aws

ONTAP 用户指南

FSx for ONTAP

FSx for ONTAP: ONTAP 用户指南

Table of Contents

什么是 ONTAP 版 Amazon FS NetApp x？

适用于 NetApp ONTAP 的 Amazon FSx 是一项完全托管的服务，它基于广受欢迎的 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。 NetAppFSx for ONTAP 将 NetApp 文件系统熟悉的特性、性能、功能和 API 操作与完全托管的敏捷性、可扩展性和简单性相结合。 AWS 服务

FSx for ONTAP 提供功能丰富、快速且灵活的共享文件存储，可在本地或本地运行的 Linux、Windows 和 macOS 计算实例中广泛访问这些存储空间。 AWS 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、备份或突发 AWS 到本地的理想解决方案，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 还提供了与其他 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高达每秒数十 GB (GBps)
- 使用网络文件系统（NFS）、服务器消息块（SMB）和互联网小型计算机系统接口（iSCSI）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
- Support 对 NetApp的 SnapMirror 复制功能的支持
- S NetApp upport 对本地缓存解决方案的支持： NetApp 全局文件缓存和 FlexCache
- Support 支持使用本机 AWS 或 NetApp 工具和 API 操作进行访问和管理
  - AWS Management Console、 AWS Command Line Interface (AWS CLI) 和 SDK
  - NetApp ONTAP CLI、REST API 和 BlueXP
- 支持以下数据保护和安全功能：
  - 使用加密文件系统数据和静态备份 AWS KMS keys
  - 使用 SMB Kerberos 会话密钥对传输中的数据进行加密
  - 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
  - NetAppSnapLockWORM 功能，支持合规卷和企业卷

安全与数据保护

Amazon FSx 提供多个级别的安全性和合规性，便于保护您的数据。它使用您在 AWS Key Management Service (AWS KMS) 中管理的密钥自动加密文件系统和备份中的静态数据。您还可以使用适用于 NFS 和 SMB 客户端的 Kerberos 对传输中数据进行加密。

经评估，Amazon FSx 符合以下标准：

- 国际标准组织（ISO）
- 支付卡行业数据安全标准 (PCI DSS)
- 系统和组织控制（SOC）认证
- 1996 年版健康保险流通与责任法案（HIPAA）

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

Amazon FSx 还提供以下级别的访问控制：

- 在文件系统级别，Amazon FSx 使用 Amazon Virtual Private Cloud（Amazon VPC）安全组来控制访问权限。
- 在 API 级别，Amazon FSx 通过使用 AWS Identity and Access Management (IAM) 访问策略提供访问控制。
- 为提供文件和文件夹级别的访问控制，Amazon FSx 支持 Unix 权限、NFS 访问控制列表（ACL）和 NTFS ACL。当您将 Amazon FSx 加入 Active Directory 时，正在访问文件系统的用户可以使用其 Active Directory 凭证进行身份验证。

为了让您可以看到用户对您的亚马逊 FSx 资源执行的操作，Amazon FSx 与之集成， AWS CloudTrail 以监控和记录您的 Amazon FSx API 调用。有关更多信息，请参阅 使用 AWS CloudTrail 对 FSx for ONTAP API 调用进行日志记录。

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。

FSx for ONTAP 的定价

文件系统的费用按以下类别来计费：

- 固态硬盘存储容量（每月 GB 或 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）

有关与该服务相关的定价和费用的更多信息，请参阅适用于 NetApp ONTAP 的 Amazon FSx 定价。

FSx for ONTAP 论坛

如果您在使用 Amazon FSx 时遇到问题，请通过 FSx for ONTAP 论坛获取答案。

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. 如果您不熟 AWS悉设置 FSx for ONTAP，请参阅设置 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。

适用于 ONTAP 的 Amazon FSx 的工作原理 NetApp

本主题介绍了适用于 NetApp ONTAP 文件系统的 Amazon FSx 的主要功能及其工作原理，并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 for ONTAP 文件系统

文件系统是 ONTAP 资源的主要 FSx，类似于本地 ONTAP 集群。 NetApp 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。

您的文件系统可以有 1 到 12 个高可用性 (HA) 对，具体取决于其配置。HA 对由两台采用主动-备用配置的文件服务器组成。具有单个 HA 对的文件系统称为纵向扩展文件系统。具有多个 HA 对的文件系统称为横向扩展文件系统。有关更多信息，请参阅 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。访问 FSx for ONTAP 文件系统中的数据时，客户端和工作站会使用 SVM 的端点 IP 地址与 SVM 进行交互。有关更多信息，请参阅 管理 SVM。

您可以将 SVM 加入 Microsoft Active Directory 进行文件访问身份验证和授权。有关更多信息，请参阅 在 FSx for ONTAP 中使用 Microsoft Active Directory。

卷

FSx for ONTAP 卷是用于组织数据和对数据进行分组的虚拟资源。卷是托管在 SVM 上的逻辑容器，存储在其中的数据会消耗文件系统的物理存储容量。

创建卷时，需要设置其大小，这决定了无论数据存储在哪个存储层上，您都可以在其中存储的物理数据量。您还可以设置卷类型，即 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。

适用于 ONTAP 卷的 FSx 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。对于精简配置的卷，无需提前预留存储容量。相反，存储空间是根据需要动态分配的。删除卷或 LUN 中的数据后，可用空间将释放回文件系统。例如，您可以在配置有 10 TiB 可用存储容量的文件系统上创建三个 10 TiB 卷，前提是这三个卷中存储的数据总量在任何时候都不超过 10 TiB。卷上物理存储的数据量计入您的总体存储容量消耗。有关更多信息，请参阅 管理 FSx for ONTAP 卷。

存储层

FSx for 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 for ONTAP 存储层。

数据分层

数据分层是 Amazon FSx f NetApp or ONTAP 自动在固态硬盘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，用于控制数据在变为非活动状态（冷）时是否将其移动到容量层。卷的分层策略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

适用于 NetApp ONTAP 的 Amazon FSx 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 FSx for ONTAP 存储效率。

访问存储在 FSx for ONTAP 文件系统上的数据

您可以通过 NFS（v3、v4、v4.1、v4.2）和 SMB 协议，同时从多个 Linux、Windows 或 macOS 客户端访问 FSx for ONTAP 卷上的数据。您还可以使用 iSCSI（块）协议以编程方式访问数据。有关更多信息，请参阅 访问 数据。

管理 FSx for ONTAP 资源

您可以通过多种方式与 FSx for ONTAP 文件系统交互并管理其资源。您可以使用这两种 AWS 工具和 ONTAP 管理工具管理您的 FSx for NetApp ONTAP 资源：

- AWS 管理工具
  - 的 AWS Management Console
  - 的 AWS Command Line Interface (AWS CLI)
  - Amazon FSx API 和 SDK
  - AWS CloudFormation
- NetApp 管理工具：
  - NetApp BlueXP
  - NetApp ONTAP CLI
  - NetApp ONTAP REST API

有关更多信息，请参阅 管理资源。

设置 FSx for ONTAP

首次使用 Amazon FSx 前，请完成以下任务：

1. 注册获取 AWS 账户
2. 创建具有管理访问权限的用户

主题

注册获取 AWS 账户

如果您没有 AWS 账户，请完成以下步骤来创建一个。

报名参加 AWS 账户

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

   在注册时，将接到一通电话，要求使用电话键盘输入一个验证码。

   当您注册时 AWS 账户，就会创建AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务 和资源。作为安全最佳实践，请为用户分配管理访问权限，并且只使用根用户来执行需要根用户访问权限的任务。

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

创建具有管理访问权限的用户

注册后，请保护您的安全 AWS 账户 AWS 账户根用户 AWS IAM Identity Center，启用并创建管理用户，这样您就不会使用 root 用户执行日常任务。

保护你的 AWS 账户根用户

1. 选择 Root 用户并输入您的 AWS 账户 电子邮件地址，以账户所有者的身份登录。AWS Management Console在下一页上，输入您的密码。

   要获取使用根用户登录方面的帮助，请参阅《AWS 登录 用户指南》中的以根用户身份登录。

2. 为您的根用户启用多重身份验证 (MFA)。

   有关说明，请参阅 I A M 用户指南中的为 AWS 账户 根用户启用虚拟 MFA 设备（控制台）。

创建具有管理访问权限的用户

1. 启用 IAM Identity Center

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的启用 AWS IAM Identity Center。

2. 在 IAM Identity Center 中，为用户授予管理访问权限。

   有关使用 IAM Identity Center 目录 作为身份源的教程，请参阅《用户指南》 IAM Identity Center 目录中的使用默认设置配置AWS IAM Identity Center 用户访问权限。

以具有管理访问权限的用户身份登录

- 要使用您的 IAM Identity Center 用户身份登录，请使用您在创建 IAM Identity Center 用户时发送到您的电子邮件地址的登录网址。

  有关使用 IAM Identity Center 用户登录的帮助，请参阅AWS 登录 用户指南中的登录 AWS 访问门户。

将访问权限分配给其他用户

1. 在 IAM Identity Center 中，创建一个权限集，该权限集遵循应用最低权限的最佳做法。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的创建权限集。

2. 将用户分配到一个组，然后为该组分配单点登录访问权限。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的添加组。

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。

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。

主题

第 1 步：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。

快速创建选项可创建具有单个高可用性对 (HA)、单个存储虚拟机 (SVM) 和单个卷的文件系统。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。

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 FSx for ONTAP 文件系统。

要创建文件系统，请执行以下操作：

1. 通过以下网址打开 Amazon FSx 控制台：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，选择多可用区或单可用区。
    - 多可用区文件系统可复制数据并支持在同一 AWS 区域的多个可用区之间进行失效转移。

- 单可用区文件系统可复制数据，并在单个可用区内提供自动失效转移。

有关更多信息，请参阅 可用性与持久性。

7. 对于 SSD 存储容量，请指定文件系统的存储容量，以 GiB (GiB) 为单位。输入 1024 – 196608 内的任意整数。如果您需要更多的 SSD 存储容量，则可以使用标准创建。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. 对于吞吐容量，Amazon FSx 会根据您的固态硬盘存储自动提供建议的吞吐容量。您还可以选择文件系统的吞吐量（最高 4,096 Mbps）。如果您需要更高的吞吐容量，则可以使用标准创建。

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

10. 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。

11. （仅限多可用区）端点 IP 地址范围指定 IP 地址范围，用于访问您文件系统的端点将在此范围中创建。

    端点 IP 地址范围选择快速创建选项：

    - VPC 中未分配的 IP 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 IP 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。

    - VPC 外的浮动 IP 地址范围 – 选择此选项可使 Amazon FSx 使用的 198.19.x.0/24 地址范围尚未被任何具有相同 VPC 和路由表的其他文件系统使用。

    您也可以在标准创建选项中指定自己的 IP 地址范围。

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。

步骤 2：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。

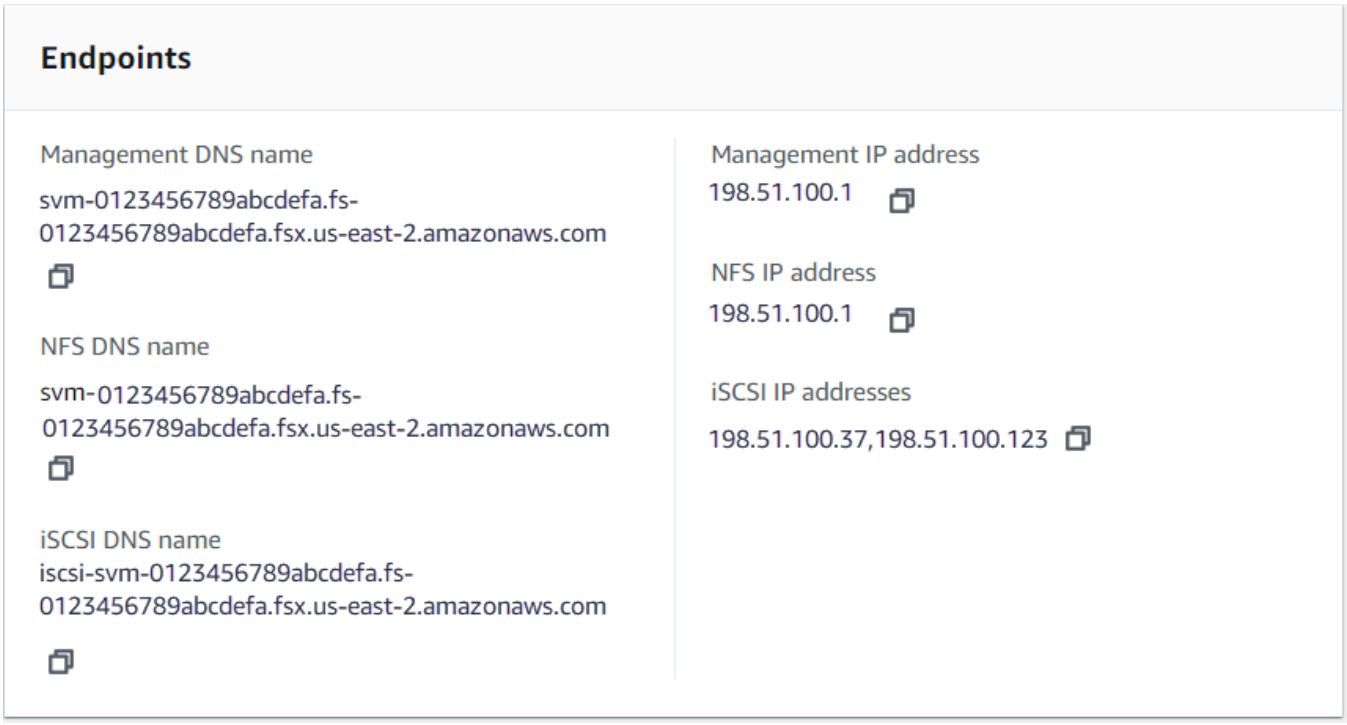
从 Amazon EC2 挂载文件系统

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
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您的 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，将 *`mount-point`* 替换为您自己的信息。

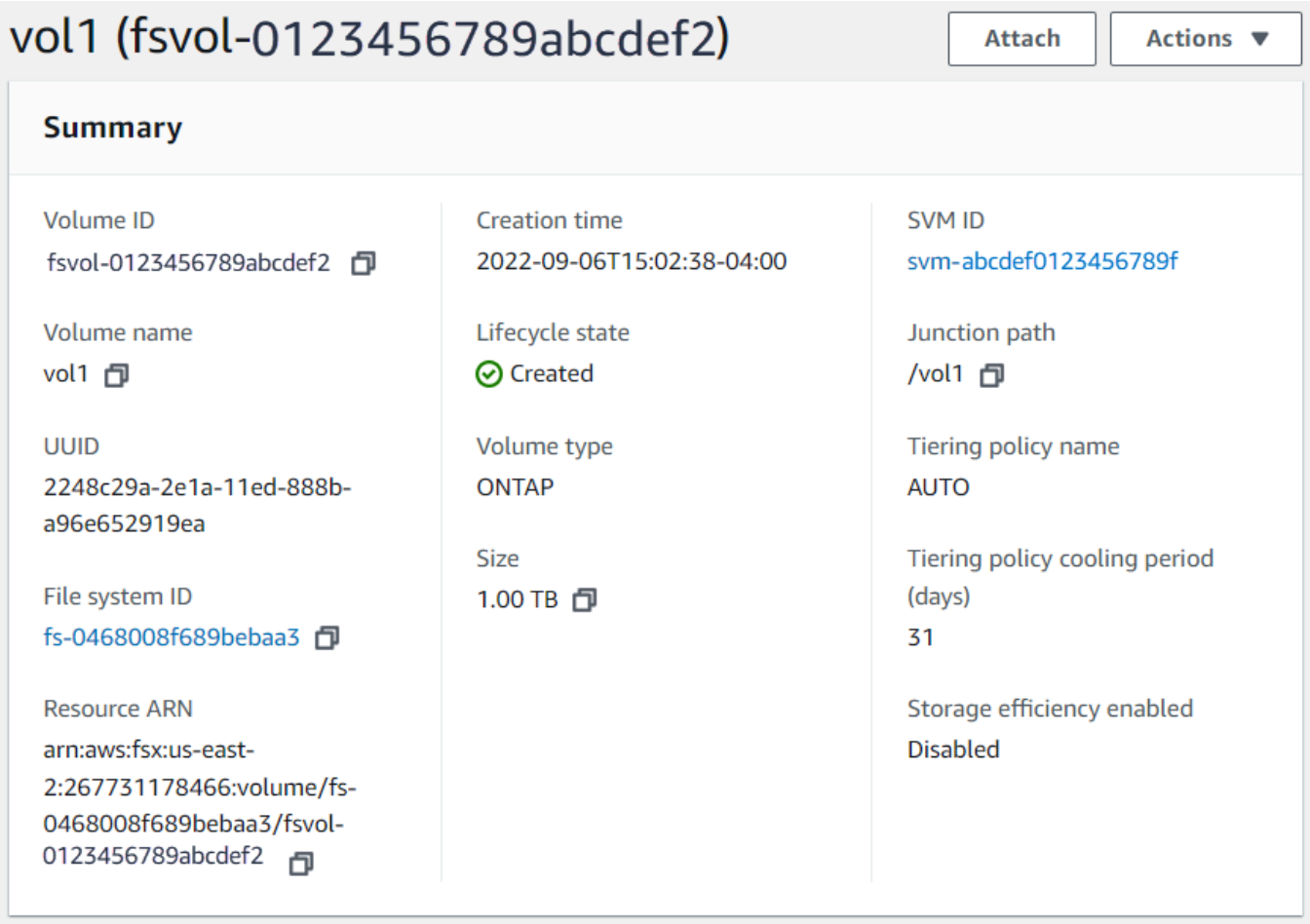
   ```
   $ sudo mkdir /mount-point
   ```

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 名称位于端点面板上，如下图所示。



- *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，如下图所示。



- *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 实例疑难解答。

步骤 3：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 用户指南中的终止您的实例。
2. 通过以下网址打开 Amazon FSx 控制台：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。

访问 数据

无论是在本地环境中，还是在本地环境中，您都可以使用各种支持的客户端和方法来访问您的 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`— 用于使用互联网小型计算机系统接口 (iSCSI) 协议进行连接（仅适用于向上扩展的文件系统）。
- `Management`— 用于使用 NetApp ONTAP CLI 或 API 或 BlueXP 管理 SVM NetApp

主题

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。

支持将以下 AWS 计算实例与 FSx for ONTAP 配合使用：

- 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 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 Amazon Elastic Container Service 与 FSx for ONTAP 一起使用。
- 亚马逊 Elastic Kubernetes Service — 要了解更多信息，请参阅亚马逊 EKS 用户指南中的亚马逊 FSx for 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 使用 Amazon 和 F WorkSpaces Sx for ONTAP。
- 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 FSx 为无服务器工作负载启用 SMB 访问权限。
- 在 VMware 云 AWS 环境中运行的虚拟机 (VM)。有关更多信息，请参阅使用适用于 ONTAP 的 Amazon FSx 配置为外部存储和使用适用于 NetApp ONTAP 的 A AWS mazon FSx 配置为外部存储和开启 VMware Cloud 部署指南。 NetApp

挂载后，FSx for ONTAP 文件系统在 NFS 和 SMB 上显示为本地目录或驱动器号，提供完全托管式共享网络文件存储，可供多达数千个客户端同时访问。通过 iSCSI 挂载时，iSCSI LUN 可以作为块设备进行访问。

从内部访问数据 AWS

每个 Amazon FSx 文件系统都与虚拟私有云（VPC）相关联。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 FSx for ONTAP 文件系统。您也可以从其他 VPC 访问您的文件系统，这些VPC可能位于不同的 AWS 账户中，或者 AWS 区域。除了以下各节中描述的访问 FSx for 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。

主题

- 访问同一 VPC 中的数据
- 从部署 VPC 外部访问数据

访问同一 VPC 中的数据

在创建适用于 NetApp ONTAP 文件系统的亚马逊 FSx 时，您可以选择它所在的亚马逊 VPC。与 NetApp 适用于 ONTAP 的 Amazon FSx 文件系统关联的所有 SVM 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。有关更多信息，请参阅 挂载卷。

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，然后选择要挂载其卷的 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部署 VPC 之外的 AWS 位置访问适用于 ONTAP 文件系统终端节点的 FSx。

访问多可用区文件系统上的 NFS、SMB 和 ONTAP 管理端点

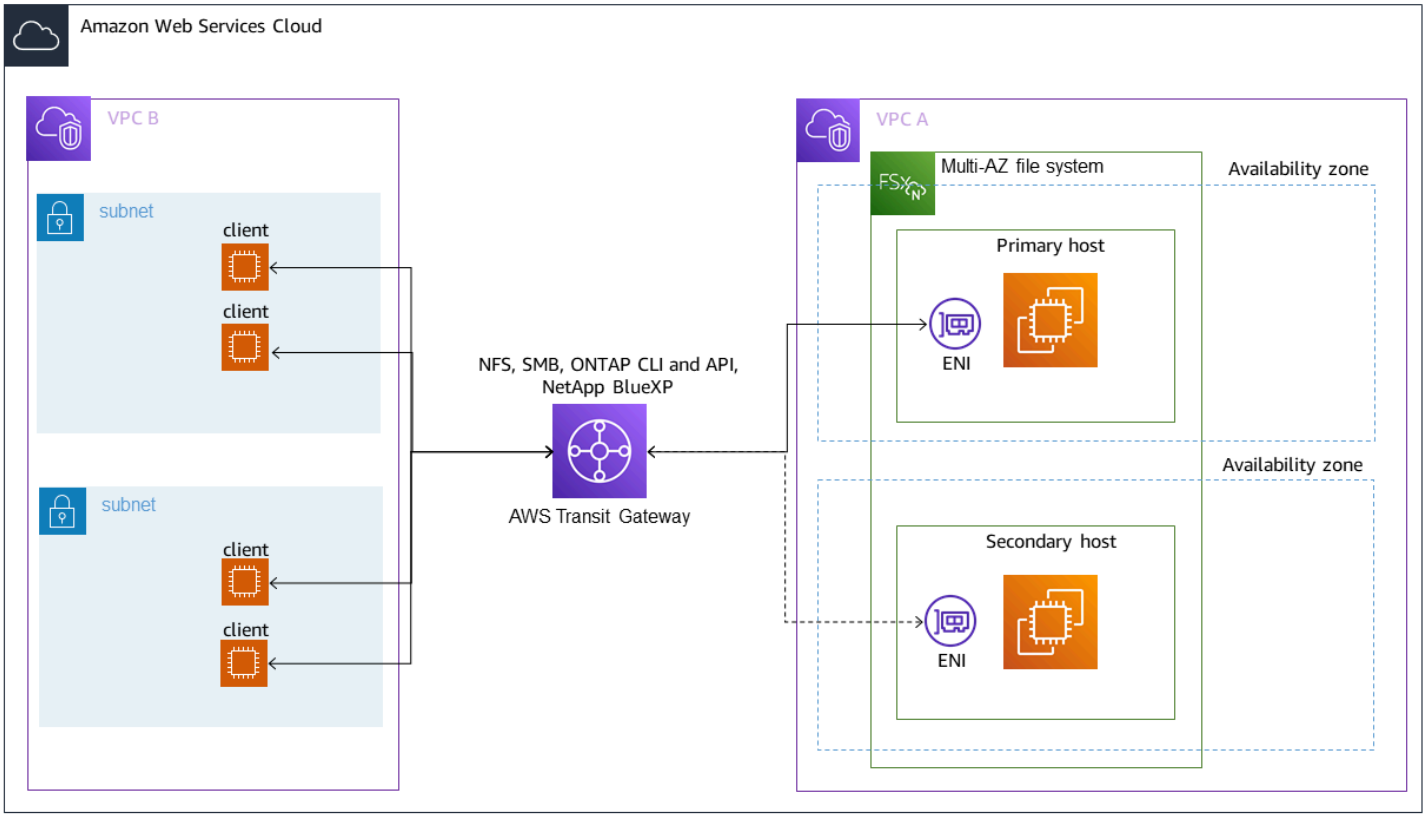
适用于 ONTAP 多可用区文件系统的 Amazon FSx 上的 NFS、SMB 和 NetApp ONTAP 管理终端节点使用浮动互联网协议 (IP) 地址，因此在故障转移事件期间，连接的客户端可以在首选文件服务器和备用文件服务器之间无缝切换。有关故障转移的更多信息，请参阅FSx for ONTAP 失效转移过程。

这些浮动 IP 地址是在您与文件系统关联的 VPC 路由表中创建的，并且位于您可以在创建时指定的文件系统的 `EndpointIpAddressRange` 中。根据文件系统的创建方式，`EndpointIpAddressRange` 使用以下地址范围：

- 使用 Amazon FSx 控制台创建的多可用区文件系统默认使用 VPC 主要 CIDR 范围中的最后 64 个 IP 地址作为文件系统的 `EndpointIpAddressRange`。
- 默认情况下，使用 AWS CLI 或 Amazon FSx API 创建的多可用区文件系统使用地址块内`198.19.0.0/16`的 IP 地址范围。`EndpointIpAddressRange`

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 AWS Direct Connect、、 AWS 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。



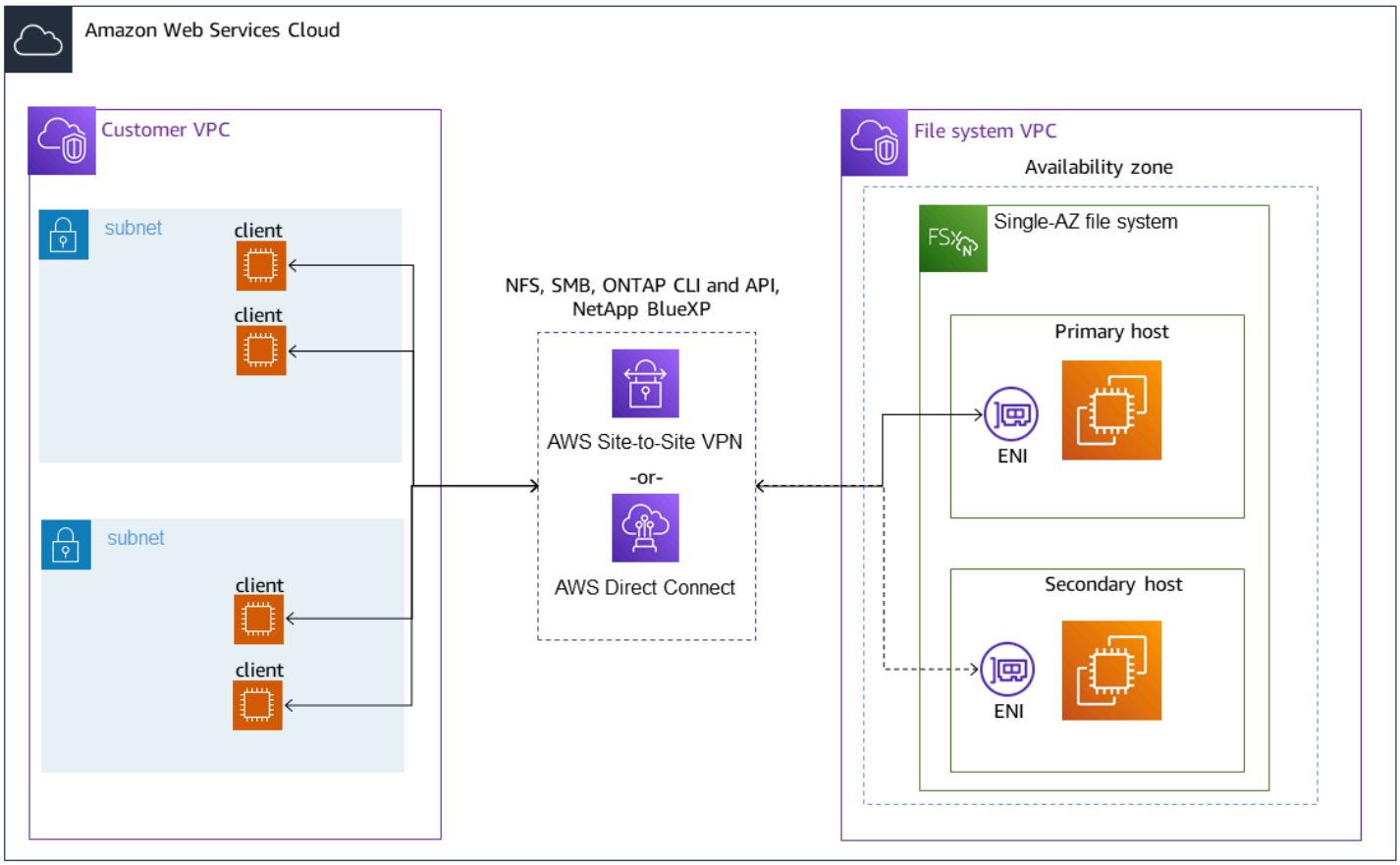
> **Note**
>
> 确保您使用的所有路由表都与您的多可用区文件系统相关联。这样做有助于防止失效转移期间出现不可用问题。有关将 Amazon VPC 路由表与文件系统关联的信息，请参阅 更新文件系统。

有关何时需要使用中转网关访问 FSx for ONTAP 文件系统的信息，请参阅 什么时候需要中转网关？。

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 for ONTAP 单可用区文件系统，以及用于使用 ONTAP CLI 或 REST API 管理文件系统的终端节点是活动文件服务器 ENI 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 AWS 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 AWS VPN 或用 AWS 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？
通过 NFS、SMB 或 NetApp ONTAP REST API、CLI 或 BlueXP 访问 FSx	前提是： • 从对等（例如本地）网络进行访问，以及 • 您不是通过 NetApp FlexCache 或全局文件缓存实例访问 FSx
通过 iSCSI 访问数据	否
将 SVM 加入 Active Directory	否
SnapMirror	否

数据访问	需要中转网关？
FlexCache 缓存	否
全局文件缓存	否

使用 AWS Transit Gateway配置路由

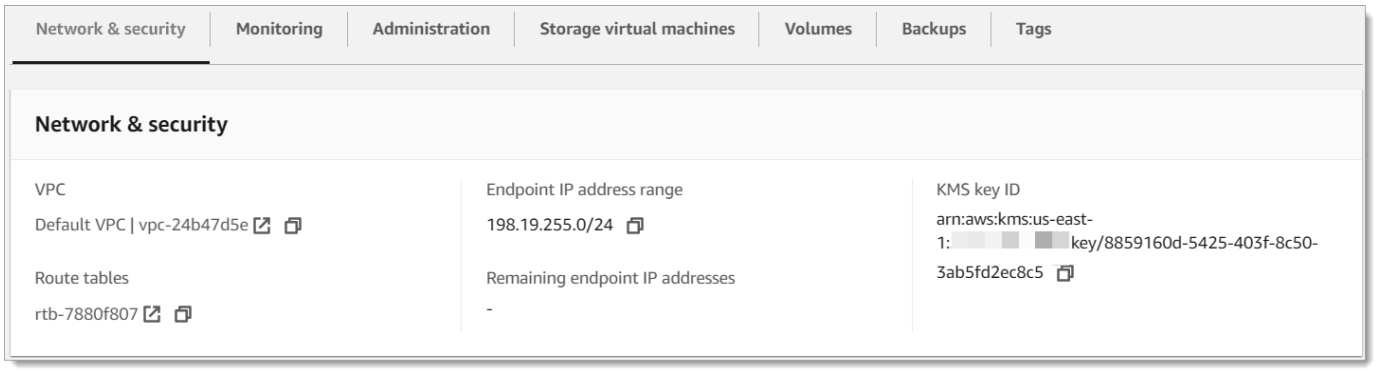
如果您的多可用区文件系统超出您`EndpointIPAddressRange`的 VPC 的 CIDR 范围，则需要在中设置额外的路由，才能从 AWS Transit Gateway 对等网络或本地网络访问您的文件系统。

> **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**
>
> 对于位于您的 VPC 的 IP 地址范围内使用 `EndpointIPAddressRange` 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。

要使用配置路由 AWS Transit Gateway

1. 通过以下网址打开 Amazon FSx 控制台：https://console.aws.amazon.com/fsx/。
2. 选择您配置对等网络访问权限的 FSx for ONTAP 文件系统。
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 FSx 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。

在部署 VPC 外部访问 iSCSI 或集群间端点

您可以使用 VPC 对等互连，也可以从文件系统的部署 VPC 外部访问文件系统的 iSCSI 或集群间终端节点。 AWS Transit Gateway 您可以使用 VPC 对等在 VPC 之间路由 iSCSI 和集群间流量。VPC 对等连接是两个 VPC 之间的网络连接，通过此连接，您可以使用私有 IPv4 地址在这两个 VPC 之间路由流量。您可以使用 VPC 对等连接相同的 VPC 内部 AWS 区域 或不同的 VPC 之间。 AWS 区域有关 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 AWS VPN 和 AWS Direct Connect 从本地访问 FSx for ONTAP 文件系统；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、ONTAP CLI 或 REST API 端点

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

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，或者从 NetApp FlexCache 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失效转移，Amazon FSx 使用浮动 IP 地址作为用于 NFS、SMB 和 ONTAP 管理端点的接口。由于

NFS、SMB 和管理端点使用浮动 IP，因此必须与本地网络配合使用AWS Transit Gateway AWS Direct Connect 或从本地网络 AWS 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 `EndpointIpAddressRange` 范围内。如果在 Amazon FSx 控制台中创建文件系统，默认情况下，Amazon FSx 会从 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 IP 地址范围。如果您使用 AWS CLI 或 Amazon FSx API 创建文件系统，则默认情况下，亚马逊 FSx 会从 IP 地址范围内选择 IP 地址范围。`198.19.0.0/16`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。

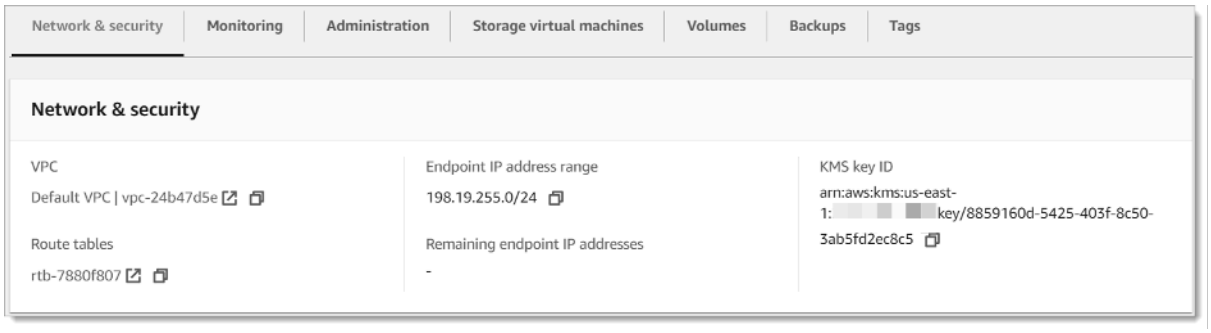
> **Important**
>
> 要使用中转网关访问多可用区文件系统，必须在其路由表与您的文件系统关联的子网中创建中转网关的每个附件。

配置 AWS Transit Gateway 为从您的 VPC 外部进行访问

如果您的多可用区文件系统超出您`EndpointIPAddressRange`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**
>
> 对于位于您的 VPC 的 IP 地址范围内使用 `EndpointIPAddressRange` 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. 通过以下网址打开 Amazon FSx 控制台：https://console.aws.amazon.com/fsx/。
2. 选择您配置对等网络访问权限的 FSx for ONTAP 文件系统。
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 FSx 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。

要将路由表添加到您的文件系统，请参阅 更新文件系统。

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。

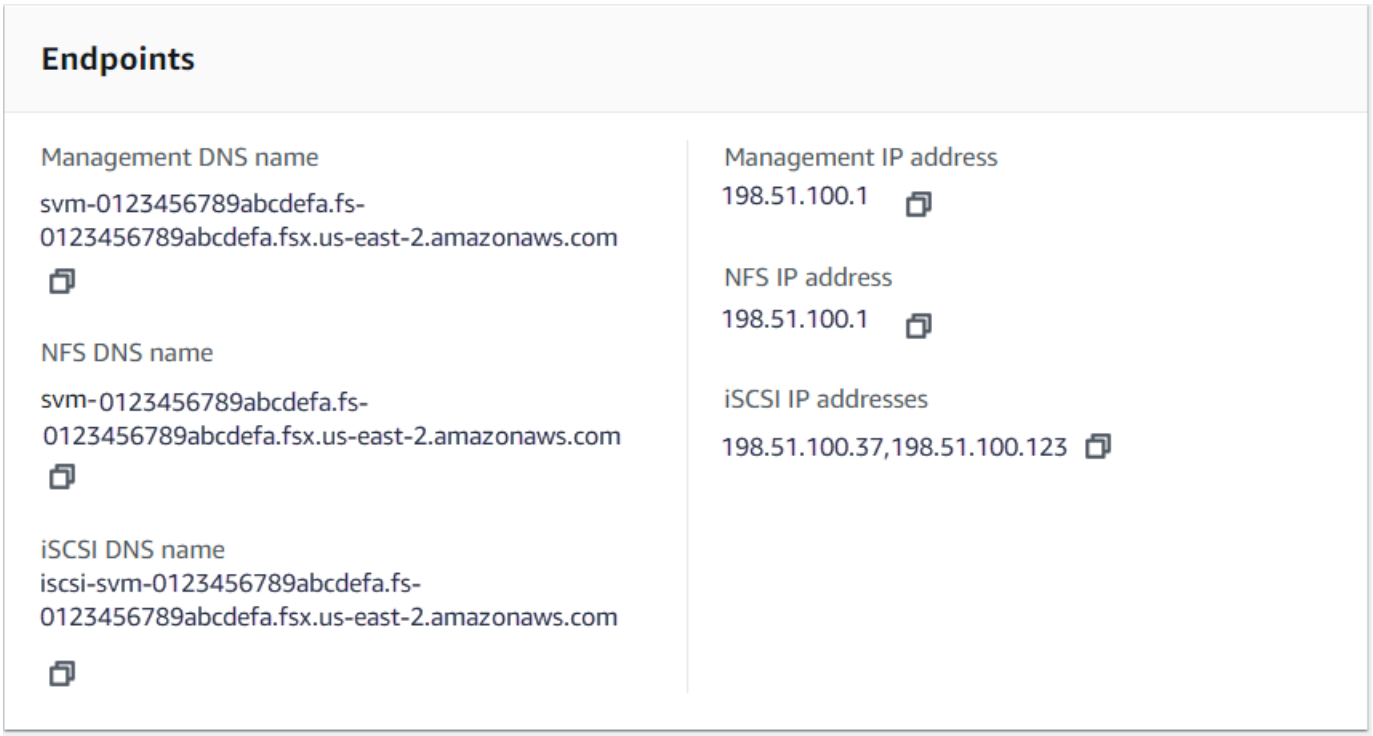
从本地访问集群间端点

适用于 ONTAP 的 FSx 的集群间终端节点专门用于 ONTA NetApp P 文件系统之间的复制流量，包括本地部署 NetApp 和 ONTAP 的 FSx 之间的复制流量。复制流量包括 SnapMirror、 FlexCache、存储虚拟机 (SVM) 与不同文件系统中的卷之间的 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端点使用的 IP 地址属于您在创建 FSx for ONTAP 文件系统时提供的 VPC 的 CIDR 范围，因此您无需使用中转网关即可在本地和 AWS Cloud之间路由集群间流量。但是，本地客户端仍然必须使用 AWS VPN 或 AWS Direct Connect 与您的 VPC 建立安全连接。

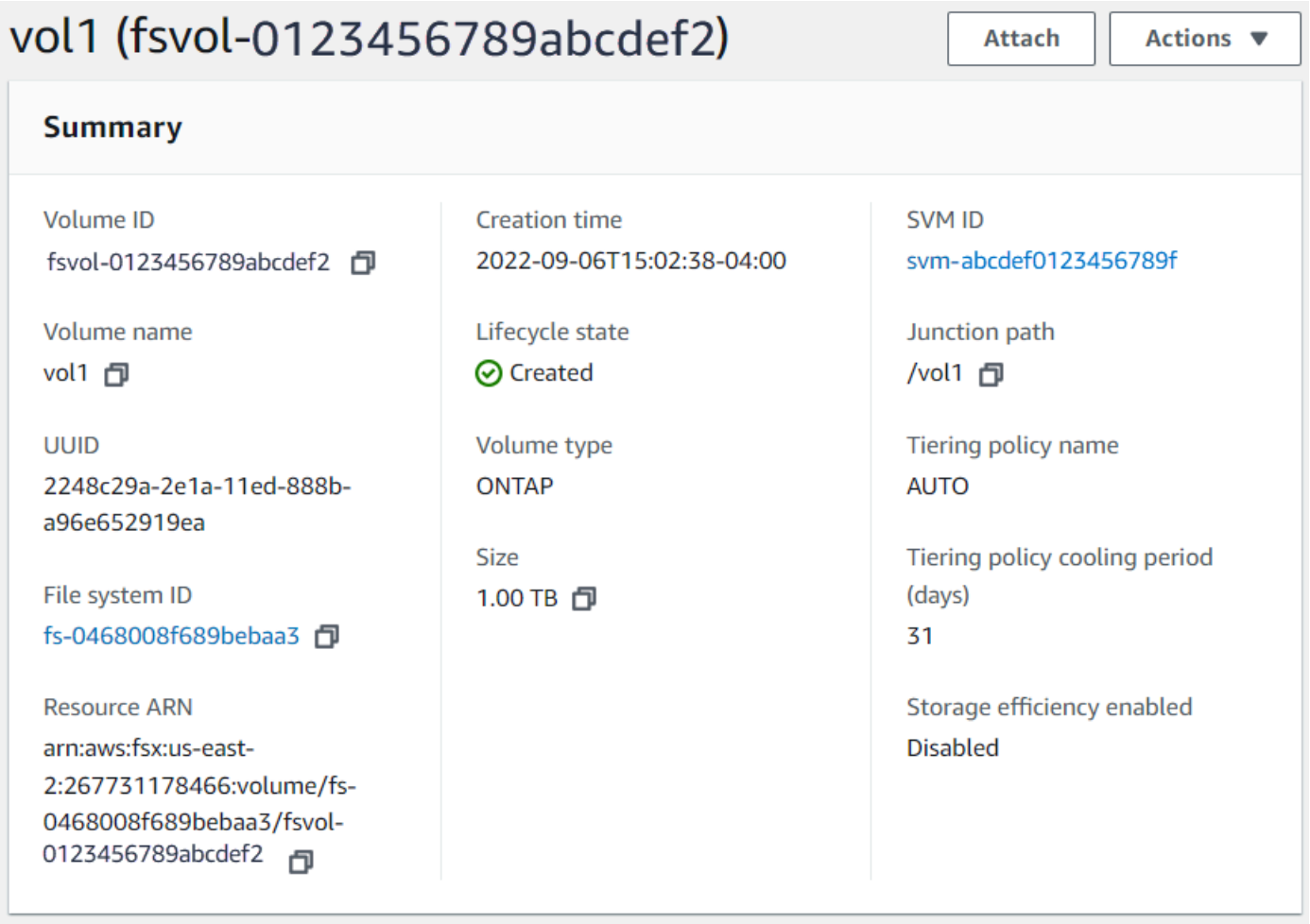
挂载卷

您可以通过在客户端上挂载卷来访问 FSx for ONTAP 中的数据。本节中的命令使用创建卷的 SVM 的 DNS 名称或 IP 地址来挂载或连接卷。您可以在 Amazon FSx 控制台中选择 ONTAP > 存储虚拟机，或者在文件系统详细信息页面的存储虚拟机选项卡上找到 SVM 的 DNS 名称和 IP 地址，如下图所示。



或者，您可以在 DescribeStorageVirtualMachinesAPI 操作的响应中找到它们。

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，如下图所示。



主题

- 在 Linux 客户端上挂载
- 在 Microsoft Windows 客户端上挂载
- 在 macOS 客户端上挂载

在 Linux 客户端上挂载

我们建议将要附加 Linux 客户端的 SVM 卷的安全样式设置为 `UNIX` 或 `mixed`。有关更多信息，请参阅管理 FSx for ONTAP 卷。

> **Note**
>
> 默认情况下，FSx for ONTAP NFS 挂载的是 `hard` 挂载。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. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
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您的 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 SVM 来代替其 DNS 名称。我们建议使用 DNS 名称来装载客户机以横向扩展文件系统，因为它有助于确保您的客户端在文件系统的高可用性 (HA) 对之间保持平衡。

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

   > **Note**
   >
   > 对于横向扩展文件系统，parallel NFS (PnFS) 协议默认处于启用状态，并且默认情况下，任何装载 NFS v4.1 或更高版本的卷的客户机都使用并行 NFS (PnFS) 协议。

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 for ONTAP 文件系统不支持在 Amazon EC2 Mac 实例上使用 `/etc/fstab` 自动挂载。

> **Note**
>
> 确保您已创建 FSx for ONTAP 文件系统，然后才能更新 EC2 实例的 `/etc/fstab` 文件。有关更多信息，请参阅 创建 FSx for ONTAP 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

本节介绍如何使用运行 Microsoft Windows 操作系统的客户端访问 FSx 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 中，或者 AWS 账户 AWS 区域，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 for ONTAP 存储虚拟机。有关使用工作组的更多信息，请参阅文档中心工作组概述中的设置 SMB 服务器。NetApp
- 您要附加的卷的安全样式设置为 NTFS 或 mixed。有关更多信息，请参阅 管理 FSx for ONTAP 卷。

使用 SMB 和 Active Directory 在 Windows 客户端上附加 ONTAP 卷

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

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 for ONTAP 存储虚拟机。

3. 连接到您的 Amazon EC2 Windows 实例。有关更多信息，请参阅 Amazon EC2 用户指南中的连接到您的 Windows 实例。

4. 打开命令提示符。

5. 运行以下命令。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。
   - `SHARE_NAME`替换为 SMB 共享的名称。 `C$`是 SVM 命名空间根目录下的默认 SMB 共享，但您不应将其挂载，因为这会将存储暴露给根卷并可能导致安全和服务中断。您应该提供 SMB 共享名来装载，而不是。`C$`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 名称来装载客户机以横向扩展文件系统，因为它有助于确保您的客户端在文件系统的高可用性 (HA) 对之间保持平衡。

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

在 macOS 客户端上挂载

本节介绍如何使用运行 macOS 操作系统的客户端访问 FSx 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. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
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您的 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 名称来装载客户机以横向扩展文件系统，因为它有助于确保您的客户端在文件系统的高可用性 (HA) 对之间保持平衡。

   ```
   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. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
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您的 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 SVM 来代替其 DNS 名称。我们建议使用 DNS 名称来装载客户机以横向扩展文件系统，因为它有助于确保您的客户端在文件系统的 HA 对之间保持平衡。

   ```
   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 SVM 来代替其 DNS 名称。我们建议使用 DNS 名称来装载客户机以横向扩展文件系统，因为它有助于确保您的客户端在文件系统的高可用性 (HA) 对之间保持平衡。

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

挂载 iSCSI 逻辑单元号

适用于 NetApp ONTAP 的 Amazon FSx 通过 iSCSI（互联网小型计算机系统接口）协议提供共享块存储支持。您可以通过预置 LUN（逻辑单元号）并将其映射到启动程序组（igroups）来启用 iSCSI 存储，以及将块存储暴露给您的 Linux 和 Windows 主机。

> **Note**
>
> 适用于 ONTAP 横向扩展文件系统的 FSx 不支持 iSCSI 协议，这些文件系统具有多对高可用性 (HA) 文件服务器。

主题

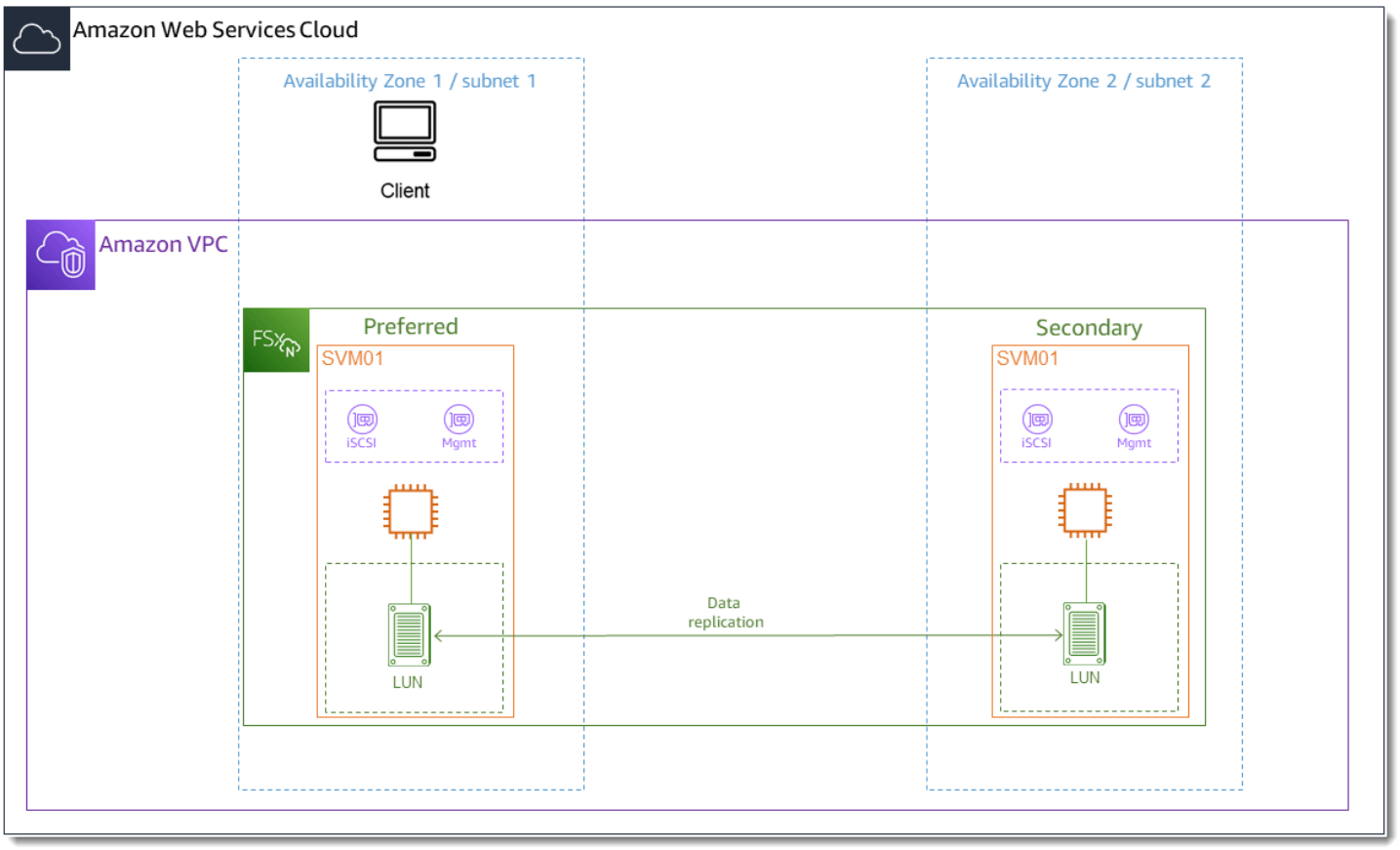
将 iSCSI LUN 挂载到 Linux 客户端

这些过程中提供的示例使用以下设置：

- 正在挂载到 Linux 主机的 iSCSI LUN 已创建。有关更多信息，请参阅创建 iSCSI LUN。
- 挂载 iSCSI LUN 的 Linux 主机是运行 Amazon Linux 2 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。
- Linux 主机和 FSx for ONTAP 文件系统位于同一 VPC 和 AWS 账户中。如果主机位于其他 VPC 中，则可以使用 VPC 对等或 AWS Transit Gateway 授予其他 VPC 访问该卷的 iSCSI 终端节点的权限。有关更多信息，请参阅 从部署 VPC 外部访问数据。

  如果您使用的是运行其他 Linux AMI 的 EC2 实例，则主机上安装的某些实用程序可能已完成预装，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。

  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

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

安装和配置 Linux 客户端

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. 使用以下命令连接到您在 NetApp 其中创建 iSCSI LUN 的 FSx for ONTAP 文件系统上的 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 lun igroup create命令创建启动程序组 (`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 lun igroup 创建。

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。如果没有，创建 iSCSI LUN请参见以 step-by-step 获取操作说明。

   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

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）您可以建立与 target_initiator 的额外会话。Amazon EC2 的单流流量带宽限制为 5Gb/s（约 625MB/s），但您可以通过创建多个会话的方式从单个客户端向文件系统提供更高的吞吐量。有关更多信息，请参阅《Amazon Elastic Compute Cloud 用户指南（适用于 Linux 实例）》中的 Amazon EC2 实例网络带宽。

   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 40Gb/s（5000MB/s）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。

为块设备提供一个易记得名称

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。这是适用于 ONTAP 的 Amazon FSx 使用的 NetApp ONTAP 发行版 NetApp 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。请注意，Last sector 值将根据 iSCSI LUN 的大小（在本例中为 10GB）而改变。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）。

```
~$ 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）您可以将挂载目录的所有权更改为您的用户。将 *username* 替换为您的用户名。

```
~$ 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。

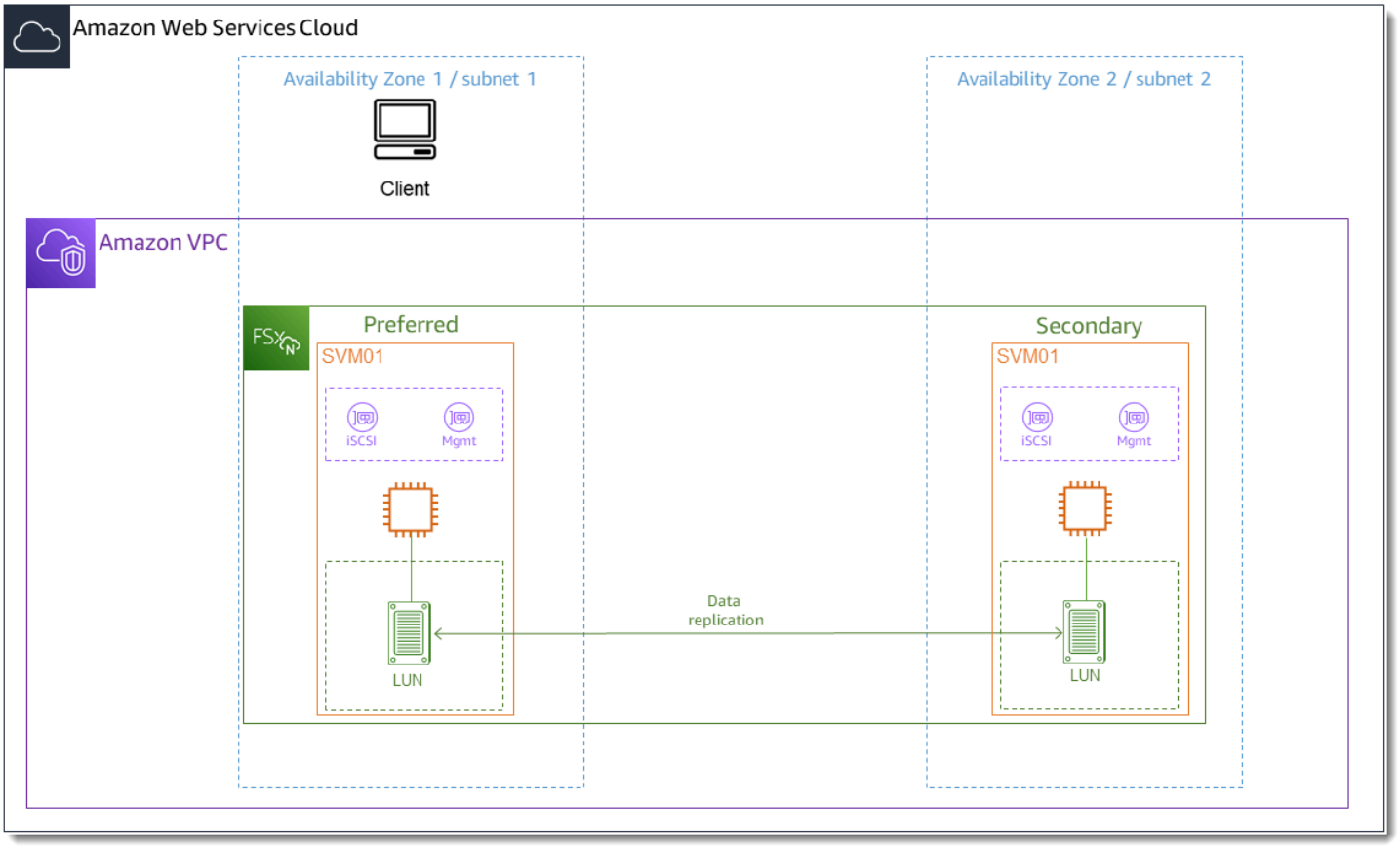
将 iSCSI LUN 挂载到 Windows 客户端

这些过程中提供的示例使用以下设置：

- 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 对等或 AWS Transit Gateway 向其他 VPC 授予访问 iSCSI 终端节点的权限。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 FSx for ONTAP 文件系统上配置 iSCSI
- 在 Windows 客户端上挂载 iSCSI LUN
- 正在验证您的 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 上为 ONTAP 文件系统配置 iSCSI 时使用此值。 NetApp

```
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 FSx for ONTAP 文件系统上配置 iSCSI

1. 使用以下命令连接到您在 NetApp 其中创建 iSCSI LUN 的 FSx for ONTAP 文件系统上的 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 lun igroup create创建启动程序组，或。`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 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*lun igroup create*中的。

3. 使用以下命令确认已成功创建 `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    windows  iqn.1994-05.com.windows:abcdef12345
```

创建 igroup 后，您就可以创建 LUN 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，使客户端能够向 iSCSI LUN 提供高达 40Gb/s（5000Mb/s）的聚合吞吐量。建立 8 个会话可确保单个客户端能够以为最高级别的 FSx for ONTAP 吞吐能力提供最大量的 4000 MB/s 的吞吐容量。您可以选择增加或减少会话数（每个会话提供高达 625MB/s 的吞吐量），方法是将 #Establish iSCSI connection 步骤中的脚本的 for 循环从 1..8 修改为另一个上限。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。

```
#iSCSI IP addresses for Preferred and Standby subnets
$TargetPortalAddresses = @("iscsi_1","iscsi_2")

#iSCSI Initator IP Address (Local node IP address)
$LocaliSCSIAddress = "ec2_ip"

#Connect to FSx for NetApp ONTAP file system
Foreach ($TargetPortalAddress in $TargetPortalAddresses) {
New-IscsiTargetPortal -TargetPortalAddress $TargetPortalAddress -
TargetPortalPortNumber 3260 -InitiatorPortalAddress $LocaliSCSIAddress
}

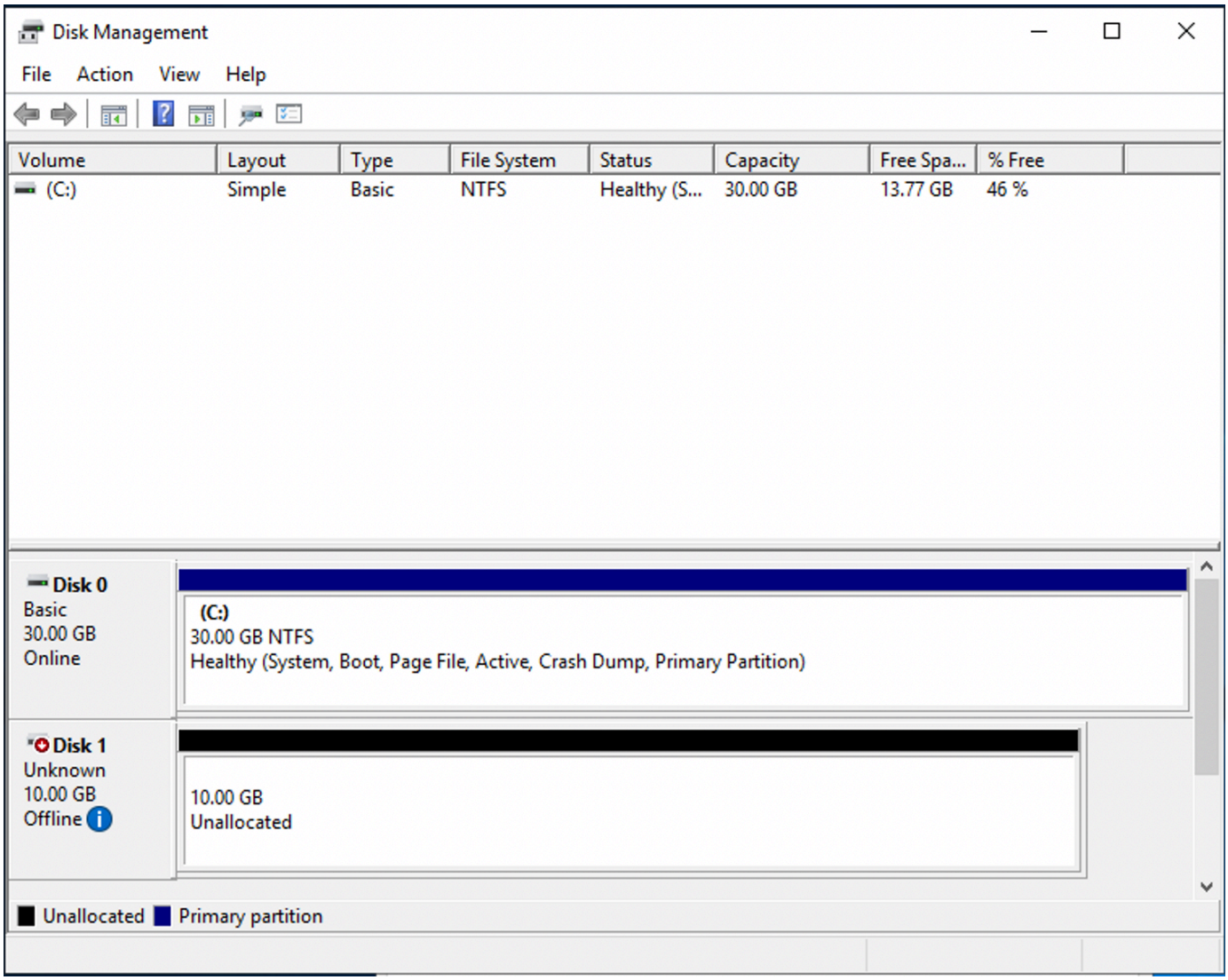
#Add MPIO support for iSCSI
```

```
New-MSDSMSupportedHW -VendorId MSFT2005 -ProductId iSCSIBusType_0x9

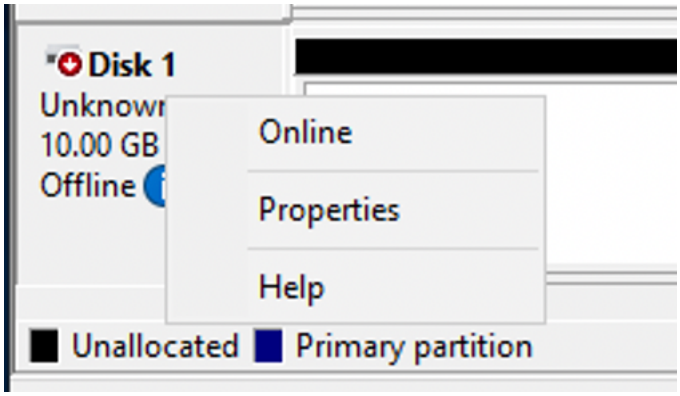
#Establish iSCSI connection
1..8 | %{Foreach($TargetPortalAddress in $TargetPortalAddresses)
{Get-IscsiTarget | Connect-IscsiTarget -IsMultipathEnabled $true -
TargetPortalAddress $TargetPortalAddress -InitiatorPortalAddress $LocaliSCSIAddress
 -IsPersistent $true}}

#Set the MPIO Policy to Round Robin
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。

正在验证您的 iSCSI 配置

我们提供了一个脚本来检查您的 iSCSI 设置是否配置正确。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。以下任务说明了如何安装和使用该脚本。

验证您的 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. 使用以下命令展开 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. 查看输出以了解您的配置的当前状态。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.

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
```

将 FSx for ONTAP 与其他 AWS 服务一起使用

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

- 使用 Amazon 和 F WorkSpaces Sx for ONTAP
- 将 Amazon Elastic Container Service 与 FSx for ONTAP 一起使用
- 将 VMware Cloud 与 FSx for ONTAP 一起使用

使用 Amazon 和 F WorkSpaces Sx for ONTAP

FSx for ONTAP 可与亚马逊一起使用， WorkSpaces 以提供共享的网络连接存储 (NAS) 或存储亚马逊账户的漫游配置文件。 WorkSpaces 通过 WorkSpaces 实例连接到 SMB 文件共享后，用户可以在文件共享上创建和编辑文件。

以下过程说明如何将 Amazon FSx 与 Amazon 配合使用， WorkSpaces 为漫游个人资料和主文件夹访问提供一致的体验，以及如何为 Windows 和 Linux 用户提供共享的团队文件夹。 WorkSpaces 如果您是亚马逊新手 WorkSpaces，则可以按照《亚马逊 WorkSpaces 管理指南》中 WorkSpaces 快速设置入门中的说明创建您的第一个亚马逊 WorkSpaces 环境。

主题

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，用户在注销 Amazon FSx 文件共享时会保存数据和桌面设置，从而可以在 WorkSpaces 不同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。

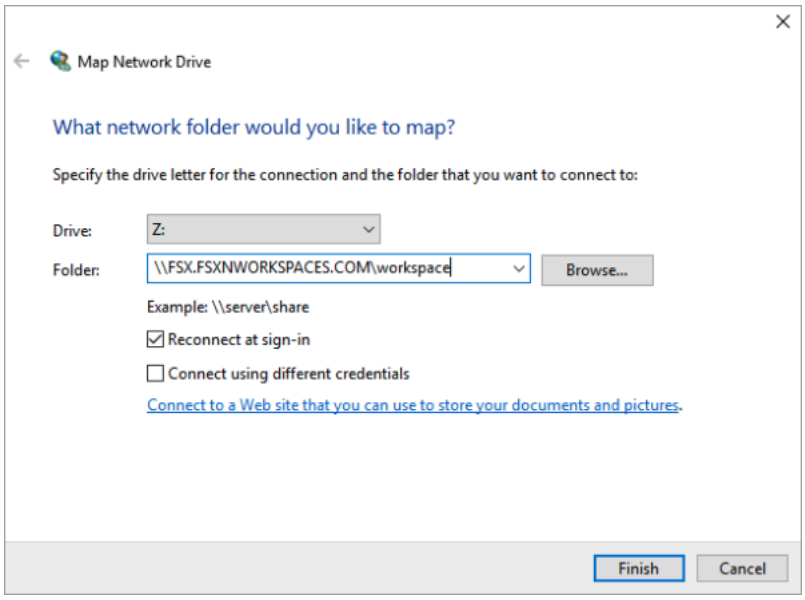
第 1 步：使用 Amazon FSx 为域用户创建配置文件文件夹位置

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。此 IP 地址范围也 WorkSpaces 用于管理流量范围，如《Amazon WorkSpaces 管理指南》的 IP 地址和端口要求中所述。 WorkSpaces 因此，要 WorkSpaces从中访问适用于 ONTAP 文件系统的多可用区 FSx，必须选择不与 198.19.0.0/16 重叠的终端节点 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. 从运行 Windows Server 的亚马逊 EC2 实例或从中访问你的 Amazon FSX SVM。 WorkSpace有关更多信息，请参阅访问 数据：
6. 你将共享映射到你的 Windows WorkSpaces 实例Z:\上：



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 “窗口” 上 WorkSpace，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. 从中注销测试用户 WorkSpace。
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。在管理员中 WorkSpaces，打开 PowerShell 控制台并使用类似于以下示例的命令（该命令使用您之前在步骤 1 中创建profiles的文件夹）：

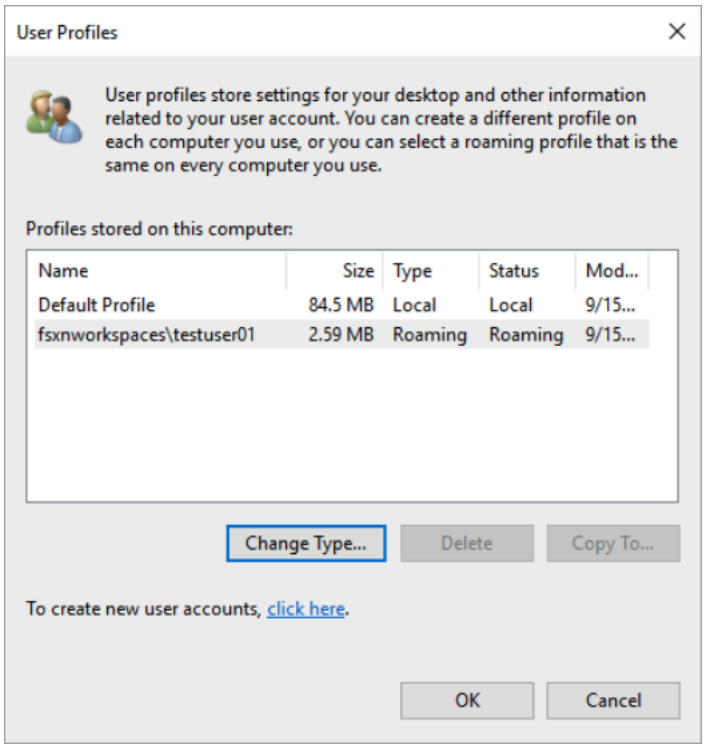
```
Set-ADUser username -ProfilePath \\filesystem-dns-
name\sharename\foldername\username
```

例如：

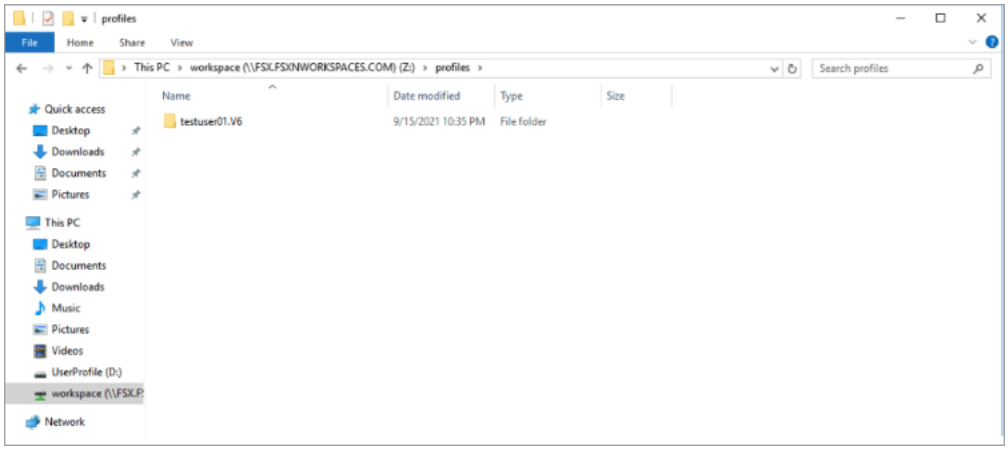
```
Set-ADUser testuser01 -ProfilePath \\fsx.fsxnworkspaces.com\workspace\profiles
\testuser01
```

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。



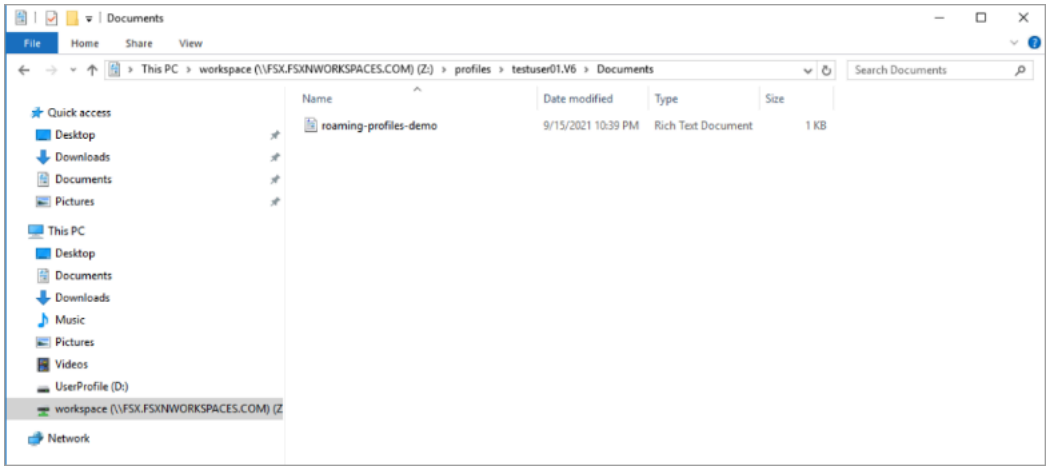
7. 浏览 FSx 查看 ONTAP 共享文件夹。在 profiles 文件夹中，您将看到该用户的文件夹。



8. 在测试用户的 Documents 文件夹中创建文档

9. 将测试用户从他们的用户注销 WorkSpace。

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 进行跨平台访问 WorkSpaces

1. 从任务栏中选择位置 > 连接到服务器。

   a. 对于服务器，输入 *file-system-dns-name*。

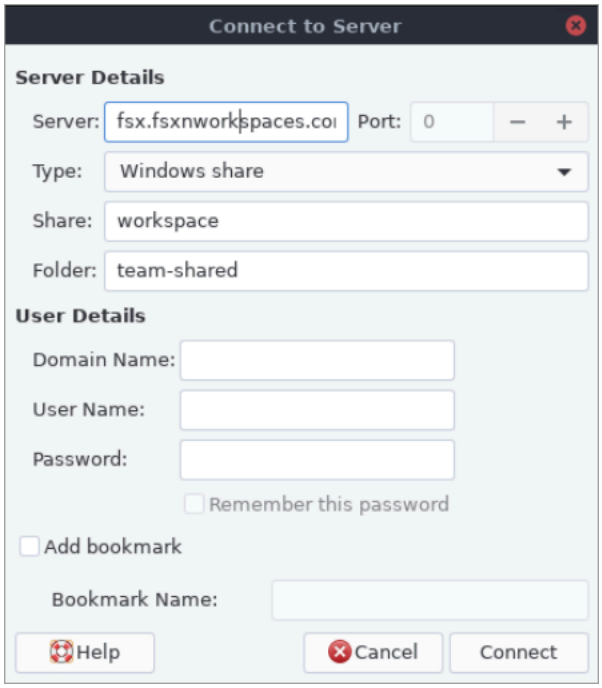
   b. 将类型设置为 `Windows share`。

   c. 将共享设置为 SMB 共享的名称，例如 `workspace`。

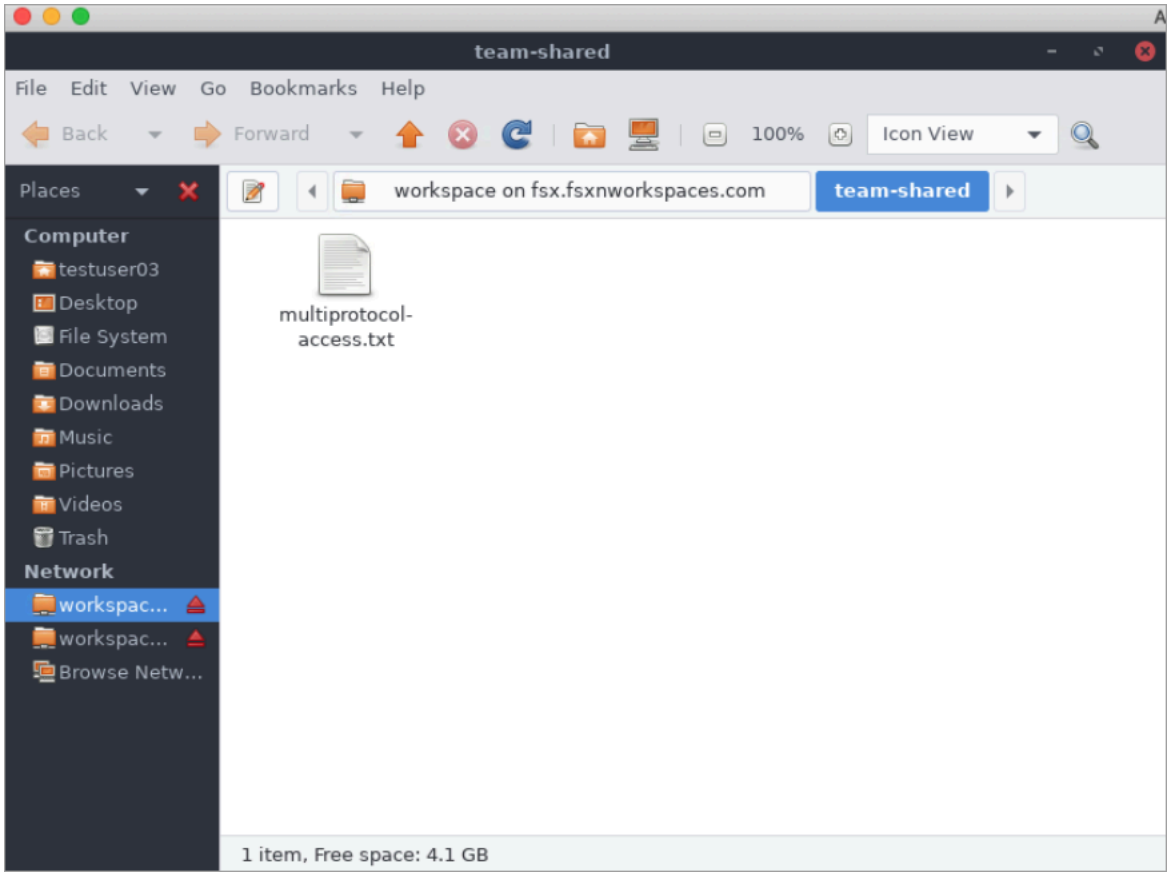
   d. 您可以将文件夹保留为 `/` 或将其设置为文件夹，例如名为 `team-shared` 的文件夹。

   e. 对于 Linux WorkSpace，如果您的 Linux 与 Amazon FSx WorkSpace 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 Amazon Elastic Container Service 与 FSx for ONTAP 一起使用

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 SVM 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 FSx for ONTAP 文件系统中的挂载点和目录。

   ```
   {
       "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 FSx 文件系统上配置为 CIFS 共享 fsxontap。

   ```
   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 FSx for ONTAP 文件系统中的挂载点和目录。

```
{
    "volumes": [
        {
            "name": "ontap-volume",
            "host": {
                "sourcePath": "mountpoint"
            }
        }
    ],
    "mountPoints": [
        {
            "containerPath": "containermountpoint",
            "sourceVolume": "ontap-volume"
        }
    ],
```

```
      .
      .
      .
}
```

将 VMware Cloud 与 FSx for ONTAP 一起使用

您可以将适用于 ONTAP 的 FSx 用作 AWS 软件定义数据中心 (SDDC) 上的 VMware Cloud 的外部数据存储库。有关更多信息，请参阅使用适用于 ONTAP 的 Amazon FSx 配置为外部存储和使用适用于 NetApp ONTAP 的 A AWS mazon FSx 配置为外部存储和开启 VMware Cloud 部署指南。 NetApp

可用性与持久性

适用于 NetApp ONTAP 的 Amazon FSx 使用两种部署类型，即单可用区和多可用区，它们提供不同级别的可用性和持久性。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。

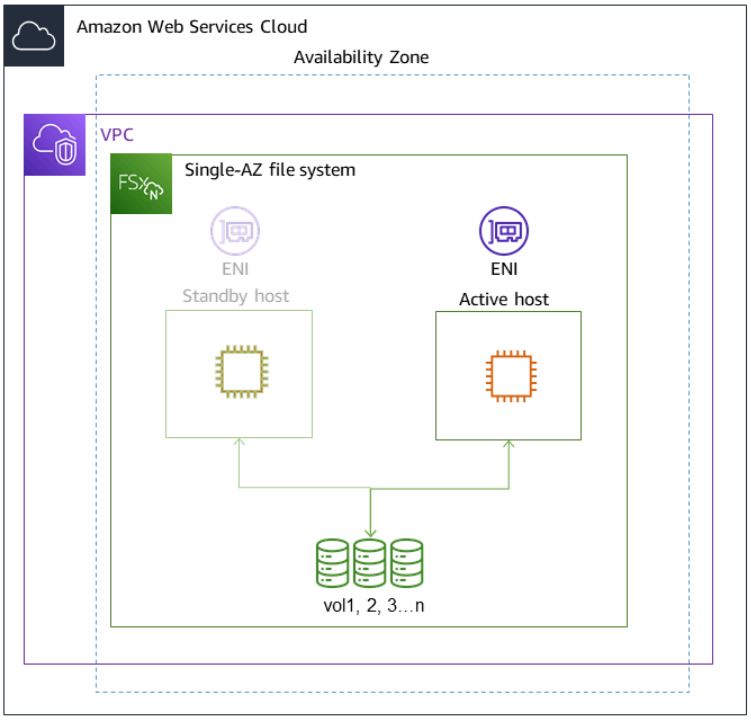
单可用区部署类型

当您创建单可用区文件系统时，Amazon FSx 会自动在活动-备用配置中配置一到十二对文件服务器，每对中的活动和备用文件服务器位于中单个可用区内的不同故障域中。 AWS 区域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将该高可用性 (HA) 对故障转移到备用文件服务器。在故障转移期间，您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或存储已存储在本地或其他地方的数据的辅助副本等用例提供了成本优化的解决方案 AWS 区域，只需在单个可用区内复制数据。

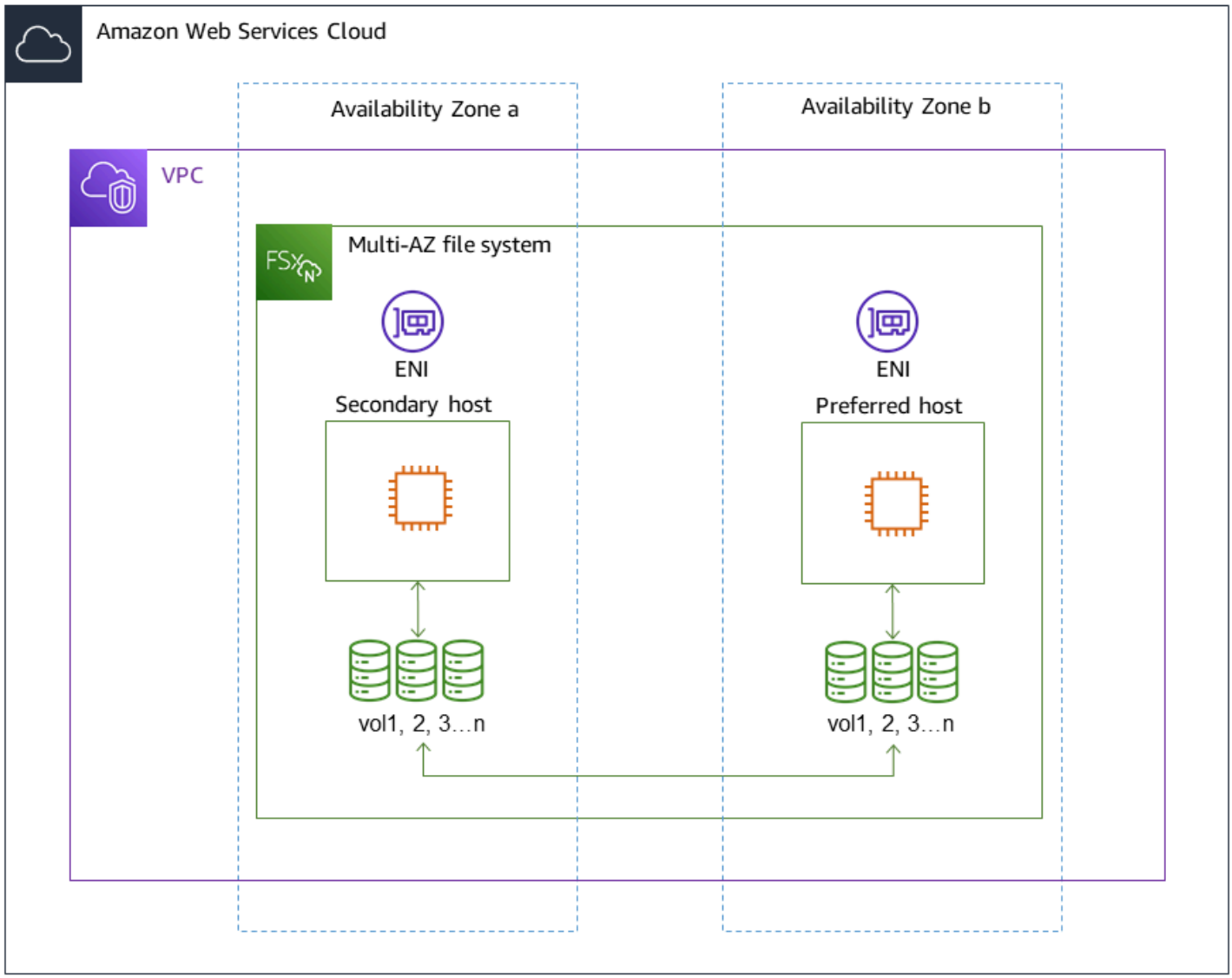
下图阐明了 FSx for ONTAP 单可用区文件系统的架构。



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。多可用区部署只有一对 HA 文件服务器，备用文件服务器部署在与 AWS 区域活动文件服务器不同的可用区中。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 多可用区文件系统的架构。



FSx for ONTAP 失效转移过程

如果出现以下任何一种情况，单可用区和多可用区文件系统会自动将给定的 HA 对从首选或活动文件服务器故障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**
>
> 对于横向扩展文件系统，每个 HA 对的故障转移行为是独立的。如果一个 HA 对的首选文件服务器不可用，则只有该 HA 对会故障转移到其备用文件服务器。

从一台文件服务器故障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为该 HA 对的所有文件系统读取和写入请求提供服务。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。

在文件系统上测试失效转移

您可以通过修改纵向扩展文件系统的吞吐容量来测试其故障转移。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。

> **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：

	单可用区（向上扩展）	单可用区（横向扩展）	多可用区（向上扩展）
子网的数量	1	1	2
弹性网络接口的数量	2	每对 HA 2	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 SVM 的数量	1 + 文件系统中 SVM 的数量

	单可用区（向上扩展）	单可用区（横向扩展）	多可用区（向上扩展）
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。

管理存储容量

适用于 NetApp ONTAP 的 Amazon FSx 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

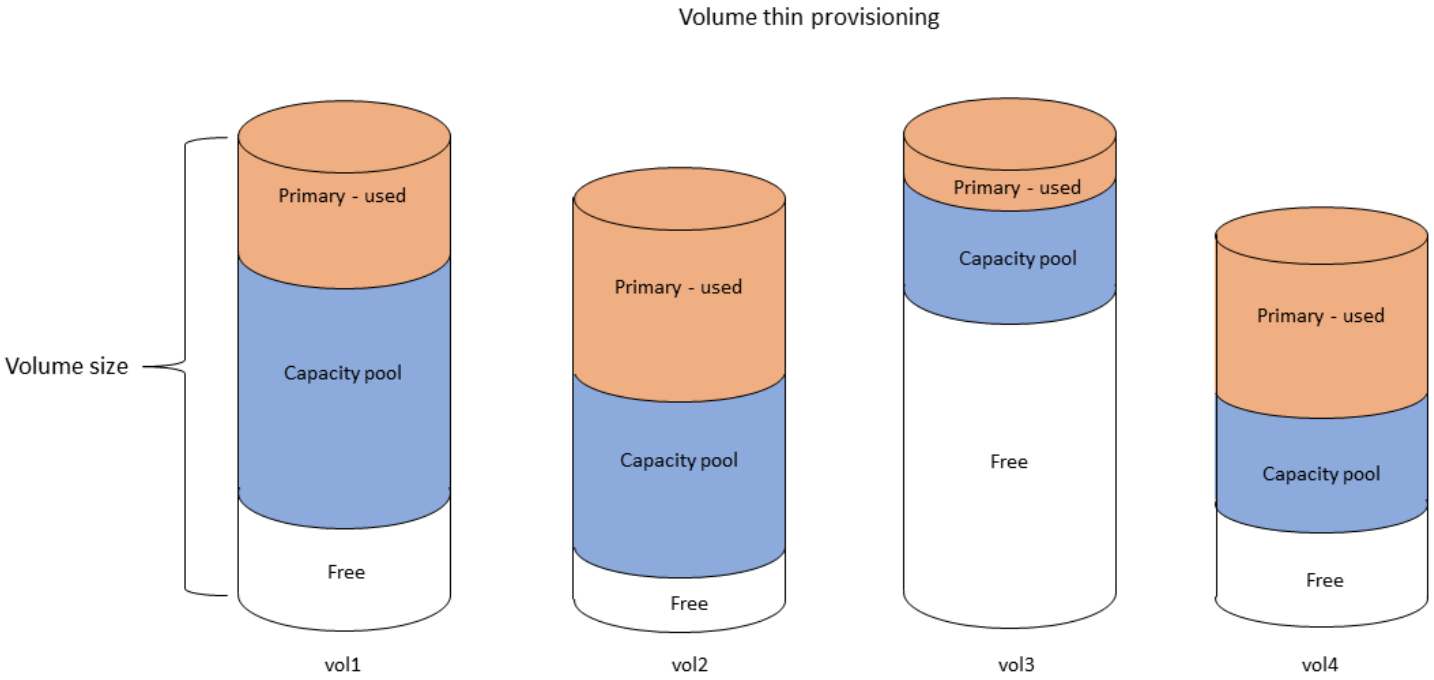
FSx for ONTAP 存储层

存储层是适用于 NetApp ONTAP 的 Amazon FSx 文件系统的物理存储介质。FSx for ONTAP 提供以下存储层：

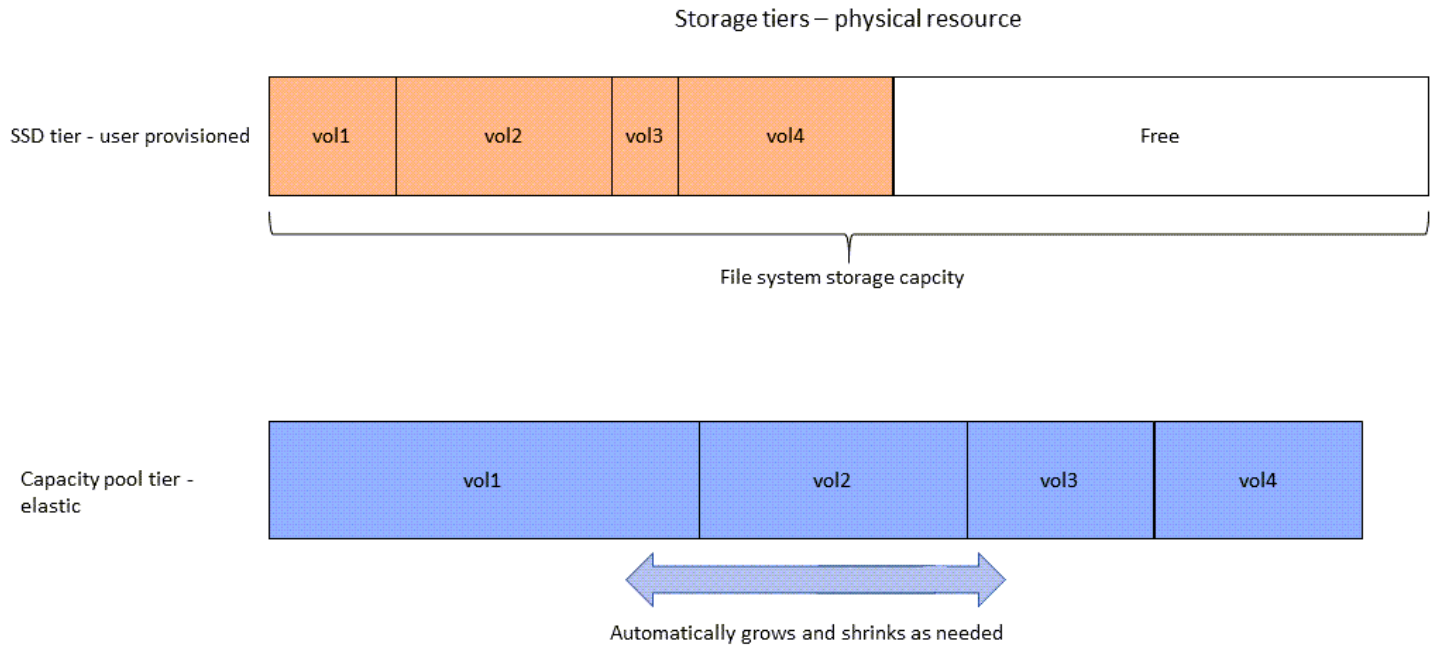
- SSD 层 – 用户预置的高性能固态硬盘（SSD）存储，专为数据集的活跃部分而构建。
- 容量池层 – 完全弹性的存储，可以自动扩展到 PB 级大小，并且针对不经常访问的数据进行成本优化。

FSx for ONTAP 卷是一种类似于文件夹的虚拟资源，不会消耗存储容量。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，您需要指定卷的大小，但可以在创建后修改其大小。FSx for ONTAP 卷是精简配置，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。

下图举例说明了跨文件系统中多个 FSx for ONTAP 卷分布的数据。



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。

选择合适数量的文件系统 SSD 存储

在为 FSx for ONTAP 文件系统选择 SSD 存储容量时，您需要记住以下事项，这些事项会影响可用于存储数据的 SSD 存储量：

- 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。对于固态硬盘存储容量超过 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%
32KB 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。无论卷采用何种分层策略，都是如此，但使用 SnapMirror 向配置了所有数据分层策略的卷传输数据除外。

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%。对于横向扩展文件系统，我们还建议您对任何文件系统聚合的持续利用率不要超过 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。

FSx for ONTAP 存储效率

NetApp ONTAP 提供数据块级存储效率功能，包括压缩、压缩和重复数据删除，可在不牺牲性能的情况下为您节省高达 65% 的存储容量，用于一般文件共享。

适用于 NetApp ONTAP 的 Amazon FSx 还支持其他可为您节省空间的 ONTAP 功能，包括快照、精简配置和卷。 FlexClone

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的文件系统节省的存储量，请参阅查看存储效率节省情况。

计算存储效率节省量

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%（80TB）的数据会自动分层到容量池层，剩余 20%（20TB）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

在创建 FSx for ONTAP 文件系统时，您需要指定 SSD 层的存储容量。对于横向扩展文件系统，您指定的存储容量在每个高可用性 (HA) 对的存储池之间平均分配；这些存储池称为聚合。

对于您预置的每 GiB SSD 存储空间，Amazon FSx 会自动将 SSD 每秒进行读写操作的次数（IOPS）预置为 3，每个文件系统最多可配置 16 万 SSD IOPS。对于横向扩展文件系统，SSD IOPS 在每个文件系统的聚合中均匀分布。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 FSx for ONTAP 文件系统预调配的 SSD IOPS 数量上限的更多信息，请参阅吞吐能力对性能的影响。

主题

更新文件系统 SSD 存储空间和 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 FSx for NetApp ONTAP 文件系统的 SSD 存储容量。使用亚马逊 FSx 控制台、亚马逊 FSx API 或 AWS Command Line Interface (AWS CLI) 增加固态硬盘存储容量。有关更多信息，请参阅 修改 SSD 存储容量和预配置 IOPS。

当增加 Amazon FSx 文件系统的 SSD 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。有关定价的更多信息，请参阅适用于 NetApp ONTAP 的 Amazon FSx 定价。

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、CLI 和 API 跟踪存储优化流程的进度。有关更多信息，请参阅 监控存储容量和 IOPS 更新。

注意事项

以下是修改文件系统的 SSD 存储容量和预配置 IOPS 时需要考虑的几个重要事项：

- 仅增加存储容量 – 您只能增加文件系统的存储容量；您不能减少存储容量。
- 存储容量的最小增加量 — 每增加 SSD 存储容量必须至少为文件系统当前 SSD 存储容量的 10%，不超过文件系统配置的最大 SSD 存储容量。
- （仅限横向扩展）存储容量分布 — 您为文件系统选择的新存储容量或 SSD IOPS 在每个文件系统的聚合中均匀分布。
- 两次增加的间隔时间 – 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。

- 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，最高可达文件系统配置的最大 SSD IOPS。

    > **Note**
    >
    > 有关您可以为 FSx for ONTAP 文件系统预调配的 SSD IOPS 数量上限的更多信息，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，请参阅适用于 NetApp ONTAP 的 Amazon FSx 定价。

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。对于横向扩展文件系统，此建议既适用于所有文件系统聚合的平均利用率，也适用于每个聚合。

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，请参阅选择合适数量的文件系统 SSD 存储。

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 存储空间和 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 SSD 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 Management Console

监控文件系统的可用固态硬盘层存储容量（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，然后选择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。

创建文件系统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 SCU 警报

您可以使用该`StorageCapacityUtilization`指标创建警报，当您的一个或多个 FSx for 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，选择以下内容：
   - 对于命名空间，选择 AWS/FSX > 详细文件系统指标。
   - 在 “指标名称” 中，选择 MAX (StorageCapacityUtilization)。
   - 对于筛选依据，您可以选择按照 ID 包含或排除特定的文件系统。如果将 F ilter by 留空，则当您的任何文件系统超过警报的存储容量利用率阈值时，将触发警报。
   - 将其余选项留空，然后选择图表查询。
5. 选择选择指标。回到向导的 “指标” 部分，为您的指标添加标签。我们建议将时段保持在 5 分钟以内。
6. 在条件下，只要您的指标大于/等于 80，请选择静态阈值类型。
7. 选择 “下一步” 转至 “配置操作” 页面。

配置警报动作

您可以为警报配置各种操作，以便在警报达到您配置的阈值时触发。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” 部分，选择警报ALARM处于状态时要通知的 SNS 主题。您可以选择现有主题或创建新主题。您将收到订阅通知，您需要先确认该通知，然后才能收到发送到该电子邮件地址的警报通知。
2. 选择下一步。

要完成警报

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，为您的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。

查看存储效率节省情况

启用后，您可以在 Amazon FSx 控制台、亚马逊 CloudWatch 控制台和 ONTAP CLI 中查看节省了多少存储容量。

查看存储效率节省情况（控制台）

在 Amazon FSx 控制台中显示的 FSx for ONTAP 文件系统的存储效率节省包括和带来的节省。FlexClones SnapShots

1. 通过以下网址打开 Amazon FSx 控制台：https://console.aws.amazon.com/fsx/。
2. 从文件系统列表中选择您要查看其存储效率节省的 FSx for ONTAP 文件系统。
3. 在文件系统详细信息页面的第二个面板上的 “监控和性能” 选项卡中选择 “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 (ONTAPCLI)

通过使用 CLI ONTAP 运行`storage aggregate show-efficiency`命令，您可以看到仅通过压缩、压缩和重复数据删除来节省存储效率，而不受快照的影响。FlexClones有关更多信息，请参阅 NetApp ONTAP文档中心中的存储聚合显示效率。

1. 要访问 NetApp ONTAP CLI，请运行以下命令在 NetApp 适用于 ONTAP 的 Amazon FSx 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. 该storage aggregate show-efficiency命令显示有关所有聚合的存储效率的信息。存储效率分为四个不同的级别：

   - Total
   - 聚合
   - Volume
   - 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
```

修改 SSD 存储容量和预配置 IOPS

您可以使用 Amazon FSx 控制台、和 API 来增加文件系统基于 SSD 的存储，也可以增加或减少预配置的 SSD IOPS 量。 AWS CLI

更新文件系统的 SSD 存储容量或预配置 IOPS（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 存储容量和 SSD IOPS 的 FSx for ONTAP 文件系统。
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。

   系统会显示 更新 SSD 存储容量和 IOPS 对话框。

Update SSD storage capacity and IOPS

File system ID

fs-01234567890abcdef

Current configuration

SSD storage capacity: 4096 GiB
IOPS mode: Automatic (3 IOPS per GiB of SSD storage)
SSD IOPS: 12288

SSD storage capacity

☑ Modify storage capacity

Input type

◉ Percentage
○ Absolute

Desired % increase

10 %

Minimum 4506 GiB (10% above current); Maximum 1048576 GiB.

Provisioned SSD IOPS

◉ Automatic (3 IOPS per GiB of SSD storage)
○ User-provisioned

Configuration preview

Attribute	Current configuration	New configuration
SSD storage capacity	4,096 GiB (2,048 GiB per HA pair)	4,506 GiB (2,253 GiB per HA pair)
	Mode: Automatic	Mode: Automatic

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 SSD IOPS，保持 3 预调配 SSD IOPS/GiB SSD 存储容量（最多 16 万），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 FSx for ONTAP 文件系统预调配的 SSD IOPS 数量上限的更多信息，请参阅吞吐能力对性能的影响。

8. 选择更新。

> **Note**
>
> 在提示符的底部，将显示您的新 SSD 存储容量和 SSD IOPS 的配置预览。对于横向扩展文件系统，还会显示每个 HA 对的值。

为文件系统更新 SSD 存储容量和预配置 IOPS (CLI)

要更新 FSx for 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或等效的 API 操作。UpdateFileSystem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，`--storage-capacity`请设置为目标存储容量值，该值必须至少比当前值大 10%。

- 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。如果您不增加存储容量，则 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 自动增加 SSD IOPS，请使用 `Mode=AUTOMATIC` 且不要使用 `Iops` 参数。在预配置的固态硬盘存储容量中，Amazon 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 FSx for ONTAP 文件系统预调配的 SSD IOPS 数量上限的更多信息，请参阅吞吐能力对性能的影响。

以下示例将文件系统的固态硬盘存储空间增加到 2000 GiB，并将用户预配置的 SSD IOPS 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。

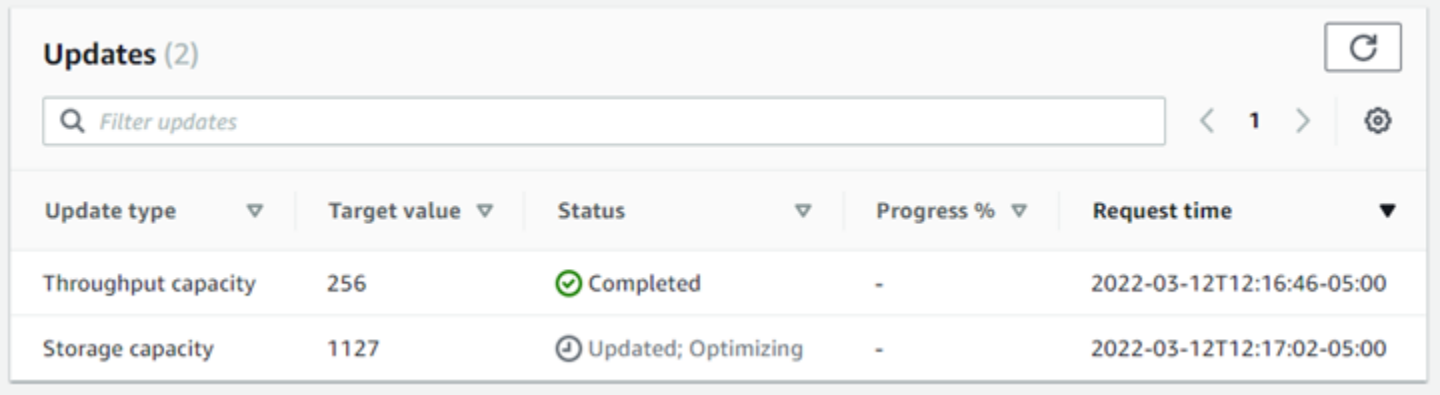
有关更多信息，请参阅适用于 NetApp ONTAP 的 Amazon FSx API 参考AdministrativeAction中。

监控存储容量和 IOPS 更新

您可以使用 Amazon 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）

访问 FSx for ONTAP 文件系统的文件系统详细信息页面，在更新选项卡中，您可以查看每种更新类型的 10 个最近更新。



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。
- 正在进行中 – Amazon FSx 正在处理更新请求。
- 已更新；正在优化 – Amazon FSx 已增加文件系统的 SSD 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 存储容量增加请求。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。

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 FSx 首先处理 FILE_SYSTEM_UPDATE 操作，为文件系统添加容量更大的新存储磁盘。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。存储容量显示新的更大值，随后 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"
    }
]
```

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"
        }
    }
```

```
]
```

动态增加 SSD 存储容量

当已使用的 SSD 存储容量超过指定的阈值时，您可以使用以下解决方案来动态增加 FSx for ONTAP 文件系统的 SSD 存储容量。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。

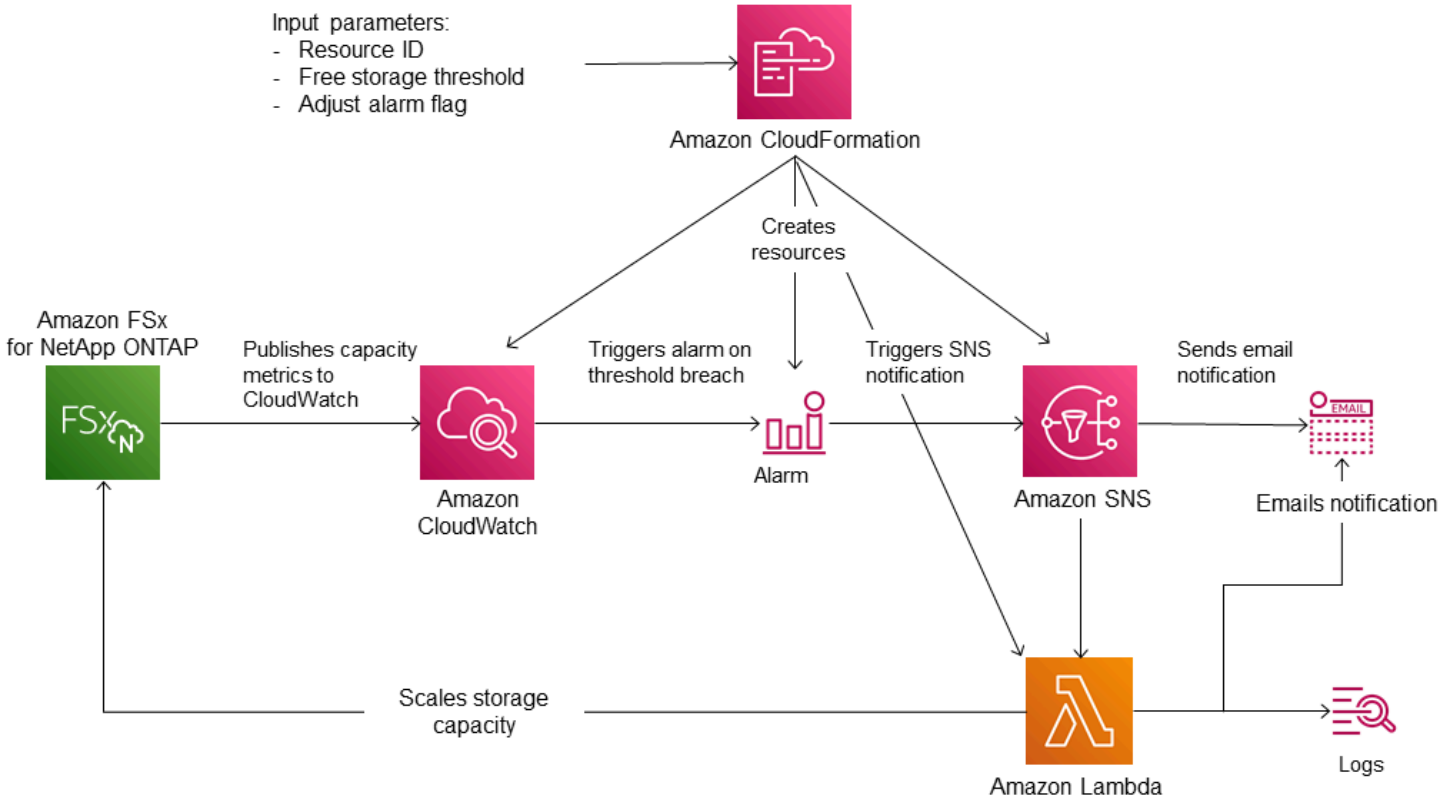
该解决方案会自动部署所需的所有组件，并采用以下参数：

- 您的 FSx for 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

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 AWS 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 Amazon 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。

AWS CloudFormation 模板

此解决方案 AWS CloudFormation 用于自动部署用于自动增加 FSx for ONTAP 文件系统的存储容量的组件。要使用此解决方案，请下载 F SxOntapDynamicStorageScaling AWS 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。

MaxF B SxSizeinGi

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 AWS CloudFormation

以下过程配置和部署 AWS CloudFormation 堆栈以自动增加 FSx for ONTAP 文件系统的存储容量。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。

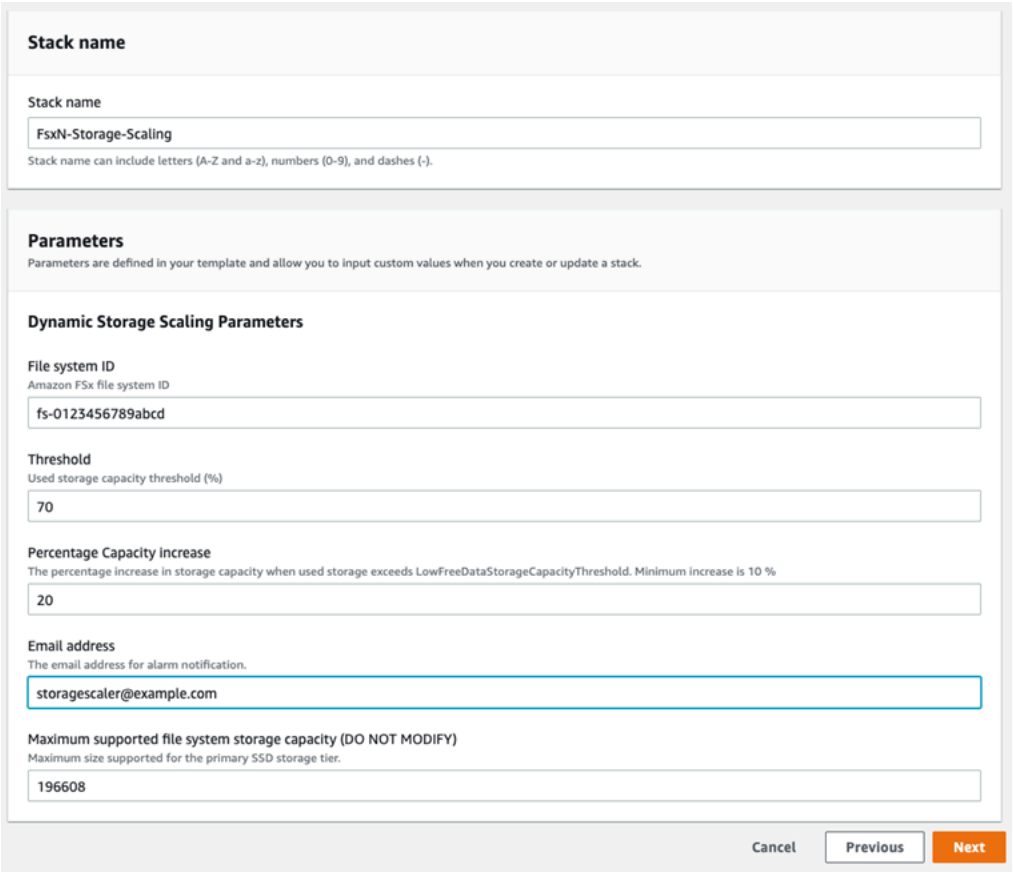
在开始之前，您必须拥有在亚马逊虚拟私有云（亚马逊 VPC）中运行的 Amazon FSx 文件系统的 ID。AWS 账户有关如何创建 Amazon FSx 资源的更多信息，请参阅开始使用适用于 ONTAP 的 Amazon FSx NetApp 。

启动自动存储容量增加解决方案堆栈

1. 下载 F SxOntapDynamicStorageScaling AWS 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《AWS 一般参考》中的 Amazon FSx 端点和配额。

2. 在 AWS 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 AWS 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。

卷存储容量

FSx for 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 for ONTAP 卷的 AWS Management Console存储容量。 AWS CLI

主题

- 卷数据分层
- 快照和卷存储容量
- 卷文件容量
- 更新卷的存储容量
- 启用音量自动调整大小
- 监控卷存储容量
- 设置卷的分层策略

- 设定最小冷却天数
- 设置卷的云检索策略
- 查看卷的文件容量
- 增加卷上文件的数量上限
- 启用卷的云写入模式

卷数据分层

适用于 NetApp ONTAP 文件系统的 Amazon FSx 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、冷却时间和阈值设置，每个卷上的数据会自动分层到容量池存储层。以下各节描述了ONTAP卷分层策略以及用于确定何时将数据分层到容量池的阈值。

卷分层策略

您可以通过为文件系统上的每个卷选择分层策略来确定如何将 FSx 用于 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NetApp 使用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。当使用 Amazon FSx 控制台创建卷时，这是默认策略。
- 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 ON NetApp TAP 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。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，则只要 SSD 利用率低于 90%，该卷中位于容量池存储的现有数据会通过后台进程移至 SSD 存储。通过故意读取数据或修改卷的云检索策略，您可以加快此后台进程。有关更多信息，请参阅 云检索策略。

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（基于卷的冷却周期），然后再移至容量池层。数据在 SSD 存储上保留至少 2 天之后，ONTAP 会对数据进行后处理压缩和重复数据删除，而且数据会在分层到容量池后保留。ONTAP 仅对 SSD 存储上的数据运行后处理压缩和重复数据删除，因此选择此策略可以帮助您长期更大限度地节省存储空间。您还可以更大限度地提高为卷创建的第一个备份的传输速度，因为要备份的数据位于 SSD 存储上。

有关如何设置或修改卷分层策略的更多信息，请参阅设置卷的分层策略。

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，请参阅设定最小冷却天数。

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，请参阅设置卷的云检索策略。

分层阈值

文件系统的 SSD 存储容量利用率决定了如何ONTAP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%。对于横向扩展文件系统，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 存储空间和 IOPS。

FSx for ONTAP 使用以下存储容量阈值来管理卷分层：

- <= 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% SSD 存储层利用率 – 达到此阈值时，Amazon FSx 会优先考虑保留 SSD 存储层中的空间。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

快照是适用于 NetApp ONTAP 的 Amazon FSx 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 快照的使用。

卷文件容量

适用于 NetApp ONTAP 卷的 Amazon FSx 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与卷的存储容量（以及卷的卷组成部分的数量）相应增加。FlexGroup默认情况下，存储容量为 648 GiB 或以上的FlexVol卷（或FlexGroup组成部分）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更多信息，请参阅查看卷的文件容量。

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

一个 FSx for ONTAP 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，请参阅增加卷上文件的数量上限。

更新卷的存储容量

您可以使用 AWS Management Console、 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。

您也可以使用 ONTAP CLI 使用`volume modify`命令修改卷的存储容量。

修改卷的大小（ONTAP CLI）

1. 要访问 NetApp ONTAP CLI，请运行以下命令在 NetApp 适用于 ONTAP 的 Amazon FSx 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 modify ONTAP CLI 命令修改卷的存储容量。运行以下命令，使用您的数据代替以下值：

   - 将 *`svm_name`* 替换为卷创建时所用存储虚拟机（SVM）的名称。
   - *`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
   ```

启用音量自动调整大小

自动调整卷大小，以便音量在达到已用空间阈值时自动增长到指定大小。您可以使用 ONTAP CLI 命令对 FlexVol 卷类型（ONTAP FSx 的默认卷类型）执行此操作。volume autosize

启用卷自动调整大小（ONTAP CLI）

1. 要访问 NetApp ONTAP CLI，请运行以下命令在 NetApp 适用于 ONTAP 的 Amazon FSx 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%。
   - 将 *min_size* 替换为卷大小的下限。使用与 *max_size* 相同的格式。
   - 将 *shrink_threshold* 替换为触发卷自动缩小的已用空间百分比。

   ```
   ::> 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
   ```

监控卷存储容量

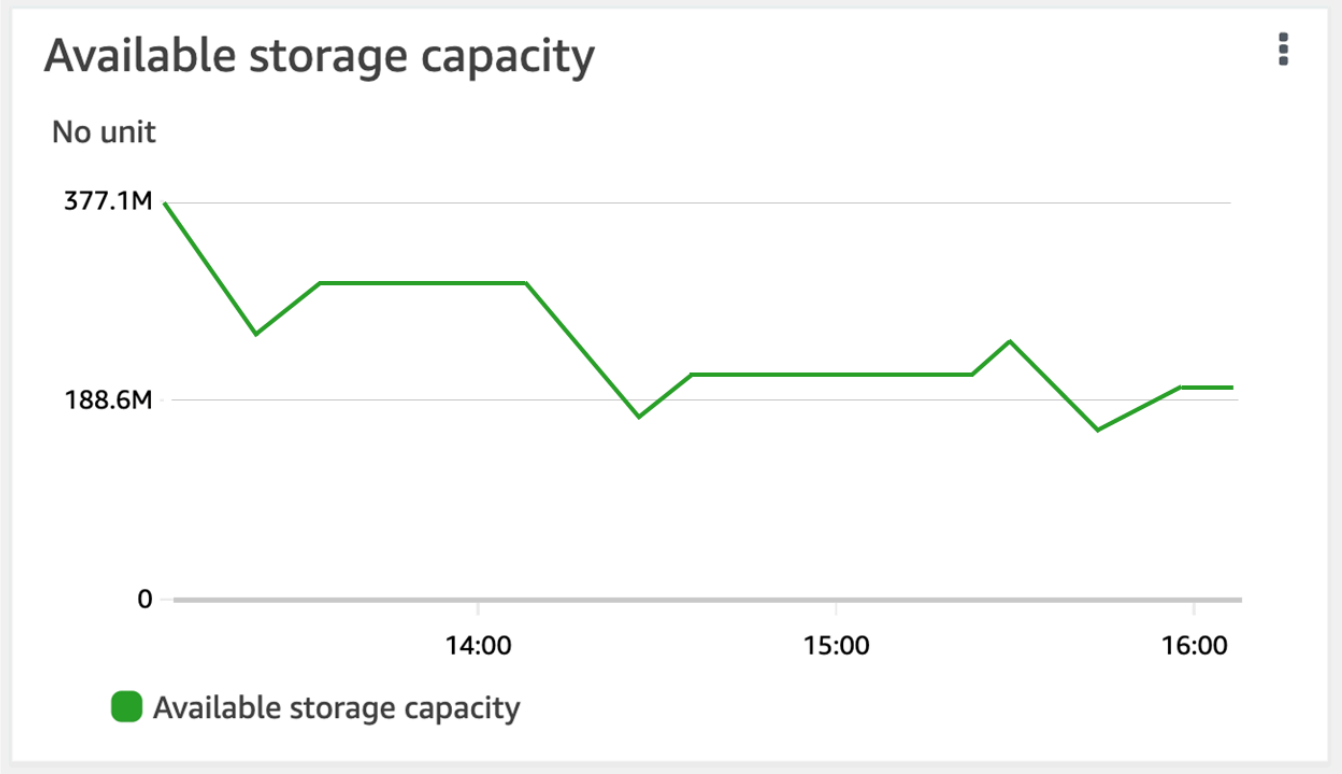
您可以在 AWS Management Console、 AWS CLI和 NetApp ONTAP CLI 中查看卷的可用存储空间及其存储分布。

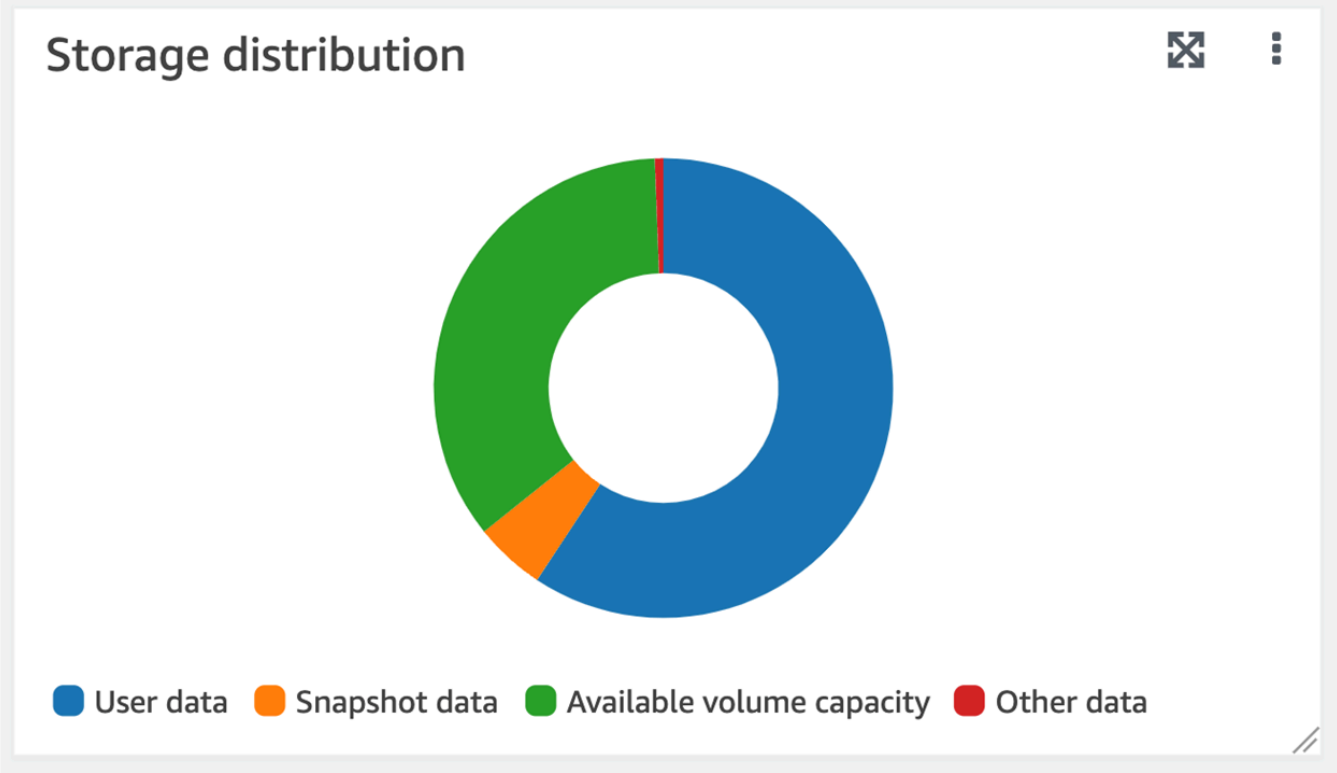
监控卷的存储容量（控制台）

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. 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 (ONTAPCLI)

您可以使用 `volume show-space` ONTAP CLI 命令监控卷存储容量的使用情况。有关更多信息，请参阅NetApp ONTAP文档中心volume show-space中的。

1. 要访问 NetApp ONTAP CLI，请运行以下命令在 NetApp 适用于 ONTAP 的 Amazon FSx 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. 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 的默认卷类型），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。

设置卷的分层策略

您可以使用 AWS Management Console、 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 Management Console修改卷的数据分层策略。

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（相当于 Amazon FSx 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 NetApp ONTAP CLI，请运行以下命令在 NetApp 适用于 ONTAP 的 Amazon FSx 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
   ```

设定最小冷却天数

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)

- 使用更新卷 CLI 命令 UpdateVolume（等同于 Amazon FSx 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 NetApp ONTAP CLI，请运行以下命令在 NetApp 适用于 ONTAP 的 Amazon FSx 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.
   ```

设置卷的云检索策略

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 NetApp ONTAP CLI，请运行以下命令在 NetApp 适用于 ONTAP 的 Amazon FSx 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
   ```

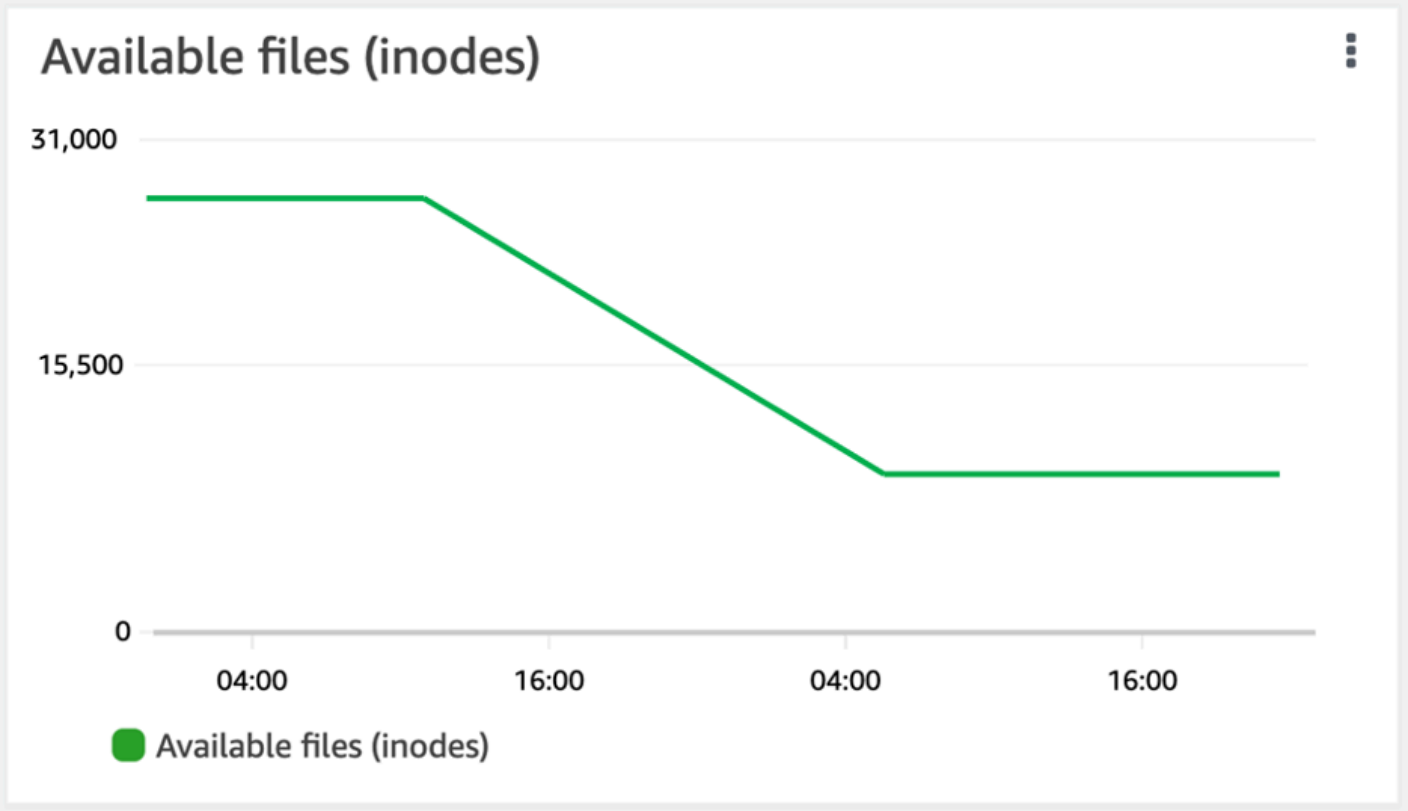
   请求成功后，系统会如下响应。

   ```
   Volume modify successful on volume vol_name of Vserver svm_name.
   ```

查看卷的文件容量

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，导航到卷的监控选项卡中的可用文件（索引节点）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）。



增加卷上文件的数量上限

当可用索引节点或文件指针的数量用完时，FSx for ONTAP 卷可能会耗尽文件容量。

增加卷上文件的最大数量 (ONTAPCLI)

您可以使用 `volume modify` ONTAP CLI 命令来增加卷上文件的最大数量。有关更多信息，请参阅 NetApp ONTAP文档中心`volume modify`中的。

1. 要访问 NetApp ONTAP CLI，请运行以下命令在 NetApp 适用于 ONTAP 的 Amazon FSx 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. 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
  ```

启用卷的云写入模式

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是：

- 该卷必须是现有卷。您只能在现有卷上启用该功能。
- 该卷必须是读写 (RW) 卷。
- 该卷必须具有 “全部分层” 策略。有关修改卷分层策略的更多信息，请参阅设置卷的分层策略。

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 NetApp ONTAP CLI，请运行以下命令在 NetApp 适用于 ONTAP 的 Amazon FSx 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，替换以下值：

   - 将 *svm_name* 替换为卷创建时所用 SVM 的名称。
   - *vol_name*替换为要为其设置云写入模式的卷名。
   - *vol_cw_mode*替换`true`为可在卷上启用云写入模式或`false`将其禁用。

   ```
   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.
   ```

保护您的数据

除了通过自动复制文件系统数据来确保高持久性之外，Amazon FSx 还为您提供了以下选项，帮助您进一步保护存储在文件系统上的数据：

- 原生 Amazon FSx 备份能够满足您在 Amazon FSx 中的备份保留和合规需求。您还可以使用 AWS Backup 在云端集中管理、自动化和保护您的备份。 AWS 服务
- 快照使用户可以轻松撤消文件更改并通过将文件恢复到早期版本来比较文件版本。
- 将您的 Amazon FSx 文件系统复制到辅助文件系统，提供数据保护和恢复。启用复制后，复制将按计划自动进行。
- SnapLock 能够通过将文件转换为“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。

主题

使用备份

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。FSx for ONTAP 备份是按卷进行的，因此每个备份仅包含特定卷中的数据。Amazon FSx 备份具有高持久性和增量性。

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。这意味着只在卷上保存在最新备份之后发生更改的数据。这样可以最大限度地减少创建备份所需的时间和备份所需的存储空间，从而通过不复制数据来节省存储成本。删除备份时，仅会删除该备份特有的数据。每个 Amazon FSx 备份都包含通过备份创建新卷所需的所有信息，从而有效地恢复文件系统卷的 point-in-time 快照。

为卷创建定期备份是一种最佳实践，有助于满足您的数据保留和合规性需求。无论是创建备份、从备份中恢复还是删除备份，使用 Amazon FSx 备份都非常简单。

Amazon FSx 支持备份ONTAPFlexVol卷（在所有文件系统上）和带有 ofRW（读写）OntapVolumeType的FlexGroup卷。

> **Note**
>
> Amazon FSx 不支持备份数据保护 (DP) 卷、负载共享 (LS) 卷或目标卷。FlexCache

每个文件系统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。

主题

备份的工作方式

Amazon FSx 备份使用快照（即卷的只读映像）来保持备份之间的增量。 point-in-time每次进行备份时，Amazon FSx 都会首先拍摄您的卷的快照。备份快照存储在您的卷中，占用 SSD 存储层上的空间。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可以在备份中保留卷节省的存储效率。

Amazon FSx 无法备份处于离线状态的卷。

存储需求

要对卷进行备份，您的卷和文件系统都必须有足够的可用固态硬盘存储容量来存储备份快照。拍摄备份快照时，快照消耗的额外存储容量不会导致卷的 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。

使用每日自动备份

创建文件系统时，默认启用文件系统卷的每日自动备份。您可以随时启用或禁用文件系统的每日自动备份。在创建文件系统时自动设置的每日备份窗口内进行每日备份。您可以随时修改每日备份窗口。对于使用您的卷以获得更好备份性能的应用程序，我们建议您选择一天中的某个时间进行每日备份，该时间不在正常运行时间之外。有关更多信息，请参阅 Backup 和恢复性能。

创建文件系统时，您可以随时在控制台中将每日自动备份的保留期设置为 1 到 90 天。默认的每日自动备份保留期为 30 天。该服务会在保留期到期后删除每日自动备份。使用 CLI 或 API，您可以将保留期设置为 0 到 90 天之间；将其设置为 0 会关闭每日自动备份。

每日备份窗口和备份保留期是文件系统级别的设置，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 来更改文件系统的备份窗口和备份保留期，并开启或关闭每日自动备份。有关更多信息，请参阅 更新文件系统。

如果卷处于脱机状态，则无法创建卷备份。有关更多信息，请参阅 备份和离线卷。

> **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 AWS Backup 服务将其删除。

您可以使用控制台、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创建该卷的最终备份的选项。除非您将其删除，否则最终备份将永久保存。有关更多信息，请参阅删除备份。

使用用户启动备份

借助 Amazon FSx，您可以随时使用 AWS Management Console 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。即使您删除了创建备份的卷或文件系统，用户启动的备份也会保留。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。有关更多信息，请参阅 删除备份。

如果卷处于脱机状态，则无法创建卷备份。有关更多信息，请参阅 备份和离线卷。

将标签复制到备份

使用 CLI 或 API 创建或更新卷时，可以启用CopyTagsToBackups自动将卷上的任何标签复制到其备份中。但是，如果您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命名备份，则CopyTagsToBackups即使启用了该服务，该服务也不会从卷中复制标签。

Backup 和恢复性能

多种因素可能会影响备份和恢复操作的性能。Backup 和恢复操作是后台进程，这意味着它们相对于客户端 IO 操作的优先级较低。客户端 IO 操作包括 NFS、CIFS 和 iSCSI 数据的读取和写入。所有后台进程，包括备份和恢复操作，都仅使用文件系统吞吐量中未使用的部分，可能需要几分钟到几小时才能完成，具体取决于备份的大小和文件系统上未使用的吞吐容量。

影响备份和恢复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。当大部分数据存储在 SSD 存储上时，我们建议您创建卷的第一个备份。与大多包含大文件的大小相似的数据集相比，主要包含小文件的数据集的性能通常较低。这是因为处理大量小文件比处理较少的大文件消耗更多的 CPU 周期和网络开销。

通常，在备份存储在 SSD 存储层中的数据时，您可以预期以下备份速率：

- 多个并发备份（主要包含大文件）为 750 Mbps。
- 多个并发备份中包含 100 Mbps，主要包含小文件。

通常，您可以预期恢复速率如下：

- 在多个并行恢复中，速度为 250 Mbps，主要包含大型文件。
- 在多个并行恢复中包含 100 Mbps，主要包含小文件。

AWS Backup 与 Amazon FSx 搭配使用

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。 AWS Backup 可以更轻松地为法律、监管和专业合规制定集中备份策略。 AWS Backup 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，与您从卷中获取的任何其他 Amazon FSx 备份（用户启动或自动）相比是增量的，并且提供的还原选项与通过 Amazon FSx 控制台进行的备份相同。如果您使用 AWS Backup 来管理这些备份，则可以获得其他功能，例如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保管库中来添加额外的防御层，以保护备份免遭意外或恶意删除。 AWS Backup

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。您可以在 Amazon FSx 控制台、CLI 和 API AWS Backup 中查看和恢复由创建的备份。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。

将备份恢复到新卷

您可以使用控制台、CLI 或 API 将卷备份还原到新卷，从而有效地恢复卷的 point-in-time 快照。

恢复备份时，首先将所有数据写入 SSD 存储层，然后服务开始根据您为恢复的卷设置的分层策略将数据分层到容量池存储。将备份恢复到分层策略为的卷时`All`，定期的后台进程会将数据分层到容量池。将备份恢复到分层策略为`Snapshot Only`或的卷时`Auto`，如果文件系统的固态硬盘利用率大于50%，并且冷却速率由分层策略的冷却期决定，则数据将分层到容量池。

当您在与原始文件系统具有不同数量的高可用性 (HA) 对的文件系统上恢复FlexGroup卷备份时，Amazon FSx 可能会添加其他组成卷以确保组成部分均匀分布。

有关将备份恢复到新卷的 step-by-step 说明，请参阅将备份恢复到新卷。

> **Note**
>
> 恢复后的卷始终与原始卷具有相同的音量样式。恢复时无法更改音量风格。

删除备份

您可以删除卷的每日自动备份和用户启动的备份。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。有关描述如何删除备份的说明，请参阅删除备份。

您无法在 Amazon FSx 控制台 AWS Backup、CLI 或 API 中删除由创建的、类型AWS Backup为的备份。有关删除由创建的备份的信息 AWS Backup，请参阅《 AWS Backup 开发人员指南》中的删除备份。

如果卷处于脱机状态，则无法删除该卷的备份。有关更多信息，请参阅 备份和离线卷。

> **Important**
>
> 请勿删除卷上的公共快照，因为它用于在备份之间保持增量。删除卷上的常用快照将导致下一次备份是整个卷的备份，而不仅仅是增量备份。

备份和离线卷

如果该卷处于脱机状态，则无法创建或删除该卷备份。使用 C `volume show`ONTAPLI 命令确定卷的当前状态和状态。

要使离线卷恢复联机，请使用 `volume online`ONTAPCLI 命令，如下例所示：

```
::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

创建用户启动的备份

以下过程介绍如何使用 Amazon FSx 控制台创建用户启动的卷备份。

如果卷处于脱机状态，则无法创建卷备份。有关更多信息，请参阅 备份和离线卷。

创建用户启动的卷备份（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”，然后选择要为其备份卷ONTAP的文件系统。

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 控制台中找到包含所有备份的表。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。

将备份恢复到新卷

以下过程介绍如何使用和将 FSx for ONTAP 备份还原到新卷。 AWS Management Console AWS CLI

将卷备份恢复到新卷（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. 在右上角的 “操作” 菜单中，选择 “恢复备份”。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 ONTAP 文件系统和存储虚拟机的 FSx。
5. 在 “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。
6. 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）。
7. 对于卷类型，选择 Read-Write (RW) 以创建可读写卷，或者选择数据保护 (DP) 以创建只读卷并可用作或关系的NetAppSnapMirror目标。SnapVault有关更多信息，请参阅 卷类型。
8. 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`。
9. 要提高存储效率，请选择 “启用” 以启用ONTAP存储效率功能（重复数据删除、压缩和压缩）。有关更多信息，请参阅 FSx for ONTAP 存储效率。
10. 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。

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。

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. 在 “高级” 部分的 “SnapLock配置” 中，您可以保留默认的 “禁用” 设置或选择 “启用” 来配置SnapLock音量。有关配置SnapLock Compliance卷或SnapLock Enterprise卷的更多信息，请参阅创建 SnapLock Compliance 卷和创建 SnapLock Enterprise 卷。有关 SnapLock 的更多信息，请参阅使用以下方法保护您的数据 SnapLock。

14. 选择确认即可创建卷。

将卷备份恢复到新卷 (CLI)

使用 create-volume-from-backupCLI 命令或等效 CreateVolumeFromBackup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}
  ```

  成功请求后的系统响应：

  ```
  {
        "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",

        }
    }
```

删除备份

您可以使用 Amazon FSx 控制台、CLI 和 API 删除每日自动备份和用户启动的备份，如以下过程所述。

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. 通过以下网址打开 Amazon FSx 控制台：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，确认显示的备份的 ID 是要删除的备份。
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
```

系统响应包括正在删除的备份的 ID 及其生命周期状态，并DELETED表示请求成功。

```
{
    "BackupId": "backup-a0123456789abcdef",
    "Lifecycle": "DELETED"
}
```

快照的使用

快照是适用于 NetApp ONTAP 的 Amazon FSx 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。借助快照，您的用户可以轻松查看和恢复早期快照中的单个文件或文件夹，以撤消更改、恢复已删除的内容和比较文件版本。

快照包含自上次快照以来发生更改的数据，这些数据消耗了文件系统的固态硬盘存储容量。任何卷备份中均不包含快照。默认情况下，使用快照策略在您的卷上启用default快照。快照存储于卷根的 .snapshot 目录中。在任何时间点，每个卷最多可以存储 1,023 个快照。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
- 还原单个文件和文件夹
- 从快照恢复文件
- 删除快照
- 创建快照自动删除策略
- 删除快照
- 禁用自动快照
- 快照储备
- 更新卷的快照预留空间

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。FSx for ONTAP 有三种内置快照策略：

- 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）。有关更改时区的信息，请参阅 Su NetApp pport 文档中的显示和设置系统时区。

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 Amazon 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。

还原单个文件和文件夹

用户可通过 Amazon FSx 文件系统上的快照快速还原单个文件或文件夹以前的版本。这样，用户就可以还原在共享文件系统中已被删除或更改的文件。用户可直接在自己的桌面上以自助服务的方式自行还原文件，无需管理员协助。这种自助服务方法提高了工作效率，减少了管理工作负载。

Linux 和 macOS 客户端可在卷根的 .snapshot 目录中查看快照。Windows 客户端可在 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。

从快照恢复文件

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。

删除快照

快照仅消耗自上次快照以来发生变化的卷上的数据的存储容量。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量存储容量。

例如，`volume show-space`ONTAPCLI 命令输出显示 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。您可以通过创建快照自动删除策略或手动删除快照来实现此目的。删除快照会删除快照中存储的已更改数据。

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。使用卷快照自动删除修改 ONTAP CLI 命令为卷建立自动删除策略。

使用此命令时，请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。

删除快照

使用 volume snapshot deleteONTAPCLI 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 Amazon FSx 备份，则 Amazon FSx 会为每个卷的最新 Amazon FSx 备份保留快照。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。

```
FsxIdabcdef01234567892::> volume snapshot delete -vserver svm_name -volume vol_name -
snapshot snapshot_name
```

禁用自动快照

在 FSx for ONTAP 文件系统中，默认快照策略会为卷启用自动快照。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 Management Console、 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. 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，请选择无。
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 (ONTAPCLI)

将卷的快照策略设置为使用none默认策略关闭自动快照。

1. 使用 C volume snapshot policy showONTAPLI 命令显示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 modifyONTAPCLI 命令将卷的快照策略设置为none以禁用自动快照。用您的数据替换以下占位符值：

   - *svm_name*— 使用你的 SVM 的名字。
   - *vol_name*— 使用您的卷名。

   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.
```

快照储备

Snapshot 副本预留设置卷存储容量的特定百分比用于存储 Snapshot 副本，默认值为 5%。Snapshot 副本保留空间必须为 Snapshot 副本（包括卷备份）分配足够的空间。如果 Snapshot 副本超过 Snapshot 保留空间，则必须从活动文件系统中删除现有 Snapshot 副本以恢复存储容量以供文件系统使用。您还可以修改分配给 Snapshot 副本的磁盘空间百分比。

每当快照占用超过 100% 的快照预留空间时，它们就会开始占用主 SSD 存储空间。此过程称为快照泄露。当快照继续占用活动文件系统空间时，文件系统有变满的风险。如果由于快照溢出导致文件系统已满，则只有在删除足够的快照后才能创建文件。

当 Snapshot 保留区中有足够的磁盘空间可供快照使用时，从主 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 Snapshot 副本仅占用 Snapshot 副本保留空间中的空间。

由于无法阻止快照消耗的磁盘空间超过为其保留的容量（快照预留空间），因此必须为快照预留足够的磁盘空间，以便主 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时创建的，则从主 SSD 层中删除文件不会创建任何可用空间，因为新创建的快照也会引用所有这些数据。要创建或更新任何文件，必须删除快照才能释放存储空间。

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。

更新卷的快照预留空间

您可以使用 NetApp ONTAP CLI 或 API 更改卷上的 Snapshot 预留量，如以下过程所述。

1. 要访问 NetApp ONTAP CLI，请运行以下命令在 NetApp 适用于 ONTAP 的 Amazon FSx 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 `snap reserve` ONTAP CLI 命令更改用于 Snapshot 副本保留的磁盘空间百分比。*vol_name*替换为卷名，然后 *percent* `with the percent of disk space you want to reserve for Snapshot copies.`

   ```
   ::> snap reserve vol_name percent
   ```

   以下示例将 vol1 的快照预留更改为卷存储容量的 25%。

   ```
   ::> snap reserve vol1 25
   ```

使用计划复制 NetApp SnapMirror

您可以使用安排 NetApp SnapMirror 将 FSx for ONTAP 文件系统定期复制到第二个文件系统或从第二个文件系统复制。此功能适用于区域内和跨区域部署。

NetApp SnapMirror 可以高速复制数据，因此无论您是在内部的两个 Amazon FSx 文件系统之间复制，还是从本地复制到 ONTAP 系统，您都可以获得高数据可用性和跨越ONTAP系统的快速数据复制。 AWS AWS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。

当您将数据复制到 NetApp 存储系统并不断更新辅助数据时，您的数据会保持最新状态，并且随时可用。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 BlueXP 文档中的了解复制服务。

除了 ONTAP CLI 和 REST API 之外，您还可以创建数据保护 (DP) 目标卷 AWS CLI，以便 NetApp SnapMirror使用亚马逊 FSx 控制台、和亚马逊 FSx AP NetApp I。有关使用 Amazon FSx 控制台创建目标卷的信息 AWS CLI，请参阅。创建卷

您可以使用 NetApp BlueXP 或 NetApp ONTAP CLI 来安排文件系统的复制。

> **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。

使用 NetApp BlueXP 来安排复制

您可以使用 NetApp BlueXP SnapMirror 在 FSx for ONTAP 文件系统上设置复制。有关更多信息，请参阅 NetApp BlueX P 文档中的在系统之间复制数据。

使用 NetApp ONTAP CLI 安排复制

您可以使用 NetApp ONTAP CLI 来配置定时卷复制。有关信息，请参阅 NetApp ONTAP 文档中心中的管理 SnapMirror 卷复制。

使用以下方法保护您的数据 SnapLock

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。

适用于 NetApp ONTAP 的 Amazon FSx 支持合规和企业保留模式。SnapLock有关更多信息，请参阅 SnapLock Compliance和 SnapLock Enterprise。

您可以在 2023 年 7 月 13 日当天或之后创建的 FSx for ONTAP 文件系统上创建 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。适用于 NetApp ONTAP 的 Amazon FSx 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	SnapLock Compliance	SnapLock Enterprise
描述	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。
用例	• 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	是	是
基于事件的保留（EBR）*	是	是
依法保留*	是	否
特权删除	否	是
卷附加模式	是	是
SnapLock 审计日志卷	是	是

* ONTAP CLI 和 REST API 支持 EBR 和依法保留操作。

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

- 运行以下命令。将 *svm_name* 和*SnapLockAdmin*替换为你自己的信息。

```
cluster1::> security login create -vserver SVM_name -user-or-group-
name SnapLockAdmin -application ssh -authentication-method password -role vsadmin-
snaplock
```

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 Amazon FSx 控制台、AWS CLI、Amazon FSx API、以及 ONTAP CLI 和 REST API 创建 SnapLock 审计日志卷。

Note

数据保护（DP）卷不能用作 SnapLock 审计日志卷。

以下步骤介绍如何在 Amazon FSx 控制台上创建 SnapLock 审计日志卷。

要在 Amazon FSx 控制台上创建 SnapLock 审计日志卷，请采取以下操作

1. 通过以下网址打开 Amazon FSx 控制台：https://console.aws.amazon.com/fsx/。
2. 按照以下部分中创建新卷的步骤进行操作：创建卷。
3. 在 “高级” 部分的 “SnapLock 配置” 中，选择 “启用”。

   选中该复选框以确认有关在卷上启用 SnapLock 的警告。
4. 对于审计日志卷，选择已启用。

   确保将连接路径设置为 `/snaplock_audit_log`。

5. 按照以下部分中创建新卷的剩余步骤进行操作：创建卷。
6. 选择确认即可创建卷。

要使用 Amazon FSx API 打开 SnapLock 审计日志卷，请在 `CreateSnaplockConfiguration` 中使用 `AuditLogVolume`。

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 Compliance

适用于 NetApp ONTAP 的 Amazon FSx 支持SnapLock合规卷。

使用 SnapLock Compliance 模式

本节介绍 Compliance 保留模式的用例和注意事项。

SnapLock Compliance 模式用例

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。SnapLock根据这些规定和法规，对 Amazon FSx for NetApp ONTAP 的合规性进行了评估。Cohasset Associates有关更多信息，请参阅适用于 ONTAP 的 Amazon FSx 合规评估报告。NetApp
- 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。

SnapLock Compliance 模式注意事项

以下是有关 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。

创建 SnapLock Compliance 卷

您可以使用 Amazon FSx 控制台、AWS CLI、Amazon FSx API、以及 ONTAP CLI 和 REST API 创建 SnapLock Compliance 卷。

要使用 Amazon FSx API 创建 SnapLock Compliance 卷，请在 `CreateSnaplockConfiguration` 中使用 `SnaplockType`。

以下步骤介绍如何在 Amazon FSx 控制台上创建 SnapLock Compliance 卷。

要在 Amazon FSx 控制台上创建 SnapLock Compliance 卷，请采取以下操作

1. 通过以下网址打开 Amazon FSx 控制台：https://console.aws.amazon.com/fsx/。
2. 按照以下部分中创建新卷的步骤进行操作：创建卷。
3. 在 “高级” 部分的 “SnapLock 配置” 中，选择 “启用”。

   选中该复选框以确认有关在卷上启用 SnapLock 的警告。
4. 对于保留模式，请选择 Compliance。
5. 对于审计日志卷，请选择已启用或已禁用。

   如果选择已启用，请确保将连接路径设置为 `/snaplock_audit_log`。

   有关更多信息，请参阅 SnapLock 审计日志卷。
6. 在保留期中，输入默认保留期、最短保留期和最长保留期的值。然后为每个保留期选择一个对应的单位。

   有关更多信息，请参阅 SnapLock 中的保留期。
7. 对于自动提交，请选择已启用或已禁用。

如果选择已启用，则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。

有关更多信息，请参阅 自动提交。

8. 对于卷附加模式，请选择已启用或已禁用。

有关更多信息，请参阅 卷附加模式。

9. 按照以下部分中创建新卷的剩余步骤进行操作：创建卷。
10. 选择确认即可创建卷。

SnapLock Enterprise

适用于 NetApp ONTAP 的 Amazon FSx 支持企业卷SnapLock。

使用 SnapLock Enterprise

本节介绍 Enterprise 保留模式的用例和注意事项。

SnapLock Enterprise 模式用例

您可以为以下用例选择 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。

使用 SnapLock Enterprise 模式的注意事项

以下是有关 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。

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 Amazon FSx 控制台、AWS CLI、Amazon FSx API 以及 ONTAP CLI 和 REST API 开启或关闭特权删除。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，请在 `CreateSnaplockConfiguration` 中使用 `PrivilegedDelete`。

以下步骤介绍如何在 Amazon FSx 控制台上开启特权删除功能。

要在 Amazon FSx 控制台上对 SnapLock Enterprise 卷启用特权删除，请采取以下操作

1. 通过以下网址打开 Amazon FSx 控制台：https://console.aws.amazon.com/fsx/。
2. 按照以下部分中创建新卷的步骤进行操作：创建卷。
3. 在 “高级” 部分的 “SnapLock 配置” 中，选择 “启用”。

   选中该复选框以确认有关在卷上启用 SnapLock 的警告。
4. 对于保留模式，请选择 Enterprise。
5. 对于特权删除，选择已启用。
6. 按照以下部分中创建新卷的剩余步骤进行操作：创建卷。
7. 选择确认即可创建卷。

> **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，请在 `CreateSnaplockConfiguration` 中使用 `PrivilegedDelete`。

要在 Amazon FSx 控制台上对 SnapLock Enterprise 卷永久关闭特权删除功能，请采取以下操作

1. 通过以下网址打开 Amazon FSx 控制台：https://console.aws.amazon.com/fsx/。
2. 按照以下部分中创建新卷的步骤进行操作：创建卷。
3. 在 “高级” 部分的 “SnapLock 配置” 中，选择 “启用”。

   选中该复选框以确认有关在卷上启用 SnapLock 的警告。
4. 对于保留模式，请选择 Enterprise。
5. 对于特权删除，选择已永久禁用。
6. 按照以下部分中创建新卷的剩余步骤进行操作：创建卷。
7. 选择确认即可创建卷。

创建 SnapLock Enterprise 卷

您可以使用 Amazon FSx 控制台、AWS CLI、Amazon FSx API、以及 ONTAP CLI 和 REST API 创建 SnapLock Enterprise 卷。

要使用 Amazon FSx API 创建 SnapLock Enterprise 卷，请在 `CreateSnaplockConfiguration` 中使用 `SnaplockType`。

要在 Amazon FSx 控制台上创建 SnapLock Enterprise 卷，请采取以下操作

1. 通过以下网址打开 Amazon FSx 控制台：https://console.aws.amazon.com/fsx/。
2. 按照以下部分中创建新卷的步骤进行操作：创建卷。
3. 在 “高级” 部分的 “SnapLock 配置” 中，选择 “启用”。

   选中该复选框以确认有关在卷上启用 SnapLock 的警告。
4. 对于保留模式，请选择 Enterprise。
5. 对于审计日志卷，请选择已启用或已禁用。

   如果选择已启用，请确保将连接路径设置为 `/snaplock_audit_log`。

   有关更多信息，请参阅 SnapLock 审计日志卷。

6. 在保留期中，输入默认保留期、最短保留期和最长保留期的值。然后为每个保留期选择一个对应的单位。

   有关更多信息，请参阅 SnapLock 中的保留期。

7. 对于自动提交，请选择已启用或已禁用。

   如果选择已启用，则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。

   有关更多信息，请参阅 自动提交。

8. 对于特权删除，请选择已启用、已禁用或已永久禁用。

   有关更多信息，请参阅 特权删除。

9. 对于卷附加模式，请选择已启用或已禁用。

   有关更多信息，请参阅 卷附加模式。

10. 按照以下部分中创建新卷的剩余步骤进行操作：创建卷。
11. 选择确认即可创建卷。

绕过 Enterprise 模式

如果您使用的是 Amazon FSx 控制台或 Amazon FSx API，则必须具有 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 Enterprise 卷。

有关更多信息，请参阅 删除 SnapLock 卷。

SnapLock 中的保留期

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。

类型	值	注意事项
秒	0-65,535	
分钟	0-65,535	
小时	0-24	
天	0-365	
Months	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*	-	保留文件，直到您设置保留期。 仅适用于默认保留期。

*当您将保留期未指定的文件转换到 WORM 时，系统会为它们提供为该 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 Amazon FSx 控制台、AWS CLI、Amazon FSx API、以及 ONTAP CLI 和 REST API 设置 SnapLock 卷的保留期。

要使用 Amazon FSx API 设置保留期，请使用 `SnaplockRetentionPeriod` 配置。

以下步骤介绍如何在 Amazon FSx 控制台上设置保留期。

要在 Amazon FSx 控制台上设置 SnapLock 卷的保留期，请采取以下操作

1. 通过以下网址打开 Amazon FSx 控制台：https://console.aws.amazon.com/fsx/。
2. 按照以下部分中创建新卷的步骤进行操作：创建卷。
3. 在 “高级” 部分的 “SnapLock 配置” 中，选择 “启用”。

   选中该复选框以确认有关在卷上启用 SnapLock 的警告。
4. 在保留期中，输入默认保留期、最短保留期和最长保留期的值。然后为每个保留期选择一个对应的单位。
5. 按照以下部分中创建新卷的剩余步骤进行操作：创建卷。
6. 选择确认即可创建卷。

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 Amazon FSx 控制台、AWS CLI、Amazon FSx API 以及 ONTAP CLI 和 REST API 开启自动提交功能。

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
分钟	5-65,535
小时	1-65,535
天	1-3,650
Months	1-120
年	1-10

要使用 Amazon FSx API 开启自动提交功能，请在 `CreateSnaplockConfiguration` 中使用 `AutocommitPeriod`。

以下步骤介绍如何在 Amazon FSx 控制台上开启自动提交功能。

要在 Amazon FSx 控制台上开启自动提交功能，请采取以下操作

1. 通过以下网址打开 Amazon FSx 控制台：https://console.aws.amazon.com/fsx/。
2. 按照以下部分中创建新卷的步骤进行操作：创建卷。
3. 在 “高级” 部分的 “SnapLock 配置” 中，选择 “启用”。

   选中该复选框以确认有关在卷上启用 SnapLock 的警告。
4. 对于自动提交，选择已启用。
5. 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。
6. 按照以下部分中创建新卷的剩余步骤进行操作：创建卷。
7. 选择确认即可创建卷。

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 Amazon FSx 控制台、AWS CLI、Amazon FSx API 以及 ONTAP CLI 和 REST API 开启卷附加模式。

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 启用卷附加模式，请在 `CreateSnaplockConfiguration` 中使用 `VolumeAppendModeEnabled`。

以下步骤介绍如何在 Amazon FSx 控制台上开启卷附加模式。

要在 Amazon FSx 主机上开启卷附加模式，请采取以下操作

1. 通过以下网址打开 Amazon FSx 控制台：https://console.aws.amazon.com/fsx/。
2. 按照以下部分中创建新卷的步骤进行操作：创建卷。
3. 在 “高级” 部分的 “SnapLock 配置” 中，选择 “启用”。

   选中该复选框以确认有关在卷上启用 SnapLock 的警告。
4. 对于卷附加模式，请选择已启用。
5. 按照以下部分中创建新卷的剩余步骤进行操作：创建卷。
6. 选择确认即可创建卷。

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

运行以下命令。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

运行以下命令。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

运行以下命令。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

运行以下命令。将每个 *p1* 替换为您自己的信息。

```
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

运行以下命令。将 *litigation1*、*slc_vol1* 和 *file1* 替换为您自己的信息。

```
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

运行以下命令。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

运行以下命令。将 *litigation1*、*slc_vol1* 和 *file1* 替换为您自己的信息。

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume slc_vol1 -
path /file1
```

使用 ONTAP CLI 对 SnapLock Compliance 卷中的所有文件结束依法保留

运行以下命令。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

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**
>
> 您无法备份SnapLock FlexGroup音量。

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。

有关备份的更多信息，请参阅使用备份。

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 AWS 账户 时，AWS 和 FSx for ONTAP 会将您的账户暂停 90 天，同时保持数据完整。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，AWS 都会删除您的数据，包括 SnapLock 卷中的数据。

如果您拥有相应的权限，则可以随时删除 SnapLock Enterprise 卷。您必须是 Amazon FSx 管理员。此外，如果您使用的是 Amazon FSx 控制台或 Amazon FSx API，则必须具有 IAM `fsx:BypassSnapLockEnterpriseRetention` IAM 权限才能删除包含具有有效保留策略的 WORM 数据的 SnapLock Enterprise 卷。

> **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。

要在 Amazon FSx 控制台上删除 SnapLock Enterprise 卷，请执行以下操作

1. 通过以下网址打开 Amazon FSx 控制台：https://console.aws.amazon.com/fsx/。
2. 在左侧导航窗格中，选择卷。
3. 选择要删除的卷。
4. 对于操作，请选择删除卷。
5. 对于 “绕过 SnapLock 企业保留”，选择 “是”。
6. 在确认对话框中，为创建最终备份执行下列操作之一：
   - 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。
7. 在确认删除字段中输入 **`delete`** 即可确认删除卷。
8. 选择删除卷。

在 FSx for ONTAP 中使用 Microsoft Active Directory

亚马逊 FSx 与微软 Active Directory 合作，与你的现有环境集成。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。

您可以选择将适用于 ONTAP 存储虚拟机 (SVM) 的 FSx 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，还可以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 FSx，而无需进行任何修改。

当您将适用于 NetApp ONTAP 的 Amazon FSx 加入活动目录时，您可以独立地将文件系统的 SVM 加入活动目录。这意味着你可以拥有一个文件系统，其中一些 SVM 已加入 Active Directory，而其他 SVM 则未加入 Active Directory。

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
- 自行管理的活动目录服务账号用户名和密码

主题

将 SVM 加入自行管理的 Microsoft AD 的先决条件

在将 FSx for ONTAP SVM 加入自行管理的 Microsoft AD 域之前，请确保 Active Directory 和网络符合以下部分中描述的要求。

主题

- Active Directory 服务账户要求

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。此活动目录应具有以下配置：

- Active Directory 域控制器域功能级别为 Windows Server 2000 或更高版本。
- Active Directory 使用的域名不是单一标签域 (SLD) 格式。Amazon FSx 不支持 SLD 域。
- 如果您定义了 Active Directory 站点，请确保与 FSx for ONTAP 文件系统关联的 VPC 子网是在相同的 Active Directory 站点中定义的，并且您的 VPC 子网与 Active Directory 站点上的子网之间不存在冲突。

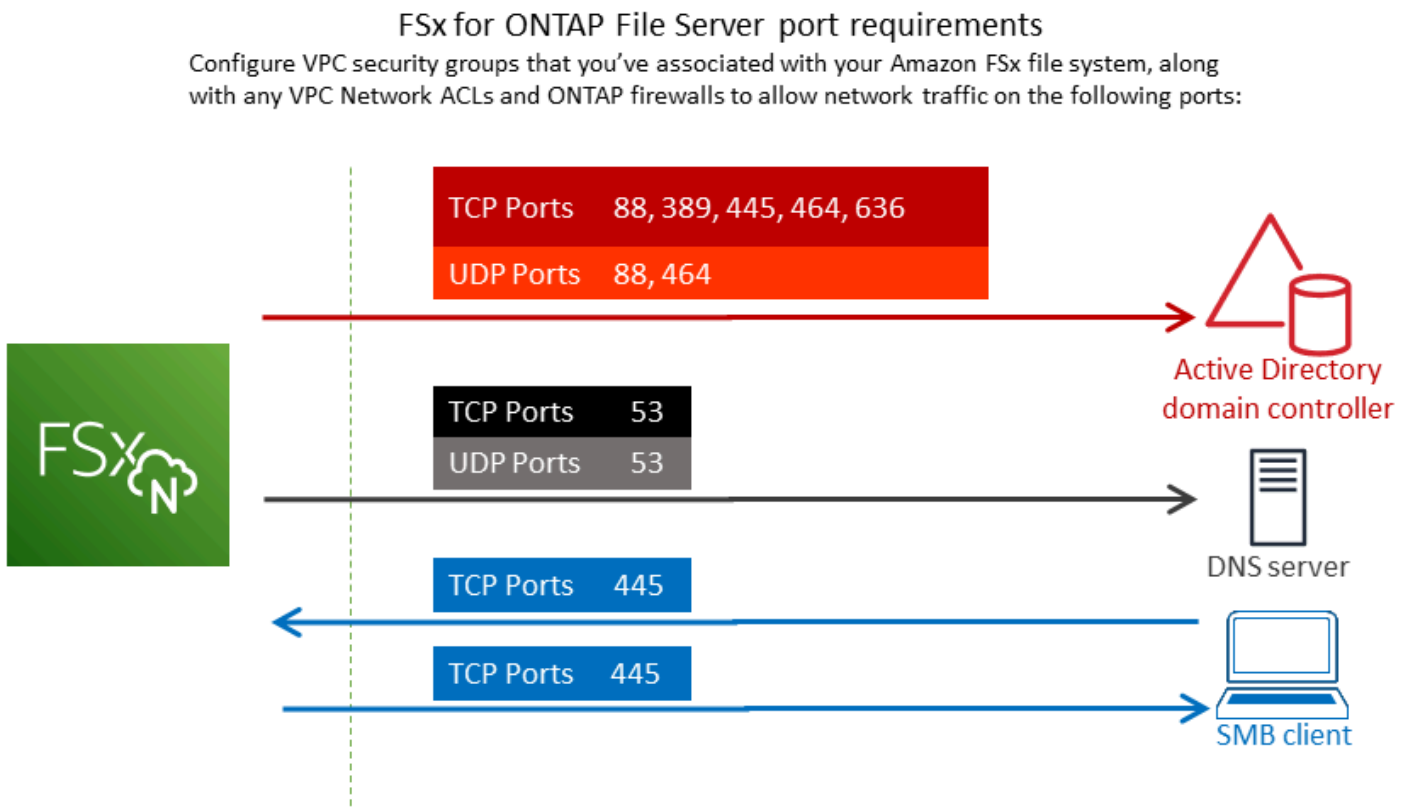
> **Note**
>
> 如果您使用的是 AWS Directory Service，则适用于 ONTAP 的 FSx 不支持将 SVM 加入简单活动目录。

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**
>
> 要将 SVM 加入 Active Directory，您需要确保本主题中介绍的端口允许所有 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（LIF））之间的流量。

- DNS 服务器和 Active Directory 域控制器 IP 地址。
- 使用 AWS Direct Connect、AWS 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。
- 要在其上创建文件系统的子网的安全组和 VPC 网络 ACL 必须允许下图所示端口和方向上的流量。



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	基于 TLS/SSL 的轻型目录访问协议（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 FSx 管理员的防火墙上。

> **Important**
>
> 虽然 Amazon VPC 安全组要求仅在发起网络流量的方向打开端口，但大多数 Windows 防火墙和 VPC 网络 ACL 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。服务帐户是您自行管理的 Active Directory 中的一个用户帐户，该帐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。

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 Amazon FSx 服务账户委托权限。

> **Important**
>
> Amazon FSx 在 Amazon FSx 文件系统的整个生命周期中都需要有一个有效的服务账户。Amazon FSx 必须能够完全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。使用 Amazon FSx 更新您的 Active Directory 配置信息，包括服务账户凭证。要了解更多信息，请参阅使用 Amazon FSx 确保 Active Directory 配置不断更新。

如果这是您首次使用 AWS 适用于 ONTAP 的 FSx，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**
>
> 在创建 SVM 后，请勿移动 Amazon FSx 在 OU 中创建的计算机对象，也不要在 SVM 已加入 Active Directory 时将其删除。这样做会导致您的 SVM 配置错误。

使用 Active Directory 的最佳实践

以下是将适用于 NetApp ONTAP 的 Amazon FSX SVM 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。

向 Amazon FSx 服务账户委托权限

请务必为 Amazon FSx 服务账户配置必要的最低权限。此外，将组织单位（OU）与其他域控制器问题分开。

要将 Amazon FSX SVM 加入您的域，请确保服务账户具有委托的权限。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 for ONTAP SVM 所需的权限委托给您的域。

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。

为您的 Microsoft Active Directory 域创建服务帐户

1. 确保你以 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 Tasks to Delegate (要委派的任务) 页面上，选择 Create a custom task to delegate (创建要委派的自定义任务)，然后选择 Next (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**
>
> 创建 SVM 后，请勿移动 Amazon FSx 在 OU 中创建的计算机对象。这样做会导致您的 SVM 配置错误。

使用 Amazon FSx 确保 Active Directory 配置不断更新

要使 Amazon FSX SVM 一直可用，请在更改自行管理的 AD 设置时更新 SVM 自行管理的 Active Directory（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，请在密码重置后立即使用 Amazon FSx 更新服务账户密码。为此，请使用 Amazon FSx 控制台、Amazon 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，请在更改发生后立即使用 Amazon FSx 更新 DNS 服务器 IP 地址。

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 Management Console、 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 Amazon FSx 文件系统的弹性网络接口关联的 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”。

将 SVM 加入 Microsoft Active Directory

无论是在本地还是在云中，您的组织都可能使用 Active Directory 管理身份和设备。使用适用于 ONTAP 的 FSx，您可以通过以下方式将 SVM 直接加入现有的 Active Directory 域：

- 在创建时将新 SVM 加入活动目录：
  - 使用 Amazon FSx 控制台中的标准创建选项为 ONTAP 文件系统创建新的 FSx，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 FSx for ONTAP 文件系统上创建新的 SVM。AWS CLI有关更多信息，请参阅创建存储虚拟机。
- 将现有 SVM 加入活动目录：
  - 使用 AWS Management Console 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 加入活动目录。您还可以更新已加入活动目录的 SVM 的某些活动目录配置属性。有关更多信息，请参阅管理 SVM 活动目录配置。
  - 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 管理 SVM 活动目录配置 NetApp 。

> **Important**
>
> - 如果使用 Microsoft DNS 作为默认 DNS 服务，Amazon FSx 仅注册 SVM 的 DNS 记录。如果使用第三方 DNS，则必须在创建 Amazon FSX SVM 后手动为其设置 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。

当您将适用于 ONTAP 的 FSx 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

无论您选择哪种 API 操作，在将 SVM 加入 Active Directory 时，您都必须提供有关活动目录的以下信息：

- 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，该名称在您的活动目录中必须是唯一的。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。

- 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 块范围内的 IP 地址：198.19.0.0/16
- Amazon FSx 在将 SVM 加入 Active Directory 域时使用的 Active Directory 域上的服务账户的用户名和密码。有关服务账户要求的更多信息，请参阅 Active Directory 服务账户要求。
- （可选）域中 SVM 所加入的组织单位（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 AWS Directory Service 创建的默认 OU 中。 AWS这是因为 AWS 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，Amazon FSx 会默认将此授权委派给 Active Directory 域中的域管理员组。

管理 SVM 活动目录配置

本节介绍如何使用 AWS Management Console、 AWS CLI、fsX API 和 ONTAP CLI 来执行以下操作：

- 将现有 SVM 加入活动目录
- 修改现有 SVM 活动目录配置
- 从活动目录中删除 SVM

要从 Active Directory 中删除 SVM，必须使用 NetApp ONTAP CLI。

主题

使用 AWS Management Console、 AWS CLI 和 API 将 SVM 加入活动目录

使用以下步骤将现有 SVM 加入活动目录。在此过程中，SVM 尚未加入 Active Directory。

将 SVM 加入 Active Directory () AWS Management Console

1. 通过以下网址打开 Amazon FSx 控制台：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 SVM 的列表，请在左侧导航窗格中，展开 ONTAP，然后选择存储虚拟机。中将显示您账户中所有 SVM AWS 区域 的列表。

从列表中选择要加入活动目录的 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. 为要加入 SVM 的 Active Directory 输入以下信息：

   - 要为你的 SVM 创建的 Active Directory 计算机对象的 NetBIOS 名称。这是 Active Directory 中 SVM 的名称，该名称在您的活动目录中必须是唯一的。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 – 域的 DNS 服务器的 IPv4 地址。
   - 服务账户用户名 – 现有 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）组织单位（OU）– 要将 SVM 加入到的组织单位的可分辨路径名称。
   - 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 Active Directory，请在活动目录中使用该群组的名称。默认组为 `Domain Admins`。
5. 选择加入活动目录，使用您提供的配置将 SVM 加入 Active Directory。

将 SVM 加入 Active Directory (AWS CLI)

- 要将适用于 ONTAP 的 FSx SVM 加入活动目录，请使用 CL update-storage-virtual-machineI 命令（或等效的 UpdateStorageVirtualMachineAPI 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
```

在成功创建存储虚拟机后，Amazon FSx 会以 JSON 格式返回存储虚拟机描述，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 Management Console、 AWS CLI和 API 更新现有 SVM Active Directory 配置

使用以下过程更新已加入活动目录的 SVM 的 Active Directory 配置。

更新 SVM 活动目录配置 () AWS Management Console

1. 通过以下网址打开 Amazon FSx 控制台：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–

   - 要显示所有可用 SVM 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. 您可以在此窗口中更新以下 Active Directory 配置属性。

- DNS 服务器 IP 地址 – 域的 DNS 服务器的 IPv4 地址。
- 服务账户用户名 – 现有 Active Directory 中服务账户的用户名。请勿包含域前缀或后缀。对于 EXAMPLE\ADMIN，请使用 ADMIN。
- 服务帐户密码-Active Directory 服务帐户的密码。

5. 输入更新后，选择更新 Active Directory 进行更改。

使用以下过程更新已加入活动目录的 SVM 的 Active Directory 配置。

更新 SVM 活动目录配置 () 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（或等效的 UpdateStorageVirtualMachineAPI 操作），如下例所示。

```
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 管理 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 CLI 将 SVM 加入活动目录

您可以使用 ONTAP CLI 将现有 SVM 加入活动目录，如以下过程所述。即使 SVM 已加入活动目录，您也可以执行此操作。

1. 要访问 NetApp ONTAP CLI，请运行以下命令在 NetApp 适用于 ONTAP 的 Amazon FSx 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. 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。将 *svm_name* 替换为您自己的信息。

```
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`，输入希望 SVM 加入的 OU，以及 DC 格式的完整 DNS 名称。

```
::>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

您可以使用 ONTAP CLI 修改现有的 Active Directory 配置。

1. 要访问 NetApp ONTAP CLI，请运行以下命令在 NetApp 适用于 ONTAP 的 Amazon FSx 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. 如果您需要修改 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
```

   您可以使用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. 如果您需要修改 Active Directory 配置本身，则可以使用以下命令更改现有字段，替换：

   - *computer_name*，如果要修改 SVM 的 NetBIOS（计算机账户）名称。
   - *domain_name*，如果要修改域名。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）。

   您将需要重新输入用于将此设备加入活动目录的 Active Directory 凭据。

   ```
   ::>vserver cifs modify -vserver svm_name -cifs-server computer_name -
   domain domain_name -OU organizational_unit
   ```

   您可以使用vserver cifs check -vserver *svm_name*命令验证 Active Directory 连接的连接状态。

5. 修改完您的 Active Directory 和 DNS 配置后，请运行以下命令恢复 CIFS 服务器：

   ```
   ::>vserver cifs modify -vserver svm_name -status-admin up
   ```

使用 ONTAP CLI 从您的 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 NetApp ONTAP CLI，请运行以下命令在 NetApp 适用于 ONTAP 的 Amazon FSx 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. 运行以下命令，将从活动目录中取消加入设备的 CIFS 服务器删除。要让 ONTAP 删除您的 SVM 的计算机帐户，请提供您最初用于将 SVM 加入 Active Directory 的凭据。

   ```
   FsxId0123456789a::>vserver cifs modify -vserver svm_name -status-admin down
   ```

3. 如果您需要修改 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. 通过运行以下命令删除 Active Directory 的 DNS 服务器：

```
::vserver services name-service dns delete -vserver svm_name
```

如果您看到类似以下的警告（表示dns应将其删除），ns-switch并且您不打算将此设备重新加入 Active Directory，则可以删除这些条目。ns-switch

```
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
```

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

用于衡量文件系统性能的因素包括其延迟、吞吐量和每秒 I/O 操作数（IOPS）。

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 文件系统可提供高达数十 Gb/s 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 取决于文件系统的总吞吐量和存储容量配置，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

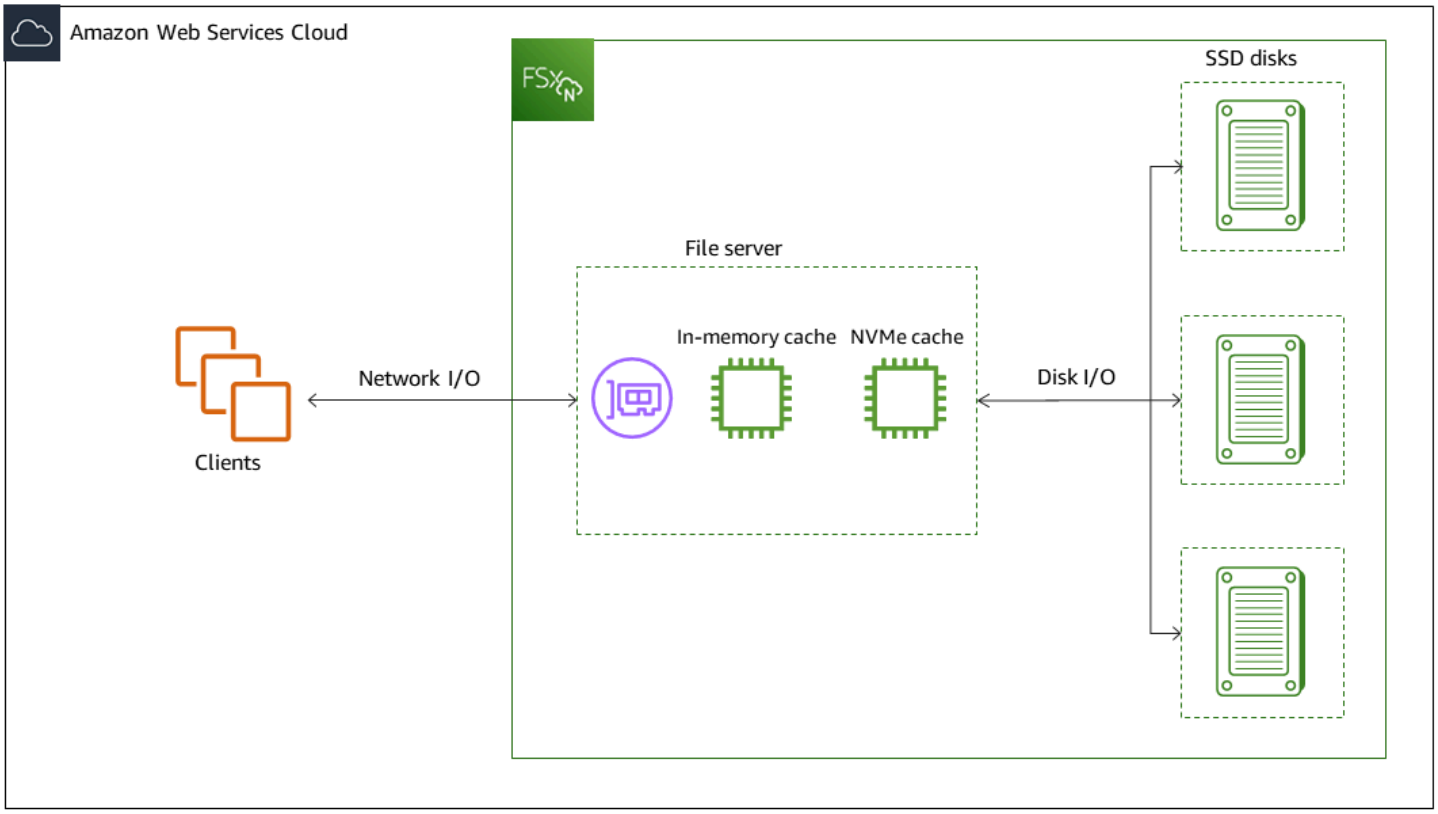
借助 Amazon FSx，您可以将 SMB 多渠道配置为在单个 SMB 会话中提供ONTAP和客户端之间的多个连接。SMB 多通道会在客户端和服务器之间同时使用多个网络连接，以此来聚合网络带宽，从而最大化利用率。有关使用 NetApp ONTAP CLI 配置 SMB 多通道的信息，请参阅配置 SMB 多通道以实现性能和冗余。

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，请参阅对 NFSv ONTAP 4.1 的支持。

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 后面都有一个NetApp ONTAP文件服务器，它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：客户端和文件服务器之间请求的吞吐量/IOPS（总计）
- 文件服务器上的内存缓存和 NVMe 缓存大小：可满足缓存的活动工作集的大小
- 磁盘 I/O 性能：文件服务器和存储磁盘之间请求的吞吐量/IOPS

决定文件系统的这些性能特征的因素有两个：SSD IOPS 的总量和您为其配置的吞吐容量。前两个性能特征（网络 I/O 性能以及内存和 NVMe 缓存大小）完全取决于吞吐能力，而第三个特征（磁盘 I/O 性能）则同时取决于吞吐能力和 SSD IOPS。

基于文件的工作负载通常处于尖峰状态，其特点是短暂而剧烈的高 I/O 周期，且两次突增之间有大量的空闲时间。为了支持尖峰工作负载，除了文件系统可以全天候维持的基准速度外，Amazon FSx 还提供在一段时间内突增至更高速度的功能，以用于网络 I/O 和磁盘 I/O 操作。Amazon FSx 会使用网络 I/O 点数机制，根据平均利用率分配吞吐量和 IOPS，即当文件系统的吞吐量和 IOPS 用量低于其基准限制时，文件系统会累积点数，然后可以在执行 I/O 操作时使用这些点数。

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复制，因此一次写入操作产生的网络吞吐量是原来的两倍。

部署类型对性能的影响

您可以使用 FSx for ONTAP 创建两种类型的文件系统。具有一对高可用性 (HA) 文件服务器的文件系统称为纵向扩展文件系统。具有多个 HA 对的文件系统称为横向扩展文件系统。有关更多信息，请参阅高可用性 (HA) 对。

FSx for ONTAP 多可用区和单可用区文件系统为 SSD 存储提供一致的亚毫秒级文件操作延迟，为容量池存储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：

- 多可用区文件系统
- 2022 年 11 月 28 日之后创建的吞吐容量至少为 2 Gbps 的单可用区纵向扩展文件系统

下表显示了文件系统可以扩展到的吞吐容量，具体取决于诸如高可用性 (HA) 对的数量和 AWS 区域 可用性等因素。

Scale-up

这些性能规格适用于向上扩展的文件系统。

纵向扩展文件系统每对 HA 的 SSD 存储的最大吞吐量

	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）
单可用区	4,096*	1000	2,048	750
多可用区	4,096*	1800	2,048	1,300

> **Note**
>
> * 要预置 4 Gbps 的吞吐容量，您的文件系统必须配置至少 5,120 GiB 的固态硬盘存储容量和 160,000 个固态硬盘 IOPS。

Scale-out

这些性能规格适用于横向扩展文件系统。

横向扩展文件系统每对 HA 的 SSD 存储的最大吞吐量

	读取吞吐量（MBps）	写入吞吐量（MBps）
单可用区横向扩展	6,144*	1,100*

> **Note**
>
> * 每对 HA（最多 12 个）。有关更多信息，请参阅 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容量
- 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，您的文件系统的 SSD 存储可提供高达以下级别的磁盘吞吐量和 IOPS：

- 磁盘吞吐量（每 TiB 存储空间 Mbps）：768
- 磁盘 IOPS（每 TiB 存储的 IOPS 数）：3072

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。您的文件系统的吞吐容量决定了网络 I/O 性能的级别，或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。更高级别的吞吐容量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。

Single-AZ (scale-up)

这些性能规范适用于 2022 年 11 月 28 日之后在指定中创建的单可用区向上扩展文件系统。 AWS 区域

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吞吐容量 (Mbps)	网络吞吐能力（Mbps）		网络 IOPS	内存缓存（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

FSx吞吐容量 (Mbps)	网络吞吐能力（Mbps）		网络IOPS	内存缓存（GB）	NVMe读取缓存（GB）	磁盘吞吐量（MBps）		SSD 驱动器IOPS *	
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可用 AWS 区域 FSx for ONTAP 的单可用区向上扩展文件系统。

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	内存缓存（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	600	18,750	–

FSx 吞吐能力（Mbps）	网络吞吐能力（Mbps）		网络 IOPS	内存缓存（GB）	磁盘吞吐量（MBps）		SSD 驱动器 IOPS *	
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。

Single-AZ (scale-out)

这些性能规格适用于横向扩展文件系统。

横向扩展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	内存缓存（GB）	磁盘吞吐量（MBps）		SSD 驱动器 IOPS *	
	基准	突增			基准	突增	基准	突增
3,072**	6,250	–	数十万基准	128	3,072	–	100000	–
6,144**	12,500	–		256	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。
> ** 每对 HA（最多 12 个）。有关更多信息，请参阅 高可用性 (HA) 对。

Multi-AZ (scale-up)

这些性能规范适用于 2022 年 11 月 28 日之后在指定的中创建的多可用区纵向扩展文件系统。AWS 区域

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	内存缓存（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
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可用 AWS 区域 FSx for ONTAP 的多可用区向上扩展文件系统。

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	内存缓存（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	600	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。

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 固态硬盘存储容量和 512 Mbps 吞吐容量的纵向扩展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 Management Console、、 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、管理帐户和密码、密码要求、SMB 和 iSCSI 协议、网络可访问性

主题

管理 FSx for ONTAP 文件系统

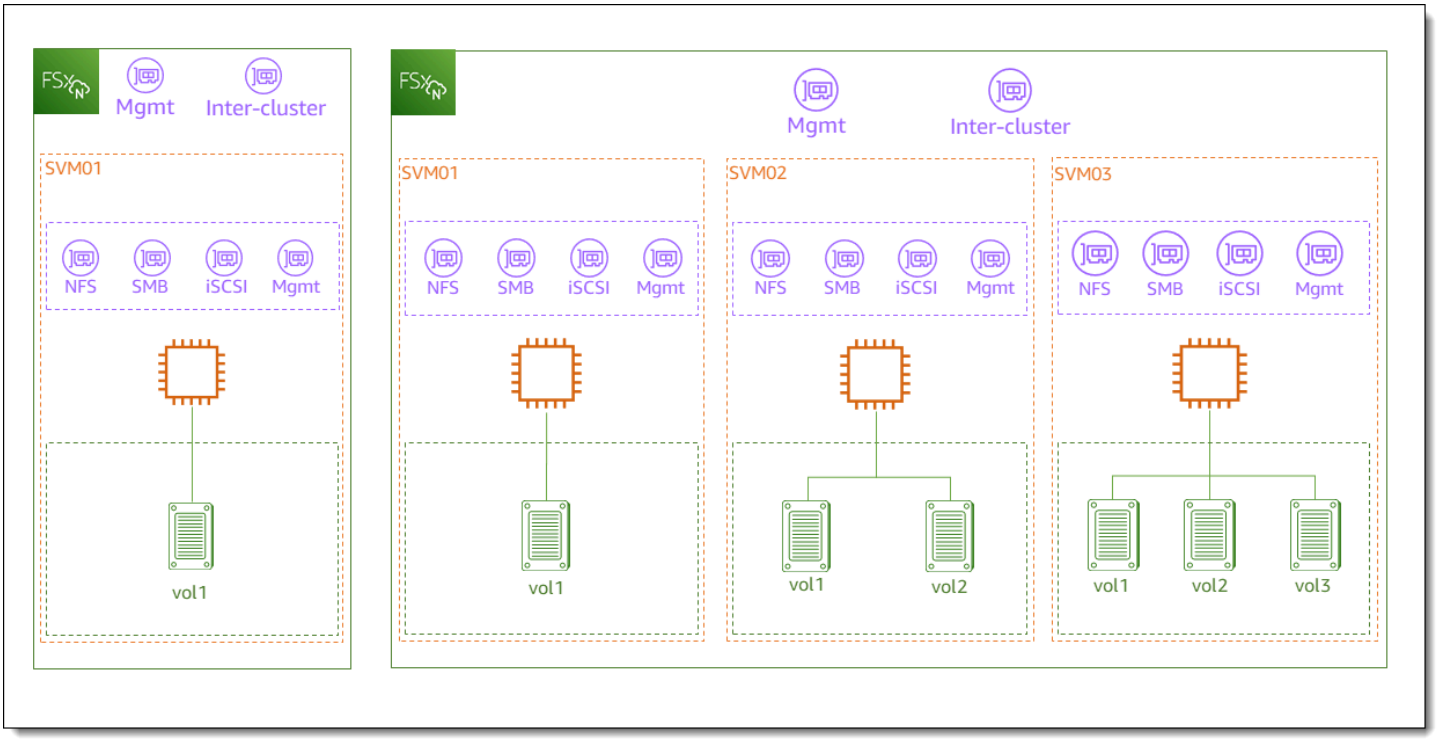
文件系统是主要 Amazon FSx 资源，类似于本地 ONTAP 集群。您可以为文件系统指定固态硬盘（SSD）存储容量和吞吐能力，然后选择用于创建文件系统的虚拟私有云（VPC）。每个文件系统都有一个管理端点，您可以使用该端点通过 ONTAP CLI 或 REST API 管理资源和数据。

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)。向上扩展文件系统有一个 HA 对，横向扩展文件系统有两个或更多 HA 对。每个 HA 对都有一个名为聚合的存储池。所有 HA 对的聚合集构成了您的 SSD 存储层。
- 一个或多个存储虚拟机（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。

下图说明了具有一个 HA 对的 ONTAP 文件系统的纵向扩展 FSx 的架构，以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（多可用区或单可用区）。单可用区文件系统可复制您的数据并在单个可用区内提供自动故障转移，并提供横向扩展文件系统。多可用区文件系统还可复制数据并支持在同一个 AWS 区域的多个可用区之间进行失效转移，从而提高恢复能力。

- 存储容量 — 这是固态硬盘存储量，纵向扩展文件系统最高为 192 太字节 (TiB)，横向扩展文件系统最高为 1 PB (PiB)。
- 固态硬盘 IOPS — 默认情况下，每 GB 固态硬盘存储包括三个 SSD IOPS（不超过您的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。对于多可用区文件系统，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 都有以下文件系统终端节点，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 使用应用程序管理 ONTAP 资源的 FSx NetApp 和 使用计划复制 NetApp SnapMirror。

高可用性 (HA) 对

每个 FSx for ONTAP 文件系统均由一对或多对高可用性 (HA) 文件服务器提供支持，采用主动-备用配置。在此配置中，有一个主动为流量提供服务的首选文件服务器和一个在活动服务器不可用时接管的辅助文件服务器。适用于 ONTAP 纵向扩展文件系统的 FSx 由一个 HA 对提供支持，可提供高达 4 Gbps 的吞吐容量和 160,000 个固态硬盘 IOP。适用于 ONTAP 横向扩展文件系统的 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）。

当您通过 Amazon FSx 控制台创建文件系统时，Amazon FSx 会根据所需的固态硬盘存储建议您应使用的 HA 对数量。您也可以根据工作负载和性能要求手动选择 HA 对的数量。如果您的文件系统要求通过高达 4 Gbps 的吞吐容量和 160,000 个 SSD IOP 来满足，我们建议您使用单个 HA 对；如果您的工作负载需要更高级别的性能可扩展性，则建议您使用多个 HA 对。

每个 HA 对都有一个聚合，这是一组逻辑物理磁盘。

> **Note**
>
> 您无法向现有文件系统添加 HA 对。相反，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（具有不同的 HA 对）之间迁移数据。 AWS DataSync

创建 FSx for ONTAP 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 中创建多可用区文件系统时，需要考虑一些注意事项。本主题解释了这些注意事项。

默认情况下，当您通过 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，从而允许通过网络文件系统 (NFS) 协议快速访问 Linux 实例中的数据。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，请参阅第 1 步：创建适用于 NetApp ONTAP 文件系统的亚马逊 FSx。

1. 通过以下网址打开 Amazon FSx 控制台：https://console.aws.amazon.com/fsx/。
2. 在仪表板上，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，选择多可用区或单可用区。
     - 多可用区文件系统可复制数据并支持在同一 AWS 区域的多个可用区之间进行失效转移。

- 单可用区文件系统可复制数据，并在单个可用区内提供自动失效转移。

> **Note**
>
> 如果您希望创建具有两个或更多高可用性 (HA) 对（最多 12 个）的文件系统，请选择单可用区。有关更多信息，请参阅 高可用性 (HA) 对。

有关更多信息，请参阅 可用性与持久性。

- 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 范围内的任意整数（最多 1 pebibyte [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）。
  - 如果要指定 IOPS 数，请选择用户预调配。每个文件系统最多可以预配置 200,000 个固态硬盘 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。

- 对于吞吐容量，您可以使用两个选项来确定以每秒兆字节 (MBps) 为单位的吞吐容量：
  - 如果您希望 Amazon FSx 根据您选择的存储容量自动选择吞吐容量，请选择推荐吞吐容量。
  - 如果要指定吞吐容量，请选择指定吞吐容量。如果选择此选项，则会出现吞吐量容量下拉列表，并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 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“网络”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，您可以选择与文件系统的网络接口关联的安全组。如果您未指定安全组，Amazon FSx 会将 VPC 的默认安全组与您的文件系统相关联。

- 为文件服务器指定子网。如果要创建多可用区文件系统，还要为备用文件服务器选择备用子网。
- （仅限多可用区）对于 VPC 路由表，指定 VPC 路由表以创建文件系统的端点。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 会选择您的 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多可用区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 多可用区文件系统创建 FSX 时， AWS CloudFormation 我们建议您手动添加标签。`Key: AmazonFSx; Value: ManagedByAmazonFSx`

- （仅限多可用区）端点 IP 地址范围指定 IP 地址范围，用于访问您文件系统的端点将在此范围中创建。

  端点 IP 地址范围有三个选项：

  - 未从 VPC 分配 IP 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 IP 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）。

  - 在“首选子网”中，为您的文件服务器指定子网。如果要创建多可用区文件系统，还要为备用文件服务器选择备用子网。
  - （仅限多可用区）对于 VPC 路由表，指定 VPC 路由表以创建文件系统的端点。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 会选择您的 VPC 的默认路由表。
  - （仅限多可用区）端点 IP 地址范围指定 IP 地址范围，用于访问您文件系统的端点将在此范围中创建。

    端点 IP 地址范围有三个选项：

- 未从 VPC 分配 IP 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 IP 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）。

- VPC 之外的浮动 IP 地址范围 – Amazon FSx 选择的 198.19.x.0/24 地址范围尚未被任何具有相同 VPC 和路由表的其他文件系统使用。
- 输入 IP 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 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。

> **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

7. 在安全和加密部分，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 CLI 管理 SVM ONTAP。

  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。

- 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 for ONTAP 中使用 Microsoft 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 – 您的域的域名系统（DNS）服务器的 IPv4 地址。
  - 服务账户用户名 – 现有 Active Directory 中服务账户的用户名。请勿包含域前缀或后缀。
  - 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）组织单位（OU）– 文件系统要加入的组织单位的可分辨路径名称。
  - 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，提供使用您的文件系统创建的默认卷的以下信息：

- 在卷名字段中，填入卷的名称。您最多可以使用 203 个字母数字或下划线 (_) 字符。
- （仅限向上扩展文件系统）对于 “卷” 样式，请选择或FlexVol。FlexGroup FlexVol卷是通用卷，大小可达 300 TiB。 FlexGroup卷专为高性能工作负载而设计，大小最高可达 20 PiB。
- 对于卷大小，请输入 800 千兆字节 (GiB) 到 2,000 Pebibytes (PiB) 范围内的任意整数。
- 对于卷类型，选择 Read-Write (RW) 以创建可读写卷，或者选择数据保护 (DP) 以创建只读卷并可用作或关系的NetAppSnapMirror目标。SnapVault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 FSx for ONTAP 存储效率。
- 对于卷安全类型，请在 Unix (Linux)、NTFS 和混合卷之间进行选择。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。

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。

13. 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。

14. 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。
15. 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CreateFile系统 API 操作），如以下示例所示。

```
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 或卷。要创建 SVM，请参阅创建存储虚拟机；要创建卷，请参阅创建卷。

为共享子网中的 ONTAP 文件系统创建 FSX

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 单可用区和多可用区文件系统创建 FSX。要让参与者账户创建多可用区文件系统，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 管理多可用区文件系统的共享 VPC 支持。

> **Note**
>
> 参与者账户有责任与 VPC 所有者协调，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

在共享子网中为 ONTAP 文件系统创建 FSx 时，请注意以下几点：

- VPC 子网的所有者必须与参与者账户共享子网，然后该账户才能在子网中为 ONTAP 文件系统创建 FSX。
- 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所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。所有者账户可以看到参与者创建的安全组，但不能对其执行任何操作。如果所有者账户想要删除或修改这些安全组，则创建安全组的参与者必须采取行动。
- 参与者账户可以查看、创建、修改和删除所有者账户与其共享的子网中的单可用区文件系统及其关联资源。
- 参与者账户可以创建、查看、修改和删除所有者账户与其共享的子网中的多可用区文件系统及其关联资源。此外，所有者账户还必须向 Amazon FSx 服务授予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，请参阅管理多可用区文件系统的共享 VPC 支持
- 共享 VPC 所有者无法查看、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 用户指南中的所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

与将在共享子网中为 ONTAP 文件系统创建 FSx 的参与者帐户共享子网时，您需要执行以下操作：

- 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 所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您的 VPC。

- 要使参与者账户为 ONTAP 多可用区文件系统创建 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 多可用区文件系统的 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。发生故障转移事件时，Amazon FSx 会更新与文件系统关联的所有路由表中的所有路由，使其指向当前活动的文件服务器。

管理多可用区文件系统的共享 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 文件系统创建多可用区 FSx AWS CLI，如以下 AWS Management Console各节所述。

管理多可用区文件系统的 VPC 共享（控制台）

通过以下网址打开 Amazon FSx 控制台：https://console.aws.amazon.com/fsx/。

1. 在导航窗格中，选择 Settings（设置）。
2. 在 “设置” 页面上找到多可用区共享 VPC 设置。
   - 要在您共享的 VPC 子网中为多可用区文件系统启用 VPC 共享，请选择启用参与者账户的路由表更新。
   - 要在您拥有的所有 VPC 中禁用多可用区文件系统的 VPC 共享，请选择禁用参与者账户的路由表更新。将显示确认屏幕。

   > **Important**
   >
   > 我们强烈建议先删除参与者在共享 VPC 中创建的多可用区文件系统，然后再禁用此功能。禁用该功能后，这些文件系统将进入`MISCONFIGURED`状态并面临不可用的风险。

3. 输入**`confirm`**并选择 “确认” 以禁用该功能。

管理多可用区文件系统的 VPC 共享 ()AWS CLI

1. 要查看多可用区 VPC 共享的当前设置，请使用 describe-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
```

该服务对成功请求的响应如下：

```
{
    "EnableFsxRouteTableUpdatesFromParticipantAccounts": "false"
}
```

2. 要管理多可用区共享 VPC 配置，请使用 upd ate-shared-vpc-configuration CLI 命令或等效的 AP I 命令。UpdateSharedVpcConfiguration以下示例为多可用区文件系统启用 VPC 共享。

```
$ aws fsx update-shared-vpc-configuration --enable-fsx-route-table-updates-from-participant-accounts true
```

该服务对成功请求的响应如下：

```
{
    "EnableFsxRouteTableUpdatesFromParticipantAccounts": "true"
}
```

3. 要禁用该功能，请EnableFsxRouteTableUpdatesFromParticipantAccounts将设置为false，如以下示例所示。

```
$ aws fsx update-shared-vpc-configuration --enable-fsx-route-table-updates-from-participant-accounts false
```

该服务对成功请求的响应如下：

```
{
    "EnableFsxRouteTableUpdatesFromParticipantAccounts": "false"
}
```

更新文件系统

本主题说明您可以更新现有文件系统的哪些属性，并提供使用控制台和 CLI 进行更新的过程。

您可以使用亚马逊 FSx 控制台、和 Amazon FSx 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。有关备份的更多信息，请参阅使用每日自动备份。
- 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。有关维护时段的更多信息，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。对于多可用区 FSx for ONTAP 文件系统，用于通过 NFS 或 SMB 访问数据的端点以及用于访问 ONTAP CLI、API 和 BlueXP 的管理端点使用与文件系统关联的 Amazon VPC 路由表中的浮动 IP 地址。您可以将创建的新路由表与现有的多可用区文件系统关联，这样便可以配置随着网络发展，哪些客户端可以访问您的数据。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`。使用为 ONTAP 多可用区文件系统创建或更新 FSx 时， AWS 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）

以下过程为您提供有关如何使用更新现有 FSx for ONTAP 文件系统的说明。 AWS Management Console

更新每日自动备份

1. 通过以下网址打开 Amazon FSx 控制台：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. 通过以下网址打开 Amazon FSx 控制台：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. 通过以下网址打开 Amazon FSx 控制台：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 管理窗格中的 ONTAP 管理员密码下选择更新。
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**
>
> 如果您收到错误消息，指出新密码不符合密码要求，则可以使用 `security login role config show`ONTAPCLI 命令查看文件系统上的密码要求设置。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账户密码失败。

更新多可用区文件系统上的 VPC 路由表

1. 通过以下网址打开 Amazon FSx 控制台：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，选择管理路由表。此选项仅适用于多可用区文件系统。
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）

以下过程说明如何使用更新适用于 ONTAP 的现有 FSx 文件系统。 AWS CLI

1. 要更新适用于 ONTAP 文件系统的 FSx 的配置，请使用更新文件系统 CLI 命令（或等效的UpdateFile系统 AP I 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，请将该AutomaticBackupRetentionDays属性设置为 0。

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --ontap-configuration AutomaticBackupRetentionDays=0
```

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 – 按照步骤 3：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 delete-file-system CLI 命令或系统 API DeleteFile操作。

查看文件系统详细信息

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

要查看详细的文件系统信息，请执行以下操作：

- 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。

  以下选项卡提供了详细的配置信息以及可以修改的属性的编辑：

  - 网络与安全
  - 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高级摘要
    - 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终端节点的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
  - Backup 设置-更改文件系统的每日自动备份设置。
  - 更新-显示用户发起的对文件系统配置的更新的状态。
  - 标签-查看、编辑、添加、删除标签键:值对。
- 使用 CLI 或 API — 使用 d escribe-file-systems CLI 命令或DescribeFile系统 API 操作。

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 操作系统来查看 Amazon FSx 文件系统的状态。DescribeFile

文件系统状态	描述
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。

管理 FSx for ONTAP 存储虚拟机

在 FSx for ONTAP 中，卷托管于名为存储虚拟机（SVM）的虚拟文件服务器。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 FSx for ONTAP 中的数据时，客户端和工作站会使用 SVM 的端点（IP 地址）挂载由 SVM 托管的卷、SMB 共享或 iSCSI LUN。

当您使用 AWS Management Console创建文件系统时，Amazon FSx 会自动在文件系统上创建默认 SVM。您可以随时使用控制台、、 AWS CLI Amazon FSx API 和软件开发工具包在文件系统上创建其他 SVM。您无法使用 ONTAP CLI 或 REST API 创建 SVM。

您可以将 SVM 加入 Microsoft Active Directory，以进行文件访问身份验证和授权。有关更多信息，请参阅 在 FSx for ONTAP 中使用 Microsoft Active Directory。

每个文件系统的 SVM 数量上限

下表列出了您可以为文件系统创建的 SVM 的数量上限。SVM 的数量上限取决于以每秒兆字节（MBps）为单位预置的吞吐能力。

Deployment type（部署类型）	吞吐能力（MBps）	每个文件系统的 SVM 数量上限
单可用区（向上扩展）和多可用区（向上扩展）	128	6
	256	6

Deployment type（部署类型）	吞吐能力（MBps）	每个文件系统的 SVM 数量上限
	512	14
	1024	14
	2,048	24
	4,096	24
单可用区（横向扩展）	任何	5

主题

- 创建存储虚拟机
- 更新存储虚拟机
- 删除存储虚拟机（SVM）
- 查看存储虚拟机配置详细信息

创建存储虚拟机

您可以使用、和 API 为 ONTAP SVM 创建 FSx。 AWS Management Console AWS CLI

您可以为文件系统创建的最大 SVM 数量取决于文件系统的部署类型和预配置的吞吐容量。有关更多信息，请参阅 每个文件系统的 SVM 数量上限。

SVM 属性

创建 SVM 时，需要定义以下属性：

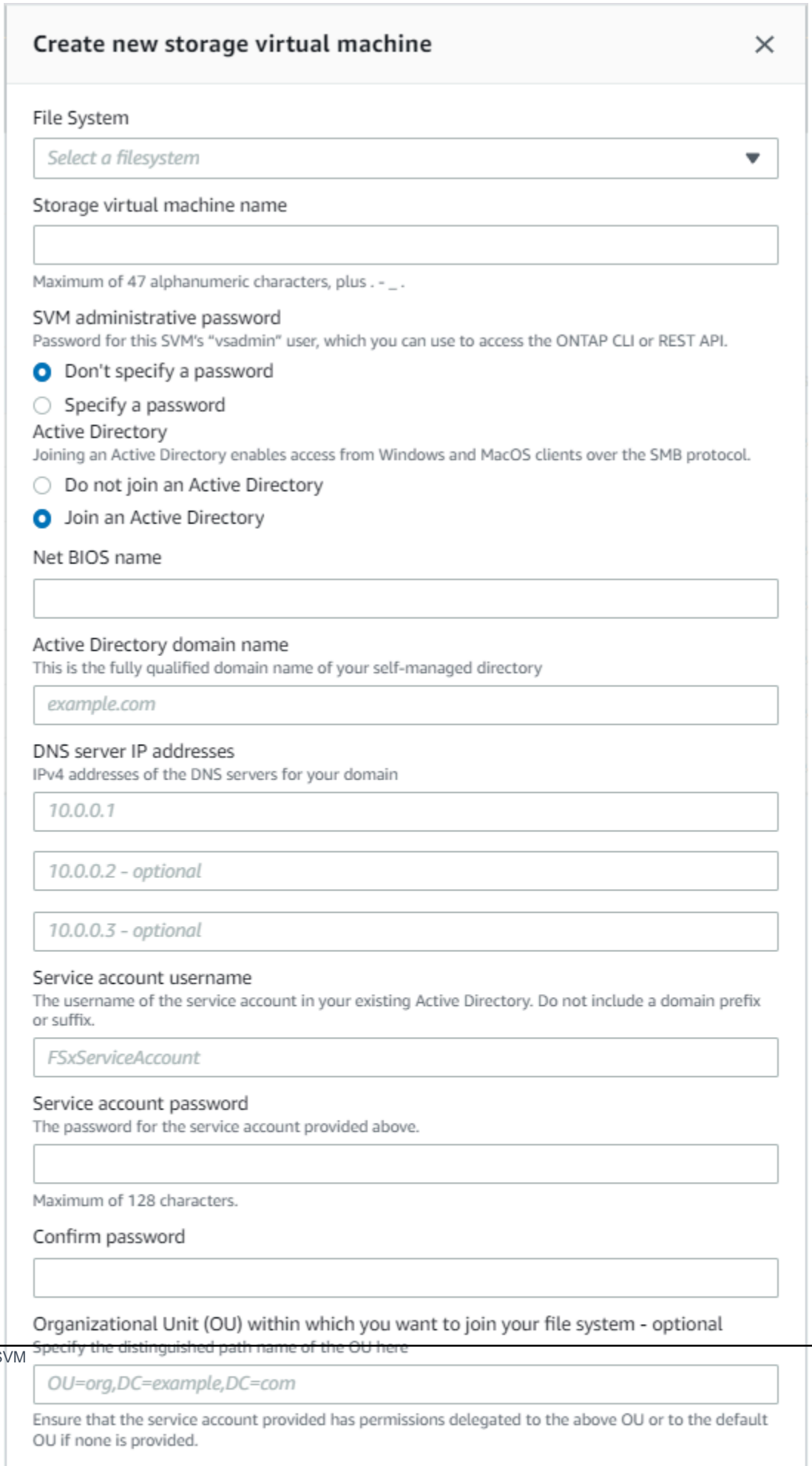
- SVM 所属的 FSx for ONTAP 文件系统。
- Microsoft Active Directory（AD）配置 – 您可以选择性将 SVM 加入自行管理的 AD，对 Windows 和 macOS 客户端进行身份验证和访问控制。有关更多信息，请参阅 在 FSx for ONTAP 中使用 Microsoft Active Directory。
- 根卷安全风格 – 设置根卷安全风格（Unix、NTFS 或 Mixed），与您在 SVM 中访问数据时使用的客户端类型保持一致。有关更多信息，请参阅 卷安全风格。

- 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 CLI 管理 SVM ONTAP。

创建存储虚拟机（控制台）

1. 通过以下网址打开 Amazon FSx 控制台：https://console.aws.amazon.com/fsx/。
2. 在左侧导航窗格中，选择存储虚拟机。
3. 选择创建新的存储虚拟机。

   系统会显示创建新的存储虚拟机对话框。


Create new storage virtual machine
File System
Select a filesystem
Storage virtual machine name
Maximum of 47 alphanumeric characters, plus . - _ .
SVM administrative password
Password for this SVM's "vsadmin" user, which you can use to access the ONTAP CLI or REST API.
Don't specify a password
Specify a password
Active Directory
Joining an Active Directory enables access from Windows and MacOS clients over the SMB protocol.
Do not join an Active Directory
Join an Active Directory
Net BIOS name
Active Directory domain name
This is the fully qualified domain name of your self-managed directory
example.com
DNS server IP addresses
IPv4 addresses of the DNS servers for your domain
10.0.0.1
10.0.0.2 - optional
10.0.0.3 - optional
Service account username
The username of the service account in your existing Active Directory. Do not include a domain prefix or suffix.
FSxServiceAccount
Service account password
The password for the service account provided above.
Maximum of 128 characters.
Confirm password
Organizational Unit (OU) within which you want to join your file system - optional
Specify the distinguished path name of the OU here
OU=org,DC=example,DC=com
Ensure that the service account provided has permissions delegated to the above OU or to the default OU if none is provided.

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 CLI 管理 SVM ONTAP。

   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 – 域的 DNS 服务器的 IPv4 地址。
     - 服务账户用户名 – 现有 Active Directory 中服务账户的用户名。请勿包含域前缀或后缀。对于 `EXAMPLE\ADMIN`，请使用 `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）组织单位（OU）– 文件系统要加入的组织单位的可分辨路径名称。
     - 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`。
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）

- 要为 ONTAP 存储虚拟机 (SVM) 创建 FSx，请使用 CL create-storage-virtual-machineI 命令（或等效的 CreateStorageVirtualMachineAPI 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
```

在成功创建存储虚拟机后，Amazon FSx 会以 JSON 格式返回存储虚拟机描述，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

您可以使用 Amazon FSx 控制台 AWS CLI和 Amazon FSx API 更新以下存储虚拟机 (SVM) 配置属性：

- 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 活动目录配置。

更新 SVM 管理员账户凭证（控制台）

1. 通过以下网址打开 Amazon FSx 控制台：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–

   - 要显示当前所有可用的 SVM 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）

- 要更新适用于 ONTAP SVM 的 FSx 的配置，请使用 CL update-storage-virtual-machineI 命令（或等效的 UpdateStorageVirtualMachineAPI 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 \
```

在成功创建存储虚拟机后，Amazon FSx 会以 JSON 格式返回存储虚拟机描述，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"
      }
    }
  }
}
```

删除存储虚拟机（SVM）

您只能使用亚马逊 FSx 控制台、和 API 删除适用于 ONTAP SVM 的 FSx。 AWS CLI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. 通过以下网址打开 Amazon FSx 控制台：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–

   - 要显示所有可用 SVM 的列表，请展开 ONTAP，然后选择存储虚拟机。

   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 ONTAP 存储虚拟机的 FSx，请使用 CL delete-storage-virtual-machineI 命令（或等效的 DeleteStorageVirtualMachineAPI 操作），如以下示例所示。

```
aws fsx delete-storage-virtual-machine --storage-virtual-machine-id svm-
abcdef0123456789d
```

查看存储虚拟机配置详细信息

您可以使用亚马逊 FSx 控制台、和 Amazon FSx API 查看文件系统上当前位于文件系统中的 FSx for ONTAP 存储虚拟机。 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。

  系统响应是您账户在 AWS 区域中所有 SVM 的一系列完整描述。

管理 FSx for ONTAP 卷

FSx for ONTAP 文件系统上的每个存储虚拟机（SVM）都可以有一个或多个卷。卷是用于文件、目录或 iSCSI 逻辑单元（LUN）的独立数据容器。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。

创建 iSCSI LUN（共享块存储）后，您可以通过网络文件系统（NFS）协议、服务器消息块（SMB）协议或 Internet 小型计算机系统接口（iSCSI）协议，从 Linux、Windows 或 macOS 客户端访问卷。FSx for ONTAP 还支持对同一卷进行多协议访问（NFS 和 SMB 并发访问）。

您可以使用 AWS Management Console、 AWS CLI、Amazon FSx API 或 NetApp BlueXP 来创建卷。您还可以使用 NetApp ONTAP CLI 或 REST API 使用文件系统或 SVM 的管理端点来创建、更新和删除卷。

> **Note**
>
> 每个 HA 对可以创建 500 个卷，在所有 HA 对中最多可以创建 1,000 个卷。 FlexGroup成分量计入此限制。默认情况下，每个聚合物有八个成分卷FlexGroup。

创建卷时，需要定义以下属性：

- 音量样式-音量样式可以是FlexVol或FlexGroup。
- 卷名-卷的名称。

- 卷类型 – 卷类型可以是“读写（RW）”或“数据保护（DP）”。DP 卷是只读的，在NetAppSnapMirror或SnapVault关系中用作目标。
- 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（包括数据压缩、压缩和重复数据删除）可为通用文件共享工作负载节省65%的存储空间。
- 卷安全风格（Unix、NTFS 或混合）-确定在授权用户时使用哪种权限访问卷上的数据。
- 数据分层 — 分层策略定义了哪些数据存储在经济实惠的容量池层中。
- 分层策略冷却期 — 定义何时将数据标记为冷却并移至容量池存储。
- 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策略中进行选择，也可以使用使用 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卷中的所有标签复制到备份中。您可以使用 AWS CLI 或 Amazon FSx API 来设置此选项。

主题

音量样式

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 Amazon FSx 控制台、和 Amazon FSx AWS CLI API 创建 FlexVol 或 FlexGroup 卷。

- FlexVol卷为具有一对高可用性 (HA) 的文件系统提供了最简单的体验，并且是向上扩展文件系统的默认卷风格。FlexVol卷的最小大小为 20 兆字节 (MiB)，最大大小为 314,572,800 MiB。
- FlexGroup卷由多个组成FlexVol卷组成，与具有多个 HA 对的文件系统的FlexVol卷相比，它们能够提供更高的性能和存储可扩展性。 FlexGroup卷是横向扩展文件系统的默认卷风格。FlexGroup卷的最小大小为每个成分 100 千兆字节 (GiB)，最大大小为 20 Pebibytes (PiB)。

您可以使用 ONTAP CLI 将带有该FlexVol样式的卷转换为FlexGroup样式，这会创建FlexGroup包含单一成分的。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成分。

> **Note**
>
> 如果要使用 ONTAP CLI 将FlexVol卷转换为FlexGroup卷，请确保在转换之前删除该FlexVol卷的所有备份。 ONTAP不会在转换过程中自动重新平衡数据，因此各成分之间的数据可能不平衡。FlexGroup

FlexGroup成分

体FlexGroup积由成分组成，即体FlexVol积。默认情况下，FSx for ONTAP 会为每个 HA FlexGroup 对的卷分配八个成分。

创建FlexGroup体积时，其大小将在其组成部分之间平均分配。例如，如果您创建一个包含八个成分的 800 千兆字节 (GB) FlexGroup 卷，则每个组成部分的大小为 100 GB。FlexGroup卷的大小可以介于 100 GB 到 20 PiB 之间，但总大小取决于各组成部分的大小。每个成分的最小大小为 100 GB，最大大小为 300 TiB。例如，包含八个成分的FlexGroup卷的最小大小为 800 GB，最大大小为 20 PiB。

ONTAP 在各组成部分之间以文件级别分发数据。在FlexGroup卷的每个组成部分中，您最多可以存储 20 亿个文件。

当您更新FlexGroup体积的大小时，新大小将在其现有成分中均匀分布。

您还可以使用 ONTAP CLI 或 REST API 向FlexGroup交易量添加更多成分。但是，我们建议您仅在需要额外的存储容量并且所有成分都已达到最大容量（每个成分 300 TiB）时才这样做。添加成分可能会导致各组成部分之间的数据和 I/O 不平衡。在各组成部分保持平衡之前，写入吞吐量可能比平衡FlexGroup卷低 5-10%。当向FlexGroup卷中写入新数据时，ONTAP 会优先将其分配给新成分，直到各组成部分保持平衡。如果您确实添加了新的成分股，我们建议您选择一个偶数，并且每个成分总数不超过八个。

> **Note**
>
> 如果您添加新的组成部分，则现有快照将成为部分快照；因此，它们不能用于将FlexGroup卷完全恢复到以前的状态。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，部分快照可用于恢复单个文件和目录、创建新卷或使用进行复制 SnapMirror。

卷类型

FSx for ONTAP 提供两种类型的卷，您可以使用亚马逊 FSx 控制台和亚马逊 FSx API 创建 AWS CLI 这些卷。

- 大多数情况下都使用读写 (RW) 卷。顾名思义，它们是可读写的。
- 数据保护 (DP) 卷是用作NetAppSnapMirror或SnapVault关系目标的只读卷。若要迁移或保护单个卷的数据，应使用 DP 卷。

FlexVol并且FlexGroup卷可以是 RW 或 DP。

> **Note**
>
> 创建卷后，您无法更新卷的类型。

卷安全风格

适用于 ONTAP 的 FSx 支持 3 种不同的卷安全风格：Unix、NTFS 和混合。每种安全方式对数据权限的处理方式都有不同的影响。您必须了解不同的影响，以确保根据自己的目的选择合适的安全风格。

重要的是要明白，安全风格并不能决定哪些客户端类型可以或不能访问数据。安全风格仅决定 FSx for ONTAP 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。

用于确定卷安全模式的两个因素是管理文件系统的管理员类型和访问卷上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模式位或 NFS v4.x ACL。
- 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 安全风格来修改权限，并且用于文件和目录的权限类型为 NTFS ACL。

- 混合 – 此为高级设置。有关更多信息，请参阅NetApp文档中心中的安全样式及其效果主题。

创建卷

除了 ONTAP 命令行界面 (CLI) 和 REST API 之外，您还可以使用 Amazon FSx 控制台、 AWS CLI Amazon FSx API 和 ONTAP NetApp 命令行界面 (CLI) 和 REST API 为 ONTAP FlexVol 或FlexGroup 卷创建 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. 通过以下网址打开 Amazon FSx 控制台：https://console.aws.amazon.com/fsx/。
2. 在左侧导航窗格中，选择卷。
3. 选择创建卷。
4. 对于文件系统类型，请选择适用于 ONTAP 的 Amazon FSx。 NetApp
5. 在文件系统详细信息部分，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 “音量风格” 部分中，选择FlexVol。
7. 在卷详细信息部分，提供以下信息：
   - 在卷名字段中，填入卷的名称。您最多可以使用 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 Read-Write (RW) 以创建可读写卷，或者选择数据保护 (DP) 以创建只读卷并可用作或关系的NetAppSnapMirror目标。SnapVault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 FSx for ONTAP 存储效率。

- 对于卷安全类型，请在 Unix (Linux)、NTFS 和混合卷之间进行选择。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，提供以下信息：

   - 对于容量池分层策略，请为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。
   - 如果您选择“自动”或“仅限快照”，则可以设置分层策略冷却期，以定义在未访问的数据被标记为冷却并移至容量池存储之前的天数。您可以提供介于 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，在“启用”和“禁用”之间进行选择。有关配置SnapLock合规卷或SnapLock企业卷的更多信息，请参阅创建 SnapLock Compliance 卷和创建 SnapLock Enterprise 卷。有关 SnapLock 的更多信息，请参阅使用以下方法保护您的数据 SnapLock。
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 控制台为横向扩展文件系统创建FlexGroup卷。要为横向扩展文件系统创建FlexVol卷，请使用 AWS CLI Amazon FSx API 或管理工具。 NetApp

1. 通过以下网址打开 Amazon FSx 控制台：https://console.aws.amazon.com/fsx/。
2. 在左侧导航窗格中，选择卷。
3. 选择创建卷。
4. 对于文件系统类型，请选择适用于 ONTAP 的 Amazon FSx。 NetApp
5. 在文件系统详细信息部分，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“音量风格”部分中，选择FlexGroup。
7. 在卷详细信息部分，提供以下信息：

   - 在卷名字段中，填入卷的名称。您最多可以使用 203 个字母数字或下划线 (_) 字符。
   - 对于卷大小，请输入 800 千兆字节 (GiB) 到 2,000 Pebibytes (PiB) 范围内的任意整数。
   - 对于卷类型，选择 Read-Write (RW) 以创建可读写卷，或者选择数据保护 (DP) 以创建只读卷并可用作或关系的NetAppSnapMirror目标。SnapVault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 FSx for ONTAP 存储效率。
   - 对于卷安全类型，请在 Unix (Linux)、NTFS 和混合卷之间进行选择。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，提供以下信息：

   - 对于容量池分层策略，请为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。
   - 如果您选择“自动”或“仅限快照”，则可以设置分层策略冷却期，以定义在未访问的数据被标记为冷却并移至容量池存储之前的天数。您可以提供介于 2-183 天之间的值。默认设置为 31 天。

9. 在“高级”部分的“SnapLock配置”中，在“启用”和“禁用”之间进行选择。有关配置SnapLock合规卷或SnapLock企业卷的更多信息，请参阅创建 SnapLock Compliance 卷和创建 SnapLock Enterprise 卷。有关 SnapLock 的更多信息，请参阅使用以下方法保护您的数据 SnapLock。
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）

- 要为 ONTAP 卷创建 FSx，请使用 create-volume CLI 命令（或等效CreateVolume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
```

在成功创建卷后，Amazon FSx 会以 JSON 格式返回该卷描述，如下例所示。

```
{
    "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"


    }
}
```

您也可以通过将卷的备份恢复到新卷来创建新卷。有关更多信息，请参阅 将备份恢复到新卷。

更新卷

除了 ONTAP NetApp 命令行界面 (CLI) 和 REST API 之外，您还可以使用 Amazon FSx 控制台、AWS CLI Amazon FSx API 更新适用于 ONTAP 卷的 FSx 配置。您可以修改现有 FSx for ONTAP 卷的以下属性：

- 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 for ONTAP 卷。

更新卷配置（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体积，最大大小为 300 TiB 乘以您FlexGroup拥有的组成体积总数，最大为 20 PiB。
8. 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），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。
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 ONTAP 卷的 FSx 配置，请使用更新卷 CLI 命令（或等效的 UpdateVolumeAP I 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
```

删除卷

除了 ONTAP 命令行界面 (CLI) 和 REST API 之外，您还可以使用 Amazon FSx 控制台、 AWS CLI Amazon FSx API、ONTAP NetApp 命令行界面 (CLI) 和 REST API 删除 ONTAP 卷的 FSx。

> **Important**
>
> 仅当卷启用了 Amazon FSx 备份时，您才能使用 Amazon FSx 控制台、API 或 CLI 删除该卷。

> **Important**
>
> 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。您可以从备份创建新卷。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。使用 CLI 命令 `delete-volume` 删除卷时，Amazon FSx 会默认进行最终备份。

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。

删除卷（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. 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。
7. 在 Confirm delete 字段中输入 delete 即可确认删除卷。
8. 选择删除卷。

删除卷（CLI）

- 要删除 ONTAP 卷的 FSx，请使用删除卷 CLI 命令（或等效的 DeleteVolumeAPI 操作），如以下示例所示。

```
aws fsx delete-volume --volume-id fsvol-1234567890abcde
```

查看卷

您可以使用亚马逊 FSx 控制台、Amazon FSx API 和软件开发工具包查看文件系统上当前位于文件系统中的 ONTAP 卷 AWS CLI的 FSx。

要查看文件系统上的卷，请如下操作：

- 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。

创建 iSCSI LUN

此过程介绍如何使用 ONTAP CLI 命令在 Amazon FSx for NetApp ONTAP 扩展文件系统上创建 iSCSI LUN。 NetApp lun create有关更多信息，请参阅 NetApp ONTAP 文档中心lun create中的。

> **Note**
>
> 横向扩展文件系统不支持 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 NetApp ONTAP CLI，请运行以下命令在 NetApp 适用于 ONTAP 的 Amazon FSx 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 CL lun create NetApp I 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，请参阅将 iSCSI LUN 挂载到 Linux 客户端或将 iSCSI LUN 挂载到 Windows 客户端。

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系统管理器与 BlueXP。

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。有关更多信息，请参阅 Amazon EC2 用户指南中的连接到您的 Windows 实例。
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。

文件访问审计

Amazon FSx for NetApp ONTAP 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

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
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
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）。	文件访问

事件 ID（EVT/EVTX）	事件	描述	类别
		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。	
N/A/4664	硬链接	OBJECT ACCESS：尝试创建硬链接	文件访问
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

事件 ID（EVT/EVTX）	事件	描述	类别
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。

    您可以选择以下操作之一：

    - 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 命令系列来配置 NTFS 审计策略。

例如，以下命令将名为 p1 的安全策略应用于名为 vs0 的 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。

扩展 SSD 存储容量和预调配 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 FSx for NetApp ONTAP 文件系统的固态硬盘 (SSD) 存储容量。您可以使用 Amazon FSx 控制台、Amazon FSx API 或 AWS Command Line Interface （ AWS CLI ）做到。

您还可以在增加主要 SSD 存储容量时更改文件系统的预调配 SSD IOPS，也可以作为独立操作进行更改。有关扩展文件系统主要 SSD 存储容量和预调配 IOPS 的更多信息，请参阅更新文件系统 SSD 存储空间和 IOPS。

管理吞吐能力

FSx for ONTAP 会在您创建文件系统时配置吞吐能力。您可以随时修改纵向扩展文件系统的吞吐容量，但不能修改横向扩展文件系统的吞吐容量。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，要为纵向扩展文件系统预置 4 Gbps 的吞吐容量，您的文件系统需要至少具有 5,120 GiB 固态硬盘存储容量和 160,000 个固态硬盘 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Performance：

当您修改文件系统的吞吐能力时，Amazon FSx 会关闭为文件系统提供支持的文件服务器。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 “维护时段”：

主题

何时修改吞吐能力

Amazon FSx 与亚马逊集成 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 “如何使用 FSx 获取 ONTAP 指标 CloudWatch”：

> **Note**
>
> 您无法修改横向扩展文件系统的吞吐容量。

如何处理并发吞吐量和存储扩展请求

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 会按照如下顺序处理上述两项请求：

- 如果您同时提交 SSD/IOPS 更新和吞吐能力更新，则服务器将接受两个请求。SSD/IOPS 更新的优先于吞吐能力更新。

- 如果您在 SSD/IOPS 更新过程中提交吞吐能力更新，服务器会接受吞吐能力更新请求，并将其加入队列，待 SSD/IOPS 更新之后进行。吞吐能力更新会在 SSD/IOPS 更新完成（有新值可用）之后的优化步骤中启动。这通常会在 10 分钟内完成。
- 如果您在吞吐能力更新过程中提交 SSD/IOPS 更新，服务器会接受 SSD/IOPS 存储更新请求，并将其加入队列，待吞吐能力更新完成（有新的吞吐能力可用）之后启动。这通常需要 20 分钟。

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。

如何修改吞吐能力

您可以使用 Amazon FSx 控制台、AWS Command Line Interface（AWS CLI）或 Amazon FSx API 修改文件系统的吞吐能力。

修改文件系统的吞吐能力（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。

> **Note**
>
> 您可以更改任何 FSx for ONTAP 文件系统的吞吐能力。但是，只有在 2021 年 12 月 9 日当天或之后创建的文件系统才支持 128 MB/s 或 256 MB/s 的吞吐能力。

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 Amazon FSx 控制台、AWS CLI 和 API 来监控更新进度。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 Amazon FSx 控制台、AWS CLI 和 API 来监控更新进度。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 AWS CLI 监控吞吐能力的修改进度。

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。
- 正在进行中 – 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。

通过 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。文件系统的吞吐能力为 128 MB/s，目标吞吐能力为 256 MB/s。

```
.
.
.
    "ThroughputCapacity": 128,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "PENDING",
        "TargetFileSystemValues": {
          "OntapConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

Amazon FSx 成功处理该操作后，状态将变为 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。

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。对于纵向扩展文件系统，从维护窗口开始算起，修补通常只需要30分钟。对于横向扩展文件系统，从维护时段开始算起，修补最多需要 90 分钟。在这几分钟时间内，文件系统会自动进行故障转移和故障自动恢复。您可以在创建文件系统期间选择维护时段。如果您没有时间偏好，则会分配 30 分钟的开始时间。

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地移动维护时段，前提是维护时段至少每 14 天出现一次。如果已发布补丁但未在 14 天内进入维护窗口，则 FSx for ONTAP 将继续维护文件系统，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 或其中一个 AWS 软件开发工具包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-systemCLI 命令更改每周维护时段，请参阅更新文件系统（CLI）。

标记 Amazon FSx 资源

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。本主题介绍标签并说明如何创建标签。

主题

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您的资源。
- 您可以修改标签的密钥和值，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 policy 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 policy 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 policy 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，请参阅使用备份。有关启用 CopyTagsToBackups 的更多信息，请参阅《Amazon FSx for NetApp ONTAP 用户指南》中的 创建卷（CLI） 和 更新卷配置（CLI），或者《Amazon FSx for NetApp ONTAP 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 policy 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。

使用应用程序管理 ONTAP 资源的 FSx NetApp

除了 AWS Management Console、、 AWS CLI、 AWS API 和软件开发工具包之外，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

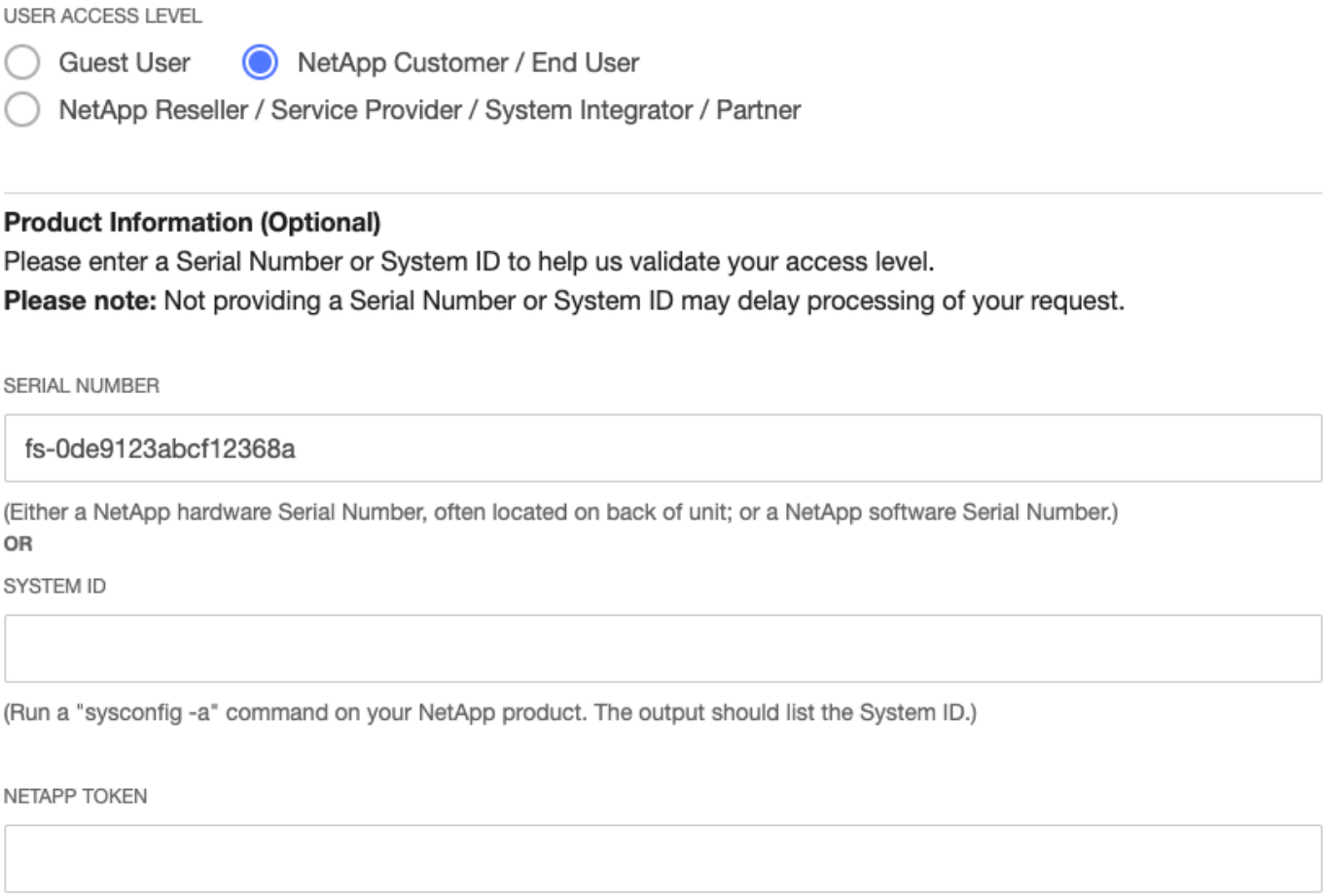
- 注册一个NetApp账号
- 使用 NetApp BlueXP
- 使用 NetApp ONTAP CLI
- 使用 ONTAP REST API

> **Important**
>
> 为了确保一致性，Amazon FSx 会定期ONTAP与同步。如果您使用NetApp应用程序创建或修改卷，则这些更改可能需要几分钟才能反映在 AWS Management Console、 AWS CLI、API 和 SDK 中。

注册一个NetApp账号

要下载某些NetApp软件（例如BlueXPSnapCenter、和ONTAP防病毒连接器），您需要拥有一个NetApp帐户。要注册NetApp账户，请执行以下步骤：

1. 前往NetApp用户注册页面并注册一个新的NetApp用户帐户。
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

拥有现有NetApp产品的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。除了NetApp将他们的 NSS 账户升级到客户级别访问权限外，还将使用标准业务惯例加入新客户。提供文件系统 ID 有助于加快此过程。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 BlueXP

NetApp BlueXP 是一个统一的控制平面，可简化本地和云环境中存储和数据服务的管理体验。BlueXP 提供了一个集中式用户界面，用于管理、监控和自动化 ONTAP 内部 AWS 和内部部署。有关更多信息，请参阅 NetApp BlueXP 文档和适用于 ONTAP 的 Amazon FSx 的 NetApp BlueXP 文档。 NetApp

> **Note**
>
> NetApp BlueXP不支持横向扩展文件系统。

将NetApp系统管理器与 BlueXP

您可以直接使用系统管理器管理适用于 NetApp ONTAP 文件系统的 Amazon FSx。BlueXP BlueXP允许您使用习惯使用的相同的 System Manager 界面，因此您可以从单个控制平面管理混合多云基础架构。您还可以访问 BlueXP 的其他功能。有关更多信息，请参阅 NetApp ONTAP 文档中的系统管理器与 BlueXP 的集成主题。

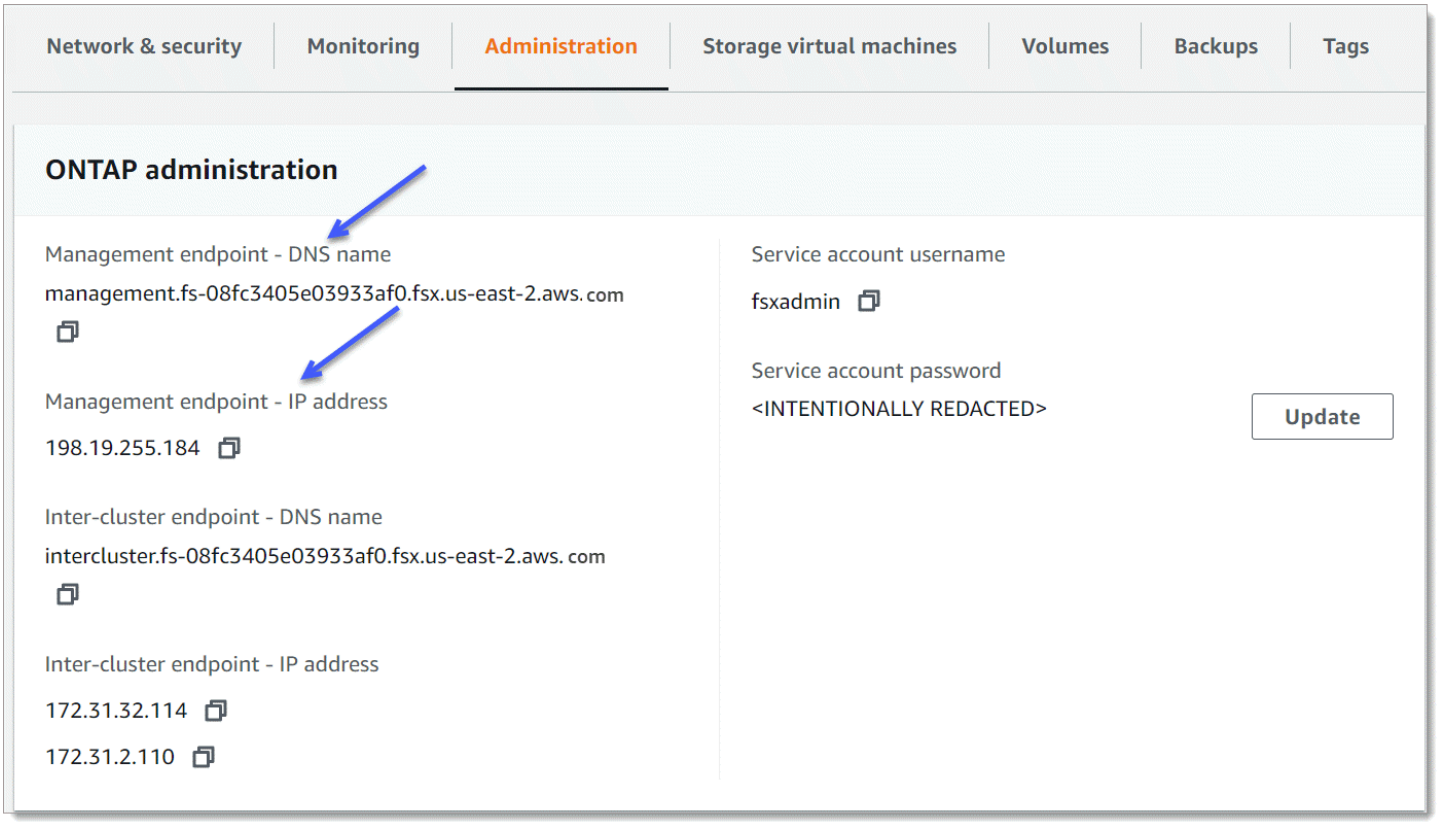
> **Note**
>
> NetApp 横向扩展文件系统不支持系统管理器。

使用 NetApp ONTAP CLI

您可以使用 CLI 管理适用于 NetApp ONTAP 的 Amazon FSx 资源。NetApp ONTAP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，类似于在集群上运行这些命令。NetApp ONTAP通过与文件系统的管理端点建立安全 shell (SSH) 连接，使用`fsxadmin`用户名和密码登录，即可访问文件系统上的 ONTAP CLI。使用自定义创建流程或使用创建文件系统时，您可以选择设置密码 AWS CLI。如果您使用快速创建选项创建了文件系统，则未设置`fsxadmin`密码，因此您需要设置一个密码才能登录 ONTAP CLI。有关更多信息，请参阅 更新文件系统。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管理终端节点的 DNS 名称和 IP 地址，如下图所示。



要通过 SSH 连接到文件系统的管理端点，请使用`fsxadmin`用户名和密码。您可以从与文件系统位于同一 VPC 中的客户端通过 SSH 访问文件系统的管理终端节点 IP 地址或 DNS 名称，如以下示例所示。

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

带有示例值的 SSH 命令：

```
ssh fsxadmin@198.51.100.0
```

使用管理端点 DNS 名称的 SSH 命令：

```
ssh fsxadmin@file-system-management-endpoint-dns-name
```

使用示例 DNS 名称的 SSH 命令：

```
$ ssh fsxadmin@management.fs-0abcdef123456789.fsx.us-east-2.aws.com
  Password: fsxadmin-password

This is your first recorded login.
```

```
FsxId0abcdef123456789::>
```

可用的 ONTAP CLI 命令范围 **fsxadmin**

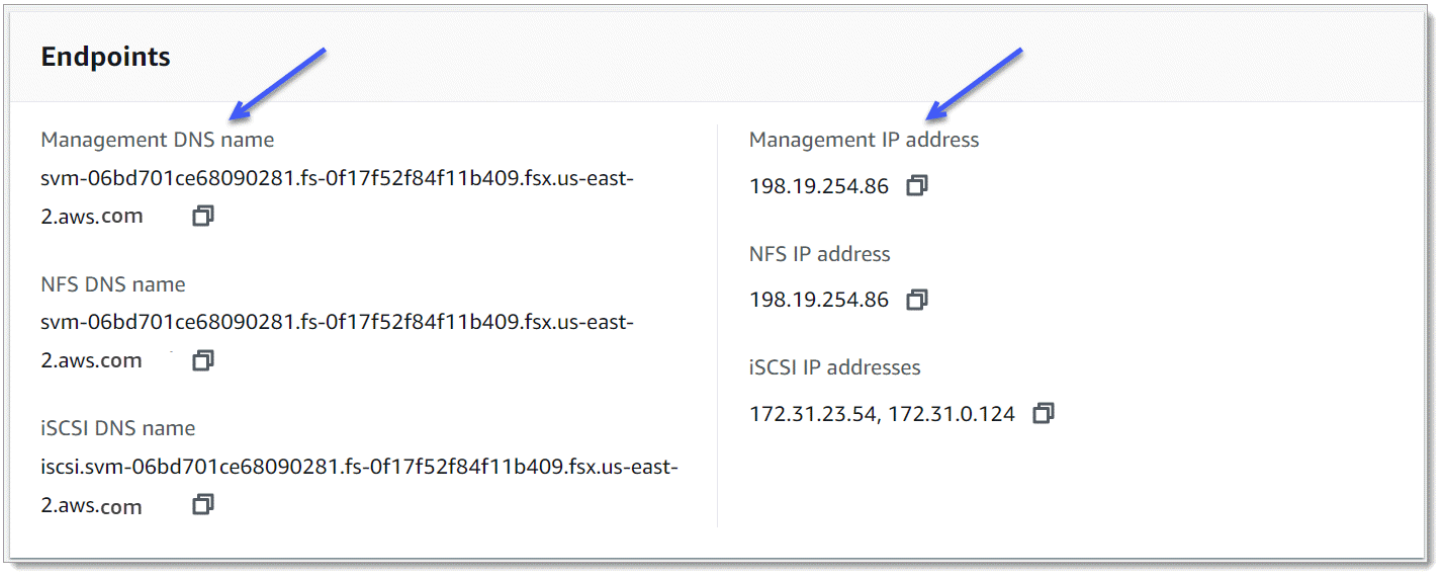
fsxadmin的管理视图位于文件系统级别，其中包括文件系统中的所有 SVM 和卷。该fsxadmin角色扮演ONTAP集群管理员的角色。由于适用于 NetApp ONTAP 文件系统的 Amazon FSx 是完全托管的，因此该fsxadmin角色可以运行一部分可用 CLI ONTAP 命令。

要查看fsxadmin可以运行的命令列表，请使用以下 security login role showONTAPCLI 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
.
.
.
363 entries were displayed.
```

使用 CLI 管理 SVM ONTAP

您可以使用fsxadmin或vsadmin用户名和密码与 SVM 的管理端点建立安全外壳 (SSH) 连接，从而访问 SVM 上的 ONTAP CLI。您可以在 Amazon FSx 控制台的存储虚拟机详细信息页面的终端节点面板中找到 SVM 的管理终端节点 DNS 名称和 IP 地址，如下图所示。



要通过 SSH 连接到 SVM 的管理端点，您可以使用vsadmin或fsxadmin用户名和密码。如果您在创建 SVM 时没有为vsadmin用户设置密码，则可以随时设置vsadmin密码。有关更多信息，请参阅 更新存储虚拟机。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 CLI 命令NetApp ONTAP。

有关 NetApp ONTAP CLI 命令的完整参考，请参阅 ONTAP 命令：手册页参考。

使用 ONTAP REST API

使用`fsxadmin`凭据使用 R ONTAP EST API 访问适用于 ONTAP 的 FSx 文件系统时，请执行以下操作之一：

- 禁用 TLS 验证。

  Or
- 信任 AWS 证书颁发机构 (CA)-可在以下 URL 中找到每个区域 CA 的证书包：
  - https://fsx-aws-certificates.s3.amazonaws.com/bundle-*aws-region .pem* for Public AWS 区域
  - https://fsx-aws-us-gov-certificates.s3.us-gov-west-1.amazonaws.com/bundle-适用于*### aw* s-region .pem AWS GovCloud
  - https://fsx-aws-cn-certificates.s3.cn-north-1.amazonaws.com.cn/bundle-*aws-region* .pem 适用于中国区域 AWS

有关 NetApp ONTAP REST API 命令的完整参考，请参阅 NetApp ONTAPREST API 在线参考。

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。作为AWS 合规计划合规计划合规计划合的一部分，第三方审计师定期测试和验证我们安全的有效性。要了解适用于 Amazon 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 分担责任模型分担责任模型适用于适用于 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设

施上的内容的控制。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。有关欧洲数据保护的信息，请参阅 AWS 安全性博客 上的 AWS 责任共担模式和 GDPR 博客文章。

出于数据保护目的，我们建议您保护 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。我们还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证 (MFA)。
- 使用 SSL/TLS 与资源通信。 AWS 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。
- 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 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-2 版》。

我们强烈建议您切勿将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网址，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

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 协议传输的基于 Kerberos 的加密。

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 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。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 AES-256 加密算法对静态 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。您可以选择用于加密和解密文件系统（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。
- 客户托管 KMS 密钥 – 这是使用最灵活的 KMS 密钥，因为您可以配置其密钥政策以及为多个用户或服务提供授权。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: K GenerateData ey* 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

本主题说明了在 FSx for ONTAP 文件系统和连接的客户端之间传输文件数据时，可用于对文件数据进行加密的不同选项。它还提供指导，帮助您选择最适合您的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基于 Nitro 的自动加密。

- 通过 NFS 和 SMB 协议进行基于 Kerberos 的加密。
- 通过 NFS、iSCSI 和 SMB 协议进行基于 IPsec 的加密

所有支持的传输中数据加密方法都使用行业标准的 AES-256 加密算法，提供企业级加密。

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。
- 如果你使用的是微软 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基于 Amazon Nitro 的加密。 AWS 区域 基于 Nitro 的加密在以下 AWS 区域提供：

- 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）

此外，基于 Nitro的加密可用于亚太地区（悉尼）的横向扩展文件系统。 AWS 区域

客户端实例类型

如果访问您文件系统的客户端在任何支持的 Amazon EC2 Mac、Linux 或 Windows 实例类型上运行，并且您的工作流程满足使用基于 Nitro 的加密的所有其他要求，则可以使用基于 Amazon Nitro 的加密。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，只要流量不会通过虚拟网络设备或服务（如传输网关），便也可以使用任何支持的加密方法。如果客户端不在同一或对等 VPC 中，或者流量通过虚拟网络设备或服务，则无法使用基于 Nitro 的加密。

网络性能

使用基于 Amazon Nitro 的加密技术对网络性能没有影响。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。

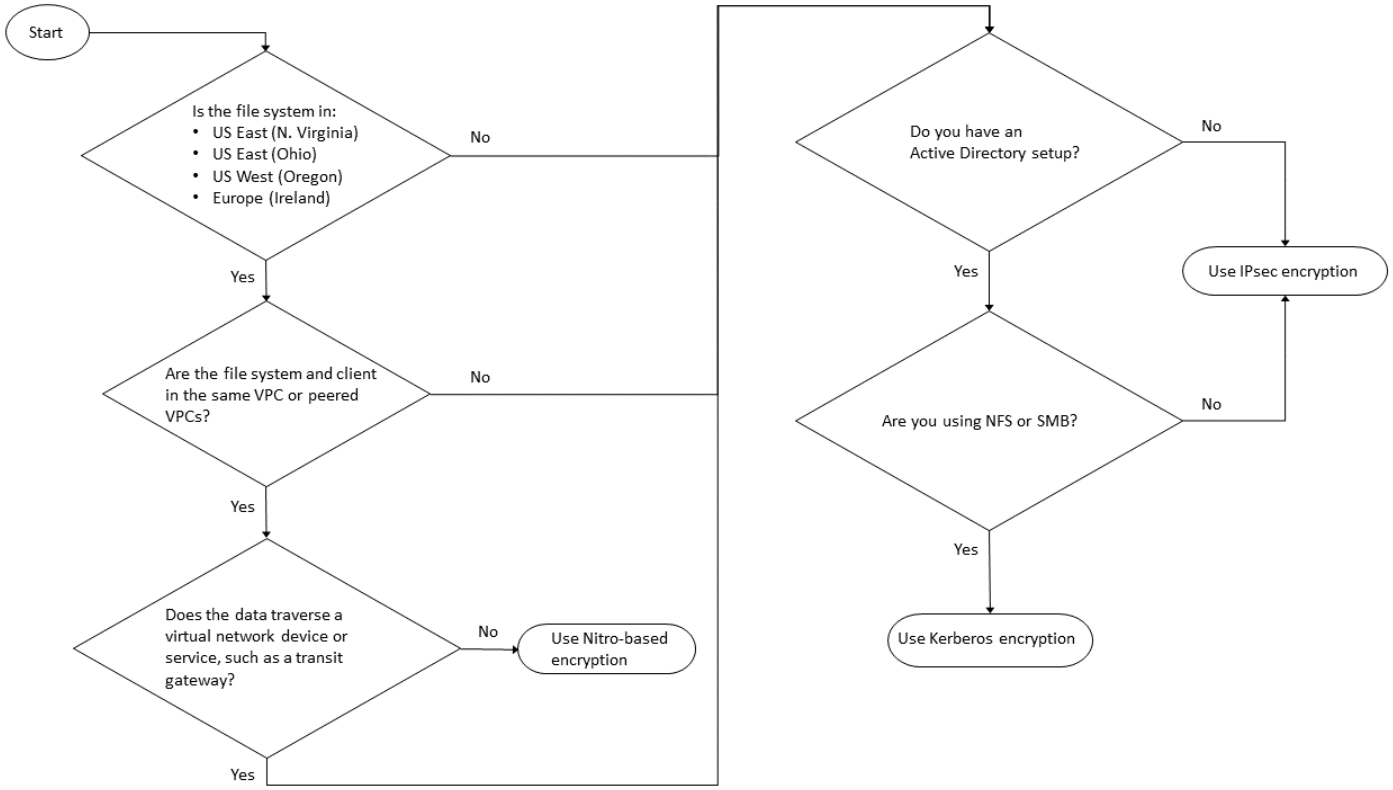
数据协议

您可以将基于 Amazon Nitro 的加密和 IPsec 加密与所有支持的协议（NFS、SMB 和 iSCSI）配合使用。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基于 Amazon Nitro 的加密。
- 您使用的不是 Microsoft Active Directory 域。

使用 AWS Nitro 系统对传输中的数据进行加密

如果使用基于 Nitro 的加密，当访问您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，传输中数据会自动加密。

使用基于 Amazon Nitro 的加密对网络性能没有影响。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。

当支持的客户端实例类型位于同一 AWS 区域 和同一 VPC 中或位于与文件系统的 VPC 对等的 VPC 中时，将自动启用基于 Nitro 的加密。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（如传输网关）以自动启用基于 Nitro 的加密。有关基于 Nitro 的加密的更多信息，请参阅《适用于 Linux 或 Windows 实例类型的 Amazon EC2 用户指南》中的传输中加密部分。

基于 Nitro 的传输中加密可用于 2022 年 11 月 28 日之后创建的文件系统，具体如下： AWS 区域

- 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）

此外，基于 Nitro的加密可用于亚太地区（悉尼）的横向扩展文件系统。 AWS 区域

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。

使用基于 Kerberos 的加密进行传输中数据加密

如果你使用的是 Act Microsoft ive Directory，则可以通过 NFS 和 SMB 协议使用基于 Kerberos 的加密来加密已加入 Microsoft Active Directory 的 SV M 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。这包括来自微软 Windows Server 2012 及更高Microsoft Windows版本以及微软 Windows 8 及更高版本的所有版本。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 CLI 管理 SVM ONTAP 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 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 为所有支持的 IP 流量（NFS、iSCSI 和 SMB 协议）为 ONTAP 文件系统的 FSx 之间传输的数据提供 end-to-end 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 基于 Nitro 的加密的客户端访问数据时，如果您的客户端和 SVM 未加入基于 Kerberos 的加密所必需的 Active Directory，我们建议您使用 IPsec 对通过 NFS、SMB 和 iSCSI 协议进行的传输中数据进行加密。如果 iSCSI 客户端不支持基于 Nitro 的加密，则 IPsec 加密是唯一可用于对 iSCSI 流量进行传输中数据加密的选项。

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 客户端必须支持带有 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 加密的高级步骤如下：

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 的更多信息，请参阅文档中心中的通过线路加密配置 IP 安全 (IPsec)。NetApp ONTAP

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 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 vserver cifs security modifyNetApp ONTAPCLI 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 vserver cifs security showNetApp ONTAPCLI 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 CLI 管理 SVM ONTAP 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

以下主题提供了在适用于 ONTAP 文件系统的 FSx 和运行 Libreswan IPsec 的客户端上使用证书身份验证配置 IPsec 加密的说明。此解决方案使用 AWS Certificate Manager 和 AWS Private Certificate Authority 来创建私有证书颁发机构并生成证书。

在 FSx 上为 ONTAP 文件系统和连接的客户端使用证书身份验证配置 IPsec 加密的高级步骤如下：

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 以实现多个客户端访问。

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 Private Certificate Authority 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 Private Certificate Authority，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 Private 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 Private Certificate Authority 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 Private Certificate Authority 用户指南》中的创建 CA 的步骤。
4. 使用 create-certificate-authority AWS Private 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 Private Certificate Authority 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。

```
$ cat exported_cert.json | jq -r .PrivateKey > prv.key

cat exported_cert.json | jq -r .Certificate > cert.pem
openssl rsa -in prv.key -passin pass:$passphrase -out decrypted.key
```

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。您
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 NetApp ONTAP CLI，请运行以下命令在 NetApp 适用于 ONTAP 的 Amazon FSx 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。
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 自签名根 CA），否则必须将双向身份验证期间使用的所有 CA 证书（包括 ONTAP 端和客户端 CA）安装到 ONTAP 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

要允许特定子网（例如 192.168.134.0/24）上的所有客户端使用单个 SPD 策略条目连接到单个 SVM IP 地址，必须以子网形式指定 `remote-ip-subnets`。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 NetApp ONTAP CLI，请运行以下命令在 NetApp 适用于 ONTAP 的 Amazon FSx 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. 按如下方式使用 `security ipsec policy create` NetApp ONTAP CLI 命令，将##值替换为您的具体值。

   ```
   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）连接到启用了 SVM IPsec 的 IP 地址，请在指定 `remote-ip-subnets` 字段时使用 `0.0.0.0/0` 通配符。

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`。

此外，使用 0.0.0.0/0 通配符时，必须配置要使用的特定本地或远程端口号。例如，NFS 端口 2049。

1. 要访问 NetApp ONTAP CLI，请运行以下命令在 NetApp 适用于 ONTAP 的 Amazon FSx 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. 按如下方式使用 `security ipsec policy create` NetApp ONTAP CLI 命令，将##值替换为您的具体值。

   ```
   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
- 使用身份进行身份验证
- 使用策略管理访问

- 适用于 NetApp ONTAP 的 Amazon FSx 如何与 IAM 配合使用
- 适用于 ONTAP 的 Amazon FSx 的基于身份的策略示例 NetApp
- 针对 NetApp ONTAP 身份和访问权限的 Amazon FSx 进行故障排除
- 在 Amazon FSx 上使用标签
- 使用 Amazon FSx 的服务相关角色

受众

您的使用方式 AWS Identity and Access Management (IAM) 会有所不同，具体取决于您在 Amazon FSx 中所做的工作。

服务用户 – 如果您使用 Amazon FSx 服务来完成任务，则您的管理员会为您提供所需的凭证和权限。随着您使用更多 Amazon FSx 功能来完成工作，您可能需要额外权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问 Amazon FSx 中的功能，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 – 如果您在公司负责管理 Amazon FSx 资源，您可能对 Amazon FSx 具有完全访问权限。您有责任确定您的服务用户应访问哪些 Amazon FSx 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要了解有关您的公司如何将 IAM 与 Amazon FSx 搭配使用的更多信息，请参阅 适用于 NetApp ONTAP 的 Amazon FSx 如何与 IAM 配合使用。

IAM 管理员 – 如果您是 IAM 管理员，您可能需要详细了解如何编写策略以管理对 Amazon FSx 的访问。要查看您可在 IAM 中使用的 Amazon FSx 基于身份的策略示例，请参阅适用于 ONTAP 的 Amazon FSx 的基于身份的策略示例 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 用户身份或通过担 AWS 账户根用户任 IAM 角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 AWS IAM Identity Center （ IAM Identity Center ）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。当您以联合身份登录时，您的管理员以前使用 IAM 角色设置了身份联合验证。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》中的如何登录到您 AWS 账户的。

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅 IAM 用户指南中的签署 AWS API 请求。

无论使用何种身份验证方法，您可能需要提供其他安全信息。例如， AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《AWS IAM Identity Center 用户指南》中的多重身份验证和《IAM 用户指南》中的在 AWS中使用多重身份验证（MFA）。

AWS 账户 root 用户

创建时 AWS 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 AWS 服务 和资源。此身份被称为 AWS 账户 root 用户，使用您创建账户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）使用与身份提供商的联合身份验证 AWS 服务 通过临时证书进行访问。

联合身份是指您的企业用户目录、Web 身份提供商、Identity C enter 目录中的用户，或者任何使用 AWS 服务 通过身份源提供的凭据进行访问的用户。 AWS Directory Service当联合身份访问时 AWS 账户，他们将扮演角色，角色提供临时证书。

要集中管理访问权限，建议您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中创建用户和群组，也可以连接并同步到您自己的身份源中的一组用户和群组，以便在您的所有 AWS 账户 和应用程序中使用。有关 IAM Identity Center 的信息，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

I AM 用户是您 AWS 账户 内部对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的使用场景定期轮换访问密钥。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅《IAM 用户指南》中的何时创建 IAM 用户（而不是角色）。

IAM 角色

I AM 角色是您内部具有特定权限 AWS 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。您可以 AWS Management Console 通过切换角色在中临时担任 IAM 角色。您可以通过调用 AWS CLI 或 AWS API 操作或使用自定义 URL 来代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的 使用 IAM 角色。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 联合用户访问 – 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色的信息，请参阅《IAM 用户指南》中的 为第三方身份提供商创建角色。如果您使用 IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的权限集。
- 临时 IAM 用户权限 – IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取 – 您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些资源 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅《IAM 用户指南》中的 IAM 角色与基于资源的策略有何不同。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 Amazon S3 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。
  - 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。
  - 服务相关角色-服务相关角色是一种与服务相关联的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 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相关角色的权限。

- 在 A@@ mazon EC2 上运行的应用程序 — 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时证书。这优先于在 EC2 实例中存储访问密钥。要向 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建附加到该实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅《IAM 用户指南》中的 使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限。

要了解是使用 IAM 角色还是 IAM 用户，请参阅《IAM 用户指南》中的何时创建 IAM 角色（而不是用户）。

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。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。 AWS 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的结构和内容的更多信息，请参阅《IAM 用户指南》中的 JSON 策略概览。

管理员可以使用 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。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

IAM 策略定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设您有一个允许 `iam:GetRole` 操作的策略。拥有该策略的用户可以从 AWS Management Console AWS CLI、或 AWS API 获取角色信息。

基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的创建 IAM 策略。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 AWS 账户。托管策略包括 AWS 托管策略和客户托管策略。要了解如何在托管式策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管式策略与内联策略之间进行选择。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Simple Storage Service（Amazon S3）存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用 IAM 中的 AWS 托管策略。

访问控制列表 (ACL)

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Amazon S3 和 Amazon VPC 就是支持 ACL 的服务示例。 AWS WAF要了解有关 ACL 的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》 中的访问控制列表（ACL）概览。

其他策略类型

AWS 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界 - 权限边界是一个高级功能，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅《IAM 用户指南》中的 IAM 实体的权限边界。
- 服务控制策略 (SCP)-SCP 是 JSON 策略，用于指定组织或组织单位 (OU) 的最大权限。 AWS Organizations AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果在组织内启用了所有功能，则可对任意或全部账户应用服务控制策略 (SCP)。SCP 限制成员账户中的实体（包括每个 AWS 账户根用户实体）的权限。有关 Organizations 和 SCP 的更多信息，请参阅《AWS Organizations 用户指南》中的 SCP 的工作原理。
- 会话策略 – 会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅《IAM 用户指南》中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 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
基于身份的策略	是
基于资源的策略	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
服务相关角色	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。

Amazon FSx 基于身份的策略

支持基于身份的策略	是

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅 IAM 用户指南中的创建 IAM 策略。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

Amazon FSx 基于身份的策略示例

要查看 Amazon FSx 基于身份的策略示例，请参阅 适用于 ONTAP 的 Amazon FSx 的基于身份的策略示例 NetApp 。

Amazon FSx 基于资源的策略

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。策略操作通常与关联的 AWS API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

要查看 Amazon FSx 操作的列表，请参阅《服务授权参考》中的 Amazon FSx for Lustre 定义的操作。

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 适用于 ONTAP 的 Amazon FSx 的基于身份的策略示例 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。语句必须包含 `Resource` 或 `NotResource` 元素。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符 (*) 指示语句应用于所有资源。

```
"Resource": "*"
```

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 适用于 ONTAP 的 Amazon FSx 的基于身份的策略示例 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。

在 Condition 元素（或 Condition 块）中，可以指定语句生效的条件。Condition 元素是可选的。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 AWS 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 AWS 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM 策略元素：变量和标签。

AWS 支持全局条件密钥和特定于服务的条件密钥。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 适用于 ONTAP 的 Amazon FSx 的基于身份的策略示例 NetApp 。

Amazon FSx 中的访问控制列表（ACL）

支持 ACL	否

Amazon FSx 基于属性的访问权限控制（ABAC）

支持 ABAC（策略中的标签）	是

基于属性的访问控制（ABAC）是一种授权策略，该策略基于属性来定义权限。在中 AWS，这些属性称为标签。您可以向 IAM 实体（用户或角色）和许多 AWS 资源附加标签。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

要基于标签控制访问，您需要使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件键在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为部分。

有关 ABAC 的更多信息,请参阅《IAM 用户指南》中的什么是 ABAC？。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，请参阅标记 Amazon FSx 资源。

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

当你使用临时证书登录时，有些 AWS 服务 不起作用。有关更多信息，包括哪些 AWS 服务 适用于临时证书，请参阅 IAM 用户指南中的AWS 服务 与 IA M 配合使用的信息。

如果您使用除用户名和密码之外的任何方法登录，则 AWS Management Console 使用的是临时证书。例如，当您 AWS 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的 切换到角色（控制台）。

您可以使用 AWS CLI 或 AWS API 手动创建临时证书。然后，您可以使用这些临时证书进行访问 AWS。 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 中的临时安全凭证。

亚马逊 FSx 的转发访问会话

支持转发访问会话 (FAS)	是

当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

Amazon FSx 的服务角色

支持服务角色	否

Amazon FSx 的服务相关角色

支持服务相关角色	是

服务相关角色是一种链接到的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 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相关角色的权限。

有关创建或管理 Amazon FSx 服务相关角色的详细信息，请参阅 使用 Amazon FSx 的服务相关角色。

适用于 ONTAP 的 Amazon FSx 的基于身份的策略示例 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。他们也无法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 执行任务。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅《IAM 用户指南》中的创建 IAM policy。

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

基于身份的策略确定某个人是否可以创建、访问或删除您账户中的 Amazon 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，请遵循以下准则和建议：

- 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 AWS 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 IAM Acess Analyzer 策略验证。
- 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 配置受 MFA 保护的 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实操。

使用 Amazon 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 亚马逊 FSx 的托管策略中查看 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访问我 AWS 账户 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，表明您无权执行某个操作，则您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访问我 AWS 账户 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，可以担任角色。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 角色与基于资源的策略有何不同。

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它们应用标签。

```
{
  "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，请参阅标记 Amazon FSx 资源。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 policy。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，请参阅标记 Amazon FSx 资源。

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。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource",
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id: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。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateVolumeFromBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateVolumeFromBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id: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。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteFileSystem"
            ],
            "Resource": "arn:aws:fsx:region:account-id:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id: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。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteVolume"
            ],
```

```
            "Resource": "arn:aws:fsx:region:account-id:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

使用 Amazon FSx 的服务相关角色

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类型的 IAM 角色，与 Amazon FSx 直接相关。服务相关角色由 Amazon FSx 预定义，包括该服务代表您调用 AWS 其他服务所需的所有权限。

服务相关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 定义其服务相关角色的权限，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，您才能删除服务相关角色。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他服务的信息，请参阅使用 IAM 的AWS 服务并查找服务相关角色列中显示为是的服务。选择是，可转到查看该服务的服务相关角色文档的链接。

Amazon FSx 的服务相关角色权限

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

有关本政策的更新，请参阅 AmazonF SxService RolePolicy

权限详细信息

权限详细信息

AWSServiceRoleForAmazonFSx 角色权限由 AmazonF SxService RolePolicy 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 FSx for ONTAP。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。 AWS 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。
  - 为可用于 VPC 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。
- logs— 允许 Amazon FSx 描述日志流并写入 CloudWatch 日志流。这样，用户就可以将 FSx for Windows File Server 文件系统的文件访问审核日志发送到日志 CloudWatch 流。
- firehose— 允许 Amazon FSx 描述和写入亚马逊 Data Firehose 传送流。这样，用户就可以将适用于 Windows 文件服务器的 Amazon FSx 文件系统的文件访问审核日志发布到亚马逊数据 Firehose 传输流。

```
{
    "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"
                }
            }
        },
        {
```

```
            "Sid": "PutCloudWatchLogs",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/fsx/*"
        },
        {
            "Sid": "ManageAuditLogs",
            "Effect": "Allow",
            "Action": [
                "firehose:DescribeDeliveryStream",
                "firehose:PutRecord",
                "firehose:PutRecordBatch"
            ],
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
        }
    ]
}
```

亚马逊 FSx 更新了托管政策 AWS 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、编辑或删除服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的服务相关角色权限。

为 Amazon FSx 创建服务相关角色

您无需手动创建服务相关角色。当您在 AWS Management Console、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，此服务相关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。

如果您删除该服务相关角色，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相关角色。

为 Amazon FSx 编辑服务相关角色

Amazon FSx 不允许您编辑 AWSServiceRoleForAmazonFSx 服务相关角色。创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。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》中的编辑服务相关角色。

删除 Amazon FSx 的服务相关角色

如果不再需要使用某个需要服务相关角色的功能或服务，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相关角色。

> **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 手动删除服务相关角色

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》中的删除服务相关角色。

Amazon FSx 服务相关角色支持的区域

Amazon FSx 支持在该服务可用的所有区域中使用服务相关角色。有关更多信息，请参阅 AWS 区域和端点。

AWS 亚马逊 FSx 的托管策略

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您的使用场景的客户管理型策略来进一步减少权限。

您无法更改 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。

AmazonF SxService RolePolicy

允许 Amazon FSx 代表您管理 AWS 资源。请参阅使用 Amazon FSx 的服务相关角色，了解更多信息。

AWS 托管策略：亚马逊 SxDelete ServiceLinked RoleAccess

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相关角色。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 的服务相关角色。

该策略授予管理权限，允许 Amazon FSx 删除用于访问 Amazon S3 的服务相关角色，仅供 Amazon FSx for Lustre 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 服务相关角色进行查看、删除及查看其删除状态。

要查看此策略的权限，请参阅《 AWS 托管策略参考指南》SxDeleteServiceLinkedRoleAccess中的 AmazonF。

AWS 托管策略：AmazonF 访问权限 SxFull

您可以将 AmazonF 附加SxFullAccess 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 AWS Directory Service 目录的信息。
- ec2

  - 允许委托人在指定条件下创建标签。
  - 为可用于 VPC 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 服务相关角色。这是必需的，这样 Amazon FSx 才能代表用户管理 AWS 资源。
- `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。
- `firehose`— 允许委托人向 Amazon Data Firehose 写入记录。这是必需的，这样用户才能通过向 Firehose 发送审核访问日志来监控 FSx 的 Windows 文件服务器文件系统访问权限。

要查看此策略的权限，请参阅《 AWS 托管策略参考指南》中的 AmazonF A SxFull c cess。

AWS 托管策略：亚马逊 SxConsole FullAccess

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 Management Console

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 AWS Directory Service 目录的信息。
- `ec2`
  - 允许委托人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。
  - 允许委托人对可用于 VPC 的所有安全组提供增强的安全组验证。
- `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）。
- `iam` – 授予创建服务相关角色的权限，允许 Amazon FSx 代表用户执行操作。

要查看此策略的权限，请参阅《 AWS 托管策略参考指南》SxConsoleFullAccess中的 AmazonF。

AWS 托管策略：AmazonF 访问权限 SxConsole ReadOnly

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 Management Console

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 AWS Directory Service 管理控制台中查看有关目录的信息。
- ec2
  - 允许委托人在 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。
  - 为可用于 VPC 的所有安全组提供增强的安全组验证。
- 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。
- firehose— 允许委托人描述与提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《 AWS 托管策略参考指南》中的 AmazonF A SxConsole ReadOnly c cess。

AWS 托管策略：亚马逊 SxRead OnlyAccess

您可以将 AmazonFSxReadOnlyAccess 策略附加到 IAM 身份。

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。

- ec2— 为可用于 VPC 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《 AWS 托管策略参考指南》SxReadOnlyAccess中的 AmazonF。

亚马逊 FSx 更新了托管政策 AWS

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
亚马逊 SxService RolePolicy-对现有政策的更新	Amazon FSx 增加了新权限ec2:GetSecurityGroupsForVpc ，允许委托人对可用于 VPC 的所有安全组提供增强的安全组验证。	2024 年 1 月 9 日
亚马逊 SxRead OnlyAccess-对现有政策的更新	Amazon FSx 增加了新权限ec2:GetSecurityGroupsForVpc ，允许委托人对可用于 VPC 的所有安全组提供增强的安全组验证。	2024 年 1 月 9 日
AmazonF SxConsole ReadOnly 访问权限-更新现有政策	Amazon FSx 增加了新权限ec2:GetSecurityGroupsForVpc ，允许委托人对可用于 VPC 的所有安全组提供增强的安全组验证。	2024 年 1 月 9 日
AmazonF SxFull 访问权限-更新现有政策	Amazon FSx 增加了新权限ec2:GetSecurityGroupsForVpc ，允许委托人对可用于 VPC 的所有安全组提供增强的安全组验证。	2024 年 1 月 9 日
亚马逊 SxConsole FullAccess-对现有政策的更新	Amazon FSx 增加了新权限ec2:GetSecurityGro	2024 年 1 月 9 日

更改	描述	日期
	upsForVpc ，允许委托人对可用于 VPC 的所有安全组提供增强的安全组验证。	
AmazonF SxFull 访问权限-更新现有政策	Amazon FSX 增加了新的权限，使用户能够为 OpenZFS 文件系统的 FSX 执行跨区域和跨账户数据复制。	2023 年 12 月 20 日
亚马逊 SxConsole FullAccess-对现有政策的更新	Amazon FSX 增加了新的权限，使用户能够为 OpenZFS 文件系统的 FSX 执行跨区域和跨账户数据复制。	2023 年 12 月 20 日
AmazonF SxFull 访问权限-更新现有政策	Amazon FSX 添加了一项新权限，允许用户按需复制适用于 OpenZFS 文件系统的 FSX 卷。	2023 年 11 月 26 日
亚马逊 SxConsole FullAccess-对现有政策的更新	Amazon FSX 添加了一项新权限，允许用户按需复制适用于 OpenZFS 文件系统的 FSX 卷。	2023 年 11 月 26 日
AmazonF SxFull 访问权限-更新现有政策	Amazon FSx 添加了新的权限，使用户能够查看、启用和禁用对适用于 ONTAP 多可用区文件系统的 FSx 的共享 VPC 支持。	2023 年 11 月 14 日
亚马逊 SxConsole FullAccess-对现有政策的更新	Amazon FSx 添加了新的权限，使用户能够查看、启用和禁用对适用于 ONTAP 多可用区文件系统的 FSx 的共享 VPC 支持。	2023 年 11 月 14 日

更改	描述	日期
AmazonF SxFull 访问权限-更新现有政策	Amazon FSx 增加了新的权限，允许 Amazon FSx 管理 FSx for OpenZFS 多可用区文件系统的网络配置。	2023 年 8 月 9 日
AWS 托管策略：AmazonF SxService RolePolicy — 更新现有政策	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
AmazonF SxFull 访问权限-更新现有政策	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
亚马逊 SxConsole FullAccess-对现有政策的更新	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
AmazonF SxConsole ReadOnly 访问权限-更新现有政策	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
亚马逊 SxConsole FullAccess-对现有政策的更新	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
亚马逊 SxRead OnlyAccess — 已开始执行追踪政策	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

更改	描述	日期
亚马逊 SxDelete ServiceLinked RoleAccess — 已开始执行追踪政策	此策略授予管理权限，允许 Amazon FSx 删除用于访问 Amazon S3 的服务相关角色。	2022 年 1 月 7 日
亚马逊 SxService RolePolicy-对现有政策的更新	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
AmazonF SxFull 访问权限-更新现有政策	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
亚马逊 SxConsole FullAccess-对现有政策的更新	亚马逊 FSx 添加了新的权限，允许亚马逊 FSx 为 ONTAP 多可用区文件系统创建亚马逊 FSX。 NetApp	2021 年 9 月 2 日
亚马逊 SxConsole FullAccess-对现有政策的更新	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
亚马逊 SxService RolePolicy-对现有政策的更新	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
亚马逊 SxService RolePolicy-对现有政策的更新	亚马逊 FSx 增加了新的权限，允许亚马逊 FSx 描述和写入亚马逊数据 Firehose 传输流。 这是必需的，这样用户才能使用 Amazon Data Firehose 查看 FSx for Windows File Server 文件系统的文件访问审核日志。	2021 年 6 月 8 日
AmazonF SxFull 访问权限-更新现有政策	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
AmazonF SxFull 访问权限-更新现有政策	亚马逊 FSx 增加了新的权限，允许委托人向亚马逊数据 Firehose 描述和写入记录。 这是必需的，这样用户才能使用 Amazon Data Firehose 查看 FSx for Windows File Server 文件系统的文件访问审核日志。	2021 年 6 月 8 日

更改	描述	日期
亚马逊 SxConsole FullAccess-对现有政策的更新	Amazon FSx 添加了新的权限，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
亚马逊 SxConsole FullAccess — 更新现有政策	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 Data Firehose 传送流。 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 Firehose 传送流。	2021 年 6 月 8 日
AmazonF SxConsole ReadOnly 访问权限-更新现有政策	Amazon FSx 添加了新的权限，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
AmazonF SxConsole ReadOnly 访问权限-更新现有政策	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 Data Firehose 传送流。 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 AWS 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 Amazon EC2 控制台，网址为 https://console.aws.amazon.com/ec2。
2. 在导航窗格中，选择安全组。
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 NFS、SMB 或 iSCSI 访问文件系统中数据的 Linux、Windows 和/或 macOS 客户端。
   - 您将与您的文件系统对等的任何 ONTAP 文件系统/集群（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、Connector 或 BlueXP）。 NetApp NetApp

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	通过 TCP 和 NetBIOS 帧进行的 Microsoft SMB/CIFS
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，可以删除与文件系统的弹性网络接口关联的所有安全组，并将其替换为没有入站/出站规则的组。

适用于 ONTAP 的亚马逊 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。 AWS 提供了以下资源来帮助实现合规性：

- 安全与合规性快速入门指南 — 这些部署指南讨论了架构注意事项，并提供了在这些基础上 AWS 部署以安全性和合规性为重点的基准环境的步骤。
- 在 A@@ mazon Web Services 上构建 HIPAA 安全与合规架构 — 本白皮书描述了各公司如何使用 AWS 来创建符合 HIPAA 资格的应用程序。

> **Note**
>
> 并非所有 AWS 服务 人都符合 HIPAA 资格。有关更多信息，请参阅符合 HIPAA 要求的服务参考。

- AWS 合规资源AWS — 此工作簿和指南集可能适用于您所在的行业和所在地区。

- AWS 客户合规指南 — 从合规角度了解责任共担模式。这些指南总结了保护的最佳实践， AWS 服务并将指南映射到跨多个框架（包括美国国家标准与技术研究院 (NIST)、支付卡行业安全标准委员会 (PCI) 和国际标准化组织 (ISO)）的安全控制。
- 使用AWS Config 开发人员指南中的规则评估资源 — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- AWS Security Hub— 这 AWS 服务 提供了您内部安全状态的全面视图 AWS。Security Hub 通过安全控件评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控件的列表，请参阅 Security Hub 控件参考。
- Amazon GuardDuty — 它通过监控您的 AWS 账户环境中是否存在可疑和恶意活动，来 AWS 服务检测您的工作负载、容器和数据面临的潜在威胁。 GuardDuty 通过满足某些合规性框架规定的入侵检测要求，可以帮助您满足各种合规性要求，例如 PCI DSS。
- AWS Audit Manager— 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

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，该技术使您无需互联网网关AWS PrivateLink、NAT 设备、VPN 连接或 AWS 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 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，例如 AWS 区域，使用其默认 DNS 名称。`fsx.us-east-1.amazonaws.com`对于中国（北京）和中国（宁夏） AWS 区域，您可以分别使用`fsx-api.cn-north-1.amazonaws.com.cn`和`fsx-api.cn-northwest-1.amazonaws.com.cn`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 提供多个物理分隔和隔离的可用区，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、容错性和可扩展性。

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。

备份与还原

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 使用备份。

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 快照的使用。

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。

多可用区文件系统

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 可用性与持久性。

单可用区文件系统

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 可用性与持久性。

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（临时 Diffie-Hellman）或 ECDHE（临时椭圆曲线 Diffie-Hellman）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service（AWS STS）生成临时安全凭证来对请求进行签名。

使用带有 FSx 的 NetApp ONTAP vScan for ONTAP

您可以使用 NetApp ONTAP 的 Vscan 功能来运行支持的第三方防病毒软件。有关更多信息，请参阅以下资源，了解各种支持的解决方案。

- McAfee — 集群模式 Data 防病毒解决方案指南 ONTA P： McAfee
- SentinelOne — Vscan 合作伙伴解决方案和 S SentinelOne ingularity Cloud 数据安全
- 赛门铁克 — Vscan 合作伙伴解决方案和赛门铁克保护引擎
- Trend Micro – Antivirus Solution Guide for Clustered Data ONTAP: Trend Micro

适用于 ONTAP 的 Amazon FSx 中的角色和用户 NetApp

NetApp ONTAP包括强大且可扩展的基于角色的访问控制 (RBAC) 功能。 ONTAP角色定义了使用 CLI 和 REST AP ONTAP I 时的用户能力和权限。每个角色定义不同的管理权能和权限级别。您可以为用户分配角色，以便在使用 R ONTAP EST API 和 CLI 时控制他们对 FSx for ONTAP 资源的访问权限。ONTAP 文件系统用户和存储虚拟机 (SVM) 用户分别有 FSx 可用的ONTAP角色。

在为 ONTAP 文件系统创建 FSx 时，将在文件系统级别和 SVM 级别创建默认ONTAP用户。您可以创建其他文件系统和 SVM 用户，也可以创建其他 SVM 角色以满足组织的需求。本章介绍ONTAP用户和角色，并提供创建其他用户和 SVM 角色的详细过程。

文件系统管理员角色和用户

默认ONTAP文件系统用户是`fsxadmin`，已为其分配了`fsxadmin`角色。您可以为文件系统用户分配两个预定义的角色，如下所示：

- **`fsxadmin`**—具有此角色的管理员在系统中拥有不受限制的ONTAP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 级资源。
- **`fsxadmin-readonly`**—具有此角色的管理员可以在文件系统级别查看所有内容，但不能进行任何更改。

  此角色非常适合与监视应用程序一起使用，例如NetApp Harvest因为它对所有可用资源及其属性具有只读访问权限，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他们分配`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 为文件系统和 SVM 管理创建新ONTAP用户。

下表描述了文件系统管理员角色对 ONTAP CLI 和 REST API 命令和命令目录的访问级别。

角色名称	访问级别	到以下命令或命令目录
`fsxadmin`	all	适用于 ONTAP 的 FSx 中所有可用的命令目录
`fsxadmin-readonly`	all	`security login password` 仅用于管理自己的用户帐户、本地密码和密钥信息

角色名称	访问级别	到以下命令或命令目录
	none	security
	只读	适用于 ONTAP 的 FSx 中可用的所有其他命令目录

SVM 管理员角色和用户

每个 SVM 都有一个单独的身份验证域，可以由自己的管理员独立管理。对于文件系统上的每个 SVM，默认用户是 vsadmin，默认情况下会为其分配vsadmin角色。除角色外，还有其他预定义的 SVM 角色，这些角色提供限定范围的权限，您可以将这些权限分配给 SVM 用户。vsadmin您还可以创建自定义角色，以提供满足组织需求的访问控制级别。

SVM 管理员的预定义角色及其权限如下：

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 • 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

角色名称	功能
	• 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 • 对恢复的卷进行读/写 • 管理 SnapMirror 关系和快照副本 • 查看卷和网络信息
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，请参阅创建新的 SVM 角色。

使用活动目录对ONTAP用户进行身份验证

你可以对 Windows Active Directory 域用户访问适用于 ONTAP 文件系统和 SVM 的 FSx 进行身份验证。在 Active Directory 账户可以访问您的文件系统之前，您必须完成以下任务：

- 您需要配置 Active Directory 域控制器对 SVM 的访问权限。

  用于配置为 Active Directory 域控制器访问的网关或隧道的 SVM 必须启用 CIFS、加入活动目录，或者两者兼而有之。如果您没有启用 CIFS，而只是将隧道 SVM 加入活动目录，请确保 SVM 已加入您的活动目录。有关更多信息，请参阅 将 SVM 加入 Microsoft Active Directory。
- 您需要启用 Active Directory 域用户帐户才能访问文件系统。

  对于访问 CLI 或 REST AP ONTAP I 的 Windows 域用户，你可以使用密码身份验证或 SSH 公钥身份验证。

有关描述如何用于为文件系统和 SVM 管理员配置 Active Directory 身份验证的过程，请参阅为ONTAP用户配置活动目录身份验证。

为文件系统和 SVM 管理创建新ONTAP用户

每个ONTAP用户都与 SVM 或文件系统相关联。具有该`fsxadmin`角色的文件系统用户可以使用`security login create`ONTAPCLI 命令创建新的 SVM 角色和用户。

该`security login create`命令为管理实用程序创建登录方法。登录方法由用户名、应用程序（访问方法）和身份验证方法组成。一个用户名可以与多个应用程序关联。它可以选择包含访问控制角色名称。如果使用 Active Directory、LDAP 或 NIS 组名，则登录方法允许属于指定组的用户访问权限。如果用户是安全登录表中配置的多个组的成员，则该用户将可以访问为各个组授权的命令的组合列表。

有关如何创建新ONTAP用户的信息，请参阅创建新的 ONTAP 用户。

主题

- 创建新的 ONTAP 用户
- 创建新的 SVM 角色
- 为ONTAP用户配置活动目录身份验证
- 配置公钥认证
- 更新文件系统和 SVM 角色的密码要求

- 更新fsxadmin账户密码失败

创建新的 ONTAP 用户

创建新的 SVM 或文件系统用户 (ONTAPCLI)

只有具有该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 NetApp ONTAP CLI，请运行以下命令在 NetApp 适用于 ONTAP 的 Amazon FSx 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 `security login create` ONTAP CLI 命令在 FSx 上为 ONTAP 文件系统或 SVM 创建一个新的用户帐户。

   为示例中的占位符插入数据，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。如果您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身份验证方法和和ssh应用程序指定 Active Directory 组名。ontapi
   - `-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：
     - 域-用于活动目录身份验证
     - 密码-用于密码认证
     - publickey — 用于公钥身份验证的用户
   - `-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）您还可以在命令中使用以下一个或多个参数：

   - `[-comment]`— 用于为用户帐户添加注释或注释。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 — 用于公钥身份验证
  - nswitch — 用于 NIS 或 LDAP 身份验证
  - none — 如果未指定，则为默认值

```
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
```

以下命令使用new_fsxadmin带有密码的 SSH 创建具有分配fsxadmin-readonly角色的新文件系统用户。出现提示时，请为用户提供密码。

```
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 new_vsadmin 上创建具有该vsadmin_readonly角色的新 fsx SVM 用户，该用户配置为使用带有密码的 SSH 进行登录。出现提示时，请为用户提供密码。

```
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::>
```

创建新的 SVM 角色

您创建的每个 SVM 都有一个默认 SVM 管理员，该管理员被分配了预定义vsadmin的角色。除了预定义的 SVM 角色集外，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。此命令可供具有该fsxadmin角色的文件系统管理员使用。

创建新的 SVM 角色（ONTAP CLI）

1. 您可以使用以下security login role createONTAP CLI命令创建新的 SVM 角色：

```
Fsx0123456::> security login role create -role vol_role -cmddirname volume
```

2. 在命令中指定以下必需的参数：

   - -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 “管理员” 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ONTAP用户配置活动目录身份验证

使用 ONTAP CLI 为ONTAP文件系统和 SVM 用户配置 Active Directory 身份验证的使用。

您必须是具有相应fsxadmin角色的文件系统管理员才能使用此过程中的命令。

为ONTAP用户设置 Active Directory 身份验证 (ONTAPCLI)

此过程中的命令可供具有该fsxadmin角色的文件系统用户使用。

1. 要访问 NetApp ONTAP CLI，请运行以下命令在 NetApp 适用于 ONTAP 的 Amazon FSx 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. 使用如图所示的security login domain-tunnel create命令建立用于对 Windows Active Directory 用户进行身份验证的域隧道。将 *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 域用户帐户。

   在命令中指定以下必需的参数：

   - -vserver— 配置了 CIFS 并已加入您的活动目录的 SVM 的名称。它将用作向文件系统验证 Active Directory 域用户身份的隧道。将创建新角色或用户。
   - -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：
     - 域-用于活动目录身份验证
     - 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文件系统创建一个 Active Directory 域用户帐户CORP\Admin。

```
FSxId012345::> security login create -vserver filesystem1 -username CORP\Admin -
application ssh -authmethod domain -role fsxadmin
```

以下示例使用公钥身份验证创建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"
```

使用 SSH 使用 Active Directory 凭据登录文件系统

- 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	描述
-vserver（可选）	账户访问的 SVM 的名称 如果您要为文件系统用户配置 SSH 公钥身份验证，请不要包括-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。
-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 modifyONTAPCLI 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该fsxadmin角色的文件系统管理员帐户。修改密码要求时，如果有任何具有该角色的现有用户将受到更改的影响，系统将发出警告。

以下示例将在 fsx SVM 上拥有该角色的用户的最小密码长度要求修改为 12 个字符。vsadmin-readonly在此示例中，有具有此角色的现有用户。

```
FsxId0123456::> security login role config modify -role vsadmin-readonly -vserver fsx -
passwd-minlength 12
```

由于存在用户，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账户密码失败

更新fsxadmin用户密码时，如果密码不符合文件系统上设置的密码要求，则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 NetApp ONTAP CLI，请运行以下命令在 NetApp 适用于 ONTAP 的 Amazon FSx 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. 该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，请指定以下任一或全部：

   - 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
```

迁移到适用于 ONTAP 的 Amazon FSx NetApp

以下各节提供有关如何将现有 NetApp ONTAP 文件系统迁移到适用于 ONTAP 的 Amazon FSx NetApp 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

- 使用迁移到适用于 ONTAP 的 FSx NetApp SnapMirror
- 使用 AWS DataSync 迁移至 FSx for ONTAP

使用迁移到适用于 ONTAP 的 FSx NetApp SnapMirror

您可以使用将您的 NetApp ONTAP 文件系统迁移到适用于 ONTAP 的 Amazon F NetApp Sx。NetApp SnapMirror

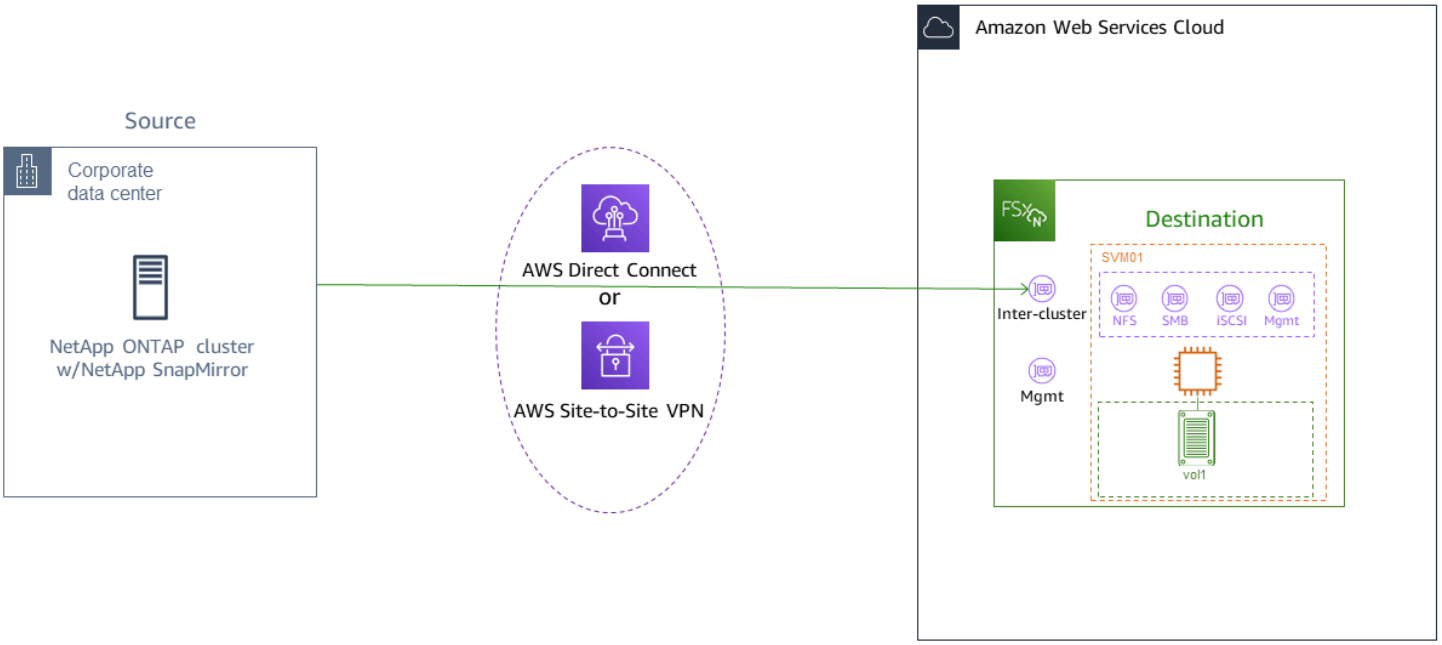
NetApp SnapMirror 在两个 ONTAP 文件系统之间使用块级复制，将数据从指定的源卷复制到目标卷。我们建议使用将本地 NetApp ONTAP 文件系统迁移 SnapMirror 到适用于 ONTAP 的 FSx。 NetApp SnapMirror的块级复制既快速又高效，即使对于具有以下特性的文件系统也是如此：

- 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。将您的本地 NetApp ONTAP 文件系统迁移到适用于 ONTAP 的 FSx 涉及以下高级任务：

1. 在 Amazon FSx 中创建目标卷。
2. 收集源和目标逻辑接口（LIF）。
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 FSx for ONTAP 文件系统。

下图阐明了本节中描述的迁移方案。



主题

- 开始之前
- 创建目标卷
- 记录源和目标集群间 LIF
- 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 FSx for ONTAP 文件系统
- 割接到 Amazon FSx

开始之前

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 优先考虑客户端流量，而非后台任务，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 对等连接、中转网关、AWS Direct Connect 或 AWS VPN 进行对等连接的网络中。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 和什么是 VPC 对等连接？。
- FSx for ONTAP 文件系统的 VPC 安全组具有入站和出站规则，允许集群间端点（LIF）在端口 443、10000、11104 和 11105 上使用 ICMP 和 TCP。
- 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。
- 您已通过 SVM 为 ONTAP 文件系统创建了目标 FSx，但尚未创建目标卷。有关更多信息，请参阅 创建 FSx for ONTAP 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 F SxIdabcdef 1234567890a）。
- *`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 for ONTAP 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 for ONTAP SnapMirror 文件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 ONTAP NetApp 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 AWS CLI 创建目标卷的信息，请参阅创建卷。

在以下步骤中，您将使用 NetApp ONTAP CLI 在 FSx for ONTAP 文件系统上创建目标卷。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
   ```

记录源和目标集群间 LIF

SnapMirror 使用集群间逻辑接口 (LIF) (每个都有唯一的 IP 地址) 来促进源集群和目标集群之间的数据传输。

1. 对于目标 FSx for ONTAP 文件系统，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 控制台检索集群间端点 – IP 地址。
2. 对于源 NetApp ONTAP 集群，使用 ONTAP CLI 检索集群间 LIF IP 地址。运行以下命令：

```
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**
>
> 对于横向扩展文件系统，每个高可用性 (HA) 对都有两个集群间 IP 地址。保存这些值以备后用。

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互连。对于横向扩展文件系统，您需要提供每个集群间 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。对于横向扩展文件系统，您需要提供每个集群间 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

建立集群对等后，下一步是 SVM 对等。使用 vserver peer 命令在目标集群（FSx-Dest）上创建 SVM 对等关系。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 SVM 之间创建 SVM 对等关系。

```
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 SVM 进行了对等，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 FSx for 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 FSx for ONTAP 之前，您还可以安排每小时或每日更新。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
```

割接到 Amazon FSx

要为切换到 FSx for ONTAP 文件系统做准备，请执行以下操作：

- 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 FSx for ONTAP 文件系统。

1. 要确保源集群中的所有数据都传输到 FSx for 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 FSx 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 数据。

使用 AWS DataSync 迁移至 FSx for ONTAP

我们建议使用 AWS DataSync 在 FSx for ONTAP 文件系统和非 ONTAP 文件系统之间传输数据，包括 FSx for Lustre、FSx for OpenZFS、FSx for Windows File Server、Amazon EFS、Amazon S3 和本地文件管理器。如果您要在适用于 ONTAP 的 FSx 和 ONTAP 之间传输文件，我们 NetApp 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。AWS 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 在两个 FSx for ONTAP 文件系统之间传输文件，也可以将数据移动到另一个 AWS 区域或帐户中的文件系统。AWS您也可以将适用于 ONTAP 文件系统的 FSx 用于其他任务。DataSync 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 文件系统的 FSx 的终端节点。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，对于吞吐能力至少为 512 MBp 的文件系统，200 MBp 的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，您需要符合要求的服务器和网络。 DataSync 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，然后激活（如果在 AWS 服务 之间传输，则不需要）。
- 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：

- 在自行管理的存储和 AWS 之间传输数据
- 为 ONTAP 的 Amazon FSx 创建位置 NetApp

监控 ONTAP 的 Amazon FSx NetApp

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 FSx for ONTAP 的原始数据并将其处理为可读的指标。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 – 您可以使用由 ONTAP 事件管理系统（EMS）生成的事件来监控 FSx for 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 云见解 — 您可以使用 Cloud Insights 服务监控适用于 ONTAP 文件系统的 FSx 的配置、容量和性能指标。 NetApp 您也可以根据指标条件创建警报。
- NetApp Harvest 和 NetApp Grafana — 你可以使用 Harvest 和 Grafana 监控你的 FSx for ONTAP 文件系统。 NetApp NetApp NetApp Harvest 通过从 FSx 收集 ONTAP 文件系统的性能、容量和硬件指标来监控 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 捕获所有 Amazon FSx 的 API 调用作为事件。这些事件提供了用户、角色或 AWS 服务在 Amazon FSx 中所执行操作的记录。

主题

使用 Amazon 进行监控 CloudWatch

您可以使用 Amazon 监控文件系统 CloudWatch，它会收集来自 Amazon FSx for NetApp ONTAP 的原始数据，并将其处理为可读的近乎实时的指标。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，确定文件系统的运行状况。默认情况下，ONTAP 的 FSx 指标数据会以 1 分钟为周期自动

发送到 CloudWatch 。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，FSx for ONTAP 以 1 分钟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 FSx for ONTAP 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：F ile-system-level 性能和存储容量指标。
- 详细的文件系统指标：每个ile-system-level 存储层（ SSD 和容量池）的 F 个存储指标。
- 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。

适用于 ONTAP 的 FSx 的所有 CloudWatch 指标都将发布到中的`AWS/FSx`命名空间。 CloudWatch

主题

如何使用 FSx 获取 ONTAP 指标 CloudWatch

Amazon FSx 报告的 CloudWatch 指标提供了有关您的 FSx for ONTAP 文件系统和卷的重要信息。

主题

- 在 Amazon FSx 控制台中监控文件系统指标
- 在 Amazon FSx 控制台中监控卷指标

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：MetadataO

监控和性能	如何...	图表	相关指标
			perationTime * 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} 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

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
	...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 控制台中监控卷指标

您可以在 Amazon FSx 控制台中的卷控制面板上，使用监控面板查看其他性能指标。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

监控	如何...	图表	相关指标
			平均写入延迟：DataWriteOperationTime * 1000/DataWriteOperations 平均元数据延迟：MetadataOperationTime * 1000/MetadataOperations
	...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

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
- 亚马逊 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. 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 CloudWatch 控制台查看您的交易量指标

使用 Amazon FSx 控制台查看您的交易量 CloudWatch 指标

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 FSx for ONTAP 文件系统指标添加到亚马逊控制台的控制面板中。
CloudWatch

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

- 调用统GetMetric计 API 操作。有关更多信息，请参阅 Amazon CloudWatch API 参考。

文件系统指标

您的 Amazon FSx 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。

请注意以下关于 Amazon FSx 何时向其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，Amazon FSx 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`
- 对于所有其他指标，每个周期都会发出一个数据点，对应于所有活动文件服务器（例如文件服务器指标）或所有聚合（例如`DataReadBytes`存储指标）的指标`DiskReadBytes`的总值。

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	描述
NetworkThroughputUtilization	文件系统的网络吞吐量利用率百分比。 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）。

指标	描述
	Sum 统计数据是指定时间段内文件系统收到的字节总数。 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	描述
DataReadOperations	从客户端读取到文件系统的读取操作（网络 I/O）次数。 Sum 统计数据是发生在指定时间段内的 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 统计数据是发生在指定时间段内的 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 统计数据是发生在指定时间段内的 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	描述
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	描述
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	描述
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	描述
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	描述
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。这对预配置的吞吐能力不高于 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	描述
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。这对预配置的吞吐能力不高于 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	描述
FileServerCacheHitRatio	由文件系统 RAM 和 NVMe 缓存中的数据提供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	描述
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	描述
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	描述
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	描述
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	描述
	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	描述
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	描述
StorageCapacityUtilization	每个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文件系统性能层的平均存储容量利用率。 该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。 该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	描述
	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

横向扩展文件系统指标

以下是针对具有两个或更多高可用性 (HA) 对的 ONTAP 文件系统的 FSx 的指标。对于指标，将为每个 HA 对和每个聚合（存储利用率指标）发出一个数据点。

> **Note**
>
> 如果您的文件系统具有多个 HA 对，则还可以使用单 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）。奇数文件服务器是首选的文件服务器（也就是说，除非文件系统已故障转移到辅助文件服务器，否则它们会为流量提供服务），而偶数文件服务器是辅助文件服

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	描述
NetworkThroughputUtilization	网络吞吐量利用率占文件系统可用网络吞吐量的百分比。该指标等同于您的文件系统一个 HA 对的最大网络吞吐量容量NetworkSentBytes NetworkReceivedBytes 以及占网络吞吐量容量的百分比。此指标将考虑所有流量，包括后台任务（例如 SnapMirror分层和备份）。每个文件系统的文件服务器每分钟都会发布一个指标。 Average统计数据是指定文件服务器在指定时间段内的平均网络吞吐量利用率。 该Minimum统计数据是给定文件服务器在指定时间段内在一分钟内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在一分钟内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	您的文件系统发送的字节数（网络 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）。每个文件系统的文件服务器每分钟都会发布一个指标。 Sum统计数据是指定文件服务器在指定时间段内通过网络发送的总字节数。 Average统计数据是指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	描述
	Minimum统计数据是指定文件服务器在指定时间段内通过网络发送的最小字节数。 Maximum统计数据是指定文件服务器在指定时间段内通过网络发送的最大字节数。 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：SumAverage、Minimum、和Maximum

指标	描述
NetworkReceivedBytes	您的文件系统接收的字节数（网络 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）。每个文件系统的文件服务器每分钟都会发布一个指标。 Sum统计数据是指定文件服务器在指定时间段内通过网络接收的总字节数。 Average统计数据是指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统计数据是指定文件服务器在指定时间段内每分钟通过网络接收的最小字节数。 Maximum统计数据是指定文件服务器在指定时间段内每分钟通过网络接收的最大字节数。 要计算任何统计数据的接收吞吐量（每秒字节数），请将统计数据除以该周期内的秒数。 单位：字节 有效统计数据：SumAverage、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	描述
CPUUtilization	文件系统 CPU 资源的利用率百分比。每个文件系统的文件服务器每分钟都会发布一个指标。 Average 统计数据是指定时间段内文件系统的平均 CPU 利用率。

指标	描述
	Minimum统计数据是指定文件服务器在指定时间段内的最低 CPU 使用率。 Maximum统计数据是指定文件服务器在指定时间段内的最高 CPU 使用率。 单位：百分比 有效统计数据：Average、Minimum 和 Maximum
FileServerDiskThroughputUtilization	文件服务器和聚合之间的磁盘吞吐量，占预配置限制的百分比，由吞吐量决定。此指标将考虑所有流量，包括后台任务（例如 SnapMirror分层和备份）。该指标等同于您的文件系统一个 HA 对的文件服务器磁盘吞吐容量的总DiskReadBytes 和DiskWriteBytes 及百分比。每个文件系统的文件服务器每分钟都会发布一个指标。 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统计数据是指定时间段内给定文件服务器的最低文件服务器磁盘吞吐量利用率。 Maximum统计数据是指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	描述
FileServerDiskIopsUtilization	文件服务器可用磁盘 IOPS 容量的 IOPS 利用率，以其磁盘 IOPS 限制的百分比表示。不同之处DiskIopsUtilization 在于，与预配置的磁盘 IOPS 相比，磁盘 IOPS 的利用率超过了文件服务器可以处理的最大值。此指标将考虑所有流量，包括后台任务（例如 SnapMirror分层和备份）。每个文件系统的文件服务器每分钟都会发布一个指标。 Average统计数据是指定文件服务器在指定时间段内的平均磁盘 IOPS 利用率。 Minimum统计数据是指定文件服务器在指定时间段内的最低磁盘 IOPS 利用率。 Maximum统计数据是指定文件服务器在指定时间段内的最高磁盘 IOPS 利用率。 单位：百分比 有效统计数据：Average、Minimum 和 Maximum

指标	描述
FileServerCacheHitRatio	对于每个 HA 对（例如，HA 对中的活动文件服务器），驻留在文件系统 RAM 或 NVMe 缓存中的数据所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与总读取量的比率越高。将考虑所有 I/O，包括后台任务（例如 SnapMirror 分层和备份）。每个文件系统的文件服务器每分钟都会发布一个指标。 单位：百分比 Average统计数据是文件系统中某个 HA 对在指定时间段内的平均缓存命中率。 该Minimum统计数据是您的文件系统中某个 HA 对在指定时间段内的最低缓存命中率。 该Maximum统计数据是您的文件系统的其中一个 HA 对在指定时间段内的最高缓存命中率。 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— 您的文件系统的性能层由多个称为聚合的存储池组成。每个 HA 对都有一个聚合。例如，在 HA 对中聚合到文件服务器FsxId01234567890abcdef-01（活动文件服务器）和文件服务器FsxId01234567890abcdef-02（辅助文件服务器）的aggr1映射。

指标	描述
DiskReadBytes	从该聚合中读取任何磁盘的字节数（磁盘 IO）。此指标将考虑所有流量，包括后台任务

指标	描述
	（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。 Sum统计数据是在指定时间段内每分钟从给定聚合中读取的字节总数。 Average统计数据是在指定时间段内每分钟从给定聚合中读取的平均字节数。 Minimum统计数据是在指定时间段内每分钟从给定聚合中读取的最小字节数。 Maximum统计数据是在指定时间段内每分钟从给定聚合中读取的最大字节数。 要计算任何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周期内的秒数。 单位：字节 有效统计数据：SumAverage、Minimum、和 Maximum

指标	描述
DiskWriteBytes	任何磁盘写入此聚合的字节数（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。 Sum统计数据是在指定时间段内写入给定聚合的总字节数。 Average统计数据是在指定时间段内每分钟写入给定聚合的平均字节数。 Minimum统计数据是在指定时间段内每分钟写入给定聚合的最小字节数。 Maximum统计数据是在指定时间段内每分钟写入给定聚合的最大字节数。 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：SumAverage、Minimum、和Maximum

指标	描述
DiskIopsUtilization	一个聚合的磁盘 IOPS 利用率，以该聚合的磁盘 IOPS 限制的百分比表示（即文件系统的总 IOPS 除以文件系统的 HA 对数）。不同之处FileServerDiskIopsUtilization 在于，它是预配置磁盘 IOPS 的利用率与预配置 IOPS 限制的对比，而不是文件服务器支持的最大磁盘 IOPS（即由您配置的每个 HA 对的吞吐容量决定）。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。 Average统计数据是给定聚合在指定时间段内的平均磁盘 IOPS 利用率。 该Minimum统计数据是给定聚合在指定时间段内的最低磁盘 IOPS 利用率。 Maximum统计数据 ii 指定聚合在指定时间段内的最高磁盘 IOPS 利用率。 单位：百分比 有效统计数据：Average、Minimum 和 Maximum

指标	描述
DiskReadOperations	此聚合的读取操作数（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。 Sum统计数据是给定聚合在指定时间段内执行的读取操作的总数。 Average统计数据是给定聚合在指定时间段内每分钟执行的平均读取操作数。 该Minimum统计数据是给定聚合在指定时间段内每分钟执行的最低读取操作数。 Maximum统计数据是给定聚合在指定时间段内每分钟执行的最大读取操作数。 要计算一段时间内的平均磁盘 IOPS，请使用Average统计数据并将结果除以 60（秒）。 单位：计数 有效统计数据：SumAverage、Minimum、和Maximum

指标	描述
DiskWriteOperations	此聚合的写入操作（磁盘 IO）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。 Sum统计数据是给定聚合在指定时间段内执行的写入操作的总数。 Average统计数据是给定聚合在指定时间段内每分钟执行的平均写入操作数。 要计算一段时间内的平均磁盘 IOPS，请使用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要么有FileSystemIdStorageTier、和DataType维度，要么有FileSystemId、StorageTierDataType、和Aggregate维度。

- 如果未提供Aggregate维度，则指标适用于您的整个文件系统。StorageUsed和StorageCapacity指标每分钟都有一个数据点，对应于文件系统的总消耗存储空间（每个存储层）和总存储容量（对于 SSD 层）。同时，该StorageCapacityUtilization指标每分钟为每个聚合生成一个指标。
- 提供Aggregate维度时，指标是针对每个聚合的。

尺寸的含义如下：

- FileSystemId— 您的文件系统的 AWS 资源 ID。
- Aggregate— 您的文件系统的性能层由多个称为聚合的存储池组成。每个 HA 对都有一个聚合。例如，在 HA 对中聚合到文件服务器FsxId01234567890abcdef-01（活动文件服务器）和文件服务器FsxId01234567890abcdef-02（辅助文件服务器）的aggr1映射。

- StorageTier— 表示该指标所测量的存储层，可能的值为SSD和StandardCapacityPool。
- DataType— 表示指标衡量的数据类型，并附上可能的值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	描述
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。 该Average统计数据是给定聚合在指定时间段内的平均存储容量利用率。 该Minimum统计数据是给定聚合在指定时间段内的最低存储容量利用率。 该Maximum统计数据是给定聚合在指定时间段内的最大存储容量利用率。 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。 该Average统计数据是给定聚合在指定时间段内的平均存储容量。 该Minimum统计数据是给定聚合在指定时间段内的最小存储容量。 该Maximum统计数据是给定聚合在指定时间段内的最大存储容量。 单位：字节

指标	描述
	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段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段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段内在给定存储层上消耗的最大物理存储容量。 单位：字节 有效统计数据：Average、Minimum 和 Maximum

卷指标

适用于 NetApp ONTAP 的 Amazon FSx 文件系统可以有一个或多个卷来存储您的数据。其中的每个卷都有一组指标，这些指标被归类为卷指标或详细的卷指标。

- 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	描述
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）。 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。

指标	描述
	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
MetadataOperations	客户端进行元数据活动时产生的对卷的 I/O 操作（网络 I/O）次数。 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

指标	描述
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
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	描述
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	描述
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	描述
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、Minimum 和 Maximum
StorageCapacityUtilization	卷的存储容量利用率。 单位：百分比

指标	描述
	有效统计数据：Average
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、Minimum 和 Maximum
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	描述
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

指标	描述
	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。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

性能警告和建议

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，FSx for ONTAP 就会显示一条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 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。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。

仪表板部分	如果有针对此指标的警告	请执行该操作
存储	主存储容量利用率	如果您的文件系统尚未达到最大 SSD 存储容量，请增加文件系统的主存储容量。有关更多信息，请参阅 修改 SSD 存储容量和预配置 IOPS。 如果您的文件系统有多个 HA 对，并且您的文件系统聚合子集（构成主存储层的存储池）的主存储容量利用率仅更高，则您还可以重新平衡工作负载，以便在文件系统中更均匀地分配主存储容量利用率。有关重新平衡工作负载的更多信息，请参阅监控 FSx 的 ONTAP 工作负载平衡。
文件服务器性能	网络吞吐量 磁盘吞吐量 磁盘 IOPS CPU 使用率	如果您的文件系统尚未达到最大吞吐容量，请增加文件系统的吞吐容量。有关更新吞吐容量的更多信息，请参阅如何修改吞吐能力。 如果您的文件系统有多个 HA 对，并且只有一部分文件服务器的利用率很高，那么您还可以重新平衡工作负载，以便更均匀地利用文件系统每个 HA 对的性能能力来实现工作负载。有关重新平衡工作负载的更多信息，请参阅监控 FSx 的 ONTAP 工作负载平衡。
磁盘性能	磁盘 IOPS	如果您的文件系统尚未达到文件系统当前吞吐量的最大 SSD IOPS，请提高 SSD IOPS。有关更新文件系统的预配置 IOPS 的更多信息，请参阅。修改 SSD 存储容量和预配置 IOPS 如果您的文件系统有多个 HA 对，并且文件系统聚合子集（构成主存储层的存储池）的磁盘 IOPS 利用率仅更高，则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，请参阅监控 FSx 的 ONTAP 工作负载平衡。

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 Amazon FSx 控制台或亚马逊 CloudWatch 控制台创建警报。

以下过程介绍了如何使用 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. 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. 请按照使用 Amazon FSx 控制台设置警报中的过程，从步骤 6 开始操作。

要使用设置警报 AWS CLI

- 调用 CLI 命令 put-metric-alarm。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PutMetric警报 API 接口。有关更多信息，请参阅 Amazon CloudWatch API 参考。

监控 FSx 的 ONTAP 工作负载平衡

如果您的文件系统具有多个 HA 对，则其性能和吞吐量将分布在每个 HA 对中。FSx for ONTAP 会在文件写入文件系统时自动平衡文件，但在极少数情况下，您的工作负载数据或 I/O 可能会在 HA 对之间变得不平衡，从而影响工作负载的整体性能。您可以监控工作负载，以确保工作负载在文件系统的每个 HA 对（以及它们相应的文件服务器和聚合，即构成主存储层的存储池）之间保持平衡。

主题

主存储利用率平衡

文件系统的主存储容量在称为聚合的存储池中的每个 HA 对之间平均分配。每个 HA 对都有一个聚合。我们建议您将主存储层的平均利用率持续保持在 80% 以内。对于具有多个 HA 对的文件系统，我们建议您将每个聚合的平均利用率保持在 80%。

保持 80% 的利用率可确保有可用空间容纳新的传入数据，并保持可观的维护操作开销，这可能会暂时占用聚合上的可用空间。

如果您发现聚合不平衡，则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），也可以使用 ONTAP CLI 中的卷移动命令在聚合之间移动卷。

文件服务器和磁盘性能利用率不平衡

文件系统的总性能能力（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）在文件系统的 HA 对之间平均分配。对于所有性能限制，我们建议您将平均利用率保持在 50% 以下（最大峰值利用率保持在 80% 以下），这既适用于所有 HA 对中的文件系统文件服务器资源的总体利用率，也适用于每个文件服务器。

如果您注意到您的文件服务器性能利用率不平衡，并且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 进一步诊断性能失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一步诊断的后续步骤。

如果你的文件系统是...	则...
文件服务器磁盘吞吐量或文件服务器磁盘 IOPS 不平衡	您可能遇到 HA 对子集（包含正在访问的大量数据的卷子集）上的 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。对于每台利用率高的文件服务器，请检查利用率最高的卷，以查看聚合中哪些卷的活动最多。有关此过程的更多信息，请参阅重新平衡利用率高的卷。
网络吞吐量不平衡，但您的文件服务器磁盘吞吐量、文件服务器磁盘 IOPS 或磁盘 IOPS 并非不平衡	您的数据在 HA 对之间均匀分布，但您的客户端却不是。对于网络吞吐量利用率高于其他文件服务器的文件服务器，请检查每台文件服务器的顶级客户端，然后通过从这些客户端上卸载任何卷，然后在不同 HA 对上使用不同的端点重新装载这些客户端，从而重新平衡这些客户端。有关此过程的更多信息，请参阅重新平衡高流量客户端。

将 CloudWatch 维度映射到 ONTAP CLI 和 REST API 资源

您的横向扩展文件系统的亚马逊 CloudWatch 指标为`FileServer`或`Aggregate`维度。为了进一步诊断不平衡的情况，您需要在 ONTAP CLI 或 REST API 中将这些维度值映射到特定的文件服务器（或节点）和聚合。

- 对于文件服务器，每个文件服务器名称都映射到 ONTAP 中的文件服务器（或节点）名称（例如`FsxId01234567890abcdef-01`）。奇数文件服务器是首选的文件服务器（也就是说，除非文件系统已故障转移到辅助文件服务器，否则它们会为流量提供服务），而偶数文件服务器是辅助文件服务器（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，每个聚合名称都映射到 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`和`FsxId01234567890abcdef-02`（活动文件服务器）和（辅助文件服务器）共享，聚合`aggr2`由文件服务器`FsxId01234567890abcdef-03`共享`FsxId01234567890abcdef-04`，依此类推。

您可以使用 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《适用于 ONTAP 的 Amazon FSx 用户指南》一使用 NetApp ONTAP CLI节中记录的步骤 NetApp 进行操作。

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. 使用存储聚合 show 命令指定-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.
```

重新平衡高流量客户端

如果您遇到文件服务器之间的 I/O 不平衡问题（特别是在网络吞吐量利用率方面），那么高的 I/O 客户机可能是原因。要识别高流量客户端，请使用 ONTAP CLI。

1. 要通过 SSH 登录文件系统的 NetApp ONTAP CLI，请按照《适用于 ONTAP 的 Amazon FSx 用户指南》一使用 NetApp ONTAP CLI节中记录的步骤 NetApp 进行操作。

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. 要查看流量最高的客户端，请使用统计顶级客户端 show ONTAP CLI 命令。您可以选择将-node参数指定为仅查看特定文件服务器的顶级客户端。如果您要诊断特定文件服务器的不平衡，请使用-node参数，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，提供输出每个报告之前的测量间隔（以秒为单位）。增加间隔（例如，最大为 300 秒）可以为每个卷的流量提供较长期的样本。默认值为5（秒）。

```
::> statistics top client show -node FsxId01234567890abcdef-01 [-interval [5,300]]
```

   在输出中，排名靠前的客户端按其 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
```

3. 您可以将列出的高流量客户端中的一部分重新平衡到其他文件服务器。为此，请从客户端卸载该卷，然后使用 SVM 的 NFS/SMB 端点的 DNS 名称将其重新挂载——这将返回一个与随机 HA 对相对应的随机端点。

   我们建议您重复使用 DNS 名称，但您可以选择明确选择给定客户端挂载的 HA 对。为确保将客户端安装到不同的终端节点，您可以改为指定与流量较大的节点对应的端点 IP 地址不同的终端节点 IP 地址。你可以通过运行以下命令来做到这一点：

   ```
   ::> 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.
   ```

   根据该`statistics top client show`命令的示例输出，客户端`172.17.236.53`正在将大量流量带到`FsxId01234567890abcdef-01`。`network interface show`命令的输出表明这是地址`172.31.15.89`。要挂载到其他端点，请选择任何其他地址（在本例中，唯一的其他地址是`172.31.8.112`，对应于`FsxId01234567890abcdef-03`）。

重新平衡利用率高的卷

如果您的卷或聚合之间的 I/O 不平衡，则可以重新平衡卷，以便在各卷之间重新分配 I/O 流量。

> **Note**
>
> 如果您的聚合之间出现存储利用率不平衡的情况，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，因为如果您不考虑正在考虑移动的每个卷的 I/O，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《适用于 ONTAP 的 Amazon FSx 用户指南》一使用 NetApp ONTAP CLI节中记录的步骤 NetApp 进行操作。

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. 使用 stati stics volume show ONTAP CLI 命令查看给定聚合的最高流量，但有以下更改：

   - 将####替换为聚合的名称（例如，）。aggr1
   - 您可以选择添加-interval参数，提供输出每个报告之前的测量间隔（以秒为单位）。增加间隔（例如，最大为 300 秒）可以为每个卷的流量提供较长期的样本。默认值为5（秒）。

```
::> statistics volume show -aggregate aggregate_name -sort-key total_ops [-interval
 [5,300]]
```

   根据您选择的时间间隔，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，以及流向每个聚合的流量。

```
                          *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
```

   交易量统计数据按成分股显示（例如，vol1__0015是第15个成分股 FlexGroupvol1）。从示例输出中可以看出，的成分比成aggr1分的利用率更高。aggr2要平衡聚合之间的流量，可以在聚合之间移动组成卷，以便更均匀地分配流量。

3. 要在聚合之间移动卷，请使用卷移动启动 ONTAP CLI 命令，替换以下值：

   - 将 *svm_name* 替换为托管您要移动的卷的 SVM 的名称。
   - 将 v *olume_nam* e 替换为卷组成部分的名称（例如，）。vol1__0001
   - 将####替换为卷的目标聚合的名称。

> **Important**
>
> 卷移动会消耗源文件服务器和目标文件服务器的网络和磁盘资源。因此，任何正在进行的卷移动都可能影响工作负载的性能。此外，卷移动过程还有一个切换阶段，该阶段会暂停任何流向该卷的流量的 I/O。

```
::> volume move start -vserver svm_name -volume volume_name -
destination 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.
```

要检查卷移动操作的状态，请使用 `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: aggr2
                           Source Node: FsxId01234567890abcdef-01
                            Move State: healthy
```

此命令显示完成移动的估计时间，作为其中一个信息字段。操作完成后，相同的命令将显示该`Move Phase`字段已完成。

您应确保每种FlexGroup成分均匀分布在您的聚合物中，理想情况下，每个聚合物建议使用8种成分。如果您将一个成分交易量移至另一个合计以获得原本平衡的合计FlexGroup，则应反过来将另一个（利用率较低的）成分交易量移至源合计以保持平衡。

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 事件转发到系统日志服务器

EMS 事件概述

EMS 事件是自动生成的通知，当你的 FSx for ONTAP 文件系统出现预定义的情况时，这些通知会提醒你。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，您可以监控诸如用户密码更改、容量 FlexGroup 接近满、逻辑单元号 (LUN) 已手动联机或脱机或卷大小自动调整等事件。

有关 ONTAP EMS 事件的更多信息，请参阅 ONTAP 文档中心的 “ONTAP EMS 参考 NetApp ”。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 ONTAP NetApp CLI 事件目录 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 事件日志 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。
-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

事件选项	描述

	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 登录文件系统的 NetApp ONTAP CLI，请按照《适用于 ONTAP 的 Amazon FSx 用户指南》一使用 NetApp ONTAP CLI节中记录的步骤 NetApp 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 ONTAP 文档中心的《ONTAP EMS 参考》 NetApp 。

EMS 事件转发到系统日志服务器

您可以将 EMS 事件配置为将通知转发到 Syslog 服务器。EMS 事件转发用于实时监控您的文件系统，以确定和隔离各种问题的根本原因。如果您的环境中还没有用于事件通知的 Syslog 服务器，则必须先创建一个 Syslog 服务器。必须在文件系统上配置 DNS 才能解析 Syslog 服务器名称。

配置 EMS 事件以将通知转发到 Syslog 服务器

1. 要通过 SSH 登录文件系统的 NetApp ONTAP CLI，请按照《适用于 ONTAP 的 Amazon FSx 用户指南》一使用 NetApp ONTAP CLI节中记录的步骤 NetApp 进行操作。

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. 使用事件通知目的地 create 命令创建类型为的事件通知目的地`syslog`，指定以下属性：

   - *`dest_name`*— 要创建的通知目标的名称（例如，`syslog-ems`）。事件通知目标名称的长度必须为 2 到 64 个字符。有效字符是以下 ASCII 字符：A-Z、a-z、0-9、“_” 和 “-”。名称的开头和结尾必须是：A-Z、a-z 或 0-9。
   - *`syslog_name`*— 系统日志消息发送到的系统日志服务器主机名或 IP 地址。

- *transport_protocol*— 用于发送事件的协议：
  - udp-unencrypted— 没有安全性的用户数据报协议。这是默认协议。
  - tcp-unencrypted— 没有安全性的传输控制协议。
  - tcp-encrypted— 具有传输层安全性 (TLS) 的传输控制协议。指定此选项后，FSx for ONTAP 将通过验证目标主机的证书来验证其身份。
- *port_number*— 系统日志消息发送到的 Syslog 服务器端口。默认值syslog-port参数取决于syslog-transport参数的设置。如果设置syslog-transport为tcp-encrypted，则syslog-port默认值为6514。如果设置syslog-transport为tcp-unencrypted，syslog-port则使用默认值601。否则，默认端口将设置为514。

```
::> event notification destination create -name dest_name -syslog syslog_name -
syslog-transport transport_protocol -syslog-port port_number
```

3. 使用 e vent notification create 命令为事件过滤器定义的一组事件创建新的通知，发送到在上一步中创建的通知目的地，并指定以下属性：
   - *node_name*— 事件过滤器的名称。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标的名称。

```
::> event notification create -filter-name filter_name -destinations dest_name
```

4. 使用event notification destination check命令生成测试消息并验证您的设置是否正常。使用命令指定以下属性：
   - *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标的名称。

```
::> set diag
::*> event notification destination check -node node_name -destination-
name dest_name
```

使用 Cloud Insights 监控

NetApp Cloud Insights 是一项 NetApp 服务，您可以使用它来监控适用于 NetApp ONTAP 文件系统的亚马逊 FSx 以及其他 NetApp 存储解决方案。您可以借助 Cloud Insights 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**
>
> 横向扩展文件系统不支持 Cloud Insights。

Cloud 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要求，帮助您将工作负载迁移到更高效的 FSx for ONTAP 配置。您还可以利用这些见解来规划何时需要为 FSx for ONTAP 部署更高的性能或容量。

有关云洞察的更多信息，请参阅 Cloud Cent ral 上的 NetApp NetApp 云见解。

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，并且与 ONTAP 的 FSx 兼容。你可以将 Harvest 与 Grafana 结合使用来获得开源监控解决方案。

Harvest 和 Grafana 入门

以下部分详细介绍了如何设置和配置 Harvest 和 Grafana 来衡量 FSx 的 ONTAP 文件系统的性能和存储容量利用率。

你可以使用 Harvest 和 Grafana 监控适用于 NetApp ONTAP 的亚马逊 FSx 文件系统。 NetApp Harvest 通过从 FSx 收集 ONTAP 文件系统的性能、容量和硬件指标来监控 ONTAP 数据中心。Grafana 配备的控制面板中会显示收集的 Harvest 指标。

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 ONTAP 不同。 NetApp 因此，目前仅支持以下标有标签`fsx`的 out-of-the-box Harvest 仪表板与 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。

- ONTAP：合规性
- ONTAP：数据保护快照
- ONTAP：安全性
- ONTAP：SVM
- ONTAP：卷

AWS CloudFormation 模板

首先，您可以部署一个 AWS CloudFormation 模板来自动启动运行 Harvest 和 Grafana 的 Amazon EC2 实例。作为 AWS 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 管理终端节点。部署完成后，您可以登录 Grafana 控制面板来监控您的文件系统。

此解决方案用于 AWS 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-graf AWS CloudFormation ana.template 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

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，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 连接到终端节点，因此它需要解析终端节点，需要端口 53 TCP/UDP 才能使用 DNS。此外，要访问终端节点，它需要端口 443 TCP 以进行 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 FSx for ONTAP 文件系统在亚马逊虚拟私有云（亚马逊 VPC）中运行，并且模板的参数信息如下所列。有关创建文件系统的更多信息，请参阅创建 FSx for ONTAP 文件系统。

启动 Harvest/Grafana 解决方案堆栈

1. 下载 fsx-ontap-harvest-grafana.template 模板 AWS CloudFormation 。有关创建 AWS 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，此模板在美国东部（弗吉尼亚北部）AWS 区域启动。您必须在可用 Amazon FSx AWS 区域 的地方启动此解决方案。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。
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 之外，请确保您希望用于访问 Grafana 控制面板的客户端均已打开入站端口 3000 和 9090 以及端口 53 和 443。
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。

参数	默认值	描述
子网	无默认值	为 NetApp ONTAP 文件系统的首选子网指定与您的 Amazon FSx 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
F SxEnd Point	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	AWS Secrets Manager 包含文件系统`fsxadmin`用户密码的机密名称。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 AWS 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。

欲了解更多信息，请参阅上的 NetApp Harvest 页面 GitHub。

对 Harvest 和 Grafana 进行故障排除

如果您遇到 Harvest 和 Grafana 仪表板中提及的任何数据缺失，或者在使用 FSx for ONTAP 设置 Harvest 和 Grafana 时遇到问题，请查看以下主题以获取潜在的解决方案。

主题

- SVM 和交易量仪表板为空
- CloudFormation 堆栈在超时后回滚

SVM 和交易量仪表板为空

如果 AWS CloudFormation 堆栈已成功部署并且可以联系 Grafana，但 SVM 和卷仪表板为空，请使用以下步骤对您的环境进行故障排除。你需要通过 SSH 访问部署了 Harvest 和 Grafana 的 Amazon EC2 实例。

1. SSH 进入你的 Harvest 和 Grafana 客户端正在运行的 Amazon EC2 实例。

   ```
   [~]$ ssh ec2-user@ec2_ip_address
   ```

2. 使用以下命令打开harvest.yml文件然后：

   - 验证是否已为您的 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您的fsxadmin凭据相符。

   ```
   [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用户凭证以以下格式存储在 Secrets Manager 中，以备将来的任何部署使用，并*fsxadmin_password*替换为您的密码。

```
{"username" : "fsxadmin", "password" : "fsxadmin_password"}
```

CloudFormation 堆栈在超时后回滚

如果您无法成功部署 CloudFormation 堆栈，并且正在回滚并出现错误，请使用以下步骤来解决问题。您需要通过 SSH 访问 CloudFormation 堆栈部署的 EC2 实例。

1. 重新部署 CloudFormation 堆栈，确保禁用自动回滚。
2. SSH 进入你的 Harvest 和 Grafana 客户端正在运行的 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，您应该看到五个容器，如下所示：

```
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，请按如下方式检查/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. 通过运行并连接到你的 Harvest sudo docker ps 和 Grafana 网址，验证容器是否成功启动。

使用 AWS CloudTrail 对 FSx for ONTAP API 调用进行日志记录

Amazon FSx 与 AWS CloudTrail 集成，后者是在 Amazon FSx 中提供用户、角色或 AWS 服务所采取操作的记录的服务。CloudTrail 将 Amazon FSx for NetApp ONTAP 的所有 Amazon FSx API 调用作为事件捕获。捕获的调用包含来自 Amazon FSx 控制台的调用以及对 Amazon FSx 操作的代码调用。

如果您创建跟踪，则可以使 CloudTrail 事件持续传送到 Amazon S3 桶（包括 Amazon FSx 的事件）。如果您不配置跟踪，则仍可在 CloudTrail 控制台中的事件历史记录中查看最新事件。通过使用 CloudTrail 收集的信息，可以确定已对 Amazon FSx 发出的请求。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。

要了解有关 CloudTrail 的更多信息，请参阅《AWS CloudTrail 用户指南》。

CloudTrail 中的 Amazon FSx 信息

在您创建 AWS 账户时，将在该账户上启用 CloudTrail。当 Amazon FSx 中发生 API 活动时，该活动将记录在 CloudTrail 事件中，并与其他 AWS 服务事件一同保存在事件历史记录中。您可以在 AWS 账户中查看、搜索和下载最新事件。有关更多信息，请参阅使用 CloudTrail 事件历史记录查看事件。

要持续记录 AWS 账户中的事件（包括 Amazon FSx 的事件），请创建跟踪。通过跟踪记录，CloudTrail 可将日志文件传送至 Simple Storage Service（Amazon S3）存储桶。预设情况下，在控制台中创建跟踪时，此跟踪应用于所有 AWS 区域。此跟踪记录来自 AWS 分区中的所有 AWS 区域的事件，并将日志文件传送至您指定的 Amazon S3 存储桶。此外，您可以配置其他 AWS 服务，进一步分析在 CloudTrail 日志中收集的事件数据并采取行动。有关更多信息，请参阅《AWS CloudTrail 用户指南》中的以下主题：

- 为您的 AWS 账户 创建跟踪
- AWS 服务与 CloudTrail Logs 的集成
- 为 CloudTrail 配置 Amazon SNS 通知
- 从多个区域接收 CloudTrail 日志文件和从多个账户接收 CloudTrail 日志文件

所有 Amazon FSx API 调用都由 CloudTrail 进行记录。例如，对 `CreateFileSystem` 和 `TagResource` 操作的调用将在 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。身份信息可帮助您确定以下内容：

- 请求是使用根用户凭证还是 AWS Identity and Access Management（IAM）用户凭证发出的。
- 请求是使用角色还是联合身份用户的临时安全凭证发出的。
- 请求是否由其它 AWS 服务发出。

有关更多信息，请参阅《AWS CloudTrail 用户指南》中的 CloudTrail userIdentity 元素。

了解 Amazon FSx 日志文件条目

跟踪记录是一种配置，可用于将事件作为日志文件传送到您指定的 Simple Storage Service（Amazon S3）存储桶。CloudTrail 日志文件包含一个或多个日志条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序显示。

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删除文件系统标签时的 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"
}
```

配额

接下来，您可以了解使用适用 NetApp 于 ONTAP 的 Amazon FSx 时的配额。

主题

您可以提高的配额

以下是您可以增加 AWS 区域的每个 NetApp AWS 账户 ONTAP 的 Amazon FSx 配额。

资源	默认值	描述
ONTAP 文件系统	100	您可以在此账户中创建的适用于 NetApp ONTAP 的 Amazon FSx 文件系统的最大数量。
ONTAP固态硬盘存储容量	524,288	您可以在此账户中拥有的所有 Amazon FSx for NetApp ONTAP 文件系统的最大固态硬盘存储容量（以 GiB 为单位）。
ONTAP吞吐容量	10240	您可以在此账户中拥有的所有 Amazon FSx for ONTAP 文件系统的最大吞吐容量（以 MBps NetApp 为单位）。
ONTAP固态盘 IOPS	1000000	您可以在此账户中拥有的所有 Amazon FSx f NetApp or ONTAP 文件系统的最大固态硬盘 IOPS 量。
ONTAP每个文件系统的备份	10000	您可以在此账户中拥有的所有 Amazon FSx for NetApp

资源	默认值	描述
		ONTAP 文件系统的用户启动的卷备份的最大数量。

要请求提高限额

1. 打开 AWS Support 页面，登录（如有必要），然后选择 Create case (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 限额以及您希望增加到的值（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 1,024 GiB
最大 SSD 存储容量	• 横向扩展：每对 HA 512 TiB，最多 1 PiB • 放大规模：192 TiB
最大 SSD IOPS	横向扩展：

资源	每个文件系统的限额
	• 每对 HA 20,000（最多 12 对） 扩大规模： • 160,000 在美国东部（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） • 在所有其他可用 ONTAP 的 FSx AWS 区域 的地方，有 80,000 个
最低吞吐能力	• 横向扩展：每对 HA 为 3,072 Mbps • 向上扩展：128 Mbps
最大吞吐能力	横向扩展： • 73,728 Mbps 1 扩大规模： • 4,096 Mbps [2] 位于美国东部（俄亥俄州）区域、美国东部（弗吉尼亚北部）区域、美国西部（俄勒冈）地区和欧洲（爱尔兰） • 所有其他提供适用于 ONTAP 的 AWS 区域 FSx 的地方均为 2,048 Mbps
最大卷数	• 横向扩展：1,000 • 扩大规模：500
最大快照数	每卷 1,023
最大备份数	每卷 4,091

资源	每个文件系统的限额
最大 SVM 数	横向扩展： • 5 扩大规模： • 6（128Mbps 吞吐能力） • 6（256Mbps 吞吐能力） • 14（512Mbps 吞吐能力） • 14（1024Mbps 吞吐能力） • 24（2048Mbps 吞吐能力） • 24（4096Mbps 吞吐能力）
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
每个文件系统支持的最大路由数	50 [5]

Note

[1] 在具有 12 个 HA 对的横向扩展文件系统上（每个 HA 对 6,144 Mbps）。有关更多信息，请参阅 高可用性 (HA) 对。

[2] 要预置 4 Gbps 的吞吐容量，您的 FSx for ONTAP 纵向扩展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 区域有关哪些 AWS 区域支持 4,096 Mbps 吞吐容量的更多信息，请参阅。吞吐能力对性能的影响

[3] 在任何时间点，每个卷最多可以存储 1,023 个快照。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] 在任何时间点，每个卷最多可以存储 4,091 个备份。达到此限制后，必须先删除现有备份，然后才能创建新的卷备份。

[5] 您可在任何时间点为每个文件系统配置最多 50 条路由。达到此限制后，必须先删除现有路由，然后才能配置新路由。您的文件系统拥有的路由数量由其拥有的 SVM 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：（文件系统中 1 + 个 SVM ）*（与文件系统关联的路由表）。

对适用于 ONTAP 的 Amazon FSx 进行故障排除 NetApp

参阅以下部分，帮助排查在使用 FSx for ONTAP 时遇到的问题。

主题

我的多可用区文件系统处于状态 MISCONFIGURED

导致文件系统处于某种MISCONFIGURED状态的原因有很多，每种原因都有自己的分辨率，如下所示。

主题

VPC 所有者账户已禁用多可用区 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 FSx 的多可用区 VPC 共享支持。
- 所有者账户已取消共享 VPC 子网。

如果所有者账户取消了对 VPC 子网的共享，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
```

您需要联系与您共享 VPC 子网的所有者账户以解决问题。有关更多信息，为共享子网中的 ONTAP 文件系统创建 FSX请参见以获取更多信息。

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 FSx 的多可用区 VPC 共享支持。
- 所有者账户已取消共享 VPC 子网。

您需要联系与您共享 VPC 子网的所有者账户以解决问题。有关更多信息，为共享子网中的 ONTAP 文件系统创建 FSX请参见以获取更多信息。

您无法访问您的文件系统

导致无法访问您的文件系统的潜在原因有很多，每种原因都有自己的解决方案，如下所示。

主题

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，同时不要修改或删除 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 会自动分离文件系统弹性网络接口附加的所有弹性 IP 地址，该地址是可从互联网访问的公有 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 会创建端点，用于在 VPC 路由表中访问文件系统。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 会使用 VPC 的主路由表。在创建文件系统时，您可以选择性指定一个或多个路由表，供 Amazon FSx 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 AWS CloudFormation

Amazon FSx 使用基于标签的身份验证来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`。使用为 ONTAP 多可用区文件系统创建或更新 FSx 时， AWS CloudFormation 我们建议您手动添加标签。`Key: AmazonFSx; Value: ManagedByAmazonFSx`

如果您无法访问您的多可用区文件系统，请检查与文件系统关联的 VPC 路由表是否标有`Key: AmazonFSx; Value: ManagedByAmazonFSx`标记。如果不是，那么 Amazon FSx 就无法更新这些路由表，以便在发生故障转移事件时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。

拥有者的账户已取消共享 VPC 子网

如果您在已与您共享的 VPC 子网中创建文件系统，则所有者账户可能已取消共享 VPC 子网。

如果所有者账户取消了对 VPC 子网的共享，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
```

您需要联系拥有者的账户，以便他们可以与您重新共享子网。

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 数据。

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 将 SVM 加入 Microsoft Active 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 Active Directory 域控制器，因为 SVM 的 NetBIOS 名称已在使用中
- Amazon FSx 无法与 Active Directory 域控制器通信
- 由于未满足端口要求或服务账户权限，Amazon FSx 无法连接到 Active Directory
- 由于服务账户凭证无效，Amazon FSx 无法连接到 Active Directory 域控制器
- 由于服务账户凭证不足，Amazon FSx 无法连接到 Active Directory 域控制器

- Amazon FSx 无法与 Active Directory DNS 服务器或域控制器通信
- 由于 Active Directory 域名无效，Amazon FSx 无法与 Active Directory 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：

Amazon FSx is unable to establish a connection with your Active Directory. 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 Management Console、 AWS CLI 和 API 将 SVM 加入活动目录 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：

Amazon FSx is unable to establish a connection to your Active Directory. 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 从您的 SVM 取消加入活动目录 NetApp 。
2. 按照 使用 AWS Management Console、 AWS CLI 和 API 将 SVM 加入活动目录 中所述的过程，重新尝试将 SVM 加入新 AD。

Amazon FSx 无法连接到 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 AD 的 SVM 时失败，并显示以下错误消息：

Amazon FSx is unable to establish a connection with your Active Directory. 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 Management Console、 AWS CLI 和 API 将 SVM 加入活动目录 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。

Amazon FSx 无法与 Active Directory 域控制器通信

将 SVM 加入自行管理的 AD 时失败，并显示以下错误消息：

Amazon FSx is unable to communicate with your Active Directory. To fix this problem, ensure that network traffic is allowed between Amazon FSx and your domain controllers. Then reattempt to join your SVM to your Active Directory.

要解决此问题，请执行以下操作：

1. 查看 网络配置要求 中所述的要求，进行必要的更改，以启用 Amazon FSx 与 AD 之间的网络通信。
2. 当 Amazon FSx 能够与 AD 通信后，请按照 使用 AWS Management Console、 AWS CLI 和 API 将 SVM 加入活动目录 中所述的过程重新尝试将 SVM 加入 AD。

由于未满足端口要求或服务账户权限，Amazon FSx 无法连接到 Active Directory

将 SVM 加入自行管理的 AD 时失败，并显示以下错误消息：

Amazon FSx is unable to establish a connection with your Active Directory. 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. To fix this problem, update your storage virtual machine's Active Directory configuration after resolving any permissions issues with ports and service accounts, as recommended in the Amazon FSx user guide.

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位的 AD 域。
3. 更改端口权限或服务账户后，请按照 使用 AWS Management Console、 AWS CLI 和 API 将 SVM 加入活动目录 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，Amazon FSx 无法连接到 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 FSx is unable to establish a connection with your Active Directory domain controller(s) because the service account credentials provided are invalid. 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 Management Console、 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，Amazon FSx 无法连接到 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 FSx is unable to establish a connection with your Active Directory domain controller(s). This is due to either the port requirements for the Active Directory have not been met, 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 Amazon FSx 服务账户委托权限。

Amazon FSx 无法与 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：

Amazon FSx is unable to communicate with your Active Directory. This is because Amazon FSx can't reach the DNS servers provided or domain controllers for your domain. 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 NetApp ONTAP CLI，请运行以下命令在 NetApp 适用于 ONTAP 的 Amazon FSx 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。

   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 服务器上的查询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 NetApp ONTAP CLI，请运行以下命令在 NetApp 适用于 ONTAP 的 Amazon FSx 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。

   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 AD DNS 服务器的正确 IP 地址更新 SVM 的 AD 配置。

由于 Active Directory 域名无效，Amazon FSx 无法与 Active Directory 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：

Amazon FSx has detected the provided FQDN is invalid. 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 Management Console、 AWS CLI 和 API 将 SVM 加入活动目录 中所述的过程，重新尝试将 SVM 加入 AD。请务必为 AD 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：

Amazon FSx is unable to apply your Active Directory configuration. 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 AD 域管理员组的正确名称。
2. 按照 使用 AWS Management Console、 AWS CLI 和 API 将 SVM 加入活动目录 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：

Amazon FSx is unable to establish a connection with your Active Directory. 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 AD。

您无法删除存储虚拟机或卷

每个 FSx for ONTAP 文件系统可以包含一个或多个存储虚拟机（SVM），并且每个 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 Amazon FSx 控制台、API 和 CLI 删除存储虚拟机。仅当卷启用了 Amazon FSx 备份时，您才能使用 Amazon FSx 控制台、API 或 CLI 删除该卷。

为帮助保护数据和配置，Amazon FSx 会防止在某些情况下删除 SVM 和卷。如果您尝试删除 SVM 或卷，但删除请求未成功，Amazon FSx 会在控制台 AWS Command Line Interface 、AWS CLI() 和 API 中 AWS 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。

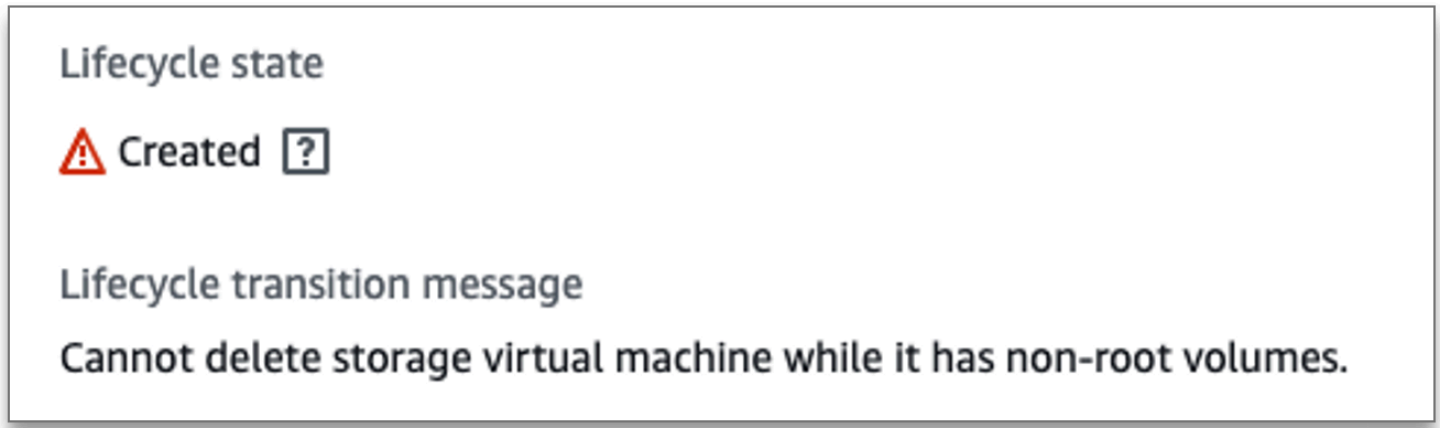
主题

- 识别失败的删除
- 删除 SVM：路由表无法访问
- 删除 SVM：对等关系
- SVM 或卷删除： SnapMirror
- 删除 SVM：启用 Kerberos 的 LIF
- 删除 SVM：其他原因
- 删除卷： FlexCache 关系

识别失败的删除

当您删除 Amazon FSX SVM 或卷时，通常在资源的 `Lifecycle` 状态变为 `DELETING` 长达几分钟后，资源才从 Amazon 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` 生命周期状态旁边显示警报图标。选中该警报图标后会显示删除失败的原因，如以下示例所示。



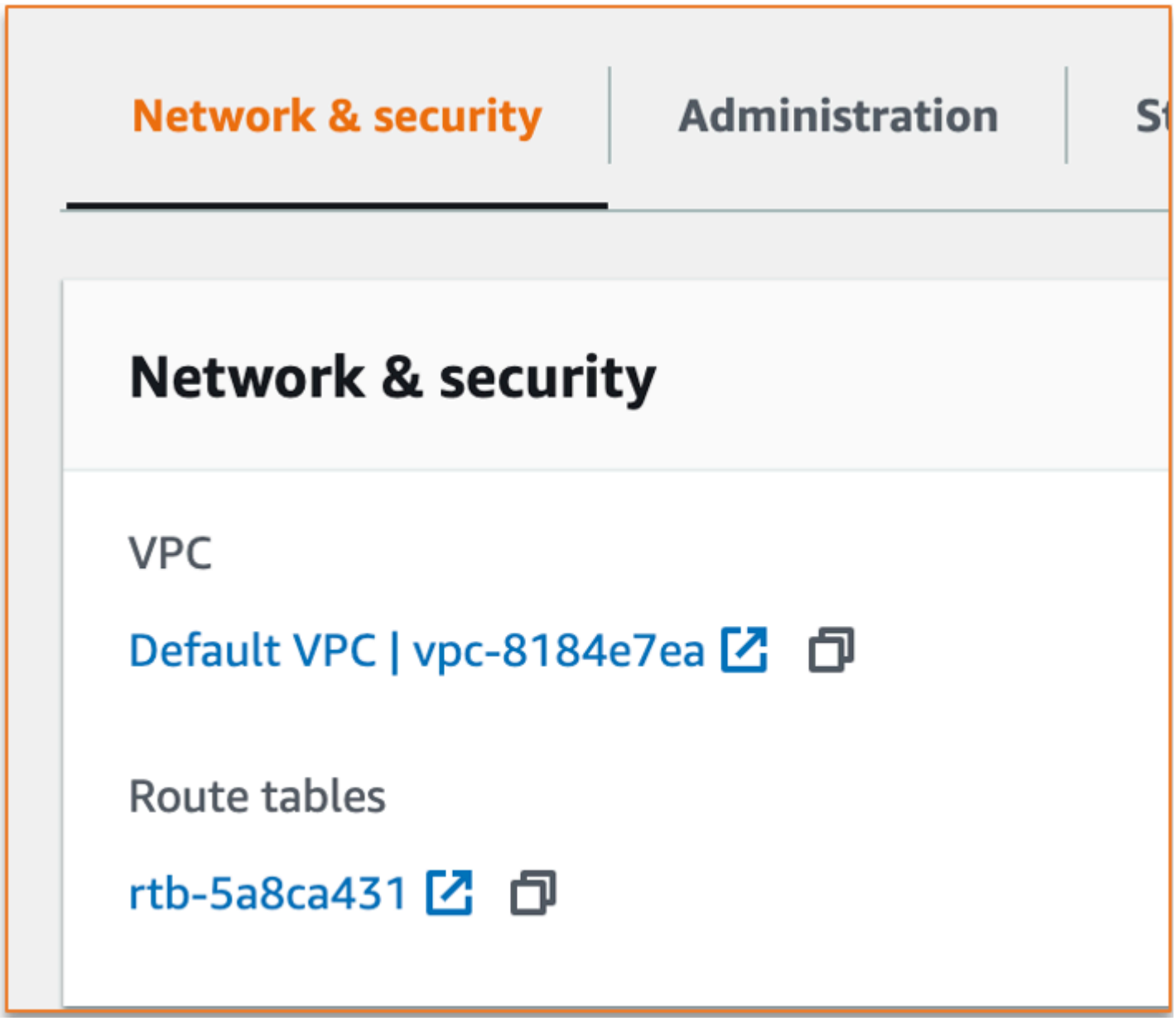
以下各节提供了 Amazon FSx 阻止 SVM 和卷删除的最常见原因，并 step-by-step 说明了如何解决这些问题。

删除 SVM：路由表无法访问

每个 FSx for ONTAP 文件系统会创建一个或多个路由表条目，以提供跨可用区的自动失效转移和故障恢复。默认情况下，这些路由表条目在 VPC 的默认路由表中创建。您可以选择性指定一个或多个非默认路由表，在其中可以创建 FSx for ONTAP 接口。Amazon FSx 会使用标签 `AmazonFSx` 标记与文件系统关联的每个路由表，如果该标签被删除，则可以阻止 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 AWS Support.
```

您可以在 Amazon FSx 控制台中，导航到文件系统的摘要页面，在网络与安全选项卡下找到文件系统的路由表：



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。此要求可防止对等的 SVM 变得不正常。如果 SVM 因对等关系而无法删除，您会看到以下 `LifecycleTransitionReason`：

Amazon FSx is unable to delete the storage virtual machine because it is part of a SVM peer or transition peer relationship. 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 for ONTAP SVM 在加入 Active Directory 时，会在 Active Directory 中创建计算机对象。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。

由于卷容量不足，每日自动备份失败

您的卷每日自动备份失败，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。根据您的情况，您可以使用以下一个或多个选项来完成此操作：

- 增加卷的存储容量
- 增加卷的快照预留空间
- 禁用快照自动删除
- 不要使用 ONTAP CLI 删除备份快照

卷容量不足

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

- 增加卷的存储容量
- 使用卷自动调整大小
- 文件系统的主存储空间已满
- 删除快照
- 增加卷的文件容量上限

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 Amazon 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 CLI 命令对 FlexVol 卷类型（即 FSx for ONTAP 的默认卷类型）执行此操作。`volume autosize` NetApp 有关更多信息，请参阅 启用音量自动调整大小。

文件系统的主存储空间已满

如果 FSx for ONTAP 文件系统的主存储空间已满，则即使某个卷显示其有足够的可用存储容量，您也无法向文件系统中的卷添加任何数据。您可以在 Amazon FSx 控制台中访问文件系统详细信息页面，在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 存储空间和 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。

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

当可用索引节点或文件指针的数量用完时，FSx for ONTAP 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，请参阅查看卷的文件容量。

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 增加卷上文件的最大数量 (ONTAPCLI)。

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过程：

- 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《适用于 ONTAP 的 Amazon FSx 用户指南》一使用 NetApp ONTAP CLI节中记录的步骤 NetApp 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：

- 将 *node_nam* e 替换为节点的名称（例如，）。FsxId01234567890abcdef-01
- 将 *svm_name* 替换为存储虚拟机的名称（例如，）。fsx
- 用卷***##### juntion_path_*** name（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 for ONTAP 中，所有网络流量都使用 e0e 接口。

使用数据包跟踪时，请注意以下几点：

- *############################/clus/ svm_name/junction-path-name*
- （可选）提供数据包跟踪的文件名。*##### filter_name#########node-name _ port-name _ yyymmdd_hhmmsss.trc*
- 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。

有关捕获数据包跟踪的更多信息，请参阅知识库中的如何在 ONTAP 9.10+ 中使用调试网络 tcpdump。NetApp

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：2024 年 4 月 30 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
为文件系统管理用户添加了对该fsxadmin-readonly 角色的支持	该fsxadmin-readonly 角色现在可供ONTAP文件系统管理用户使用，并且可用于文件系统监视应用程序，例如 NetApp Harvest。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
为 Windows 域管理用户添加了 SSH 公钥身份验证支持	现在，您可以对 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 https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/set-up-ad-auth.html。	2024 年 4 月 30 日
在横向扩展文件系统中添加了 Support 对 12 个 HA 对	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 对的文件系统可以通过 12 个高可用性 (HA) 对提供高达 72 Gbps 的吞吐容量和 2,400,000 个固态硬盘 IOPS。有关更多信息，请参阅高可用性 (HA) 对和有	2024 年 3 月 4 日

	关 ONTAP 性能的 Amazon F NetApp Sx。	
增加了对云写入模式的 Support 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
亚马逊 FSx 更新了 AmazonF、AmazonF SxFullAccess、Amazo nF SxConsoleFullAcces s、AmazonF 和 AmazonF SxReadOnlyAccess 托管政策 SxConsoleReadOnlyAccess SxServiceRolePolicy AWS	亚马逊 FSx 更新了 AmazonF、AmazonF SxFullAccess、Amazo nF SxConsoleFullAcces s、AmazonF SxReadOnl yAccess 和 AmazonF SxConsoleReadOnlyAccess 政策以添加权限SxServiceRo lePolicy 。`ec2:GetSe curityGroupsForVpc` 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

亚马逊 FSx 更新了 AmazonFSxFullAccess 和 AmazonF 托管政策 SxConsoleFullAccess AWS	亚马逊 FSx 更新了 AmazonFSxFullAccess 和 AmazonFSxConsoleFullAccess 政策以添加该操作。`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
增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，请参阅横向扩展文件系统指标。	2023 年 11 月 26 日
增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，请参阅高可用性 (HA) 对和有关 ONTAP 性能的 Amazon F NetApp Sx。	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，请参阅音量样式。	2023 年 11 月 26 日
为多可用区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 中创建多可用区文件系统。所有者账户可以在 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为 ONTAP 文件系统创建 FSx	2023 年 11 月 26 日

亚马逊 FSx 更新了 AmazonFSxFullAccess 和 AmazonF 托管政策 SxConsoleFullAccess AWS	亚马逊 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
亚马逊 FSx 更新了 AmazonFSxFullAccess 和 AmazonF 托管政策 SxConsoleFullAccess AWS	亚马逊 FSx 更新了 AmazonFSxFullAccess 和 AmazonFSxConsoleFullAccess 政策，添加了和权限。`fsx:DescribeSharedVPCConfiguration` `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 AmazonF 托管政策 SxServiceRolePolicy AWS	亚马逊 FSx 更新了 Amazon `cloudwatch:PutMetricData` F 中的权限。SxServiceRolePolicy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 Management 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 AmazonF 托管政策 SxFullAccess AWS	亚马逊 FSx 更新了 AmazonF SxFullAccess 政策，删除了`fsx:*`权限并添加了具体操作。`fsx`有关更多信息，请参阅 AmazonF SxFullAccess 政策。	2023 年 7 月 13 日
亚马逊 FSx 更新了 AmazonF 托管政策 SxConsoleFullAccess AWS	亚马逊 FSx 更新了 AmazonF SxConsoleFullAccess 政策，删除了`fsx:*`权限并添加了具体操作。`fsx`有关更多信息，请参阅 AmazonF SxConsole FullAccess 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 Managemen t Console、 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

为单可用区文件系统添加了 NVMe 读取缓存支持	于 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）创建的单可用区文件系统现在支持 NVMe 读取缓存，吞吐能力至少为 2 Gbps。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
添加了对使用 VPC 内的 IP 地址范围创建多可用区文件系统的支持	现在，您可以通过指定 VPC IP 地址范围内的端点来创建多可用区 FSx for ONTAP 文件系统。有关更多信息，请参阅创建 FSx for ONTAP 文件系统。	2022 年 11 月 28 日
添加了在多可用区文件系统上更新 VPC 路由表的支持	现在，您可以将新 VPC 路由表与现有多可用区 FSx for ONTAP 文件系统关联（添加）起来，也可以将现有 VPC 路由表与现有多可用区 FSx for 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 AWS 软件定义数据中心 (SDDC) 上的 VMware Cloud 的外部数据存储库。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 AWS 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	您可以创建单可用区 FSx for ONTAP 文件系统，这些文件系统专用于在单个可用区（AZ）内提供高可用性和耐久性。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 128 MB/s 和 256 MB/s 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。