 VPC 端点访问服务。

为 Amazon FSx 创建 VPC 端点策略

要控制对 Amazon FSx API 的访问权限，您可以将 AWS Identity and Access Management (IAM) 策略附加到您的 VPC 终端节点。此策略指定以下内容：

- 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。

适用于 ONTAP 的 Amazon FSx 中的弹性 NetApp

AWS 全球基础设施是围绕 AWS 区域 可用区构建的。 AWS 区域 提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络连接。利用可用区，您可以设计和操作在可用区之间无中断地自动实现失效转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错能力和可扩展性。

有关 AWS 区域 和可用区的更多信息，请参阅AWS 全球基础设施。

除了 AWS 全球基础设施外，Amazon FSx 还提供多项功能来帮助支持您的数据弹性和备份需求。

备份和还原

Amazon FSx 创建卷的自动备份并将其保存到适用 NetApp 于 ONTAP 的 Amazon FSx 文件系统中。在适用 NetApp 于 ONTAP 的 Amazon FSx 文件系统的备份窗口内，Amazon FSx 会自动备份您的卷。Amazon FSx 根据您指定的备份保留期保存卷的自动备份。您还可以通过创建用户启动备份来手动备份卷。您可以随时通过创建新卷来恢复卷备份，并将备份指定为源。

有关更多信息，请参阅 使用卷备份保护数据。

快照

亚马逊 FSx 为 ONTAP 卷创建亚马逊 FSx 的快照副本。 NetApp 快照副本可防止卷中的文件被最终用户意外删除或修改。有关更多信息，请参阅 使用快照保护您的数据。

可用区

适用于 NetApp ONTAP 文件系统的 Amazon FSx 旨在为数据提供持续可用性，即使在服务器出现故障时也是如此。每个文件系统都由位于至少一个可用区的两台文件服务器提供支持，每台文件服务器都有

自己的存储。Amazon FSx 会自动复制您的数据以保护其免受组件故障的影响，持续监控硬件故障，并在出现故障时自动更换基础设施组件。文件系统会根据需要自动进行失效转移和失效自动恢复（通常在 60 秒内），而客户端则自动利用文件系统进行失效转移和失效自动恢复。

Multi-AZ 文件系统

适用于 NetApp ONTAP 文件系统的 Amazon FSx 在各个可用区均具有高 AWS 可用性和耐用性，旨在即使在可用区不可用的情况下也能为数据提供持续可用性。

有关更多信息，请参阅 可用性、持久性和部署选项。

Single-AZ 文件系统

适用于 NetApp ONTAP 文件系统的 Amazon FSx 在单个可用区内具有高 AWS 可用性和耐用性，旨在在单个文件服务器或磁盘出现故障时在该可用区内提供持续可用性。

有关更多信息，请参阅 可用性、持久性和部署选项。

适用于 ONTAP 的 Amazon FSx 中的基础设施安全 NetApp

作为一项托管服务，适用于 NetApp ONTAP 的 Amazon FSx 受 AWS 全球网络安全的保护。有关 AWS 安全服务以及如何 AWS 保护基础设施的信息，请参阅AWS 云安全。要使用基础设施安全的最佳实践来设计您的 AWS 环境，请参阅 S AWS ecurity Pillar Well-Architected Fram ework 中的基础设施保护。

您可以使用 AWS 已发布的 API 调用通过网络访问 Amazon FSx。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（短暂的）或 ECDHE（椭圆曲线短暂的 Diffie-Hellman）。 Diffie-Hellman大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

使用带有 FSx 的 NetApp ONTAP vScan for ONTAP

您可以使用 NetApp ONTAP's Vscan 功能来运行支持的第三方杀毒软件。有关更多信息，请参阅以下资源，了解各种支持的解决方案。

- Deep Instinct：Vscan 合作伙伴解决方案和 Deep Instinct 文档[1]
- SentinelOne — Vscan 合作伙伴解决方案和 S SentinelOne ingularity Cloud 数据安全
- Symantec：Vscan 合作伙伴解决方案和 Symantec 保护引擎

- Trellix（以前 McAfee）— Vscan 合作伙伴解决方案和 Trellix 产品文档
- Trend Micro：Vscan 合作伙伴解决方案
- OPSWAT — Vscan 合作伙伴解决方案和 OPSWAT 产品文档

> **Note**
>
> [1] 必须登录 Deep Instinct 的门户网站才能查看相关文档。

ONTAP 角色和用户

NetApp ONTAP 包含强大且可扩展的基于角色的访问控制（RBAC）功能。ONTAP 角色定义用户在使用 ONTAP CLI 和 REST API 时的能力和权限。每个角色定义不同级别的管理功能和权限。可以为用户分配角色，以便控制他们在使用 ONTAP REST API 和 CLI 时对 FSx for ONTAP 资源的访问。有一些是 ONTAP 角色分别提供给 FSx for ONTAP 文件系统用户和存储虚拟机（SVM）用户的。

在创建 FSx for ONTAP 文件系统时，将创建文件系统级和 SVM 级的默认 ONTAP 用户。您可以创建其他文件系统用户和 SVM 用户，也可以创建其他 SVM 角色来满足贵组织的需求。本章介绍了 ONTAP 用户和角色，并提供了创建其他用户和 SVM 角色的详细步骤。

文件系统管理员角色和用户

默认 ONTAP 文件系统用户为 `fsxadmin`，该用户被分配了 `fsxadmin` 角色。您可以为文件系统用户分配两个预定义角色，如下所示：

- **`fsxadmin`** - 具有此角色的管理员在 ONTAP 系统中拥有不受限制的权限。他们可以为 ONTAP 文件系统配置 FSx 上可用的所有文件系统和 SVM-level 资源。
- **`fsxadmin-readonly`** - 具有此角色的管理员可以查看文件系统级别的所有内容，但不能进行任何更改。

  此角色非常适合与 NetApp Harvest 等监视应用程序一起使用，因为它对所有可用资源及其属性拥有只读访问权限，但无法对其进行任何更改。

您可以创建其他文件系统用户并为其分配 `fsxadmin` 或 `fsxadmin-readonly` 角色。您无法创建新角色或修改现有角色。有关更多信息，请参阅 创建新的 ONTAP 用于文件系统和 SVM 管理的用户。

下表描述了文件系统管理员角色对 ONTAP CLI 和 REST API 命令以及命令目录拥有的访问权限。

角色名称	权限级别	对以下命令或命令目录
`fsxadmin`	全部	FSx for ONTAP 中可用的所有命令目录
`fsxadmin-readonly`	全部	`security login password` 仅用于管理自己的用户账户本地密码和密钥信息
	none	`security`
	readonly	FSx for ONTAP 中可用的其他所有命令目录

SVM 管理员角色和用户

每个 SVM 都有单独的身份验证域，可以由其管理员进行独立管理。文件系统上的每个 SVM 都有一个默认用户 vsadmin，并默认为 `vsadmin` 分配了角色。除 `vsadmin` 角色外，还有其他预定义的 SVM 角色可提供缩小的权限范围，您可以将此权限分配给 SVM 用户。您还可以创建自定义角色，提供满足贵组织需求的访问控制级别。

SVM 管理员的预定义角色及其功能如下：

角色名称	功能
`vsadmin`	• 管理您的用户账户、本地密码和密钥信息 • 管理卷，但移动卷除外 • 管理配额、qtree、快照副本和文件 • 管理 LUN • 执行除特权删除之外的 SnapLock 操作 • 配置协议：NFS、SMB 和 iSCSI • 配置服务：DNS、LDAP 和 NIS • 监控作业 • 监控网络连接和网络接口

角色名称	功能
	• 监控 SVM 的运行状况
vsadmin-volume	• 管理您的用户账户、本地密码和密钥信息 • 管理卷，包括卷移动 • 管理配额、qtree、快照副本和文件 • 管理 LUN • 配置协议：NFS、SMB 和 iSCSI • 配置服务：DNS、LDAP 和 NIS • 监控网络接口 • 监控 SVM 的运行状况
vsadmin-protocol	• 管理您的用户账户、本地密码和密钥信息 • 管理 LUN • 配置协议：NFS、SMB 和 iSCSI • 配置服务：DNS、LDAP 和 NIS • 监控网络接口 • 监控 SVM 的运行状况
vsadmin-backup	• 管理您的用户账户、本地密码和密钥信息 • 管理 NDMP 操作 • 制作恢复后的音量 read/write • 管理 SnapMirror 关系和快照副本 • 查看卷和网络信息

角色名称	功能
`vsadmin-snaplock`	• 管理您的用户账户、本地密码和密钥信息 • 管理卷，但移动卷除外 • 管理配额、qtree、快照副本和文件 • 执行 SnapLock 操作，包括特权删除 • 配置协议：NFS 和 SMB • 配置服务：DNS、LDAP 和 NIS • 监控作业 • 监控网络连接和网络接口
`vsadmin-readonly`	• 管理您的用户账户、本地密码和密钥信息 • 监控 SVM 的运行状况 • 监控网络接口 • 查看卷和 LUN • 查看服务和协议

有关如何创建新 SVM 角色的更多信息，请参阅 创建 SVM 角色。

使用活动目录进行身份验证 ONTAP 用户

您可以对 Windows Active Directory 域用户访问 FSx for ONTAP 文件系统和 SVM 进行身份验证。在 Active Directory 账户可以访问文件系统之前，您必须完成以下任务：

- 需要配置 Active Directory 域控制器对 SVM 的访问权限。

  用于配置为 Active Directory 域控制器访问网关或隧道的 SVM 必须启用 CIFS、加入活动目录，或两者兼之。如果不启用 CIFS，只是将隧道 SVM 加入 Active Directory，请确保 SVM 已加入您的 Active Directory。有关更多信息，请参阅 如何加入微软 Ac SVMs tive Directory。
- 需要启用 Active Directory 域用户账户以访问文件系统。

  对于访问 ONTAP CLI 或 REST API 的 Windows 域用户，可以使用密码身份验证，也可以使用 SSH 公钥身份验证。

有关如何为文件系统和 SVM 管理员配置 Active Directory 身份验证的过程，请参阅 为配置活动目录身份验证 ONTAP 用户。

创建新的 ONTAP 用于文件系统和 SVM 管理的用户

每个 ONTAP 用户都与 SVM 或文件系统关联。具有 `fsxadmin` 角色的文件系统用户可以使用 `security login create` ONTAP CLI 命令创建新的 SVM 角色和用户。

`security login create` 命令创建管理实用程序的登录方法。登录方法由用户名、应用程序（访问方法）和身份验证方法构成。一个用户名可以与多个应用程序相关联。可以选择包含访问控制角色名称。如果使用的是 Active Directory、LDAP 或 NIS 组名，则登录方法允许访问属于指定组的用户。如果用户是安全登录表中预置的多个群组的成员，则该用户可以访问授权给各个群组的命令列表。

有关如何创建新 ONTAP 用户的信息，请参阅 Creating ONTAP 用户。

主题

- Creating ONTAP 用户
- 创建 SVM 角色
- 为配置活动目录身份验证 ONTAP 用户
- 配置公钥认证
- 更新文件系统和 SVM 角色的密码要求
- 更新 fsxadmin 帐户密码失败

Creating ONTAP 用户

创建新的 SVM 或文件系统用户 (ONTAP CLI)

只有具有 `fsxadmin` 角色的文件系统用户才能创建新的 SVM 和文件系统用户。

1. 要访问 ONTAP CLI，请运行以下命令，在适用于 NetApp ONTAP 文件系统的 Amazon FSx 或 SVM 的管理端口上建立 SSH 会话。将 *`management_endpoint_ip`* 替换为文件系统管理端口的 IP 地址。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   有关更多信息，请参阅 使用 ONTAP CLI 管理文件系统。

2. 使用 `security login create` ONTAP CLI 命令在 FSx for ONTAP 文件系统或 SVM 上创建新的用户账户。

   为示例中的占位符填入数据，以定义以下必需的属性：

   - `-vserver` – 指定要在其中创建新 SVM 角色或用户的 SVM 的名称。如果要创建文件系统角色或用户，请不要指定 SVM。
   - `-user-or-group-name` – 指定登录方法的用户名或 Active Directory 组名。只能使用 `domain` 身份验证方法以及 `ontapi` 和 `ssh` 应用程序指定 Active Directory 组名。
   - `-application` – 指定登录方法的应用。可能的值包括 http、ontapi 和 ssh。
   - `-authentication-method` – 指定登录的身份验证方法。可能的值包括：
     - domain – 用于 Active Directory 身份验证
     - 密码 - 用于密码认证
     - publickey – 用于公钥身份验证
   - `-role` – 指定登录方法的访问控制角色名称。在文件系统级别，唯一可以指定的角色是 `fsxadmin`。

   （可选）您还可以将以下一个或多个参数与命令配合使用：

   - `[-comment]` - 用于为用户账户添加注释或备注。例如 **`Guest account`**。最大长度为 128 个字符。
   - `[-second-authentication-method {none|publickey|password|nsswitch}]` – 指定第二种身份验证方法。您可以指定以下方法：
     - 密码 - 用于密码认证
     - publickey — 用于身份验证 Public-key
     - nswitch – 用于 NIS 或 LDAP 身份验证
     - 无 - 未指定时的默认值。

   ```
   Fsx0123456::> security login create -vserver vserver_name -user-or-group-
   name user_or_group_name -application login_application -authentication-
   method auth_method -role role_or_account_name
   ```

   以下命令结合使用 SSH 和登录密码创建具有 `fsxadmin-readonly` 角色的新文件系统用户 `new_fsxadmin`。在提示时，提供此用户的密码。

```
Fsx0123456::> security login create -user-or-group-name new_fsxadmin -application
 ssh -authentication-method password -role fsxadmin-readonly

Please enter a password for user 'new_fsxadmin':
Please enter it again:

Fsx0123456::>
```

3. 以下命令在 SVM fsx 上创建具有 vsadmin_readonly 角色的新 SVM 用户 new_vsadmin，配置为将 SSH 和登录密码配合使用。在提示时，提供此用户的密码。

```
Fsx0123456::> security login create -vserver fsx  -user-or-group-name new_vsadmin -
application ssh -authentication-method password -role vsadmin-readonly

Please enter a password for user 'new_vsadmin':
Please enter it again:

Fsx0123456::>
```

4. 以下命令创建一个新的只读文件系统用户harvest2-user， NetApp Harvest 应用程序将使用该用户来收集性能和容量指标。有关更多信息，请参阅 使用 Harvest 和 Grafana 监控 FSx for ONTAP 文件系统。

```
Fsx0123456::> security login create -user-or-group-name harvest2-user -application
 ssh -role fsxadmin-readonly -authentication-method password
```

查看所有文件系统和 SVM 用户的信息

- 使用以下命令查看文件系统和 SVM 的所有登录信息。

```
Fsx0123456::> security login show

Vserver: Fsx0123456
                                                                 Second
User/Group                Authentication                 Acct    Authentication
Name           Application Method        Role Name        Locked  Method
-------------- ----------- ------------- ---------------- ------  --------------
autosupport    console     password      autosupport      no      none
fsxadmin       http        password      fsxadmin         no      none
fsxadmin       ontapi      password      fsxadmin         no      none
```

```
fsxadmin       ssh          password      fsxadmin          no      none
fsxadmin       ssh          publickey     fsxadmin          -       none
new_fsxadmin   ssh          password      fsxadmin-readonly
                                                          no      none

Vserver: fsx
                                                                  Second
User/Group                 Authentication                 Acct    Authentication
Name           Application Method        Role Name        Locked  Method
-------------- ----------- ------------- ---------------- ------ --------------
new_vsadmin    ssh         password      vsadmin-readonly no     none
vsadmin        http        password      vsadmin          yes    none
vsadmin        ontapi      password      vsadmin          yes    none
vsadmin        ssh         password      vsadmin          yes    none
10 entries were displayed.

Fsx0123456::>
```

创建 SVM 角色

您创建的每个 SVM 都有一个默认 SVM 管理员，并为其分配了预定义的 `vsadmin` 角色。除了这组预定义的 SVM 角色外，您还可以创建新的 SVM 角色。如果您需要为 SVM 创建新角色，请使用 `security login role create` ONTAP CLI 命令。此命令适用于具有 `fsxadmin` 角色的文件系统管理员。

创建新的 SVM 角色（ONTAP CLI）

1. 可以使用以下 `security login role create` ONTAP CLI 命令创建新的 SVM 角色：

```
Fsx0123456::> security login role create -vserver vs1.example.com -role vol_role -
cmddirname volume
```

2. 在命令中指定以下必需的参数：
   - `-vserver` SVM 的名称
   - `-role` – 角色的名称。
   - `-cmddirname` – 角色授予访问权限的命令或命令目录。将命令子目录名称用双引号引起来。例如 `"volume snapshot"`。输入 `DEFAULT` 指定所有命令目录。
3. （可选）您还可以向命令添加以下任意参数：

- `-vserver` – 与角色关联的 SVM 的名称。
- `-access` – 角色的访问级别。对于命令目录，这包括：
  - `none` – 拒绝访问命令目录中的命令。这是自定义角色的默认值。
  - `readonly` – 授予对命令目录及其子目录中的 show 命令的访问权限。
  - `all` – 授予对命令目录及其子目录中的所有命令的访问权限。要授予或拒绝对内部命令的访问权限，必须指定命令目录。

  对于非内部命令（不以 `create`、`modify`、`delete` 或 `show` 结尾的命令）：
  - `none` – 拒绝访问命令目录中的命令。这是自定义角色的默认值。
  - `readonly` – 不适用。请勿使用。
  - `all` – 授予对命令的访问权限。
- `-query` – 用于筛选访问级别的查询对象，以命令或命令目录中命令的有效选项的形式指定。将查询对象用双引号引起来。

4. 运行 `security login role create` 命令。

   以下命令为 vs1.example.com 虚拟服务器创建名为“admin”的访问控制角色。该角色拥有对“volume”命令的所有访问权限，但只能在“aggr0”聚合中访问。

   ```
   Fsx0123456::>security login role create -role admin -cmddirname volume -query "-
   aggr aggr0" -access all -vserver vs1.example.com
   ```

为配置活动目录身份验证 ONTAP 用户

使用 ONTAP CLI 为 ONTAP 文件系统和 SVM 用户配置使用 Active Directory 身份验证。

您必须是具有 `fsxadmin` 角色的文件系统管理员才能使用此过程中的命令。

为设置活动目录身份验证 ONTAP 用户 (ONTAP CLI)

此过程中的命令适用于具有 `fsxadmin` 角色的文件系统用户。

1. 要访问 ONTAP CLI，请运行以下命令，在适用于 NetApp ONTAP 文件系统的 Amazon FSx 或 SVM 的管理端口上建立 SSH 会话。将 *`management_endpoint_ip`* 替换为文件系统管理端口的 IP 地址。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

有关更多信息，请参阅 使用 ONTAP CLI 管理文件系统。

2. 使用所示的 `security login domain-tunnel create` 命令建立一个用于对 Windows Active Directory 用户进行身份验证的域隧道。*svm_name*替换为用于域隧道的 SVM 的名称。

```
FsxId0123456::> security login domain-tunnel create -vserver svm_name
```

3. 使用 `security login create` 命令创建将访问文件系统的 Active Directory 域用户账户。

在命令中指定以下必需的参数：

- `-vserver` - 配置了 CIFS 并加入 Active Directory 的 SVM 的名称。它将用作 Active Directory 域用户访问文件系统的身份验证隧道。将创建新的角色或用户。
- `-user-or-group-name` – 登录方法的用户名或 Active Directory 组名。只能使用 `domain` 身份验证方法以及 `ontapi` 和 `ssh` 应用程序指定 Active Directory 组名。
- `-application` – 登录方法的应用。可能的值包括 http、ontapi 和 ssh。
- `-authentication-method` – 用于登录的身份验证方法。可能的值包括：
  - domain – 用于 Active Directory 身份验证
  - 密码 - 用于密码认证
  - publickey – 用于公钥身份验证
- `-role` – 登录方法的访问控制角色名称。在文件系统级别，唯一可以指定的角色是 `-role fsxadmin`。

以下示例为 `filesystem1` 文件系统创建了一个 Active Directory 域用户账户 `CORP\Admin`。

```
FSxId012345::> security login create -vserver filesystem1 -username CORP\Admin -
application ssh -authmethod domain -role fsxadmin
```

以下示例创建了使用公钥身份验证的 `CORP\Admin` 用户账户。

```
FsxId0123456ab::> security login create -user-or-group-name "CORP\Admin" -
application ssh -authentication-method publickey -role fsxadmin
Warning: To use public-key authentication, you must create a public key for user
 "CORP\Admin".
```

使用以下命令为 `CORP\Admin` 用户创建公钥：

```
FsxId0123456ab::> security login publickey create -username "CORP
\Admin" -publickey "ecdsa-sha2-nistp256 SECRET_STRING_HERE_IS_REDACTED=
 cwaltham@b0be837a91bf.ant.amazon.com"
```

结合使用 SSH 和 Active Directory 凭证来登录文件系统

- 以下示例展示了如果选择为 `-application` 类型选择 `ssh`，该如何使用 Active Directory 凭证通过 SSH 进入您的文件系统。`username` 的格式为 `"domain-name\user-name"`，即您在创建账户时提供的域名和用户名，用反斜杠分隔并用引号引起来。

  ```
  Fsx0123456::> ssh "CORP\user"@management.fs-abcdef01234567892.fsx.us-east-2.aws.com
  ```

  当系统提示输入密码时，使用 Active Directory 用户的密码。

配置公钥认证

要启用 SSH 公钥身份验证，必须使用 `security login publickey create` 命令先生成 SSH 密钥，然后将其与管理员账户关联。此操作将允许该账户访问 SVM。`security login publickey create` 命令接受以下参数。

参数	说明
`-vserver`（可选）	账户访问的 SVM 的名称 如果要为文件系统用户配置 SSH 公钥身份验证，不要包括 `-versver`。
`-username`	账户的用户名。默认值 `admin` 是集群管理员的默认名称。
`-index`	公钥的索引号。如果密钥是为账户创建的第一个密钥，默认值为 0。否则，默认值将比该账户现有的最高索引号多一。
`-publickey`	OpenSSH 公钥。将密钥用双引号引起来。
`-role`	分配给账户的访问控制角色。

参数	说明
-comment（可选）	公钥的描述性文本。将文本用双引号引起来。

以下示例将公钥与 SVM svm01 的 SVM 管理员账户 svmadmin 关联。公钥分配到的索引号为 5。

```
Fsx0123456::> security login publickey create -vserver svm01 -username svmadmin
 -index 5 -publickey "ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAspH64CYbUsDQCdW22JnK6J/
vU9upnKzd2zAk9C1f7YaWRUAFNs2Qe5lUmQ3ldi8AD0Vfbr5T6HZPCixNAIzaFciDy7hgnmdj9eNGedGr/
JNrftQbLD1hZybX
+72DpQB0tYWBhe6eDJ1oPLobZBGfMlPXh8VjeU44i7W4+s0hG0E=tsmith@publickey.example.com"
```

> **Important**
>
> 要执行此任务，您必须是 SVM 或文件系统管理员。

更新文件系统和 SVM 角色的密码要求

您可以使用 security login role config modify ONTAP CLI 命令更新文件系统或 SVM 角色的密码要求。此命令仅适用于具有 fsxadmin 角色的文件系统管理员账户。在修改密码要求时，如果有任何具有该角色的现有用户会受到更改的影响，系统将发出警告。

以下示例针对 fsx SVM 上具有 vsadmin-readonly 角色的用户将最低密码长度要求修改为 12 个字符。在此示例中，已有用户拥有该角色。

```
FsxId0123456::> security login role config modify -role vsadmin-readonly -vserver fsx -
passwd-minlength 12
```

由于存在现有的用户，系统会显示以下警告：

```
Warning: User accounts with this role exist. Modifications to the username/password
 restrictions on this role could result in non-compliant user
         accounts.
Do you want to continue? {y|n}:

FsxId0123456::>
```

更新 fsxadmin #####败

更新 fsxadmin 用户的密码时，如果密码不文件系统中设置的符合密码要求，可能会收到错误消息。您可以使用 security login role config show ONTAP CLI 或 REST API 命令查看密码要求。

查看文件系统或 SVM 角色的密码要求

1. 要访问 ONTAP CLI，请运行以下命令，在适用于 NetApp ONTAP 文件系统的 Amazon FSx 或 SVM 的管理端口上建立 SSH 会话。将 *management_endpoint_ip* 替换为文件系统管理端口的 IP 地址。

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   有关更多信息，请参阅 使用 ONTAP CLI 管理文件系统。

2. security login role config show 命令返回文件系统或 SVM 角色的密码要求。

   ```
   FsxId0123456::> security login role config show -role fsxadmin -
   fields password_requirement_fields
   ```

   对于 -fields 参数，指定以下任一或全部内容：

   - passwd-minlength – 密码的最小长度。
   - passwd-min-special-chars – 密码的最少特殊字符数。
   - passwd-min-lowercase-chars – 密码的最少小写字符数。
   - passwd-min-uppercase-chars – 密码的最小大写字符数。
   - passwd-min-digits – 密码的最小数字数量。
   - passwd-alphanum – 有关包含或排除字母数字字符的信息。
   - passwd-expiry-time – 密码过期时间。
   - passwd-expiry-warn-time – 密码过期警告时间。

3. 运行以下命令以查看所有密码要求：

   ```
   FsxId0123456::> security login role config show -role fsxadmin -fields passwd-
   minlength, passwd-min-special-chars, passwd-min-lowercase-chars, passwd-min-
   digits, passwd-alphanum, passwd-expiry-time, passwd-expiry-warn-time, passwd-min-
   uppercase-chars
   ```

```
vserver                role     passwd-minlength passwd-alphanum passwd-min-
special-chars passwd-expiry-time passwd-min-lowercase-chars passwd-min-uppercase-
chars passwd-min-digits passwd-expiry-warn-time
---------------------- -------- ---------------- ---------------
 ------------------------ ------------------ --------------------------
 -------------------------- ------------------ ------------------------
FsxId0123456           fsxadmin 3                enabled         0
       unlimited          0                       0                       0
               unlimited
```

配额

接下来，您可以了解与 Amazon FSx for NetApp ONTAP 合作时的配额。

主题

您可以提高的配额

以下是您可以增加的每个 AWS 账户 Amazon FSx for NetApp AWS 区域 ONTAP 配额。

资源	默认值	说明
ONTAP 文件系统	100	您可以在此账户中创建 FSx 的 Amazon for NetApp ONTAP 文件系统的最大数量。
ONTAP SSD 存储容量	524,288	您可以在此账户中拥有的所有 Amazon for NetApp ONTAP 文件系统的最大固态硬盘存储容量（以 GiB FSx 为单位）。
ONTAP 吞吐能力	10240	您在此账户中可以拥有的所有 Amazon FSx for NetApp ONTAP 文件系统的最大吞吐容量（英寸 MBps）。
ONTAP SSD IOPS	1000000	您在此账户中可以拥有的所有 Amazon FSx for NetApp ONTAP 文件系统的最大固态硬盘 IOPS 量。
ONTAP 备份	10000	您可以在中为所有 Amazon for NetApp ONTAP 文件系统创建

资源	默认值	说明
		FSx 的用户启动的卷备份的最大数量。 AWS 账户
Amazon S3 接入点	10000	您可以为所有支持的数据源类型（ FSx 例如 NetApp ONTAP ）创建的 Amazon S3 接入点的最大数量。 AWS 账户这也是您可以连接到 NetApp ONTAP 文件系统或卷的单 FSx 个 S3 接入点的最大数量。此配额是 Amazon S3 服务配额，可使用服务配额进行调整。

要请求提高限额

1. 打开 AWS 支持 页面，登录（如有必要），然后选择创建案例。
2. 在创建案例中选择账户和账单支持。
3. 在案例详细信息面板中输入以下条目：
   - 对于类型，选择账户。
   - 对于类别，选择其他账户问题。
   - 对于主题，请输入 **`Amazon FSx for NetApp ONTAP service limit increase request`**。
   - 提供您申请的详细描述，包括：
     - 您想要增加的 FSx 配额以及您想要增加到的值（如果已知）。
     - 您申请增加限额的原因。
     - 您申请增加限额的每个文件系统的文件系统 ID 和区域。
4. 提供您的首选联系选项，然后选择提交。

每个文件系统的资源限额

下表列出了 Amazon FSx 上每个文件系统的 NetApp ONTAP 资源配额。 AWS 区域

资源	每个文件系统的限额
最低 SSD 存储容量	每个高可用性（HA）对为 1024GiB
用于启动缩减操作的最低 SSD 存储容量	每个 HA 对 1126GiB
最小 SSD 减少百分比	比当前容量少 9%
最大 SSD 存储容量	• 第二代单可用区文件系统：每个 HA 对为 512 TiB，最高可达 1 PiB • 第二代多可用区文件系统：512 TiB • 第一代文件系统：192 TiB
建议的最大 SSD 利用率	80% 用于最佳性能和分层功能
用于减少操作次数的最大 SSD 利用率	减少操作之前和之后相差 80%
最大 SSD IOPS	第二代文件系统： • 单可用区的每个 HA 对（最多 12 对）为 20 万 • 多可用区总计为 20 万 第一代文件系统： • 160000 – 美国东部（俄亥俄州）区域、美国东部（弗吉尼亚州北部）区域、美国西部（俄勒冈州）区域和欧洲地区（爱尔兰） • 在所有其他有 ONTAP 可用 AWS 区域 的地方 FSx ，有 80,000 个
最低吞吐能力	• 第二代文件系统（1 个 HA 对）：384 MBps • 第二代文件系统（2 个或更多 HA 对）：每个 HA 对 1,536 MBps 个 • 第一代文件系统：128 MBps

资源	每个文件系统的限额
最大吞吐能力	第二代文件系统： • 73,728 MBps 1 适用于单可用区 • 6,144 适用于 MBps 多可用区 第一代文件系统： • 4,096 MBps [2] 位于美国东部（俄亥俄州）地区、美国东部（弗吉尼亚北部）地区、美国西部（俄勒冈）地区和欧洲（爱尔兰） • MBps 在所有其他可 FSx 用 ONTAP AWS 区域 的地方，有 2,048 个
最大卷数	• 第二代文件系统（1 个 HA 对）：500 • 第二代文件系统（2 个或更多 HA 对）：1,000 • 第一代文件系统：500 在文件系统中使用 S3 接入点时： • 第二代文件系统（1 个 HA 对）：491 • 第二代文件系统（2 个或更多 HA 对）：2 个 HA 对为 975（12 个 HA 对为 903 个） • 第一代文件系统：491
最大快照数	每个卷为 1023[3]
最大备份数	每个卷为 4091[4]

资源	每个文件系统的限额
最大数量 SVMs	具有一个 HA 对且 IPv4仅限网络类型的第二代文件系统： • 6（吞吐容量 MBps 的 384%） • 6（吞吐量容 MBps 量的 768） • 14（吞吐容量的 1,536 MBps 个） • 14（吞吐容量的 3,072 MBps 个） • 24（吞吐容量的 6,144 个 MBps ） 第二代文件系统（1 个 HA 对，使用双堆栈网络类型）： • 6（吞吐容量 MBps 的 384%） • 6（吞吐量容 MBps 量的 768） • 11（吞吐容量的 1,536 MBps 个） • 11（吞吐容量的 3,072 MBps 个） • 11（吞吐容量的 6,144 个 MBps ） 具有 2-12 个 HA 对且 IPv4仅限或双栈网络类型的第二代文件系统： • 11 具有 IPv4仅限网络类型的第一代文件系统： • 6（ MBps 吞吐量容量为 128） • 6（ MBps 吞吐量容量为 256） • 14（ MBps 吞吐量容量为 512） • 14（1,024 个 MBps 吞吐容量） • 24（ MBps 吞吐容量 2,048） • 24（ MBps 吞吐容量 4,096 个）

资源	每个文件系统的限额
	第一代文件系统（使用双堆栈网络类型）： • 6（ MBps 吞吐量容量为 128 ） • 6（ MBps 吞吐量容量为 256 ） • 11（ MBps 吞吐量容量为 512 ） • 11（1,024 个 MBps 吞吐容量 ） • 11（ MBps 吞吐容量 2,048 ） • 11（ MBps 吞吐容量 4,096 个 ）
最大标签数	50
自动备份的最长保留期	90 天
用户启动备份的最长保留期	没有保留期限制
每个文件系统最迟的最大路由数	50 [5]
每个文件服务器的最大客户端连接数[6]	100000

Note

[1] 在具有 12 个 HA 对的第二代单可用区文件系统上（ MBps 每对 HA 6,144 个 ）。有关更多信息，请参阅 管理高可用性（HA）对。

[2] 要预置 4 GBps 的吞吐容量，则 FSx 适用于 ONTAP 的第一代文件系统需要配置支持的最大 SSD IOPS (160,000) 和至少 5,120 GiB 的固态硬盘存储容量。 AWS 区域有关哪个 AWS 区域支持 4,096 个吞吐容 MBps 量的更多信息，请参阅。吞吐能力对性能的影响

[3] 不论何时，每个卷最多可存储 1,023 张快照。达到此限制后，必须先删除现有快照，然后才能创建卷的新快照。

[4] 不论何时，每个卷最多可存储 4,091 个备份。达到此限制后，必须先删除现有备份，然后才能创建卷的新备份。

[5] 每个文件系统在任何时间点最多可以配置 50 个路由。达到此限制后，必须删除现有路由才能配置新路由。您的文件系统拥有的路由数量由 SVMs 其拥有的路由数量以及与之关联的路由表数量决定。您可以使用以下公式确定文件系统的现有路由数量：（1 + 文件系统 SVMs 中的数量）*（与文件系统关联的路由表）。

[6] 客户端连接定义为与给定文件服务器的单个 TCP 连接。在文件系统中，每个 HA 对都有一个活动的文件服务器。一个客户端可与一个文件服务器建立多个 TCP 连接。例如，如果客户端正在使用多路径。

FSx 对亚马逊版 NetApp ONTAP 进行故障排除

使用以下部分来帮助对 ONTAP 文件系统 FSx 进行故障排除。

主题

您的文件系统处于 **MISCONFIGURED** 状态

导致文件系统处于 MISCONFIGURED 状态的潜在原因有很多，每种原因都有自己的解决方案，如下所示。

主题

VPC 所有者账户已禁用多可用区的 VPC 共享

由于以下原因之一，由共享 VPC 子网 AWS 账户 中的参与者创建的多可用区文件系统将进入MISCONFIGURED状态：

- 共享 VPC 子网的所有者账户已禁用对 ONTAP 文件系统的多可用区 VPC 共享支持。 FSx
- 所有者账户已停止共享 VPC 子网。

如果所有者账户已停止共享 VPC 子网，您将在控制台中看到该文件系统的以下消息：

```
The vpc ID vpc-012345abcde does not exist
```

为解决问题，您必须联系与您共享 VPC 子网的所有者账户。有关更多信息，请参阅 在共享子网中创建 FSx for ONTAP 文件系统 了解更多信息。

您无法在多可用区文件系统上创建新的 SVM

对于共享 VPC AWS 账户 中的参与者创建的多可用区文件系统，由于以下原因之一，您将无法创建新的 SVM：

- 共享 VPC 子网的所有者账户已禁用对 ONTAP 文件系统的多可用区 VPC 共享支持。 FSx
- 所有者账户已停止共享 VPC 子网。

为解决问题，您必须联系与您共享 VPC 子网的所有者账户。有关更多信息，请参阅 在共享子网中创建 FSx for ONTAP 文件系统 了解更多信息。

文件系统的 SSD 存储层已达 90% 以上

单可用区或多可用区文件系统的 SSD 存储层当前已达 90% 以上。我们建议 SSD 存储层的利用率不要一直超过 80%。如果您没有在文件系统的下一个维护时段之前释放 SSD 存储层中的空间， FSx 则 for ONTAP 将在修补操作期间暂时降低文件系统的吞吐量。此举旨在确保后台维护进程能在合理的时间范围内完成。为避免此情况，请将 SSD 存储层的利用率降至 90% 以下。您可以通过多种方式降低 SSD 利用率，包括：

- 增加文件系统的 SSD 存储容量。
- 删除不需要的数据。
- 删除不需要的卷快照。

有关更多信息，请参阅 管理存储容量。

您无法访问您的文件系统

本节介绍与无法访问文件系统相关的问题和解决方案。

主题

多可用区文件系统缺少路由表标签

Amazon 使用基于标签的身份验证 FSx 管理多可用区文件系统的 VPC 路由表。目前，与文件系统关联的一个或多个路由表缺少这些路由表标签。这些路由表标有 `Key: AmazonFSx; Value: ManagedByAmazonFSx`。如果您未能在下一维护时段前手动添加这些标签，则在修补操作期间，子网中与路由表关联的任何客户端都将暂时失去对文件系统的访问权限。为避免此情况，请手动添加缺少的路由表标签。

有关更多信息，请参阅 更新文件系统。

文件系统有超过 50 条路由

您的文件系统当前有超过 50 条与之关联的路由。如果未能在文件系统的下一计划维护时段前删除其中一些路由，则失效转移过程可能需要比平时更长的时间。为避免此情况，请将路由数量减少到 50 以下。以下是您可以采取的步骤，以减少与文件系统关联的路由数量：

- 删除多余路由
- 减少与文件系统 SVMs 关联的数量
- 减少与文件系统关联的路由表数量

有关更多信息，请参阅更新文件系统和删除存储虚拟机（SVM）。

文件系统缺少通往一个或多个文件服务器的路由

您的文件系统当前缺少通往一个或多个文件服务器的路由，且现有路由表没有足够空间可添加新的路由表条目。如果未能在文件系统的下一计划维护时段之前添加缺少的路由，则在修补操作期间，所有连接的客户端都将断开连接。为避免此情况，请添加缺少的路由。

有关更多信息，请参阅更新文件系统和配额。

文件系统的弹性网络接口已修改或删除

您不得修改或删除文件系统的弹性网络接口。修改或删除该网络接口可能会导致您永久丢失虚拟私有云（VPC）和文件系统之间的连接。创建新的文件系统，不要修改或删除 Amazon FSx 网络接口。有关更多信息，请参阅 使用 Amazon VPC 进行文件系统访问控制。

文件系统弹性网络接口附加的弹性 IP 地址已删除

Amazon FSx 不支持从公共互联网访问文件系统。Amazon FSx 会自动分离任何弹性 IP 地址，该地址是可从互联网访问并连接到文件系统的弹性网络接口的公有 IP 地址。有关更多信息，请参阅 支持的客户端。

文件系统的 VPC 安全组缺少所需的入站规则

查看 Amazon VPC 安全组 中指定的入站规则，并确保文件系统的关联安全组具有相应的入站规则。

计算实例的 VPC 安全组缺少所需的出站规则

查看 Amazon VPC 安全组 中指定的出站规则，并确保计算实例的关联安全组具有相应的出站规则。

计算实例的子网不使用任何与文件系统关联的路由表

FSx for ONTAP 会在 VPC 路由表中创建用于访问您的文件系统的终端节点。我们建议您将文件系统配置为使用与客户端所在子网关联的所有 VPC 路由表。默认情况下，Amazon FSx 使用您的 VPC 的主路由表。您可以选择指定一个或多个路由表，让 Amazon FSx 在创建文件系统时使用。

如果您可以 Ping 文件系统的集群间端点，但无法 Ping 文件系统的管理端点（有关更多信息，请参阅文件系统资源），则您的客户端可能不位于与文件系统的路由表关联的子网。要访问文件系统，请将文件系统的一个路由表与客户端的子网关联。有关如何更新文件系统的 Amazon VPC 路由表的信息，请参阅更新文件系统。

Amazon FSx 无法更新使用创建的多可用区文件系统的路由表 CloudFormation

Amazon 使用基于标签的身份验证 FSx 管理多可用区文件系统的 VPC 路由表。这些路由表标有 `Key: AmazonFSx; Value: ManagedByAmazonFSx`。使用 FSx 为 ONTAP 多可用区文件系统创建或更新时， CloudFormation 我们建议您手动添加`Key: AmazonFSx; Value: ManagedByAmazonFSx`标签。

如果无法访问多可用区文件系统，请查看文件系统关联的 VPC 路由表是否标有 `Key: AmazonFSx; Value: ManagedByAmazonFSx`。如果不是，则当故障转移事件发生时，Amazon FSx 无法更新这些路由表，将管理端口和数据端口的浮动 IP 地址路由到活动文件服务器。有关如何更新文件系统的 Amazon VPC 路由表的信息，请参阅更新文件系统。

无法通过 iSCSI 从其他 VPC 中的客户端访问文件系统

要通过互联网小型计算机系统接口（iSCSI）协议从其他 VPC 中的客户端访问文件系统，您可以在文件系统的关联 VPC 与客户端所在的 VPC 之间配置 Amazon VPC 对等连接或 AWS Transit Gateway 。有关更多信息，请参阅《Amazon Virtual Private Cloud》指南中的创建和接受 VPC 对等连接。

所有者账户已停止共享 VPC 子网

如果您在已与您共享的 VPC 子网中创建了文件系统，则拥有者账户可能已停止共享 VPC 子网。

如果所有者账户已停止共享 VPC 子网，您将在控制台中看到该文件系统的以下消息：

```
The vpc ID vpc-012345abcde does not exist
```

您需要联系拥有者账户与您重新共享子网。

无法通过 NFS、SMB、ONTAP CLI 或 ONTAP REST API 从其他 VPC 或本地的客户端访问文件系统

要从其他 VPC 中的客户端或本地通过网络文件系统 (NFS)、服务器消息块 (SMB) 或 NetApp ONTAP CLI 和 REST API 访问文件系统，您必须在与您的文件系统关联的 VPC 和您的客户端所在的网络之间配置路由 AWS Transit Gateway 。有关更多信息，请参阅 访问您的 fo FSx r ONTAP 数据。

您的存储虚拟机（SVM）处于 **MISCONFIGURED** 状态

导致存储虚拟机处于 MISCONFIGURED 状态的潜在原因有很多，每种原因都有自己的解决方案，如下所示。

SVM 具有离线卷

文件系统包含处于离线状态的卷。我们建议您持续保持卷在线。如果您在文件系统的下一个维护时段之前没有联机此卷，Amazon FSx 将在修补操作期间暂时将此卷联机。为避免此情况，请联机或删除该卷。

要使离线卷恢复在线，应使用 `volume online` ONTAP CLI 命令，如以下示例所示。如果仅存在一个 SVM（虚拟服务器），则无需指定 `-vserver` 参数。

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

您的 SVM 有一个带有 iSCSI LUN 或命名空间的 NVMe/TCP 离线卷

文件系统包含处于受限制状态的卷。我们建议您持续保持卷在线。如果您在文件系统的下一个维护时段之前没有联机此卷，Amazon FSx 将在修补操作期间暂时将此卷联机。为避免此情况，请联机或删除该卷。

要使离线卷恢复在线，应使用 `volume online` ONTAP CLI 命令，如以下示例所示。如果仅存在一个 SVM（虚拟服务器），则无需指定 `-vserver` 参数。

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

AWS Secrets Manager 密钥或 KMS 密钥配置不正确

亚马逊 FSx 无法与你的 Microsoft Active Directory 域控制器或控制器建立连接。这是因为您的 AWS Secrets Manager 密钥或配置不 AWS KMS key 正确。有关更多信息，请参阅 使用存储活动目录凭证 AWS Secrets Manager。

要解决配置错误问题，请执行以下操作：

- 验证密钥 ARN 是否正确且是否遵循正确的格式：`arn:aws:secretsmanager:region:account-id:secret:secret-name-6chars`。
- 验证密钥是否包含两个非空值的必填字段：
  - `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME`：AD 服务账号用户名。
  - `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD`：AD 服务账户密码。
- 验证密钥和密钥是否具有基于资源的策略，该策略授予 Amazon FSx 服务主体检索机密值的`fsx.amazonaws.com`权限。

排查 SSD 缩减操作问题

本节介绍与 SSD 容量缩减操作相关的常见问题和解决方案。

主题

- 由于 SSD 利用率较高，因此 SSD 缩减操作已暂停
- 由于 FlexClone 关系，您的 SSD 缩减操作已暂停
- 在 SSD 缩减期间，重定向客户端访问卷失败
- SSD 缩减操作的耗时超出预期

由于 SSD 利用率较高，因此 SSD 缩减操作已暂停

如果您的 SSD 存储层在缩减操作期间使用率超过 80%，Amazon FSx 会自动暂停该操作。您可能会看到类似于以下内容的管理操作消息：

```
Your file system has insufficient free space in aggr_1. Please free up space or
 increase your file system's storage capacity.
```

利用率低于 80% 后，操作将恢复。要解决此问题，您可以执行以下操作：

- 从已迁移至新磁盘的卷中删除多余数据。
- 通过修改卷分层策略，将更多数据分层到容量池中。
- 通过调用具有新目标值的 update-file-system，提交增加 SSD 容量的请求。

您应更新文件系统的 SSD 存储容量，确保在缩减操作后，文件系统的 SSD 容量利用率不超过 80%。有关更多详细信息，请参阅更新文件系统 SSD 存储和 IOPS。

通过检查 STORAGE_OPTIMIZATION 管理操作中的 Message 字段，您可以确定哪些卷已移动至新磁盘。

如果聚合为 aggr1 或 aggr1_old，也可以调用 describe-volumes。

由于 FlexClone 关系，您的 SSD 缩减操作已暂停

如果在启动 SSD 缩减操作后创建了FlexClone卷，Amazon 会 FSx 暂停该操作，直到克隆被删除。这是因为在移动卷时 ONTAP 会拆分克隆关系，这会导致新磁盘上的存储重复。要解决此问题，您可以识别并删除在缩减操作开始后创建的所有 FlexClone 卷。

删除所有 FlexClone 卷后，缩减操作将自动恢复。

在 SSD 缩减期间，重定向客户端访问卷失败

在固态硬盘缩减操作期间，Amazon FSx 需要将客户端访问权限从旧磁盘重定向到每个卷的新磁盘。如果此过程失败，您可能会看到类似于以下内容的管理操作消息：

```
Redirecting client access for volume(s) fsvol-123 has failed due to insufficient SSD
 IOPS, throughput capacity, or because the volume is full.
```

要解决此问题，您可以执行以下操作：

- 在 Amazon CloudWatch 中查看文件系统的资源利用率指标，确保您的工作负载消耗的资源不超过以下资源的 50%：
  - NetworkThroughputUtilization
  - FileServerDiskThroughputUtilization
  - FileServerDiskIopsUtilization
  - CPUUtilization
  - DiskIopsUtilization

- 如果卷已满，则增加卷的存储容量。
- 缩减操作期间，减少文件系统上的工作负载。

解决这些问题后，Amazon FSx 将自动重试每小时一次重定向客户端访问权限。

SSD 缩减操作的耗时超出预期

完成 SSD 缩减操作所需的时间取决于多个因素，包括文件系统中存储的数据量、当前的工作负载活动以及可用的系统资源。如果操作的耗时超出预期，则可以执行以下操作：

- 验证文件系统是否有足够的可用资源（CPU、磁盘吞吐量和 SSD IOPS 利用率均低于 50%）。
- 在操作期间减少写入密集型工作负载，以最大限度地减少资源争用。

通过检查 `STORAGE_OPTIMIZATION` 管理操作中的 `ProgressPercent` 属性，您可以跟踪操作的进度。

您无法将存储虚拟机（SVM）加入 Active Directory

如果您无法将 SVM 加入 Active Directory（AD），请先查看 如何加入微软 Ac SVMs tive Directory。以下部分列出了会阻碍 SVM 加入 Active Directory 的常见问题，包括针对每种情况生成的错误消息。

主题

- SVM NetBIOS 名称与主域的 NetBIOS 名称相同。
- SVM 已加入另一个 Active Directory
- Amazon FSx 无法连接到你的 Active Directory 域控制器，因为 SVM 的 NetBIOS 名称已在使用中
- 亚马逊 FSx 无法访问您的 Active Directory 服务账户证书 AWS Secrets Manager
- 亚马逊 FSx 无法与您的 Active Directory 域控制器通信
- 由于未满足的端口要求或服务账户权限，Amazon FSx 无法连接到您的 Active Directory
- 由于服务账户凭证无效，亚马逊 FSx 无法连接到您的 Active Directory 域控制器
- 由于服务账户凭证不足，亚马逊 FSx 无法连接到您的 Active Directory 域控制器
- 亚马逊 FSx 无法与您的 Active Directory DNS 服务器或域控制器通信
- 由于活动目录域名无效，亚马逊 FSx 无法与您的活动目录通信。
- 服务账户无法访问 SVM Active Directory 配置中指定的管理员组
- Amazon FSx 无法连接到 Active Directory 域控制器，因为指定的组织单位不存在或无法访问

SVM NetBIOS 名称与主域的 NetBIOS 名称相同。

将 SVM 加入自行管理的 Active Directory 时失败，并显示以下错误消息：

FSx Amazon 无法与您的活动目录建立连接。This is because the server name you specified is the NetBIOS name of the home domain. To fix this problem, choose a NetBIOS name for your SVM that is different from the NetBIOS name of the home domain. Then reattempt to join your SVM to your Active Directory.

要解决此问题，请按照 使用 AWS 管理控制台、 AWS CLI 和 API 加入 SVMs 活动目录 中所述的过程重新尝试将 SVM 加入 Active Directory。确保为 SVM 使用与 Active Directory 主域的 NetBIOS 名称不同的 NetBIOS 名称。

SVM 已加入另一个 Active Directory

将 SVM 加入 Active Directory 时失败，并显示以下错误消息：

FSx Amazon 无法与您的活动目录建立连接。This is because the SVM is already joined to a domain. To join this SVM to a different domain, you can use the ONTAP CLI or REST API to unjoin this SVM from Active Directory. Then reattempt to join your SVM to a different Active Directory.

要解决该问题，请执行以下操作：

1. 使用 NetApp ONTAP CLI 将 SVM 从其当前 Active Directory 中取消加入。有关更多信息，请参阅 使用 ONTAP CLI 从 SVM 取消加入活动目录 NetApp。
2. 按照 使用 AWS 管理控制台、 AWS CLI 和 API 加入 SVMs 活动目录 中所述的过程，重新尝试将 SVM 加入新 Active Directory。

Amazon FSx 无法连接到你的 Active Directory 域控制器，因为 SVM 的 NetBIOS 名称已在使用中

创建加入自行管理的 Active Directory 的 SVM 失败，并显示以下错误消息：

FSx Amazon 无法与您的活动目录建立连接。This is because the NetBIOS（computer）name you specified is already in-use in your Active Directory. To fix this problem, pick a NetBIOS name for your SVM that is not in use in your Active Directory., specifying a NetBIOS（computer）Then reattempt to join your SVM to your Active Directory.

要解决此问题，请按照 使用 AWS 管理控制台、 AWS CLI 和 API 加入 SVMs 活动目录 中所述的过程重新尝试将 SVM 加入 AD。确保为 SVM 使用的 NetBIOS 名称是唯一的，并且尚未在 Active Directory 中使用。

亚马逊 FSx 无法访问您的 Active Directory 服务账户证书 AWS Secrets Manager

以下各节描述常见问题及其解决方法。

将 SVM 加入自行管理的 Active Directory 失败，并显示以下错误消息：

```
You can't provide both username/password and a domain join service account secret to connect to your Active Directory. Provide only one set of credentials.
```

要解决此问题

1. 选择是提供存储在 Secrets Manager 密钥中的凭证，还是提供以纯文本形式存储的凭证。
2. 加入 Active Directory 时，仅提供其中一个参数，不能同时提供两个参数。

将 SVM 加入自行管理的 Active Directory 失败，并显示以下错误消息：

```
The domain join service account secret ARN format you entered isn't valid. Use the format: arn:partition:secretsmanager:region:account-id:secret:secret-name-6chars
```

要解决此问题

1. 审核 使用存储活动目录凭证 AWS Secrets Manager。
2. 验证您输入的 ARN 格式是否正确。正确的格式示例为 `arn:aws:secretsmanager:us-east-1:123456789012:secret:MyDatabaseSecret-Ab3d5f`。

将 SVM 加入自行管理的 Active Directory 失败，并显示以下错误消息：

```
Amazon FSx can't access the domain join service account secret [ARN]. Add a resource permission to the secret that grants the FSx service principal (fsx.amazonaws.com) permission to access it.
```

要解决此问题

1. 审核 使用存储活动目录凭证 AWS Secrets Manager。
2. 验证您提供的 Secrets Manager 密钥是否具有 FSx 允许亚马逊使用该密钥的正确策略。

将 SVM 加入自行管理的 Active Directory 失败，并显示以下错误消息：

```
You don't have permission to access the domain join service account secret [ARN]. A resource permission needs to be added to the secret to grant you access.
```

要解决此问题

- Secrets Manager 密钥所有者或管理员需要向您的账户授予使用该密钥的访问权限。有关更多信息，请参阅基于身份的策略。

将 SVM 加入自行管理的 Active Directory 失败，并显示以下错误消息：

```
The domain join service account secret format or content isn't valid. Make sure the secret includes both CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME and CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD fields with non-empty values.
```

要解决此问题

1. 审核 使用存储活动目录凭证 AWS Secrets Manager。
2. 验证您提供的 Secrets Manager 密钥是否同时包含两个必填字段。

亚马逊 FSx 无法与您的 Active Directory 域控制器通信

将 SVM 加入自行管理的 Active Directory 时失败，并显示以下错误消息：

FSx Amazon 无法与您的活动目录通信。要解决此问题，请确保允许在 Amazon FSx 和您的域控制器之间进行网络流量。Then reattempt to join your SVM to your Active Directory.

要解决此问题，请执行以下操作：

1. 请查看中所述的要求网络配置要求，并进行必要的更改，以启用 Amazon FSx 与您的 AD 之间的网络通信。

2. Amazon 能够与您 FSx 的 AD 通信后，请按照中所述的步骤进行操作，使用 AWS 管理控制台、AWS CLI 和 API 加入 SVMs 活动目录然后重新尝试将您的 SVM 加入您的广告。

由于未满足的端口要求或服务账户权限，Amazon FSx 无法连接到您的 Active Directory

将 SVM 加入自行管理的 Active Directory 时失败，并显示以下错误消息：

FSx Amazon 无法与您的活动目录建立连接。This is due to either the port requirements for your Active Directory not being met, or the service account provided not having permissions to join the storage virtual machine to the domain with the specified organization unit. 要修复此问题，请按照亚马逊 FSx 用户指南中的建议，在解决端口和服务账户的所有权限问题后，更新存储虚拟机的 Active Directory 配置。

要解决此问题，请执行以下操作：

1. 查看 网络配置要求 中描述的要求，进行必要的更改，以满足网络要求并确保在所需端口上启用通信
2. 查看 Active Directory 服务账户要求 中所述的服务账户要求。确保服务账户拥有所需的委托权限，有权将 SVM 加入使用指定组织单元的 Active Directory 域。
3. 更改端口权限或服务账户后，请按照 使用 AWS 管理控制台、 AWS CLI 和 API 加入 SVMs 活动目录 中所述的过程进行操作，重新尝试将 SVM 加入 AD。

由于服务账户凭证无效，亚马逊 FSx 无法连接到您的 Active Directory 域控制器

将 SVM 加入自行管理的 Active Directory 时失败，并显示以下错误消息：

由于提供的服务账户凭证无效，亚马逊 FSx 无法与您的 Active Directory 域控制器建立连接。To fix this problem, update your storage virtual machine's Active Directory configuration with a valid service account.

要解决此问题，请按照 使用 AWS 管理控制台、 AWS CLI和 API 更新现有 SVM Active Directory 配置 中所述的过程更新 SVM 的服务账户凭证。在输入服务账户用户名时，请确保仅包含用户名（例如，`ServiceAcct`），不要包含任何域前缀（例如，`corp.com\ServiceAcct`）或域后缀（例如，`ServiceAcct@corp.com`）。在输入服务账户用户名（例如，`CN=ServiceAcct,OU=example,DC=corp,DC=com`）时，请勿使用可分辨名称（DN）。

由于服务账户凭证不足，亚马逊 FSx 无法连接到您的 Active Directory 域控制器

将 SVM 加入自行管理的 Active Directory 时失败，并显示以下错误消息：

Amazon 无法与您 FSx 的 Active Directory 域控制器建立连接。This is due to either unmet port requirements for the Active Directory, or the service account provided does not have permission to join the storage virtual machine to the domain with the specified organizational unit.

要解决此问题，请确保您已向提供的服务账户委托所需的权限。服务账户必须能在文件系统加入的域的 OU 中创建和删除计算机对象。服务账户还必须至少有权执行以下操作：

- 重置密码
- 限制账户读取和写入数据
- 验证写入 DNS 主机名的能力
- 验证写入服务主体名称的能力
- 能够创建和删除计算机对象
- 验证读取和写入账户限制的能力

有关如何创建具有正确权限的服务账户的更多信息，请参阅 Active Directory 服务账户要求和向您的 Amazon FSx 服务账户委派权限。

亚马逊 FSx 无法与您的 Active Directory DNS 服务器或域控制器通信

将 SVM 加入自行管理的 Active Directory 时失败，并显示以下错误消息：

FSx Amazon 无法与您的活动目录通信。这是因为 Amazon FSx 无法访问为您的域名提供的 DNS 服务器或域控制器。To fix this problem, update your storage virtual machine's Active Directory configuration with valid DNS servers and a networking configuration that allows traffic to flow from the storage virtual machine to the domain controller.

要解决此问题，请执行以下过程：

1. 如果 Active Directory 中只有部分域控制器可以访问（例如，由于地理限制或防火墙），您可以添加首选域控制器。使用此选项，Amazon FSx 会尝试联系首选域控制器。使用 `vserver cifs domain preferred-dc add` NetApp ONTAP CLI 命令添加首选域控制器，如下所示：

a. 要访问 ONTAP CLI，请运行以下命令在 Amazon FSx for NetApp ONTAP 文件系统或 SVM 的管理端口上建立 SSH 会话。将 *management_endpoint_ip* 替换为文件系统管理端口的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

有关更多信息，请参阅 使用 ONTAP CLI 管理文件系统。

b. 输入以下命令，其中：

- `-vserver vserver_name` 指定存储虚拟机（SVM）的名称。
- `-domain domain_name` 指定所规定的域控制器所属域的完全限定 Active Directory 名称（FQDN）。
- `-preferred-dc IP_address,…` 按优先顺序，以逗号分隔列表的形式指定首选域控制器的一个或多个 IP 地址。

```
FsxId123456789::> vserver cifs domain preferred-dc add -vserver vserver_name -
domain domain_name -preferred-dc IP_address, …+
```

以下命令将域控制器 172.17.102.25 和 172.17.102.24 添加到首选域控制器的列表，借此 SVM vs1 上的 SMB 服务器可以管理 cifs.lab.example.com 域的外部访问。

```
FsxId123456789::> vserver cifs domain preferred-dc add -vserver vs1 -domain
 cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

2. 检查看看域控制器是否可以通过 DNS 解析。使用 `vserver services access-check dns forward-lookup` NetApp ONTAP CLI 命令根据指定的 DNS 服务器上的查找结果或虚拟服务器的 DNS 配置返回主机名的 IP 地址。

a. 要访问 ONTAP CLI，请运行以下命令在 Amazon FSx for NetApp ONTAP 文件系统或 SVM 的管理端口上建立 SSH 会话。将 *management_endpoint_ip* 替换为文件系统管理端口的 IP 地址。

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

有关更多信息，请参阅 使用 ONTAP CLI 管理文件系统。

b. 使用以下命令进入 ONTAP CLI 高级模式。

```
FsxId123456789::> set adv
```

c. 输入以下命令，其中：

- `-vserver vserver_name` 指定存储虚拟机（SVM）的名称。
- `-hostname host_name` 指定要在 DNS 服务器上查找的主机名。
- `-node node_name` 指定要执行命令的节点的名称。
- `-lookup-type` 指定要在 DNS 服务器上查找的 IP 地址的类型，默认为 `all`。

```
FsxId123456789::> vserver services access-check dns forward-lookup \
-vserver vserver_name -node node_name \
-domains domain_name -name-servers dns_server_ip_address \
-hostname host_name
```

3. 查看将 SVM 加入 AD 时需要提供的信息。
4. 查看将 SVM 加入 AD 时的联网要求。
5. 按照 网络配置要求 中所述的过程，使用 Active Directory DNS 服务器的正确 IP 地址更新 SVM 的 Active Directory 配置。

由于活动目录域名无效，亚马逊 FSx 无法与您的活动目录通信。

将 SVM 加入自行管理的 Active Directory 时失败，并显示以下错误消息：

亚马逊 FSx 已检测到所提供的 FQDN 无效。To fix this problem, update your storage virtual machine's Active Directory configuration with an FQDN that adheres to configuration requirements.

要解决此问题，请执行以下过程：

1. 查看 将 SVM 加入 Active Directory 时所需的信息 中所述的本地 Active Directory 域名要求，确保您尝试加入的 Active Directory 域名符合该要求。
2. 按照 使用 AWS 管理控制台、 AWS CLI 和 API 加入 SVMs 活动目录 中所述的过程，重新尝试将 SVM 加入 Active Directory。请务必为 Active Directory 域的 FQDN 使用正确的格式。

服务账户无法访问 SVM Active Directory 配置中指定的管理员组

将 SVM 加入自行管理的 Active Directory 时失败，并显示以下错误消息：

FSx Amazon 无法应用您的活动目录配置。This is because the administrators group you provided either doesn't exist or isn't accessible to the service account you provided. To fix this problem, ensure that your networking configuration allows traffic from the SVM to your Active Directory's domain controller(s) and DNS servers. Then update your SVM's Active Directory configuration, providing your Active Directory's DNS servers and, specifying an administrators group in the domain that is accessible to the service account provided.

要解决此问题，请执行以下操作：

1. 查看有关提供域组的信息，对 SVM 执行管理操作。确保您使用的是 Active Directory 域管理员组的正确名称。
2. 按照 使用 AWS 管理控制台、 AWS CLI 和 API 加入 SVMs 活动目录 中所述的过程，重新尝试将 SVM 加入 AD。

Amazon FSx 无法连接到 Active Directory 域控制器，因为指定的组织单位不存在或无法访问

将 SVM 加入自行管理的 Active Directory 时失败，并显示以下错误消息：

FSx Amazon 无法与您的活动目录建立连接。This is because the organizational unit you specified either doesn't exist or isn't accessible to the service account provided. To fix this problem, update your storage virtual machine's Active Directory configuration, specifying an organizational unit to which the service account has permissions to join.

要解决此问题，请执行以下操作：

1. 查看将 SVM 加入 AD 的先决条件。
2. 查看将 SVM 加入 AD 时需要提供的信息。
3. 按照此过程，使用正确的组织单位重新尝试将 SVM 加入 Active Directory。

您无法删除存储虚拟机或卷

每个 FSx ONTAP 文件系统可以包含一个或多个存储虚拟机 (SVMs)，每个 SVM 可以包含一个或多个卷。删除资源时，您必须首先确保其所有子资源均已删除。例如，在删除 SVM 之前，您必须首先删除 SVM 中的所有非根卷。

> **Important**
>
> 您只能使用亚马逊 FSx 控制台、API 和 CLI 删除存储虚拟机。只有在卷启用了亚马逊 FSx 备份的情况下，您才能使用亚马逊 FSx 控制台、API 或 CLI 删除该卷。

为了帮助保护您的数据和配置，Amazon FSx 禁止在某些情况下删除 SVMs 和卷。如果您尝试删除 SVM 或卷，但删除请求未成功，Amazon 会在 AWS 控制台、 AWS Command Line Interface (AWS CLI) 和 API 中 FSx 为您提供有关资源未被删除的原因的信息。解决删除失败的原因后，您可以重试删除请求。

主题

识别失败的删除

当您删除 Amazon FSx SVM 或卷时，通常会在几分钟内看到资源的`Lifecycle`状态转换`DELETING`为，然后资源才会从亚马逊 FSx 控制台、CLI 和 API 中消失。

如果您尝试删除某资源，其 `Lifecycle` 状态从 `DELETING` 变回 `CREATED`，则此行为表示该资源未成功删除。在这种情况下，Amazon FSx 会在控制台中`CREATED`生命周期状态旁边报告一个警报图标。选中该警报图标后会显示删除失败的原因。

以下各节提供了亚马逊 FSx 阻止 SVM 和卷删除的最常见原因，并 step-by-step说明了如何解决这些问题。

删除 SVM：路由表无法访问

每个 FSx 适用于 ONTAP 文件系统的路由表条目都会创建一个或多个路由表条目，以提供跨可用区域的自动故障转移和故障恢复。默认情况下，这些路由表条目在 VPC 的默认路由表中创建。您可以选择指定一个或多个可在其中创建 ONTAP 接口 FSx 的非默认路由表。Amazon FSx 会为其与文件系统关

联的每个路由表AmazonFSx添加标签，如果删除此标签，则可能会阻止 Amazon FSx 删除资源。如果出现这种情况，您会看到以下 LifecycleTransitionReason：

```
Amazon FSx is unable to complete the requested storage virtual machine operation because of an inability to access one or more of the route tables associated with your file system. Please contact ##.
```

您可以在 Amazon FSx 控制台的 “网络和安全” 选项卡下导航到文件系统的摘要页面，找到您的文件系统的路由表。

选择路由表链接，转到路由表。接下来，验证与文件系统关联的每个路由表是否都使用以下键值对进行了标记：

```
Key: AmazonFSx
Value: ManagedByAmazonFSx
```

如果此标签不存在，请重新创建，然后再次尝试删除 SVM。

删除 SVM：对等关系

如果您尝试删除属于对等关系的 SVM 或卷，则必须先删除对等关系，然后才能删除 SVM 或卷。此要求可防止对等互连设备 SVMs 变得不健康。如果 SVM 因对等关系而无法删除，您会看到以下 LifecycleTransitionReason：

Amazon FSx 无法删除存储虚拟机，因为它是 SVM 对等关系或过渡对等关系的一部分。Please delete the relationship and retry.

您可以通过 ONTAP CLI 删除 SVM 对等关系。要访问 ONTAP CLI，请按照 使用 ONTAP CLI 管理文件系统 中的步骤操作。使用 ONTAP CLI，执行以下步骤。

1. 使用以下命令检查 SVM 对等关系。将 *svm_name* 替换为 SVM 的名称。

   ```
   FsxId123456789::> vserver peer show -vserver svm_name
   ```

   如果此命令成功，您将看到类似以下内容的输出：

   ```
               Peer        Peer                           Peering        Remote
   Vserver     Vserver     State        Peer Cluster      Applications   Vserver
   ----------- ----------- ------------ ----------------- -------------- ---------
   svm_name    test2       peered       FsxId02d81fef0d84734b6
   ```

```
                                                          snapmirror     fsxDest
svm_name    test3       peered       FsxId02d81fef0d84734b6
                                                          snapmirror     fsxDest
2 entries were displayed.
```

2. 使用以下命令删除每个 SVM 对等关系。将 *svm_name* 和 *remote_svm_name* 替换为实际值。

```
FsxId123456789abcdef::> vserver peer delete -vserver svm_name -peer-
vserver remote_svm_name
```

如果此命令成功，您将看到以下输出：

```
Info: 'vserver peer delete' command is successful.
```

SVM 或卷删除： SnapMirror

正如不先删除对等关系就无法删除具有对等关系的 SVM（请参阅删除 SVM：对等关系）一样，如果不先删除关系，就无法删除存在 SnapMirror关系的 SVM。 SnapMirror 要删除 SnapMirror关系，请使用 ONTAP CLI 在作为 SnapMirror 关系目标的文件系统上执行以下步骤。要访问 ONTAP CLI，请按照 使用 ONTAP CLI 管理文件系统 中的步骤操作。

> **Note**
>
> Amazon FSx 备份 SnapMirror 用于创建 point-in-time文件系统卷的增量备份。您无法在 ONTAP CLI 中删除备份的此 SnapMirror 关系。但是，当您通过 AWS CLI、API 或控制台删除卷时，此关系会自动删除。

1. 使用以下命令列出您在目标文件系统上的 SnapMirror 关系。将 *svm_name* 替换为 SVM 的名称。

```
FsxId123456789abcdef::> snapmirror show -vserver svm_name
```

如果此命令成功，您将看到类似以下内容的输出：

```
Source            Destination    Mirror  Relationship   Total             Last
Path        Type  Path           State   Status         Progress  Healthy Updated
----------- ---- ------------    ------- -------------- --------- ------- --------
sourceSvm:sourceVol
            XDP  destSvm:destVol Snapmirrored
```

```
                                        Idle            -         true    -
```

2. 通过在目标文件系统上运行以下命令来删除您的 SnapMirror 关系。

```
FsxId123456789abcdef::> snapmirror release -destination-path destSvm:destVol -
source-path sourceSvm:sourceVol -force true
```

删除 SVM：启用 Kerberos 的 LIF

如果您尝试删除具有已启用 Kerberos 的逻辑接口（LIF）的 SVM，您必须先在该 LIF 上禁用 Kerberos，然后才能删除 SVM。

您可以通过 ONTAP CLI 在 LIF 上禁用 Kerberos。要访问 ONTAP CLI，请按照 使用 ONTAP CLI 管理文件系统 中的步骤操作。

1. 使用以下命令在 ONTAP CLI 中进入诊断模式。

```
FsxId123456789abcdef::> set diag
```

当系统提示继续操作时，请输入 **y**。

```
Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y
```

2. 检查哪些接口已启用 Kerberos。将 *svm_name* 替换为 SVM 的名称。

```
FsxId123456789abcdef::> kerberos interface show -vserver svm_name
```

如果此命令成功，您将看到类似以下内容的输出：

```
(vserver nfs kerberos interface show)
               Logical
Vserver        Interface     Address         Kerberos SPN
-------------- ------------- --------------- -------- ----------------------
svm_name       nfs_smb_management_1
                             10.19.153.48    enabled
5 entries were displayed.
```

3. 使用以下命令禁用 Kerberos LIF。将 *svm_name* 替换为 SVM 的名称。您需要提供在将此 SVM 加入 Active Directory 时使用的 Active Directory 用户名和密码。

```
FsxId123456789abcdef::> kerberos interface disable -vserver svm_name -lif
 nfs_smb_management_1
```

如果此命令成功，您将看到以下输出。提供在将此 SVM 加入 Active Directory 时使用的 Active Directory 用户名和密码。当系统提示继续操作时，请输入 **y**。

```
(vserver nfs kerberos interface disable)
Username: admin
Password: *************

Warning: This command deletes the service principal name from the machine account
 on the KDC.
Do you want to continue? {y|n}: y

Disabled Kerberos on LIF "nfs_smb_management_1" in Vserver "svm_name".
```

4. 使用以下命令验证 Kerberos 是否已在 SVM 上禁用。将 *svm_name* 替换为 SVM 的名称。

```
FsxId123456789abcdef::> kerberos interface show -vserver svm_name
```

如果此命令成功，您将看到类似以下内容的输出：

```
(vserver nfs kerberos interface show)
               Logical
Vserver        Interface     Address          Kerberos SPN
-------------- ------------- ---------------- -------- ----------------------
svm_name       nfs_smb_management_1
                             10.19.153.48     disabled
5 entries were displayed.
```

5. 如果接口显示为`disabled`，请尝试通过 AWS CLI、API 或控制台再次删除 SVM。

如果无法使用上述命令删除 LIF，您可以使用以下命令强制删除 Kerberos LIF。将 *svm_name* 替换为 SVM 的名称。

> **Important**
>
> 以下命令可以将 SVM 的计算机对象锁定在 Active Directory 上。

```
FsxId123456789abcdef::> kerberos interface disable -vserver svm_name -lif
 nfs_smb_management_1 -force true
```

如果此命令成功，您将看到类似以下内容的输出。当系统提示继续操作时，请输入 **y**。

```
(vserver nfs kerberos interface disable)

Warning: Kerberos configuration for LIF "nfs_smb_management_1" in Vserver
 "svm_name" will be deleted.
The corresponding account on the KDC will not be deleted. Do you want to continue?
 {y|n}: y
```

删除 SVM：其他原因

FSx 对于 ONTAP，当他们加入您的 Active Directory 时，在您的活动目录中 SVMs 创建一个计算机对象。在某些情况下，您可能需要使用 ONTAP CLI，手动从 Active Directory 中取消 SVM 的加入。要访问 ONTAP CLI，请按照 使用 ONTAP CLI 管理文件系统 中的步骤操作，使用 `fsxadmin` 凭证在文件系统级别登录 ONTAP CLI。使用 ONTAP CLI，按照以下步骤从 Active Directory 中取消 SVM 的加入。

> **Important**
>
> 此过程可以将 SVM 的计算机对象锁定在 Active Directory 上。

1. 使用以下命令在 ONTAP CLI 中进入高级模式。

```
FsxId123456789abcdef::> set adv
```

运行此命令后，您将看到此输出。输入 **y** 以继续。

```
Warning: These advanced commands are potentially dangerous; use them only when
      directed to do so by NetApp personnel.
      Do you want to continue? {y|n}: y
```

2. 使用以下命令删除 Active Directory 的 DNS。将 *svm_name* 替换为 SVM 的名称。

```
FsxId123456789abcdef::> vserver services name-service dns dynamic-update record
 delete -vserver svm_name -lif nfs_smb_management_1
```

> **Note**
>
> 如果 DNS 记录已删除或 DNS 服务器无法访问，则此命令失败。如果发生这种情况，请继续下一步操作。

3. 使用以下命令禁用 DNS。将 *svm_name* 替换为 SVM 的名称。

```
FsxId123456789abcdef::> vserver services name-service dns dynamic-update modify -
vserver svm_name -is-enabled false -use-secure false
```

如果此命令成功，您将看到以下输出：

```
Warning: DNS updates for Vserver "svm_name" are now disabled.
     Any LIFs that are subsequently modified or deleted
     can result in a stale DNS entry on the DNS server,
     even when DNS updates are enabled again.
```

4. 从 Active Directory 中取消设备的加入。将 *svm_name* 替换为 SVM 的名称。

```
FsxId123456789abcdef::> vserver cifs delete -vserver svm_name
```

运行此命令后，您将看到以下输出，其中 *CORP.EXAMPLE.COM* 替换为您的域名。在系统提示时，输入您的用户名和密码。当系统询问您是否要删除服务器时，请输入 **y**。

```
In order to delete an Active Directory machine account for the CIFS server,
you must supply the name and password of a Windows account with sufficient
privileges to remove computers from the "CORP.EXAMPLE.COM" domain.
Enter the user name: admin
Enter the password:
Warning: There are one or more shares associated with this CIFS server
     Do you really want to delete this CIFS server and all its shares? {y|n}: y
Warning: Unable to delete the Active Directory computer account for this CIFS
 server.
     Do you want to continue with CIFS server deletion anyway? {y|n}: y
```

删除卷： FlexCache 关系

除非先删除缓存关系，否则无法删除作为 FlexCache 关系源卷的卷。要确定哪些卷有关 FlexCache 系，可以使用 ONTAP CLI。要访问 ONTAP CLI，请按照 使用 ONTAP CLI 管理文件系统 中的步骤操作。

1. 使用以下命令检查 FlexCache 关系。

```
FsxId123456789abcdef::> volume flexcache origin show-caches
```

2. 使用以下命令删除缓存关系。将 *dest_svm_name* 和 *dest_vol_name* 替换为实际值。

```
FsxId123456789abcdef::> volume flexcache delete -vserver dest_svm_name -
volume dest_vol_name
```

3. 删除缓存关系后，再次尝试通过 AWS CLI、API 或控制台删除 SVM。

您的卷处于 MISCONFIGURED 状态

导致 ONTAP 卷处于 MISCONFIGURED 状态的潜在原因有很多，如以下主题所述。

您的卷容量已达 98% 以上

文件系统当前包含的卷容量已达 98% 以上。我们建议卷的利用率不要一直超过 95%。如果您没有在文件系统的下一个维护时段之前释放卷中的空间，Amazon FSx 将禁用对卷的机会性锁定，从而打破所有现有的 “oplocks”。修补过程完成后，Amazon FSx 将在该卷上重新启用 oplocks。为避免此情况，请将卷的存储容量利用率降至 98% 以下。实现这一目标的方法包括：

- 增加卷的大小。
- 删除不需要的数据。
- 删除不需要的快照。

有关更多信息，请参阅更新存储容量和删除快照。

您的离线卷有一个 iSCSI LUN 或 NVMe/TCP 命名空间

您的文件系统当前托管一个处于脱机状态的卷，该卷包含一个 iSCSI LUN 或 NVMe/TCP 命名空间，或两者兼而有之。我们建议您持续保持卷在线。如果您在文件系统的下一个维护时段之前没有联机此卷，Amazon FSx 将在修补操作期间暂时将此卷联机。为避免此情况，请联机或删除该卷。

要使离线卷恢复在线，应使用 volume online ONTAP CLI 命令，如以下示例所示。如果仅存在一个 SVM（虚拟服务器），则无需指定 -vserver 参数。

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

离线卷是 FlexCache 来源

您的文件系统包含处于脱机状态的 FlexCache 源卷。我们建议您持续保持卷在线。如果您在文件系统的下一个维护时段之前没有联机此卷，Amazon FSx 将在修补操作期间暂时将此卷联机。在此期间，可能会使用缓存卷中的数据将数据写回 FlexCache 原始卷。为避免此情况，请联机或删除该卷。

要使离线卷恢复在线，应使用 volume online ONTAP CLI 命令，如以下示例所示。如果仅存在一个 SVM（虚拟服务器），则无需指定 -vserver 参数。

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

离线卷属于 SnapMirror 关系的一部分

文件系统当前托管的卷处于离线状态，该卷是 SnapMirror 源卷或目标卷。我们建议您持续保持卷在线。如果您在文件系统的下一个维护时段之前没有联机此卷，Amazon FSx 将在修补操作期间暂时将此卷联机并暂停SnapMirror关系。在此期间，可能会使用 SnapMirror 源卷中的数据将数据写入 SnapMirror 目标卷。为避免此情况，请联机或删除该卷。

要使离线卷恢复在线，应使用 volume online ONTAP CLI 命令，如以下示例所示。如果仅存在一个 SVM（虚拟服务器），则无需指定 -vserver 参数。

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

您的受限卷包含 iSCSI LUN 或 NVMe/TCP 命名空间

您的文件系统当前托管一个处于受限状态的卷，该卷包含一个 iSCSI LUN、一个 NVMe/TCP 命名空间或两者兼而有之。我们建议您持续保持卷在线。如果您在文件系统的下一个维护时段之前没有联机此卷，Amazon FSx 将在修补操作期间暂时将此卷联机。为避免此情况，请联机或删除该卷。

要使离线卷恢复在线，应使用 volume online ONTAP CLI 命令，如以下示例所示。如果仅存在一个 SVM（虚拟服务器），则无需指定 -vserver 参数。

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

您的受限音量是 FlexCache 来源

您的文件系统包含处于受限状态的 FlexCache 源卷。我们建议您持续保持卷在线。如果您在文件系统的下一个维护时段之前没有联机此卷，Amazon FSx 将在修补操作期间暂时将此卷联机。在此期间，可能会使用缓存卷中的数据将数据写回 FlexCache 原始卷。为避免此情况，请联机或删除该卷。

要使离线卷恢复在线，应使用 volume online ONTAP CLI 命令，如以下示例所示。如果仅存在一个 SVM（虚拟服务器），则无需指定 -vserver 参数。

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

受限制卷属于 SnapMirror 关系的一部分

文件系统当前托管的卷处于受限制状态，该卷是 SnapMirror 源卷或目标卷。我们建议您持续保持卷在线。如果您在文件系统的下一个维护时段之前没有联机此卷，Amazon FSx 将在修补操作期间暂时将此卷联机并暂停SnapMirror关系。在此期间，可能会使用 SnapMirror 源卷中的数据将数据写入 SnapMirror 目标卷。为避免此情况，请联机或删除该卷。

要使离线卷恢复在线，应使用 volume online ONTAP CLI 命令，如以下示例所示。如果仅存在一个 SVM（虚拟服务器），则无需指定 -vserver 参数。

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

卷的存储容量不足

如果卷空间不足，您可以按照此处显示的过程来诊断和解决该问题。

主题

确定卷存储容量的使用情况

您可以使用 `volume show-space` NetApp ONTAP CLI 命令查看卷存储容量的消耗情况。此类信息可以帮助您决定如何回收或节省卷存储容量。有关更多信息，请参阅 监控卷的存储容量（控制台）。

增加卷的存储容量

您可以使用亚马逊 FSx 控制台和亚马逊 FSx API 来增加卷的存储容量。 AWS CLI有关如何通过增加容量来更新卷的更多信息，请参阅更新卷。

或者，您可以使用 `volume modify` NetApp ONTAP CLI 命令增加卷的存储容量。有关更多信息，请参阅 更改卷的存储容量（控制台）。

使用卷自动调整大小

您还可以使用卷自动调整大小，以便卷在达到已用空间阈值时，自动增加指定的量或增加到指定大小。您可以使用 ONTAP `volume autosize` NetApp CLI 命令对 FlexVol 卷类型（这是 ONTAP FSx 的默认卷类型）执行此操作。有关更多信息，请参阅 启用自动调整大小。

文件系统的主存储空间已满

如果您 FSx 的 for ONTAP 文件系统的主存储空间已满，则即使某个卷显示其具有足够的可用存储容量，也无法向文件系统中的卷添加任何数据。您可以在 Amazon FSx 控制台文件系统详情页面的 “监控和性能” 选项卡中查看可用的主存储容量。有关更多信息，请参阅 监控 SSD 存储利用率。

要解决此问题，您可以增加文件系统主存储层的大小。有关更多信息，请参阅 更新文件系统 SSD 存储和 IOPS。

删除快照

默认情况下，使用默认快照策略在卷上启用快照。快照存储于卷根的 .snapshot 目录中。您可以通过以下方式管理快照的卷存储容量：

- 手动删除快照 – 通过手动删除快照来回收存储容量。
- 创建快照自动删除策略 – 创建策略，比默认快照策略更积极地删除快照。
- 关闭自动快照 – 通过关闭自动快照来节省存储容量。

当删除快照时，回收的存储量不会等于当前删除的快照的大小。您可以使用卷快照 com pute-recleamable-vserver ONTAP CLI 命令查看删除快照时可以回收的存储量，使用您的数据来替换、和。*svm_name vol_name snapshot_name*

```
fsid8970abc52::> volume snapshot compute-reclaimable -vserver svm_name -volume vol_name
 -snapshot snapshot_name
A total of 667648 bytes can be reclaimed.
```

有关删除快照和管理快照策略以节省存储容量的更多信息，请参阅删除快照。

增加卷的文件容量上限

当 FSx 可用信息节点或文件指针的数量用完时，适用于 ONTAP 的卷可能会耗尽文件容量。默认情况下，可用索引节点数与卷大小的对应关系为 1 比 32KiB。有关更多信息，请参阅 卷文件容量。

卷中索引节点的数量随卷的存储容量（最高阈值为 648 GiB）相应增加。默认情况下，存储容量为 648GiB 或以上的卷都具有相同数量的索引节点，即 21,251,126。要查看卷的文件容量上限，请参阅监控卷的文件容量。

如果您创建了大于 648 GiB 的卷，并且希望其索引节点数超过 21,251,126，您必须手动增加卷上文件的数量上限。如果卷存储容量不足，您可以检查其文件容量上限。如果已接近文件容量，您可以手动增加容量。有关更多信息，请参阅 增加卷上文件的数量上限（ONTAP CLI）。

卷容量不足导致备份失败

卷的每日自动备份失败，并显示以下消息：

```
Amazon FSx could not create a backup of your volume because the backup snapshot was
 deleted.
```

由于卷上的可用存储容量不足，每日自动备份失败。要缓解这种情况，您需要释放卷上的存储容量。您可以根据具体情况采用以下其中一种或多种选项：

- 增加卷的存储容量
- 增加卷的快照预留
- 禁用快照自动删除
- 不要使用 ONTAP CLI 删除备份快照

FSx 为 ONTAP 卷恢复已删除的内容

删除 fo FSx r ONTAP 卷后，该卷将被置于ONTAP's恢复队列中。虽然您可以使用 ONTAP CLI 直接从该队列中恢复卷，但恢复的卷不会重新出现在 AWS 控制台或 Amazon FSx API 中，并且之前应用于该卷的任何 AWS 标签都将永久丢失。要在保留 AWS 集成和基于标签的安全策略的同时正确恢复 for ONTAP 卷，您可以将备份还原到新卷，也可以使用将该卷的数据复制到新卷。 FSx SnapMirror有关ONTAP's 恢复队列的更多信息，请参阅 NetApp's 文档。

排除网络问题

如果遇到网络问题，您可以按照此处显示的过程来诊断问题。

您想捕获数据包跟踪

数据包跟踪流程验证数据包通过各层到达目的地的路径。您可以使用以下 NetApp ONTAP CLI 命令来控制数据包跟踪流程：

- network tcpdump start – 开始数据包跟踪
- network tcpdump show – 显示当前正在运行的数据包跟踪
- network tcpdump stop – 停止正在运行的数据包跟踪

这些命令可供在文件系统上拥有 `fsxadmin` 角色的用户使用。

从文件系统捕获数据包跟踪

1. 要通过 SSH 登录文件系统的 NetApp ONTAP CLI，请按照《Amazon for 使用 NetApp ONTAP CLI NetApp ONTAP 用户指南》中记录的步骤 FSx 进行操作。

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. 使用以下命令在 ONTAP CLI 中进入诊断权限级别。

```
::> set diag
```

当系统提示继续操作时，请输入 y。

```
Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y
```

3. 确定文件系统上用于保存数据包跟踪的位置。卷必须处于在线状态，并且必须安装于具有有效连接路径的命名空间中。使用以下命令检查符合以下标准的卷：

```
::*> volume show -junction-path !- -fields junction-path
vserver volume    junction-path
------- --------- -------------
fsx     test_vol1 /test_vol1
fsx     test_vol2 /test_vol2
fsx     test_vol2 /test_vol3
```

4. 使用最少的必需参数开始跟踪。替换以下内容：

   - *node_name*替换为节点的名称（例如，FsxId01234567890abcdef-01）。
   - *svm_name*替换为存储虚拟机的名称（例如，fsx）。
   - *junction_path_name*替换为卷名（例如，test-vol1）。

```
::*> debug network tcpdump start -node node_name -ipspace Default -pass-through "-i
 e0e -w /clus/svm_name/junction_path_name"
Info: Started network trace on interface "e0e"
Warning: Snapshots should be disabled on the tcpdump destination volume while
 packet traces are occurring. Use the
"volume modify -snapshot-policy none -vserver fsx -volume test_vol1" command to
 disable Snapshots on the
```

```
tcpdump destination volume.
```

> **Important**
>
> 只能在 e0e 接口和 Default IP 空间中捕获数据包跟踪。在 FSx ONTAP 中，所有网络流量都使用该e0e接口。

使用数据包跟踪时，请注意以下几点：

- 开始数据包跟踪时，必须包含要存储跟踪文件的路径，格式为：/clus//*svm_namejunction-path-name*
- （可选）提供数据包跟踪的文件名。如果未指定 filter_name，则会自动生成格式为：*node-name*_ _ .trc *port-name yyyymmdd_hhmmss*
- 如果滚动跟踪已指定，则 filter_name 后跟数字，表示旋转序列中的位置。
- ONTAP CLI 还接受以下可选 -pass-through 参数：

```
-B, --buffer-size=<KiB>
-c <number_of_packets>
-C <file_size-mB>
-F <filter_expression_filename>
-G <rotate_seconds>
--time-stamp-precision {micro|nano}
-Q, --direction {in|out|inout}
-s, --snapshot-length=<bytes>
-U, --packet-buffered
-W <rotate_file_count>
<filter-expression>
```

- 有关筛选器表达式的信息，请参阅 pcap-filter（7）手册页。

5. 查看正在进行的跟踪：

```
::*> debug network tcpdump show
Node                    IPspace  Port     Filename
----------------------  -------- -------- --------
FsxId123456789abcdef-01  Default  e0e      /clus/fsx/test_vol1/
FsxId123456789abcdef-01_e0e_20230605_181451.trc
```

6. 停止跟踪：

```
::*> debug network tcpdump stop -node FsxId123456789abcdef-01 -ipspace Default -
port e0e
Info: Stopped network trace on interface "e0e"
```

7. 返回管理员权限级别：

```
::*> set -priv admin
::>
```

8. 访问数据包跟踪。

   数据包跟踪存储在您使用 debug network tcpdump start 命令指定的卷中，可通过 NFS 导出或与该卷对应的 SMB 共享进行访问。

有关捕获包跟踪的更多信息，请参阅 如何在 NetApp Knowledge Base 的 ONTAP 9.10+ 中使用调试网络 dump。

对 I/O 错误和 NFS 锁回收失败进行故障排除

本节介绍了 ONTAP 文件系统的故障转移事件期间与 I/O 错误和 NFS 锁回收失败有关的问题，以及每个问题的解决方案。 FSx

在故障转移事件期间您遇到了 I/O 错误

在 FSx ONTAP 单可用区文件系统的故障转移开启期间，NFS 客户端可能会遇到暂时错误或长时间暂 I/O 停。对于 NFSv4 + 客户端，您可能会看到内核日志消息，例如：

```
NFS: __nfs4_reclaim_open_state: Lock reclaim failed!
```

这些消息表明，在故障转移窗口期间，客户端无法成功收回 NFS 锁。

减少故障转移事件期间的 I/O 错误

在 Linux 上，您可以在客户端上配置网络设置，将故障转移检测时间从 55-60 秒缩短到 15-20 秒。

> **Important**
>
> 务必先在非生产环境中测试这些配置。这些设置会增加地址解析协议 (ARP) 流量，该协议用于将 IP 地址映射到本地网络上的物理 (MAC) 地址，可能不适合网络受限的环境。

为 NFS 客户端配置优化的网络设置

1. 在每个 NFS 客户端上创建一个 sysctl 配置文件。以下示例用于`default`将设置应用于所有网络接口。如果您的实例有多个网络接口，则可以`default`替换为用于连接您的 for ONTAP 单可用区文件系统的特定接口名称（例如`eth0`或`ens5`）： FSx

```
$ sudo tee /etc/sysctl.d/99-fsx-failover.conf > /dev/null << 'EOF'
# NFS client optimizations for faster failover detection
# Replace 'default' with your interface name (e.g., eth0, ens5) to target a
 specific interface
net.ipv4.neigh.default.base_reachable_time_ms=5000
net.ipv4.neigh.default.delay_first_probe_time=1
net.ipv4.neigh.default.ucast_solicit=0
net.ipv4.tcp_syn_retries=3
EOF
```

2. 立即应用设置：

```
$ sudo sysctl -p /etc/sysctl.d/99-fsx-failover.conf
```

3. 验证配置是否处于活动状态。如果您使用了`default`，则可以使用以下命令进行验证。如果您指定了特定的接口，请`default`用您的接口名称替换（例如，`eth0`或`ens5`）：

```
$ sysctl net.ipv4.neigh.default.base_reachable_time_ms
$ sysctl net.ipv4.neigh.default.delay_first_probe_time
$ sysctl net.ipv4.neigh.default.ucast_solicit
$ sysctl net.ipv4.tcp_syn_retries
```

确保在同一可用区内连接到您 FSx 的 for ONTAP 文件系统的所有 NFS 客户端上一致地应用这些设置。使用这些网络优化时，请记住以下几点：

- base_reachable_time_ms=5000 — 将 ARP 缓存条目的有效期从 30 秒缩短到 5 秒，使客户端能够在故障转移事件期间更快地检测 IP 所有权的变化。
- delay_first_probe_time=1 — 将探测陈旧网络条目之前的延迟从 5 秒缩短到 1 秒。
- ucast_solicit=0 — 跳过单播邻居探测器并立即发出广播 ARP 请求，从而加快对活动文件服务器的重新发现。
- tcp_syn_retries=3 — 将 TCP 连接重试持续时间从 127 秒缩短到 15 秒。

网络设置完成后，您应监控环境以验证更改。您可以通过修改文件系统的吞吐容量来测试故障转移事件。有关更多信息，请参阅 在文件系统上测试失效转移。

应用更改后监控您的环境

- 监控系统日志中是否有 NFS 错误，以查看 NFS 相关的内核日志消息。

```
$ sudo journalctl -f | grep -i nfs
```

  确认出现的消息次数是否较少，例如。`Lock reclaim failed`
- 监控应用程序日志，以确认在故障转移事件期间减少 I/O 超时、连接错误和重试相关故障。
- 验证网络影响，确保增加的 ARP 流量不会对环境中的网络性能产生不利影响。

NFSv4 环境的替代方法

在无法修改客户端配置的 NFSv4 环境中，请考虑以下替代方案：

- 延长 NFSv4 租赁超时时间。请与您的存储管理员合作，延长 NFSv4 租赁超时时间。延长这些超时时间可以让客户端有更多时间在故障转移事件期间回收锁定。有关更多信息，请参阅NetApp ONTAP文档中的指定 NFSv4 锁定宽限期。

适用于 ONTAP 的 Amazon FSx 的文档历史记录 NetApp

- API 版本：2018-03-01
- 最新文档更新：2026 年 5 月 1 日

下表描述了 Amazon FSx NetApp ONTAP 用户指南的重要更改。如需有关文档更新的通知，您可以订阅 RSS 源。

变更	说明	日期
添加了其他 AWS 区域 支持	Second-generation (Multi-AZ 2 和 Single-AZ 2) ONTAP 文件系统的 FSx 现已在欧洲（伦敦）、亚太地区（海得拉巴）、南美（圣保罗）和 AWS GovCloud （ ）上市。US-West 有关更多信息，请参阅按 AWS 区域划分的可用性。	2026年6月3日
添加了其他 AWS 区域 支持	适用于 ONTAP 文件系统的 FSx 现已在亚太地区（新西兰）上市。有关更多信息，请参阅按 AWS 区域划分的可用性。	2026 年 5 月 1 日
为适用于 ONTAP 的 Amazon FSx 的 Amazon S3 接入点增加了支持 NetApp	适用于 NetApp ONTAP 的 Amazon FSx 的 Amazon S3 接入点提供了一种使用亚马逊 S3 API 访问存储在 FSx for ONTAP 文件系统中的数据的新方式。借助 Amazon S3 接入点，您无需更改现有文件系统配置即可简化 Amazon S3-enabled 应用程序的数据访问。有关更多信息，请参阅使用适用于 ONTAP 的 Amazon	2025 年 12 月 2 日

	FSx 的 Amazon S3 接入点。NetApp	
为 AWS Secrets Manager 集成添加了 Support	Amazon FSx 现已与集成，AWS Secrets Manager 以增强对活动目录凭证的管理。有关更多信息，请参阅使用 AWS Secrets Manager存储 Active Directory 凭证。	2025 年 11 月 5 日
AmazonFSxConsoleFullAccess— 更新现有政策	Amazon FSx 添加了一项新权限`secretsmanager:ListSecrets` ，允许委托人列出 AWS Secrets Manager 用于选择域加入服务账户凭证的密码。有关更多信息，请参阅 AWS 托管策略： AmazonFSxFullAccess。	2025 年 11 月 5 日
NetApp BlueXP 已重命名为 NetApp Console	NetApp BlueXP 现在称为 NetApp Console。有关更多信息，请参阅使用 NetApp 控制台。	2025 年 10 月 16 日
添加了对互联网协议版本 6（IPv6）的支持	适用于 ONTAP 文件系统的 FSx 现在支持两种网络类型选项： IPv4-only 和双堆栈（同时适用于 IPv4 和 IPv6）。创建文件系统时，您必须指定其中一种选项。可随时更改现有 FSx for ONTAP 文件系统的网络类型。有关更多信息，请参阅管理网络类型。	2025 年 9 月 30 日

添加了其他 AWS 区域 支持	Second-generation (Multi-AZ 2 和 Single-AZ 2) 适用于 ONTAP 文件系统的 FSx 现已在亚太地区（首尔）、加拿大（中部）、欧洲（西班牙）和欧洲（苏黎世）推出。有关更多信息，请参阅按 AWS 区域划分的可用性。	2025 年 9 月 30 日
添加了其他 AWS 区域 支持	FSx for ONTAP 文件系统现已在亚太地区（台北）区域推出。有关更多信息，请参阅按 AWS 区域划分的可用性。	2025 年 8 月 18 日
添加了对减少 SSD 存储容量的支持	FSx for ONTAP 现在允许您减少第二代文件系统上文件系统的固态硬盘（SSD）存储容量，从而帮助您针对具有不同高性能存储需求的工作负载优化存储成本。有关更多信息，请参阅何时减少 SSD 存储容量。	2025 年 8 月 14 日
亚马逊 FSx 更新了托管政策 AmazonFSxServiceRolePolicy AWS	Amazon FSx 向添加了`ec2:AssignIpv6Addresses` 和`ec2:UnassignIpv6Addresses` 权限。 AmazonFSxServiceRolePolicy有关更多信息，请参阅 Amazon FSx 对 AWS 托管策略的更新。	2025 年 7 月 22 日

亚马逊 FSx 更新了托管政策 AmazonFSxFullAccess AWS	AmazonFSxFullAccess托管策略已更新，添加了fsx:CreateAndAttachS3AccessPoint fsx:DescribeS3AccessPointAttachments 、和fsx:DetachAndDeleteS3AccessPoint 权限。	2025 年 6 月 25 日
亚马逊 FSx 更新了托管政策 AmazonFSxConsoleFullAccess AWS	AmazonFSxConsoleFullAccess托管策略已更新，添加了fsx:CreateAndAttachS3AccessPoint fsx:DescribeS3AccessPointAttachments 、和fsx:DetachAndDeleteS3AccessPoint 权限。	2025 年 6 月 25 日
FSx for ONTAP 支持 Amazon Elastic VMware Service	FSx for ONTAP 现可用作 Amazon EVS 的外部数据存储。有关更多信息，请参阅将 Amazon Elastic VMware Service 与 FSx for ONTAP 结合使用。	2025 年 6 月 9 日
添加了其他 AWS 区域 支持	Second-generation (Multi-AZ 2 和 Single-AZ 2) 适用于 ONTAP 文件系统的 FSx 现已在亚太地区（东京）和亚太地区（孟买）推出。有关更多信息，请参阅按 AWS 区域划分的可用性。	2025 年 6 月 2 日

添加了对 FlexCache 写回模式的支持	FSx for ONTAP 卷现在支持 FlexCache 写回模式。有关更多信息，请参阅使用 FlexCache 复制数据。	2025 年 5 月 28 日
添加了其他 AWS 区域 支持	FSx for ONTAP 文件系统现已在亚太地区（泰国）和墨西哥（中部）推出。有关更多信息，请参阅按 AWS 区域划分的可用性。	2025 年 5 月 8 日
现已支持自主勒索软件防护（ARP）	ARP 是一项监控和防范勒索软件和恶意软件攻击的 NetApp AI-driven 功能，FSx for ONTAP 现已支持。有关更多信息，请参阅使用自主勒索软件防护保护数据	2025 年 4 月 7 日
《FSx for ONTAP 用户指南》中的新主题描述了如何在工作组中设置 SMB 服务器	在工作组中设置 SMB 服务器描述了如何在 SVM 的工作组中设置 SMB 服务器，以此作为将 SVM 加入 Microsoft Active Directory 的替代方案。	2025 年 3 月 4 日
亚马逊 FSx 更新了托管政策 AmazonFSxConsoleReadOnlyAccess AWS	Amazon FSx 更新了 AmazonFSxConsoleReadOnlyAccess 政策以添加权限。`ec2:DescribeNetworkInterfaces` 有关更多信息，请参阅 AmazonFSxConsoleReadOnlyAccess 策略。	2025 年 2 月 25 日

现在支持其他 Harvest 控制面板	FSx for ONTAP 现在支持其他 Harvest 控制面板，包括默认情况下未启用的控制面板。还添加了 FSx for ONTAP 不支持的控制面板列表。有关更多信息，请参阅使用 Harvest 和 Grafana 监控 FSx for ONTAP 文件系统。	2025 年 2 月 18 日
《FSx for ONTAP 用户指南》中添加了全新的 FSx for ONTAP 账单和使用情况报告主题	适用于 ONTAP 的 FSx AWS 账单和使用情况报告主题说明了如何在控制台中访问 ONTAP 文件系统 FSx 的账单使用情况报告。 AWS 账单与成本管理该主题还提供两个报告中特定于 FSx for ONTAP 的所有使用类型。	2025 年 2 月 13 日
添加了对 Amazon FSx 双堆栈 VPC 接口端点的支持	现在，您可以为 Amazon FSx 创建同时具有 IPv4 和 IPv6 IP 地址和 DNS 名称的双堆栈 VPC 接口端点。有关更多信息，请参阅 FSx for ONTAP 和接口 VPC 端点。	2025 年 2 月 7 日
添加了对双堆栈 API 端点的支持	用于创建和管理文件系统的 Amazon FSx 服务 API 具有新的双堆栈端点。有关更多信息，请参阅《Amazon FSx API 参考》中的 API 端点。	2025 年 2 月 7 日

亚马逊 FSx 更新了托管政策 AmazonFSxConsoleFullAccess AWS	Amazon FSx 更新了 AmazonFSxConsoleFullAccess 政策以添加权限。`ec2:DescribeNetworkInterfaces` 有关更多信息，请参阅 AmazonFSxConsoleFullAccess 策略。	2025 年 2 月 7 日
新主题已发布，使用 FlexCache 复制数据	发布了一个新主题，该主题描述了如何使用本地 ONTAP 文件系统中的数据将本地 ONTAP 文件系统中的数据复制到 FSx for ONTAP 文件系统 FlexCache 。有关更多信息，请参阅使用复制数据。FlexCache	2024 年 12 月 19 日
添加了对第二代文件系统的支持	现在，您可以创建第二代 Single-AZ 和 Multi-AZ 文件系统。现在，单个高可用性（HA）对最高可提供 6Gbps 的吞吐能力和 20 万的 SSD IOPS。有关更多信息，请参阅 High-availability (HA) 对。	2024 年 7 月 9 日
添加了对从备份中恢复卷时读取卷中数据的支持	现在，当从第二代文件系统的备份中还原文件数据时，就可以挂载具有数据只读访问权限的卷。有关更多信息，请参阅还原备份到新卷。	2024 年 7 月 9 日
添加了对调整第二代文件系统的吞吐能力的支持	现在，在创建第二代文件系统后，您可以调整其吞吐能力。有关更多信息，请参阅管理吞吐能力。	2024 年 7 月 9 日

增加了对向第二代 Single-AZ 文件系统添加 HA 对的支持	现在，您可以在创建后将 HA 对添加到第二代 Single-AZ 文件系统中。第二代 Single-AZ 文件系统上总共可以有 12 个 HA 对。有关更多信息，请参阅添加高可用性（HA）对。	2024 年 7 月 9 日
增加了对 Non-Volatile Memory Express over TCP (NVMe/TCP) 协议的支持	现在，您可以在适用于 NetApp ONTAP NVMe/TCP 文件系统的 Amazon FSx 上使用该协议进行数据传输。有关更多信息，请参阅使用块存储协议	2024 年 7 月 9 日
添加了对文件系统管理用户的 `fsxadmin-readonly` 角色的支持	`fsxadmin-readonly` 角色现在可供 ONTAP 文件系统管理用户使用，可用于 NetApp Harvest 等文件系统监视应用程序。有关更多信息，请参阅文件系统管理员角色和用户。	2024 年 4 月 30 日
添加了对面向 Windows 域管理用户的 SSH 公钥身份验证的支持	您现在可以对 Active Directory 域文件系统和 SVM 用户使用 SSH 公钥身份验证。有关更多信息，请参阅为 ONTAP 用户配置 Active Directory 身份验证。	2024 年 4 月 30 日

添加了对横向扩展文件系统拥有 12 个 HA 对的支持	适用于 NetApp ONTAP 的 Amazon FSx 增加了对横向扩展文件系统中的 12 个 HA 对的支持。具有 12 个 HA 对的文件系统可以在这 12 个高可用性（HA）对中提供高达 72Gbps 的吞吐能力和 240 万的 SSD IOPS。有关更多信息，请参阅 High-availability (HA) 对和 Amazon FSx 以了解 NetApp ON TAP 性能。	2024 年 3 月 4 日
添加了对云写入模式的支持	适用于 NetApp ONTAP 的 Amazon FSx 增加了对卷云写入模式的支持。有关更多信息，请参阅在卷上启用云写入模式。	2024 年 2 月 6 日
添加了 Support 对使用备份 FlexGroup 卷的支持 AWS Backup	现在，您可以使用在适用 AWS Backup 于 ONTAP 文件系统的 FSx 上备份和恢复 FlexGroup 卷。有关更多信息，请参阅AWS Backup 与 Amazon FSx 配合使用。	2024 年 1 月 11 日

Amazon FSx 更新了 AmazonFSxFullAccess、 AmazonFSxConsoleFullAccess、 AmazonFSx ReadOnlyAccess AmazonFSx ConsoleReadOnlyAccess、 和托管政策 AmazonFSx ServiceRolePolicy AWS	Amazon FSx 更新了 AmazonFSxFullAccess AmazonFSxConsoleFullAccess、 AmazonFSx ReadOnlyAccess、 AmazonFSxConsoleReadOnlyAccess、和 AmazonFSxServiceRolePolicy 策略以添加权限。`ec2:GetSecurityGroupsForVpc` 有关更多信息，请参阅 Amazon FSx 对 AWS 托管策略的更新。	2024 年 1 月 9 日
Amazon FSx 更新了 AmazonFSxFullAccess 和托管政策 AmazonFSxConsoleFullAccess AWS	Amazon FSx 更新了 AmazonFSxFullAccess 和 AmazonFSxConsoleFullAccess 政策以添加操作。`ManageCrossAccountDataReplication` 有关更多信息，请参阅 Amazon FSx 对 AWS 托管策略的更新。	2023 年 12 月 20 日
添加了对横向扩展指标的支持	FSx for ONTAP 现在为具有多个 H CloudWatch A 对的文件系统提供亚马逊指标。有关更多信息，请参阅Scale-out 文件系统指标。	2023 年 11 月 26 日

添加了对横向扩展文件系统的支持	适用于 NetApp ONTAP 的 Amazon FSx 增加了对横向扩展文件系统的支持，该系统可以在六个高可用性 (HA) 对中提供高达 36 Gbps 的吞吐容量和 1200,000 个固态硬盘 IOPS。有关更多信息，请参阅 High-availability (HA) 对和 Amazon FSx 以了解 NetApp ON TAP 性能。	2023 年 11 月 26 日
为 FlexGroup 卷添加了 Support	适用于 NetApp ONTAP 的 Amazon FSx 增加了对卷的支持。 FlexGroup 有关更多信息，请参阅卷风格。	2023 年 11 月 26 日
为 Multi-AZ 文件系统增加了共享 VPC 支持	参与者账户现在可以在已与其共享的 VPC 中创建 Multi-AZ 文件系统。拥有者账户可在 Amazon FSx 控制台、CLI 和 API 中管理此功能。有关更多信息，请参阅在共享子网中创建 FSx for ONTAP 文件系统	2023 年 11 月 26 日
Amazon FSx 更新了 AmazonFSxFullAccess 和托管政策 AmazonFSxConsoleFullAccess AWS	Amazon FSx 更新了 AmazonFSxFullAccess 和 AmazonFSxConsoleFullAccess 政策以添加权限。`fsx:CopySnapshotAndUpdateVolume` 有关更多信息，请参阅 Amazon FSx 对 AWS 托管策略的更新。	2023 年 11 月 26 日

Amazon FSx 更新了 AmazonFSxFullAccess 和托管政策 AmazonFSxConsoleFullAccess AWS	Amazon FSx 更新了 AmazonFSxFullAccess 和 AmazonFSxConsoleFullAccess 政策，添加了`fsx:DescribeSharedVPCConfiguration` 和权限。`fsx:UpdateSharedVPCConfiguration` 有关更多信息，请参阅 Amazon FSx 对 AWS 托管策略的更新。	2023 年 11 月 14 日
添加了对创建其他 ONTAP 角色和用户的支持	适用于 NetApp ONTAP 的 Amazon FSx 现在支持创建其他 ONTAP 角色和用户，以在使用 ONTAP CLI 和 REST API 时定义用户能力和权限。有关更多信息，请参阅适用于 ONTAP 的 Amazon FSx 中的角色和用户。 NetApp	2023 年 9 月 6 日
增加了对其他 CloudWatch 指标和增强型监控仪表板的支持	FSx for ONTAP 现可提供更多性能指标，并增加了一个增强型监控面板，提高了对文件系统活动的可见性。有关更多信息，请参阅使用进行监控 CloudWatch。	2023 年 8 月 17 日
亚马逊 FSx 更新了托管政策 AmazonFSxServiceRolePolicy AWS	Amazon FSx 更新了中的`cloudwatch:PutMetricData` 权限。 AmazonFSx ServiceRolePolicy有关更多信息，请参阅 Amazon FSx 对 AWS 托管策略的更新。	2023 年 7 月 24 日

增加了直接使用 NetApp 系统管理器的 Support	您可以直接从 NetApp BlueXP 使用 System Manager 管理 FSx for ONTAP 文件系统。有关更多信息，请参阅在 BlueXP 中使用 NetApp 系统管理器。	2023 年 7 月 13 日
添加了对监控 EMS 事件的支持	您可以使用 NetAPP ONTAP 的本机 Events Managemen t System (EMS) 监控 FSx for ONTAP 文件系统事件。您可以使用 NetApp ONTAP CLI 查看 EMS 事件。有关更多信息，请参阅监控 FSx for ONTAP EMS 事件。	2023 年 7 月 13 日
添加了对 SnapLock 的支持	FSx for ONTAP 现可支持 SnapLock 卷。SnapLock 允许您通过将文件转换为“一次写入，多次读取”（WORM）状态来保护文件，从而在指定的保留期内防止文件修改或删除。适用于 ONTAP 的 FSx 支持合规和企业保留模式。 SnapLock 有关更多信息，请参阅使用 SnapLock。	2023 年 7 月 13 日
添加了对传输中数据进行 IPsec 加密的支持	FSx for ONTAP 现在支持使用 IPsec 加密对文件系统及连接的客户端之间的传输中数据进行加密。有关更多信息，请参阅使用 PSK 身份验证配置 IPsec 和使用证书身份验证配置 IPsec。	2023 年 7 月 13 日

增加了最大卷大小	FSx for ONTAP 将最大卷大小从 100TB 增加到 300TB。有关更多信息，请参阅开启自动调整卷大小。	2023 年 7 月 13 日
亚马逊 FSx 更新了托管政策 AmazonFSxFullAccess AWS	Amazon FSx 更新了 AmazonFSxFullAccess 政策，删除了`fsx:*`权限并添加了具体`fsx`操作。有关更多信息，请参阅AmazonFSxFullAccess政策。	2023 年 7 月 13 日
亚马逊 FSx 更新了托管政策 AmazonFSxConsoleFullAccess AWS	Amazon FSx 更新了 AmazonFSxConsoleFullAccess 政策，删除了`fsx:*`权限并添加了具体`fsx`操作。有关更多信息，请参阅AmazonFSxConsoleFullAccess政策。	2023 年 7 月 13 日
添加了将现有存储虚拟机加入 Active Directory 的支持	您可以使用 AWS 管理控制台、 AWS CLI 和 API 将现有存储虚拟机加入活动目录。有关更多信息，请参阅将 SVM 加入 Active Directory。	2023 年 6 月 13 日
为 Single-AZ 文件系统增加了对 NVMe 读取缓存的支持	2022 年 11 月 28 日之后创建且吞吐容量至少为 2 Gbps Single-AZ 的文件系统现在支持 NVMe 读取缓存，这些系统位于美国东部（俄亥俄州）区域、美国东部（弗吉尼亚北部）地区、美国西部（俄勒冈）地区和欧洲（爱尔兰）。有关更多信息，请参阅部署类型对性能的影响。	2022 年 11 月 28 日

增加了对使用 vPC 内的 IP 地址范围创建 Multi-AZ 文件系统的支持	现在，您可以通过指定位于您的 VPC 的 IP 地址范围内的终端节点来为 ONTAP 文件系统创建 Multi-AZ FSx。有关更多信息，请参阅创建 FSx for ONTAP 文件系统。	2022 年 11 月 28 日
增加了对更新 Multi-AZ 文件系统上的 VPC 路由表的 Support	现在，您可以将新的 VPC 路由表与适用于 ONTAP 文件系统的现有 Multi-AZ FSx 关联（添加），也可以将现有 VPC 路由表与现有 FSx fo Multi-AZ r ONTAP 文件系统取消关联（删除）。有关更多信息，请参阅更新文件系统。	2022 年 11 月 28 日
增加了对使用 AWS Nitro System 传输的数据进行加密的 Support	从在美国东部（俄亥俄州）区域、美国东部（弗吉尼亚州北部）区域、美国西部（俄勒冈州）区域和欧洲地区（爱尔兰）受支持的 Amazon EC2 实例中访问时，传输中数据会自动加密。有关更多信息，请参阅使用 AWS Nitro System 对传输中的数据进行加密。	2022 年 11 月 28 日
添加了对创建 DP 卷的支持	现在，您可以使用亚马逊 FSx 控制台 AWS CLI或 Amazon FSx API 创建 DP（数据保护）卷。当您想要迁移 NetApp SnapMirror 或保护单个卷的数据时，可以使用 DP 卷作为或SnapVault关系的目标。有关更多信息，请参阅卷类型。	2022 年 11 月 28 日

添加了对将卷标签复制到备份的支持	现在，您可以在 AWS CLI 或 Amazon FSx API 中启用 `CopyTagsToBackups` ，自动将标签从卷复制到备份。有关更多信息，请参阅将标签复制到备份。	2022 年 11 月 28 日
添加了对选择快照策略的支持	现在，在使用 Amazon FSx 控制台或 Amazon FSx API 创建或更新卷时 AWS CLI，您可以从三个内置快照策略中进行选择。您还可以选择您在 ONTAP CLI 或 REST API 中创建的自定义快照策略。有关更多信息，请参阅快照策略。	2022 年 11 月 28 日
添加了对额外文件系统吞吐能力选项的支持	现在，FSx for ONTAP 为 2022 年 11 月 28 日之后在美国东部（俄亥俄州）区域、美国东部（弗吉尼亚州北部）区域、美国西部（俄勒冈州）区域和欧洲地区（爱尔兰）创建的文件系统提供 4096 Mbps 吞吐能力的支持。有关更多信息，请参阅吞吐能力对性能的影响。	2022 年 11 月 28 日
添加了对额外 SSD IOPS 的支持	现在，FSx for ONTAP 支持为 2022 年 11 月 28 日之后在美国东部（俄亥俄州）区域、美国东部（弗吉尼亚州北部）区域、美国西部（俄勒冈州）区域和欧洲地区（爱尔兰）创建的文件系统提供 160,000 SSD IOPS 的支持。有关更多信息，请参阅吞吐能力对性能的影响。	2022 年 11 月 28 日

增加了对使用适用于 ONTAP 的 FSx 作为 VMware Cloud 的外部数据存储库的支持 AWS	您可以将适用于 ONTAP 的 FSx 用作 VMware Cloud on Data Center (SDDC) 的外部 AWS Software-Defined数据存储库。这种新增的支持提供了灵活性，可以独立于 AWS 工作负载上的 VMware Cloud 计算资源向上或向下扩展存储。有关更多信息，请参阅将 VMware Cloud 与 FSx for ONTAP 结合使用。	2022 年 8 月 30 日
自动增加文件系统的存储容量	使用的 SSD 存储容量超过您指定的阈值时，使用 AWS开发的可自定义 CloudFormation 模板自动增加文件系统的存储容量。有关更多信息，请参阅动态增加 SSD 存储容量。	2022 年 6 月 3 日
亚马逊 FSx 现已与 AWS Backup	现在，除了使用原 AWS Backup 生 Amazon FSx 备份外，您还可以使用备份和恢复 FSx 文件系统。有关更多信息，请参阅AWS Backup 与 Amazon FSx 配合使用。	2022 年 5 月 18 日
添加了对单可用区 ONTAP 文件系统部署的支持	您可以为 ONTAP 文件系统创建 Single-AZ FSx，这些文件系统旨在在单个可用区 (AZ) 内提供高可用性和持久性。有关更多信息，请参阅选择文件系统部署。	2022 年 4 月 13 日

为 AWS PrivateLink 接口 VPC 终端节点添加了 Support	现在可以使用接口 VPC 端点从 VPC 访问 Amazon FSx API，而无需通过互联网发送流量。有关更多信息，请参阅 Amazon FSx 和接口 VPC 端点。	2022 年 4 月 5 日
添加了对修改现有 ONTAP 文件系统吞吐能力的支持	现在，您可以修改现有 ONTAP 文件系统的可用吞吐能力。有关更多信息，请参阅管理吞吐能力。	2022 年 3 月 30 日
添加了对扩展 SSD 存储容量和预调配 IOPS 的支持	现在，您可以随着存储和 IOPS 要求的变化增加 FSx for Lustre 现有文件系统的 SSD 存储容量和预调配 IOPS。有关更多信息，请参阅管理存储容量和预调配 IOPS。	2022 年 1 月 25 日
为亚马逊 CloudWatch 指标添加了 Support	您可以使用 Amazon 监控您的文件系统 CloudWatch，Amazon 会收集来自 FSx for ONTAP 的原始数据并将其处理为可读的近乎实时的指标。有关更多信息，请参阅使用 Amazon 进行监控 CloudWatch。	2022 年 1 月 19 日
添加了对其他文件系统吞吐量选项的支持	FSx for ONTAP 现在支持 128MBps 和 256MBps 文件系统吞吐量选项。有关更多信息，请参阅吞吐能力对性能的影响。	2021 年 11 月 30 日

适用于 NetApp ONTAP 的 Amazon FSx 现已正式上市	FSx for ONTAP 是一项完全托管的服务，可在 ONTAP 文件系统上提供高度可靠、可扩展、高性能和功能丰富的文件存储。 NetApp它提供了 NetApp 文件系统熟悉的特性、性能、功能和 API，并具有完全托管 AWS 服务的敏捷性、可扩展性和简单性。	2021 年 9 月 2 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。