Amazon FSx for Windows File Server

Windows 用户指南

亚马逊云科技

Amazon FSx for Windows File Server: Windows 用户指南

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

Table of Contents

FSx for Windows File Server 是什么？

Amazon FSx for Windows File Server 提供完全托管式的 Windows 文件服务器，由完全原生的 Windows 文件系统提供支持。FSx for Windows File Server 具有功能、性能和兼容性，可轻松提升企业应用程序并将其转移到Amazon Web Services 云.

Amazon FSx 支持一系列广泛的企业 Windows 工作负载，并在 Microsoft Windows Server 上构建了完全托管的文件存储。Amazon FSX 本机支持 Windows 文件系统功能和业界标准的服务器消息块 (SMB) 协议，以便通过网络访问文件存储。Amazon FSx 针对Amazon Web Services 云具有本机 Windows 兼容性、企业性能和功能，以及一致的亚毫秒级延迟。

利用 Amazon FSx 上的文件存储，Windows 开发人员和管理员今天使用的代码、应用程序和工具可以继续保持不变。适用于 Amazon FSx 的 Windows 应用程序和工作负载包括业务应用程序、主目录、Web 服务、内容管理、数据分析、软件构建设置和媒体处理工作负载。

作为一项完全托管式服务，FSx for Windows File Server 消除了设置并预置文件服务器和存储卷的管理开销。此外，Amazon FSx 可使 Windows 软件保持最新，检测并解决硬件故障，并执行备份。它还提供了与其他人的丰富集成Amazon这样的服务AmazonIAM、Amazon Directory Service for Microsoft Active Directory、Amazon WorkSpaces、Amazon Key Management Service, 和Amazon CloudTrail.

FSx for Windows File Server 资源：文件系统、备份和文件共享

亚马逊 FSx 中的主要资源是文件系统和备份. 文件系统是存储和访问文件和文件夹的地方。文件系统由一个或多个 Windows 文件服务器和存储卷组成。创建文件系统时，您可以指定存储容量（以 GiB 为单位）和吞吐量容量（以 MB/s 为单位）。创建文件系统后，可以根据需求的变化修改这些属性。有关更多信息，请参阅 管理存储容量 (p. 112) 和 管理吞吐量容量 (p. 122)。

FSx for Windows File Server 备份是文件系统一致性、高度持久且增量的。为了确保文件系统的一致性，亚马逊 FSx 在微软 Windows 中使用卷影复制服务 (VSS)。创建文件系统时，默认情况下会启用自动每日备份，您也可以随时进行额外的手动备份。有关更多信息，请参阅 使用备份 (p. 71)。

Windows 文件共享是文件系统中的一个特定文件夹（及其子文件夹），可供计算实例使用 SMB 访问该文件夹。你的文件系统已经附带了默认的 Windows 文件共享名为`\share`. 通过在 Windows 上使用共享文件夹图形用户界面 (GUI) 工具，可以根据需要创建和管理任意数量的其他 Windows 文件共享。有关更多信息，请参阅 使用微软 Windows 文件共享 (p. 49)。

可以使用文件系统的 DNS 名称或与文件系统关联的 DNS 别名来访问文件共享。有关更多信息，请参阅 管理 DNS 别名 (p. 82)。

访问文件共享

Amazon FSx 可以通过使用 SMB 协议（支持版本 2.0 到 3.1.1）的计算实例访问。你可以从 Windows Server 2008 和 Windows 7 开始的所有 Windows 版本以及当前版本的 Linux 访问你的共享。您可以在 Amazon Elastic Compute Cloud (Amazon EC2) 实例上映射您的 Amazon FSx 文件共享 WorkSpaces 实例，Amazon AppStream 2.0 个实例和 VMware 云AmazonVM。

您可以使用以下方式从本地计算实例访问文件共享Amazon Direct Connect要么Amazon VPN. 除了访问同一 VPC 中的文件共享之外，Amazon账户，以及Amazon区域作为文件系统，您还可以访问位于不同 Amazon VPC、账户或区域中的计算实例上的共享。您可以使用 VPC 对等互连或中转网关执行此操作。有关更多信息，请参阅 支持的访问方式 (p. 14)。

安全性和数据保护

Amazon FSx 提供了多个级别的安全性和合规性，以帮助确保您的数据受到保护。它使用您在中管理的密钥自动加密静态数据（对于文件系统和备份）Amazon Key Management Service(Amazon KMS)。传输中的数据也会使用 SMB Kerberos 会话密钥自动加密。已经评估符合 ISO、PCI-DSS 和 SOC 认证，并且符合 HIPAA 资格。

Amazon FSx 通过 Windows 访问控制列表 (ACL) 提供文件和文件夹级别的访问控制。它使用 Amazon Virtual Private Cloud (Amazon VPC) 安全组在文件系统级别提供访问控制。此外，它还使用 API 级别提供访问控制Amazon Identity and Access Management(IAM) 访问策略。访问文件系统的用户将通过 Microsoft Active Directory 进行身份 Amazon FSx 与Amazon CloudTrail监控和记录 API 调用，以便您查看用户对 Amazon FSx 资源采取的操作。

此外，它通过每天自动对文件系统进行高度持久的备份来保护您的数据，并允许您在任何时候进行额外的备份。有关更多信息，请参阅 Amazon FSx 的安全性 (p. 160)。

可用性与持久性

FSx for Windows File Server 提供具有两个可用性和持久性级别的文件系统。通过自动检测和解决组件故障，单可用区文件确保单个可用区 (AZ) 内的高可用性。此外，多可用区文件系统通过在一个单独的可用区域内配置和维护备用文件服务器，跨多个可用区域提供高可用性和故障转移支持。Amazon区域。要了解有关单可用区和多可用区文件系统部署的更多信息，请可用性与持久性：单可用区和多可用区文件系统 (p. 18).

Note

多可用区文件系统在中国（北京）区域中不可用。

管理文件系统

您可以使用自定义远程管理功能管理 FSx for Windows File Server 文件系统 PowerShell 命令，或者在某些情况下使用 Windows 原生 GUI。要了解有关管理 Amazon FSx 文件系统的更多信息，请参阅管理文件系统 (p. 80).

价格和性能灵活性

FSx for Windows File Server 通过提供固态硬盘 (SSD) 和硬盘驱动器 (HDD) 存储类型，为您提供了价格和性能的灵活性。HDD 存储设计用于广泛的工作负载，包括主目录、用户和部门共享以及内容管理系统。SSD 存储设计用于最高性能和最敏感延迟的工作负载，包括数据库、媒体处理工作负载和数据分析应用程序。

借助 FSx for Windows File Server，您可以独立配置文件系统存储和吞吐量，以实现正确的成本和性能组合。您可以修改文件系统的存储和吞吐量容量以满足不断变化的工作负载需求，这样您只需为所需的容量付费。有关更多信息，请参阅 使用亚马逊 FSx 优化成本 (p. 21)。

Amazon FSx 的定价

有了 Amazon FSx，您就无前期硬件或软件成本。您只需为使用的资源付费，没有最低承诺、设置成本或额外费用。有关与服务相关联的定价和费用的信息，请参阅Amazon FSx for Windows File Server 定价.

假设

要使用亚马逊 FSx，您需要Amazon具有 Amazon EC2 实例的账户， WorkSpaces 实例， AppStream 2.0 实例，或者在 VMware Cloud 中运行的虚拟机Amazon受支持类型的环境。

在本指南中，我们做出以下假设：

- 如果您使用的是 Amazon EC2，我们假设您熟悉 Amazon EC2。有关如何使用 Amazon EC2 的更多信息，请参阅Amazon Elastic Compute Cloud 文档.
- 如果您使用的是 WorkSpaces，我们假定您熟悉 WorkSpaces。有关如何使用 WorkSpaces 的更多信息，请参阅亚马逊 WorkSpaces 用户指南.
- 如果您在使用 VMware CloudAmazon，我们假定您熟悉。有关更多信息，请参阅 。启用 VMware CloudAmazon.
- 我们假定您熟悉 Microsoft Active Directory 概念。

先决条件

要创建 Amazon FSx 文件系统，您需要以下内容：

- 网络 ACL 和安全组都允许 (因此可到达您的实例) 的发起 ping 的Amazon具有创建 Amazon FSx 文件系统和 Amazon EC2 实例所需权限的账户。有关更多信息，请参阅 设置 (p. 5)。
- 基于您要与 Amazon FSx 文件系统关联的 Amazon VPC 服务，在虚拟私有云 (VPC) 中运行 Microsoft Windows Server 的 Amazon EC2 实例。有关创建一个程序包的信息，请参阅Amazon EC2 Windows 实例入门中的Amazon EC2 用户指南（适用于 Windows 实例）。
- 亚马逊 FSx 与微软 Active Directory 合作执行用户身份验证和访问控制。您在创建 Amazon FSx 文件系统时将其加入微软 Active Directory。有关更多信息，请参阅 在 FSx for Windows File Server 中使用 Microsoft Active Directory (p. 22)。
- 本指南假设您尚未根据 Amazon VPC 服务更改 VPC 默认安全组的规则。如果有，则需要确保添加必要的规则，以允许从 Amazon EC2 实例到 Amazon FSx 文件系统的网络流量。有关更多信息，请参阅 Amazon FSx 的安全性 (p. 160)。
- 安装和配置Amazon Command Line Interface(Amazon CLI)。支持的版本为 1.9.12 及更新版本。有关更多信息，请参阅 。安装、更新和卸载Amazon CLI中的Amazon Command Line Interface用户指南。

  Note

  您可以检查的版本Amazon CLI您使用的是`aws --version`命令。

Amazon FSx for Windows File Server 论坛

如果您在使用 Amazon FSx 时遇到问题，请使用论坛.

您是 Amazon FSx 的新用户吗？

如果您是首次接触 Amazon FSx 的用户，我们建议您按顺序阅读以下内容：

1. 如果您已准备好创建第一个 Amazon FSx 文件系统，请尝试开始使用 Amazon FSx (p. 7).
2. 有关性能的信息，请参阅 FSx for Windows File Server 性能 (p. 141)。
3. 有关 Amazon FSx 安全性详细信息，请参阅Amazon FSx 的安全性 (p. 160).
4. 有关 Amazon FSx API 的信息，请参阅Amazon FSx API 参考.

设置

首次使用 Amazon FSx 前，请完成以下任务：

1. 注册Amazon (p. 5)
2. 创建 IAM 用户 (p. 5)

注册Amazon

在注册 Amazon Web Services ()Amazon)，您的Amazon Web Services 账户自动注册所有服务Amazon，包括亚马逊 FSx。

如果您已有Amazon Web Services 账户，请跳到下一个任务。如果您还没有 Amazon Web Services 账户，请使用以下步骤创建。

创建 Amazon Web Services 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，您将接到一通电话，要求您使用电话键盘输入一个验证码。

请记下您的Amazon Web Services 账户账号，因为在下一个任务中需要使用该账号。

创建 IAM 用户

中的服务AmazonAmazon FSx（例如）要求您在访问时提供凭证，以便服务能够确定您是否有权访问其资源。Amazon建议不要使用您的根凭证。Amazon Web Services 账户提出请求。而应创建一个 Amazon Identity and Access Management (IAM) 用户并向该用户授予完全访问权限。我们称作这些用户管理员用户。

您可以使用管理员用户凭证而不是您账户的根凭证来与交互。Amazon并执行任务，例如创建用户并向他们授予权限。有关更多信息，请参阅 。根账户凭证与 IAM 用户凭证中的Amazon一般参考和IAM 最佳实践中的IAM 用户指南.

如果你注册了Amazon但尚未为自己创建一个 IAM 用户，您可以使用 IAM 管理控制台自行创建。

自行创建管理员用户并将该用户添加到管理员组（控制台）

1. 选择 Root user（根用户）并输入您的 Amazon Web Services 账户 电子邮件地址，以账户拥有者身份登录 IAM 控制台。在下一页上，输入您的密码。

   Note

   强烈建议您遵守以下使用 **`Administrator`** IAM 用户的最佳实践，妥善保存根用户凭证。只在执行少数账户和服务管理任务时才作为根用户登录。
2. 在导航窗格中，选择 Users（用户），然后选择 Add users（添加用户）。
3. 对于 User name（用户名），输入 **`Administrator`**。
4. 选中 Amazon Web Services Management Console access (Amazon Web Services Management Console 管理控制台访问）旁边的复选框。然后选择自定义密码，并在文本框中输入新密码。

5. （可选）默认情况下，Amazon要求新用户在首次登录时创建新密码。您可以清除 User must create a new password at next sign-in（用户必须在下次登录时创建新密码）旁边的复选框以允许新用户在登录后重置其密码。
6. 选择 Next:。Permissions (下一步：权限)。
7. 在设置权限下，选择将用户添加到组。
8. 选择创建组。
9. 在 Create group（创建组）对话框中，对于 Group name（组名称），输入 **`Administrators`**。
10. 选择 Filter policies（筛选策略），然后选择 Amazon managed - job function（Amazon 托管 – 工作职能）以筛选表内容。
11. 在策略列表中，选中 AdministratorAccess 的复选框。然后选择 Create group（创建组）。

    Note

    您必须先激活 IAM 用户和角色对账单的访问权限，然后才能使用 `AdministratorAccess` 权限访问 Amazon Billing and Cost Management 控制台。为此，请按照"向账单控制台委派访问权限"教程第 1 步中的说明进行操作。
12. 返回到组列表中，选中您的新组所对应的复选框。如有必要，选择 Refresh（刷新）以在列表中查看该组。
13. 选择 Next:。标签。
14. (可选) 通过以键值对的形式附加标签来向用户添加元数据。有关在 IAM 中使用标签的更多信息，请参阅 IAM 用户指南中的标记 IAM 实体。
15. 选择 Next:。审核以查看要添加到新用户的组成员资格的列表。如果您已准备好继续，请选择 Create user（创建用户）。

您可使用这一相同的流程创建更多组和用户，并允许您的用户访问 Amazon Web Services 账户 资源。要了解有关使用策略限制用户对特定 Amazon 资源的权限的信息，请参阅访问管理和示例策略。

要以此新 IAM 用户的身份登录，请先从注销Amazon Web Services Management Console. 然后使用以下 URL，其中你的 _aws_count _id是你的Amazon不包含连字符的账号（例如，如果您的Amazon账号为`1234-5678-9012`，您的Amazon Web Services 账户ID 是`123456789012`)。

```
https://your_aws_account_id.signin.aws.amazon.com/console/
```

输入您刚创建的 IAM 用户名和密码。登录后，导航栏显示 your_user_name@your_aws_account_id。

如果您不希望您的登录页面 URL 包含您的Amazon Web Services 账户ID，你可以创建账户别名。为此，请从 IAM 控制面板中，选择创建账户别名然后输入别名，例如您的公司名称。要在创建账户别名后登录，请使用以下 URL。

```
https://your_account_alias.signin.aws.amazon.com/console/
```

要为您的账户验证 IAM 用户的登录链接，请打开 IAM 控制台并在控制面板的 Amazon Account Alias (亚马逊云科技账户别名) 下进行检查。

下一步

开始使用 Amazon FSx (p. 7)

开始使用 Amazon FSx

接下来，您可以了解如何开始使用 Amazon FSx。此入门练习包括以下步骤。

主题

第 1 步：创建文件系统

要创建 Amazon FSx 文件系统，您必须创建您的 Amazon Elastic Compute Cloud (Amazon EC2) 实例和 Amazon Directory Service目录。如果您还没有设置该设置，请参阅演练 1：开始使用的先决条件 (p. 145).

创建您的第一个文件系统

1. 从打开 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 FSx for Windows file Server，然后选择下一步。显示创建文件系统页面。
4. 在文件系统详细信息部分中，为您的文件系统提供一个名称。命名文件系统时，您可以更轻松地查找和管理它们。您最多可以使用 256 个 Unicode 字母、空格和数字，以及特殊字符 +-=。_:/
5. 适用于Deployment type (部署类型)选择多可用区要么单可用区.

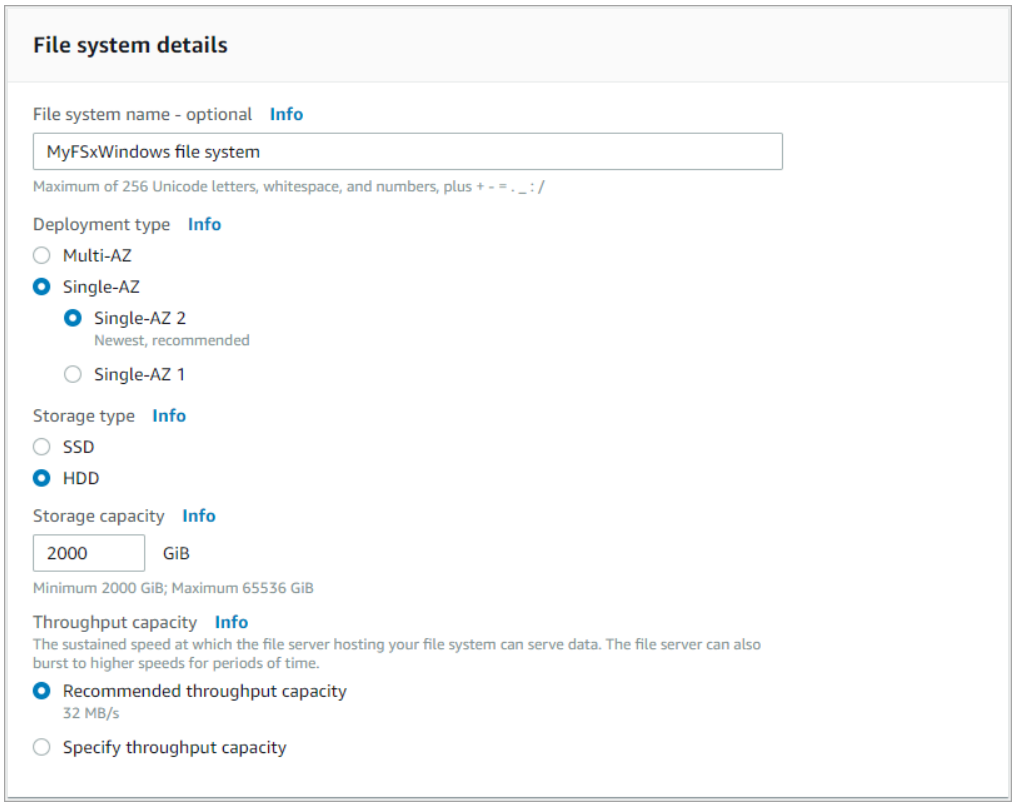
   Note

   多可用区文件系统在中国（北京）区域中不可用。

   - 选择多可用区以部署容忍可用区不可用的文件系统。此选项支持 SSD 和硬盘存储。
   - 选择单可用区部署部署在单个可用区中的文件系统。单可用区 2是最新一代的单可用区文件系统，支持 SSD 和 HDD 存储。

   有关更多信息，请参阅 可用性与持久性：单可用区和多可用区文件系统 (p. 18)。

   下图显示了中可用的所有配置选项。文件系统详情部分。



6. 适用于存储类型，您可以选择任一选择SSD要么HDD.

   FSx for Windows File Server 提供固态硬盘 (SSD) 和硬盘驱动器 (HDD) 存储类型。SSD存储设计用于最高性能和最敏感延迟的工作负载，包括数据库、媒体处理工作负载和数据分析应用程序。HDD存储设计用于广泛的工作负载，包括主目录、用户和部门文件共享以及内容管理系统。有关更多信息，请参阅使用存储类型优化成本 (p. 21)。

7. 适用于存储容量中，输入文件系统的存储容量（以 GiB 为单位）。如果您使用的是 SSD 存储，请输入 32—65,536 之间的任意整数。如果您使用的是硬盘存储，请输入 2,000 到 65,536 之间的任意整数。创建文件系统后，您可以随时根据需要增加存储容量。有关更多信息，请参阅管理存储容量 (p. 112)。

8. 保持吞吐量容量设置为原定设置。吞吐量容量是托管文件系统的文件服务器可以提供数据的持续速度。这些区域有：建议吞吐量容量设置基于您选择的存储容量。如果您需要超过建议的吞吐容量，请选择指定吞吐量容量，然后选择一个值。有关更多信息，请参阅FSx for Windows File Server 性能 (p. 141)。

   Note

   如果要启用文件访问审核，则必须选择 32 MB/s 或更高的吞吐量。有关更多信息，请参阅审计文件访问 (p. 89)。

   创建文件系统后，您可以随时根据需要修改吞吐量。有关更多信息，请参阅管理吞吐量容量 (p. 122)。

9. 在网络与安全部分中，选择要与文件系统关联的 Amazon VPC。对于本入门练习，请选择您为您选择的同一个 Amazon VPCAmazon Directory Service目录和您的 Amazon EC2 实例。

10. 适用于VPC 安全组，您的默认 Amazon VPC 的默认安全组已添加到控制台中的文件系统中。如果您没有使用默认安全组，请确保将以下规则添加到用于本练习的安全组中：

    a. 添加以下入站和出站规则以允许使用以下端口。

规则	端口
UDP	53、88、123、389、464
TCP	53、88、135、389、445、464、636、3268、3269、5985、9389、49152-65

添加与要从中访问文件系统的客户端计算实例关联的 IP 地址或安全组 ID。

b. 添加出站规则以允许所有流量到达要加入文件系统的 Active Directory。为此，请执行以下操作之一：

- 允许出站流量到与您的关联的安全组 IDAmazon托管 AD 目录。
- 允许出站流量到与自我管理的 Active Directory 域控制器关联的 IP 地址。

Note

在某些情况下，您可能修改了您的规则Amazon Managed Microsoft AD默认设置中的安全组。如果是，请确保此安全组具有所需的入站规则，以允许来自 Amazon FSx 文件系统的流量。有关所需入站规则的更多信息，请参阅Amazon Managed Microsoft AD先决条件中的Amazon Directory Service管理指南.

有关更多信息，请参阅 使用 Amazon VPC 进行文件系统访问控制 (p. 163)。

11. 如果您有多可用区部署（请参阅步骤 5），请选择首选子网主文件服务器的值和备用子网备用文件服务器的值。多可用区部署有一个主文件服务器和备用文件服务器，每个服务器都在自己的可用区和子网中。
12. 适用于Windows 身份验证，您可进行以下选择：

如果你想将文件系统加入由管理的 Microsoft Active Directory 域Amazon，选择Amazon托管 Microsoft Active Directory，然后选择您的Amazon Directory Service列表中的目录。有关更多信息，请参阅 在 FSx for Windows File Server 中使用 Microsoft Active Directory (p. 22)。

如果你想将文件系统加入自我管理的 Microsoft Active Directory 域，请选择自助管理的 Microsoft Active Directory，并为您的活动目录提供以下详细信息。

- Active Directory 的完全限定域名。

  Important

  对于单可用区 2 和所有多可用区文件系统，Active Directory 域名不能超过 47 个字符。此限制适用于Amazon托管和自行管理 Active Directory 域名。
  Amazon FSx 需要直接连接或内部流量到您的 DNS IP 地址。不支持通过互联网网关进行连接。相反，请使用 VPN、VPC 对等互连、直接 Connect 或中转网关关联。

- DNS 服务器 IP 地址— 域的 DNS 服务器的 IPv4 地址

  Note

  您的 DNS 服务器必须启用 EDNS（DNS 的扩展机制）。如果 EDNS 被禁用，您可能无法创建 Amazon FSx 文件系统。

- 服务账户用户名— 现有 Active Directory 中服务账户的用户名。切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)— 要加入文件系统的组织单位的可分辨路径名。
- （可选）委派文件系统管理员组— Active Directory 中可以管理文件系统的组的名称。默认组是 “域管理员”。

13. 对于加密，请保留 aws/fsx (原定设置)的原定设置加密密钥设置。
14. 适用于可选的审核，默认情况下，禁用文件访问审计。有关启用和配置文件访问审核的信息，请参阅创建文件系统时启用文件访问审核（控制台）(p. 92).
15. 适用于访问权限-可选中，输入要与文件系统关联的所有 DNS 别名。必须将每个别名格式化为完全限定域名 (FQDN)。有关更多信息，请参阅 管理 DNS 别名 (p. 82)。
16. 适用于Backup 和维护-可选，保留默认设置。
17. 适用于标签-可选的中，输入键和值以将标签添加到您的文件系统。标签是帮助您管理、筛选和搜索文件系统的区分大小写的键/值对。

    选择 Next（下一步）。
18. 检查创建文件系统页面上显示的文件系统配置。请注意创建文件系统后可以修改的文件系统设置，以供参考。选择 Create file system。
19. 在 Amazon FSx 创建文件系统后，在文件系统控制面板。选择Attach，并注意文件系统的完全限定域名。您将在后面的步骤中需要它。

第 2 步：将您的文件共享映射到运行 Windows Server 的 EC2 实例

现在，您可以将亚马逊 FSx 文件系统挂载到您的基于 Microsoft Windows 的 Amazon EC2 实例加入到 Amazon Directory Service目录。文件共享的名称与文件系统的名称不同。

使用 GUI 在 Amazon EC2 Windows 实例上映射文件共享

1. 在 Windows 实例上挂载文件共享之前，必须启动 EC2 实例并将其加入到Amazon Directory Service for Microsoft Active Directory. 要执行此操作，请从Amazon Directory Service管理指南：

   - 无缝加入 Windows EC2 实例
   - 手动加入 Windows 实例
2. 连接到您的实例。有关更多信息，请参阅适用于 Windows 实例的 Amazon EC2 用户指南中的连接您的 Windows 实例。
3. 连接后，打开文件资源管理器。
4. 在导航窗格中，打开的上下文 (右键单击) 菜单网络然后选择映射网络驱动器.
5. 选择你选择的驱动器盘符Drive.
6. 您可以使用 Amazon FSx 分配的默认 DNS 名称或使用自己选择的 DNS 别名来映射文件系统。本过程介绍使用默认 DNS 名称映射文件共享。如果要使用 DNS 别名映射文件共享，请参阅演练 5：使用 DNS 别名访问文件系统 (p. 152).

   适用于文件夹中，输入文件系统 DNS 名称和共享名称。默认的亚马逊 FSx 共享称为`\share`. 您可以在 Amazon FSx 控制台中找到 DNS 名称，https://console.aws.amazon.com/fsx/、Windows 文件服务器 > 网络和安全部分，或者在响应中CreateFileSystem要么DescribeFileSystemsAPI 命令。

   - 对于加入到的单可用区文件系统Amazon托管微软活动目录，DNS 名称如下所示。

     ```
     fs-0123456789abcdef0.ad-domain.com
     ```
   - 对于加入到自管 Active Directory 的单可用区文件系统以及任何多可用区文件系统，DNS 名称如下所示。

     ```
     amznfsxaa11bb22.ad-domain.com
     ```

   例如，输入 `\\fs-0123456789abcdef0.ad-domain.com\share`。

7. 选择是否应该共享文件登录时重新连接，然后选择Finish.

第 3 步：将数据写入文件共享

现在您已将文件共享映射到实例，可以像 Windows 环境中的任何其他目录一样使用文件共享。

将数据写入文件共享

1. 打开记事本文本编辑器。
2. 在文本编辑器中写一些内容。例如：`World Hello, World!`
3. 将该文件保存到您的文件共享的驱动器盘符。
4. 使用文件资源管理器，导航到文件共享并找到刚保存的文本文件。

第 4 步：备份文件系统

现在，您已有机会使用 Amazon FSx 文件系统及其文件共享，可以对其进行备份。默认情况下，每日备份会在文件系统的 30 分钟备份窗口期间自动创建。但是，您可以随时创建用户启动的备份。备份会产生与之关联的额外成本。有关备份定价的更多信息，请参阅定价.

从控制台创建文件系统的备份

1. 从打开 Amazon FSx 控制台https://console.aws.amazon.com/fsx/.
2. 在控制台控制面板中，选择您为本练习创建的文件系统的名称。
3. 从概述选项卡，选择文件系统创建备份.
4. 在创建备份打开的对话框中，提供备份的名称。此名称最多可包含 256 个 Unicode 字母，包括空格、数字和以下特殊字符：+-=。_:/
5. 选择 Create backup (创建备份)。
6. 要在列表中查看所有备份，以便恢复文件系统或删除备份，请选择备份.

创建新备份时，其状态将设置为创建正在创建的过程中。这可能需要几分钟的时间。当备份可用于使用时，其状态将更改为可用.

第 5 步：使用将文件传输到 Amazon FSx for Windows File ServerAmazon DataSync

现在您已经有了适用于 Windows 文件服务器的 Amazon FSx 的正常设置，您可以使用Amazon DataSync在现有文件系统与 Amazon FSx for Windows File Server 之间传输文件。

Amazon DataSync是数据传输服务，可以简化、自动完成并加快在本地存储系统之间移动和复制数据的过程和Amazon通过 Internet 或进行的存储服务或Amazon Direct Connect. DataSync 可以传输您的文件数据以及文件系统元数据，例如，所有权、时间戳和访问权限。

在 DataSync 中，位置对于 Amazon FSx for Windows File Server 而言，是 FSx for Windows File Server 的终端节点。您可以在 Amazon FSx for Windows 的位置和其他文件系统的位置之间传输文件。想要了解有关信息，请参阅使用位置中的Amazon DataSync用户指南.

使用服务器消息块 (SMB) 协议，DataSync for Windows File Server 访问 FSx for Windows File Server。它通过使用您在 DataSync 控制台或Amazon CLI.

开始前的准备工作

对于此步骤，我们假定您具有以下内容：

- 您可以从其中传输文件的源位置。如果此源是 Amazon EFS 文件系统，则需要可以通过 NFS 版本 3、版本 4 或 4.1 访问该源文件系统。示例文件系统包括位于本地数据中心的文件系统、自主管理型云端文件系统和 Amazon FSx for Windows File 系统。
- 将文件传输到的目标 文件系统。示例文件系统包括位于本地数据中心的文件系统、自主管理型云端文件系统和 Amazon FSx for Windows File 系统。如果没有 FSx for Windows File Server 文件系统，请创建一个文件系统。有关更多信息，请参阅 开始使用 Amazon FSx (p. 7)。
- 满足 DataSync 要求。要了解更多信息，请参阅DataSync 的要求中的Amazon DataSync用户指南.

如果您具有前面的内容，您可以按如下所述开始转移。

使用 DataSync 传输文件的基本步骤

要使用 DataSync 将文件从源位置复制到目标位置，请执行以下基本步骤：

- 在您的环境中下载并部署代理，然后激活。
- 创建并配置源和目标位置。
- 创建并配置任务。
- 运行任务，将文件从源传输到目标。

要了解如何将文件从现有本地文件系统传输到 FSx for Windows File Server，请参阅入门 DataSync中的Amazon DataSync用户指南.

如需了解如何将文件从现有云端文件系统传输到 FSx for Windows File Server，请参阅部署 DataSync 将代理部署为 Amazon EC2 实例中的Amazon DataSync用户指南.

第 6 步：清理 资源

完成本练习后，您应执行如下步骤以清理您的资源并保护您的Amazonaccount.

清除资源

1. 在 Amazon EC2 控制台上，终止您的实例。有关更多信息，请参阅 。终止您的实例中的适用于 Windows 实例的 Amazon EC2 用户指南。
2. 在 Amazon FSx 控制台上，删除文件系统。所有自动备份都将自动删除。但是，您仍然需要删除手动创建的备份。下面概括了此过程：

   a. 从打开 Amazon FSx 控制台https://console.aws.amazon.com/fsx/.
   b. 在控制台控制面板中，选择您为本练习创建的文件系统的名称。
   c. 对于 Actions，选择 Delete file system。
   d. 在删除文件系统在打开的对话框中，决定您是否要创建最终备份。如果这样做，请为最终备份提供一个名称。任何自动创建的备份也将被删除。

      Important

      可以通过备份创建新的文件系统。作为最佳实践，我们建议您创建最终备份。如果您发现在一段时间后不需要它，则可以删除此备份和其他手动创建的备份。

   e. 在中输入要删除的文件系统的 ID文件系统 ID。

f. 选择删除文件系统.
g. 文件系统现在被删除，其在仪表板中的状态更改为删除中. 删除文件系统后，它将不会再出现在控制面板中。
h. 现在，您可以删除为文件系统手动创建的任何备份。在左侧导航中，选择备份.
i. 从控制面板中，选择具有相同备份的任何备份文件系统 ID作为您删除的文件系统，然后选择删除备份.
j. 这些区域有：删除备份打开对话框。保持选中所选备份 ID 的复选框，然后选择删除备份.

您的 Amazon FSx 文件系统和相关的自动备份现在已被删除。

3. 如果你创建了Amazon Directory Service中的本练习的目录演练 1：开始使用的先决条件 (p. 145)，您可以将其删除。有关更多信息，请参阅 。删除目录中的Amazon Directory Service管理指南。

Amazon FSx 文件系统状态

您可以使用 Amazon FSx 控制台查看亚马逊 FSx 文件系统的状态Amazon CLI命令描述文件系统或者 API 操作DescribeFileSystems.

文件系统状态	描述
AVAILABLE	文件系统处于正常状态，可访问且可以使用。
CREATING	亚马逊 FSx 正在创建一个新的文件系统。
DELETING	Amazon FSx 正在删除现有文件系统。
UPDATING	文件系统正在进行客户发起的更新。
配置错误	由于 Active Directory 环境发生变化，文件系统处于受损状态。您的文件系统当前不可用或面临丧失可用性的风险，备份可能无法成功。有关恢复可用性的信息，请参阅文件系统处于错误配置状态 (p. 195).
错误配置 _ 不可用	由于 Active Directory 环境发生了变化，文件系统当前不可用。有关恢复可用性的信息，请参阅文件系统处于错误配置状态 (p. 195).
FAILED	• 文件系统已失败，Amazon FSx 无法恢复它。 • 创建新文件系统时，Amazon FSx 无法创建新的文件系统。

Amazon FSx for Windows File Server 的支持的客户、访问方法和环境

您可以使用两者中的各种受支持的客户端和方法访问 Amazon FSx 文件系统Amazon以及本地环境。

主题

支持的客户

Amazon FSx 支持从各种计算实例和操作系统连接到您的文件系统。它通过支持通过服务器消息块 (SMB) 协议（2.0 至 3.1.1 版）进行访问来实现这一目标。

以下Amazon支持计算实例与 Amazon FSx 一起使用：

- Amazon Elastic Compute Cloud (Amazon EC2) 实例，这些实例包括微软 Windows、Mac、Amazon Linux 和 Amazon Linux 2 实例。有关更多信息，请参阅 访问文件共享 (p. 49)。
- Amazon Elastic Container Service (Amazon ECS) 容器。有关更多信息，请参阅 。FSx for Windows File Server 卷中的Amazon Elastic Container Server 开发者指南.
- WorkSpaces 实例 — 要了解更多信息，请参阅Amazon博客帖子将 FSx for Windows File Server 与 Amazon WorkSpaces 结合使用.
- 亚马逊 AppStream 2.0 实例 — 要了解更多信息，请参阅Amazon博客帖子将 Amazon FSx 与 Amazon 结合使用 AppStream 2.0.
- 在 VMware Cloud 中运行的虚拟机Amazon环境 — 要了解更多信息，请参阅Amazon博客帖子在 VMware 云中使用 FSx 存储和共享适用于 Windows 文件服务器的文件Amazon环境.

支持以下操作系统与 Amazon FSx 结合使用：

- Windows Server 2008、Windows Server 2008 R2、Windows Server 2012、Windows Server 2016 和 Windows Server 2019。
- Windows Vista、Windows 7、窗户 8、窗户 8.1 和 Windows 10（包括 WorkSpaces 的 Windows 7 和 Windows 10 桌面体验）。
- Linux，使用`cifs-utils`工具。
- macOS

支持的访问方式

您可以将以下访问方法和方法与 Amazon FSx 结合使用。

使用默认 DNS 名称访问文件系统

FSx for Windows File Server 为每个文件系统提供域名系统 (DNS) 名称。您可以使用此 DNS 名称将计算实例上的驱动器盘符映射到 Amazon FSx 文件共享，以访问 FSx for Windows 文件服务器文件系统。要了解更多信息，请参阅 使用微软 Windows 文件共享 (p. 49)。

Important

如果您使用微软 DNS 作为默认 DNS，则 Amazon FSx 仅为文件系统注册 DNS 记录。如果您使用的是第三方 DNS，则必须为 Amazon FSx 文件系统手动设置 DNS 条目。有关选择要用于文件系统的正确 IP 地址的信息，请参阅获取用于 DNS 的正确文件系统 IP 地址 (p. 46).

要查找 DNS 名称：

- 在亚马逊 FSx 控制台中，选择文件系统，然后选择详细信息. 查看 DNS 名称网络和安全部分。
- 或者，在回复中查看CreateFileSystem要么DescribeFileSystemsAPI 命令。

对于所有单可用区域文件系统，都加入了Amazon托管微软活动目录，DNS 名称如下所示：`fs-0123456789abcdef0.ad-dns-domain-name`

对于加入自管 Active Directory 的所有单可用区文件系统以及任何多可用区域文件系统，DNS 名称如下所示：`amznfsxaa11bb22.ad-domain.com`

将 DNS 名称用于 Kerberos 身份验证

我们建议您在传输过程中将基于 Kerberos 的身份验证和加密与 Amazon FSx 一起使用。Kerberos 为访问文件系统的客户端提供了最安全的身份验证。要为 SMB 会话启用基于 Kerberos 的身份验证和加密传输中的数据，请使用 Amazon FSx 提供的文件系统的 DNS 名称访问您的文件系统。

如果你在你之间配置了外部信任Amazon使用 Amazon FSx Remote 托管 Microsoft Active Directory 和本地 Active Directory PowerShell 使用 Kerberos 身份验证，您必须在客户端上为林搜索顺序配置本地组策略。有关更多信息，请参阅 。配置 Kerberos 森林搜索顺序 (KFSO)在 Microsoft 文档中。

使用 DNS 别名访问文件系统

FSx for Windows File Server 为您可以用来访问文件共享的每个文件系统提供 DNS 名称。您还可以通过为 Windows 文件服务器文件系统的 FSx 注册别名来启用对 Amazon FSx 的 DNS 名称的访问权限，而不是 Amazon FSx 创建的默认 DNS 名称。

使用 DNS 别名，您可以将 Windows 文件共享数据移动到亚马逊 FSx，然后继续使用现有 DNS 名称访问 Amazon FSx 上的数据。DNS 别名还允许您使用有意义的名称，从而更轻松地管理工具和应用程序以连接到 Amazon FSx 文件系统。有关更多信息，请参阅 管理 DNS 别名 (p. 82)。

将 DNS 别名与 Kerberos 身份验证结合使用

我们建议您在传输过程中将基于 Kerberos 的身份验证和加密与 Amazon FSx 一起使用。Kerberos 为访问文件系统的客户端提供了最安全的身份验证。要为使用 DNS 别名访问 Amazon FSx 的客户端启用 Kerberos 身份验证，您必须添加与 Amazon FSx 文件系统 Active Directory 计算机对象上的 DNS 别名对应的服务主体名称 (SPN)。

通过在 Active Directory 中设置以下组策略对象 (GPO)，您可以选择强制使用 DNS 别名访问文件系统的客户端使用 Kerberos 身份验证和加密：

- 限制 NTLM: 将 NTLM 流量传出到远程服务器-使用此策略设置可拒绝或审核从计算机到运行 Windows 操作系统的任何远程服务器的传出 NTLM 流量。
- 限制 NTLM: 为 NTLM 验证添加远程服务器例外-使用此策略设置创建允许客户端设备使用 NTLM 身份验证的远程服务器的例外列表，如果网络安全：限制 NTLM: 将 NTLM 流量传出到远程服务器已配置策略设置。

有关更多信息，请参阅 演练 5：使用 DNS 别名访问文件系统 (p. 152)。

使用 FSx for Windows File Server 文件系统和 DFS 命名空间

FSx for Windows File Server 支持使用微软分布式文件系统 (DFS) 命名空间。您可以使用 DFS 命名空间将多个文件系统上的文件共享组织到一个用于访问整个文件数据集的通用文件夹结构（命名空间）中。您可以使用 DFS 命名空间中的名称来访问 Amazon FSx 文件系统，方法是将其链接目标配置为文件系统的 DNS 名称。有关更多信息，请参阅 使用 DFS 命名空间对多个文件系统进行分组 (p. 131)。

支持的环境

您可以从与文件系统位于同一 VPC 中的资源访问文件系统。有关更多信息和详细说明，请参阅演练 1：开始使用的先决条件 (p. 145).

您还可以从本地资源和不同 VPC 中的资源访问 2019 年 2 月 22 日之后创建的文件系统，Amazon账户，或Amazon区域。下表说明了 Amazon FSx 支持从每个受支持环境中客户端访问的环境，具体取决于文件系统的创建时间。

位于... 的客户	访问 2019 年 2 月 22 日之前创建的文件系统	访问 2020 年 12 月 17 日之前创建的文件系统	访问 2020 年 12 月 17 日之后创建的文件系统
在其中创建文件系统的子网	✓	✓	✓
创建文件系统的 VPC 的主 CIDR 块	✓	✓	✓
创建文件系统的 VPC 的辅助 CIDR		中有 IP 地址的客户端RFC 1918私有 IP 地址范围： • 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	IP 地址超出以下 CIDR 块范围的客户端：198.19.0.0/16
其他 cIDR 或对等互连网络			

> **Note**
>
> 在某些情况下，您可能希望使用非私有 IP 地址范围从本地访问 2020 年 12 月 17 日之前创建的文件系统。为此，请从文件系统的备份中创建一个新的文件系统。有关更多信息，请参阅 使用备份 (p. 71)。

接下来，你可以找到有关如何从本地和不同 VPC 访问你的 FSx for Windows 文件服务器文件系统的信息，Amazon账户，或Amazon地区。

从本地访问 FSx for Windows File Server 文件系统

FSx for Windows File Server 支持使用Amazon Direct Connect要么Amazon VPN以便从本地计算实例访问文件系统。有关支持Amazon Direct Connect中，FSx for Windows File Server 使您能够从本地环境通过专用网络连接访问文件系统。有关支持Amazon VPN中，FSx for Windows File Server 使您能够通过安全的私有隧道从本地设备访问文件系统。

将本地环境连接到与 Amazon FSx 文件系统关联的 VPC 之后，您可以使用其 DNS 名称或 DNS 别名访问您的文件系统。你这样做就像从 VPC 内的计算实例那样。有关 Amazon Direct Connect 的更多信息，请参阅

Amazon Direct Connect 用户指南。有关设置的更多信息Amazon VPN连接，请参阅VPN 连接中的Amazon VPC User Guide.

FSx for Windows File Server 还支持使用 Amazon FSx 文件网关来提供低延迟、无缝地从本地计算实例访问云内 FSx for Windows File Server 文件共享的 vSx。有关更多信息，请参阅 。亚马逊 FSx 文件网关用户指南.

从另一个 VPC、帐户或访问 FSx for Windows File Server 文件系统Amazon Web Services 区域

您可以从不同 VPC 中的计算实例访问 FSx for Windows File Server 文件系统。Amazon账户，或Amazon来自与您的文件系统关联的区域。为此，您可以使用 VPC 对等互连或中转网关。使用 VPC 对等连接或中转网关连接 VPC 时，一个 VPC 中的计算实例可以访问另一个 VPC 中的 Amazon FSx 文件系统。即使 VPC 属于不同的账户，并且即使 VPC 驻留在不同的账户中，也可以进行此访问Amazon地区。

一个VPC 对等连接是两个 VPC 之间的网络连接，您可以使用私有 IPv4 或 IP 版本 6 (IPv6) 地址在两个 VPC 之间路由流量。您可以使用 VPC 对等来连接Amazon区域或之间Amazon地区。有关 VPC 对等的更多信息，请参阅什么是 VPC 对等？中的Amazon VPC Peering Guide.

中转网关 是网络中转中心，您可用它来互连 VPC 和本地网络。有关使用 VPC 中转网关的更多信息，请参阅中转网关入门中的Amazon VPC Transit Gateway.

设置 VPC 对等互连或传输网关连接后，您可以使用其 DNS 名称访问文件系统。就像在关联 VPC 内的计算实例中执行的操作一样。

可用性与持久性：单可用区和多可用区文件系统

Amazon FSx for Windows File Server 提供两种文件系统部署类型：单可用区和多可用区。

Note

多可用区文件系统在中国（北京）区域中不可用。

选择单可用区或多可用区文件系统部署

对于单可用区文件系统，Amazon FSx 会自动在可用区 (AZ) 内复制您的数据，以保护数据免受组件故障的影响。它持续监控硬件故障，并在出现故障时自动更换基础架构组件。单可用区 2是最新一代的单可用区文件系统，支持 SSSSD 和 HDD 存储。单可用区 1文件系统支持 SSD 存储、Microsoft 分布式文件系统复制 (DFSR) 以及使用自定义 DNS 名称。在文件系统维护、基础设施组件更换期间以及可用区不可用时，单可用区文件系统将不可用。

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，它们旨在提供持续的数据可用性，即使在文件系统维护、基础架构组件更换期间以及可用区不可用时也是如此。在多可用区部署中，Amazon FSx 会自动在不同可用区中预置和维护备用文件服务器。写入您的文件系统中的磁盘的任何更改将跨可用区同步复制到备用区。如果进行计划的数据维护或发生未计划的服务中断，Amazon FSx 将自动故障转移到辅助文件服务器，使您能够在不进行手动干预的情况下继续访问数据。

对于要求共享 Windows 文件数据具有高可用性的大多数生产工作负载，建议使用多可用区文件系统。对于不需要多可用区解决方案的高可用性并且在数据丢失时可以从最新的文件系统备份中恢复的工作负载，单可用区文件系统可以提供更低的价位。默认情况下，Amazon FSx 每天自动备份所有文件系统。

按部署类型划分的功能支持

下表概述了 FSx Windows File Server 的部署类型：

Deployment type (部署类型)	SSSSD	HDD 存储	DFS 命名空间	DFS 复制	自定义 DNS 名称	CA 股票
单可用区 1	✓		✓	✓	✓	
单可用区 2	✓	✓	✓		✓	✓*
多可用区	✓	✓	✓		✓	✓*

Note

* 虽然您可以在单可用区 2 文件系统上创建 CA 共享，但应在 SQL Server HA 部署的多可用区文件系统上使用 CA 共享。

FSx or Windows File Server

如果出现以下任一情况，多可用区文件系统将自动从首选文件服务器故障转移到备用文件服务器：

- 可用区中断。
- 首选文件服务器变为不可用。
- 首选的文件服务器进行计划内维护。

当从一个文件服务器故障切换到另一个文件服务器时，新的活动文件服务器会自动开始处理所有文件系统的读写请求。当首选子网中的资源可用时，Amazon FSx 会自动回切到首选子网中的首选文件服务器。从在活动文件服务器上检测到故障到备用文件服务器升级为活动状态，故障转移通常在 30 秒内完成。回切到原始多可用区配置也可以在不到 30 秒的时间内完成，并且只有在首选子网中的文件服务器完全恢复后才会发生。

在文件系统进行故障切换和回切的短暂时期内，I/O 可能会暂停，Amazon CloudWatch 指标可能暂时不可用。

Windows 客户端上的故障转移体验

当从一个文件服务器故障切换到另一个文件服务器时，新的活动文件服务器会自动开始处理所有文件系统的读写请求。首选子网中的资源可用后，Amazon FSx 会自动回切到首选子网中的首选文件服务器。由于文件系统的 DNS 名称保持不变，因此故障切换对 Windows 应用程序是透明的，这些应用程序无需人工干预即可恢复文件系统操作。从在活动文件服务器上检测到故障到备用文件服务器升级为活动状态，故障转移通常在 30 秒内完成。回切到原始多可用区配置也可以在不到 30 秒的时间内完成，并且仅在首选子网中的文件服务器完全恢复后才会发生。

Linux 客户端上的故障转移体验

Linux 客户端不支持基于 DNS 的自动故障切换。因此，在故障转移期间，它们不会自动连接到备用文件服务器。在多可用区文件系统故障恢复到首选子网中的文件服务器后，它们将自动恢复文件系统操作。

在文件系统上测试故障切换

您可以通过修改多可用区文件系统的吞吐容量来测试其故障转移。当您修改文件系统的吞吐容量时，Amazon FSx 会切换文件系统的文件服务器。多可用区文件系统会自动故障转移到辅助服务器，而 Amazon FSx 会先替换首选的服务器文件服务器。然后，文件系统会自动故障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 中监控吞吐量容量更新请求的进度。更新成功完成后，文件系统将故障切换到从属服务器，并故障恢复到主服务器。有关修改文件系统的吞吐容量和监视请求进度的更多信息，请参阅管理吞吐量容量 (p. 122).

使用单可用区和多可用区文件系统资源

子网

当您创建 VPC 时，它会覆盖该区域中的所有可用区 (AZ)。可用区是被设计为可以隔离其他可用区的故障的不同位置。在创建 VPC 之后，您可以在每个可用区中添加一个或多个子网。默认 VPC 在每个可用区中有一个子网。每个子网都必须完全位于一个可用区之内，不能跨越多个可用区。创建单可用区 Amazon FSx 文件系统时，您需要为该文件系统指定一个子网。您选择的子网定义了在其中创建文件系统的可用区。

创建多可用区文件系统时，请指定两个子网，一个用于首选文件服务器。您选择的两个子网必须位于同一可用区中的不同可用区中Amazon区域。

对于 in-Amazon应用程序，我们建议您在与首选文件服务器相同的可用区中启动客户端，以最大限度减少延迟。

文件系统弹性网络接口

当您创建 Amazon FSx 时，Amazon FSx 会预置一个或多个弹性网络接口中的Amazon Virtual Private Cloud (VPC)您与您的文件系统关联的。网络接口允许您的客户端与 FSx for Windows File Server 系统。该网络接口被视为在 Amazon FSx 的服务范围内，尽管是您的账户的 VPC 的一部分。多可用区文件系统有两个弹性网络接口，每个文件服务器对应一个。单可用区文件系统有一个elastic network interface。

> **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。修改或删除网络接口可能会导致永久丢失您的 VPC 和您的文件系统之间的连接。

下表汇总了 FSx for Windows 文件服务器文件系统部署类型的子网、elastic network interface 和 IP 地址资源：

文件系统部署类型	子网的数量	弹性网络接口的数量	IP 地址数
单可用区 2	1	1	2
单可用区 1	1	1	1
多可用区	2	2	4

创建文件系统后，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 Internet。如果弹性 IP 地址（可从互联网访问的公有 IP 地址）连接到文件系统的elastic network interface，Amazon FSx 会自动将其分离。

使用亚马逊 FSx 优化成本

FSx for Windows File Server 提供了多项功能，可帮助您根据应用程序需求优化总体拥有成本 (TCO)。您可以选择存储类型（HDD 或 SSD），以实现应用程序的成本和性能需求的适当平衡。您可以灵活地将吞吐量与存储容量分开选择，以优化成本。此外，您可以使用重复数据消除功能，通过消除文件系统上的冗余数据来优化存储成本。

主题

灵活地独立选择存储和吞吐量

借助 FSx for Windows File Server，您可以独立配置文件系统的存储和吞吐量容量。这使您能够灵活地实现正确的成本和性能组合。例如，您可以选择为冷（通常是非活动）工作负载提供大量存储和相对较少的吞吐容量，以节省不必要的吞吐量成本。或者，作为另一个例子，您可以选择为相对较少的存储容量提供大量吞吐容量。更高的吞吐量随着用于在文件服务器上缓存的内存量更高。您可以利用文件服务器上的快速缓存优化主动访问数据的性能。有关更多信息，请参阅 FSx for Windows File Server 性能 (p. 141)。

您可以随时增加或减少吞吐量容量，从而为满足不断变化的性能需求提供灵活性。有关更多信息，请参阅 管理吞吐量容量 (p. 122)。创建文件系统后，您可以随时增加存储空间。有关更多信息，请参阅 管理存储容量 (p. 112)。

优化存储成本

您可以通过多种方式使用 Amazon FSx 优化存储成本，如下所述。

使用存储类型优化成本

FSx for Windows File Server 提供两种类型的存储 — 硬盘驱动器 (HDD) 和固态硬盘 (SSD)，使您能够优化成本/性能以满足工作负载需求。HDD 存储设计用于广泛的工作负载，包括主目录、用户和部门共享以及内容管理系统。SSD 存储设计用于最高性能和最敏感延迟的工作负载，包括数据库、媒体处理工作负载和数据分析应用程序。有关更多信息，请参阅 。延迟 (p. 141)和Amazon FSx for Windows File Server 定价.

使用重复数据删除优化存储成本

大型数据集通常具有冗余数据，这增加了数据存储成本。例如，用户文件共享可以有同一文件的多个副本，由多个用户存储。软件开发共享可以包含许多二进制文件，这些二进制文件从构建到构建 您可以通过打开来降低数据存储成本重复数据删除对于您的文件系统。启用重复数据消除功能后，重复数据删除只能存储一次数据集的重复部分，从而自动减少或消除冗余数据。有关重复数据删除以及如何轻松启用 Amazon FSx 文件系统的更多信息，请参阅重复数据删除 (p. 104).

在 FSx for Windows File Server 中使用 Microsoft Active Directory

Amazon FSx 与 Microsoft Active Directory (AD) 合作，与您现有的 Microsoft Windows 环境进行集成。Active Directory 是 Microsoft 目录服务，用于存储有关网络上对象的信息，并使管理员和用户轻松查找和使用此信息。这些对象通常包括共享资源，例如文件服务器、网络用户和计算机帐户。

使用 Amazon FSx 创建文件系统时，您可以将其加入 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，您的用户可以使用 Active Directory 中的现有用户身份对自己进行身份验证并访问 Amazon FSx 文件系统。用户还可以使用现有身份来控制对单个文件和文件夹的访问。此外，您可以将现有文件和文件夹以及这些项目的安全访问控制列表 (ACL) 配置迁移到 Amazon FSx，而无需任何修改。

将 Amazon FSx for FSx for Windows File Server 文件系统与 Active Directory 结合使用：使用 Amazon FSxAmazon Directory Service for Microsoft Active Directory (p. 22)和将 Amazon FSx 与自主管理的 Microsoft Active Directory 结合使用 (p. 30).

> Note
>
> Amazon FSx 支持Microsoft Azure Active Directory 域服务，你可以加入Microsoft Azure Active Directory.

为文件系统创建已加入的 Active Directory 配置后，您只能更新以下属性：

- 服务用户凭证
- DNS 服务器 IP 地址

您不能更改你加入的 Microsoft AD 的以下属性：

- DomainName
- OrganizationalUnitDistinguishedName
- FileSystemAdministratorsGroup

但是，你可以从备份创建新的文件系统，然后在该文件系统的 Microsoft Active Directory 集成配置中更改这些属性。有关更多信息，请参阅 演练 2：从备份创建文件系统 (p. 148)。

> Note
>
> 亚马逊 FSx 不支持Active Directory Connector和Simple Active Directory.

主题

使用 Amazon FSxAmazon Directory Service for Microsoft Active Directory

Amazon Directory Service for Microsoft Active Directory(Amazon Managed Microsoft AD) 在云中提供完全托管、高度可用的实际 Active Directory (AD) 目录。您可以在工作负载部署中使用这些 AD 目录。

如果你的组织正在使用Amazon Managed Microsoft AD要管理身份和设备，我们建议您将 Amazon FSx 文件系统与Amazon Managed Microsoft AD. 通过这样做，你可以获得一个使用 Amazon FSx 的交钥匙解决方案Amazon Managed Microsoft AD.Amazon处理两项服务的部署、运营、高可用性、可靠性、安全性和无缝集成，使您能够专注于有效地运营自己的工作负载。

要将亚马逊 FSx 与您的Amazon Managed Microsoft AD设置后，您可以使用 Amazon FSx 控制台。在控制台中创建新 FSx for Windows File Server 文件系统时，选择Amazon托管广告在Windows 身份验证部分。您还可以选择要使用的特定目录。有关更多信息，请参阅 第 1 步：创建文件系统 (p. 7)。

您的组织可能会在自我管理的 Active Directory 域（本地或云中）上管理身份和设备。如果是这样，您可以将 Amazon FSx 文件系统直接加入到现有的自我管理的 AD 域。有关更多信息，请参阅 将 Amazon FSx 与自主管理的 Microsoft Active Directory 结合使用 (p. 30)。

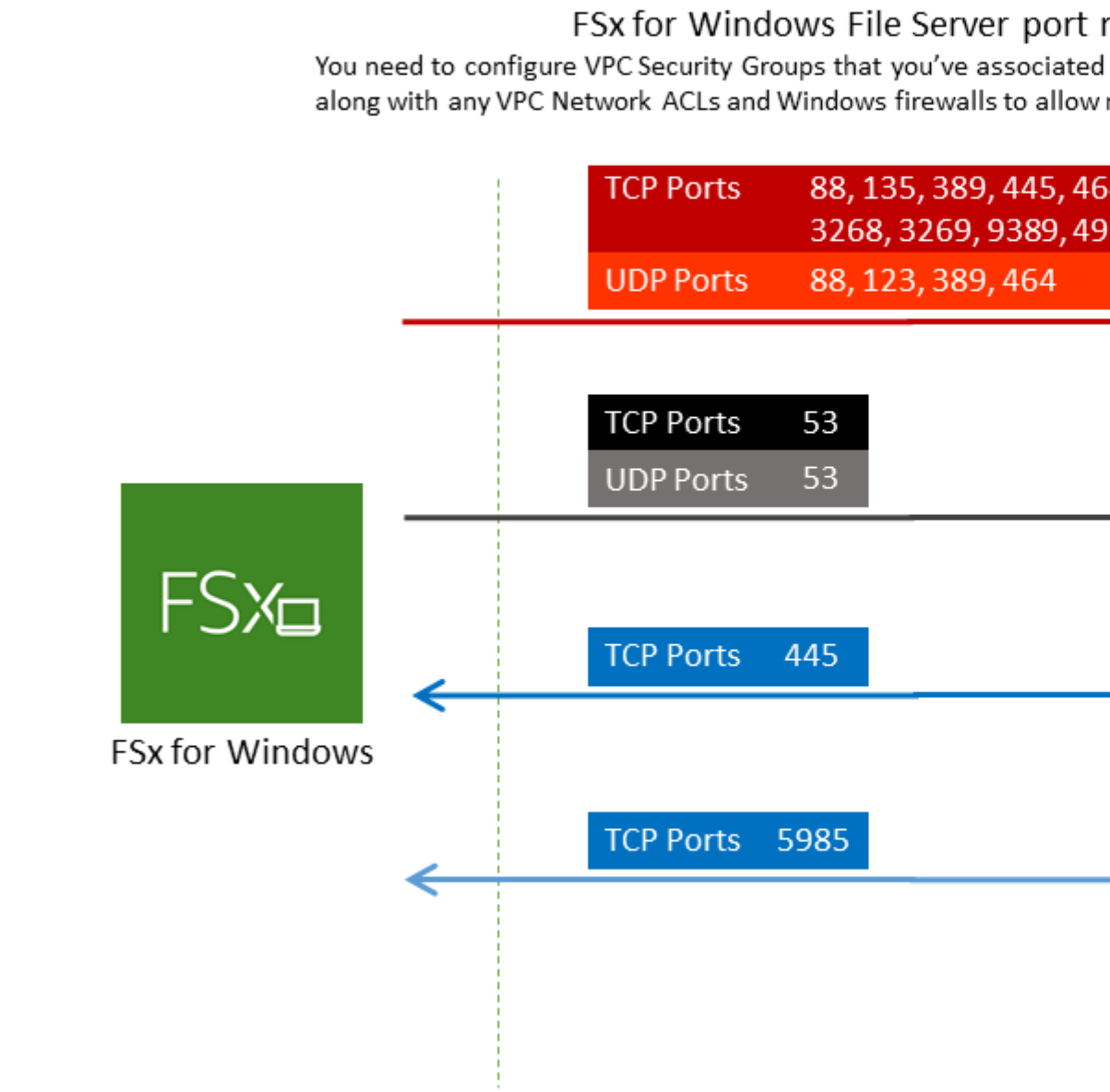
此外，您还可以将系统设置为从资源林隔离模型中受益。在此模型中，您可以将包括 Amazon FSx 文件系统在内的资源隔离到与用户所在的单独的 AD 林中。

> Important
>
> 对于单可用区 2 和所有多可用区文件系统，Active Directory 域名不能超过 47 个字符。

先决条件

在创建 FSx for Windows File Server 文件系统之前，已加入Amazon请确保已创建并设置以下网络配置：

- 适用于VPC 安全组，您的默认 Amazon VPC 的默认安全组已添加到控制台中的文件系统。请确保在其中创建 FSx 文件系统的子网的安全组和 VPC 网络 ACL 允许端口上以及下图所示的说明中的流量。



下表确定了每个端口的角色。

协议	端口	角色
TCP/UDP	53	域名系统 (DNS)
TCP/UDP	88	Kerberos 身份验证
TCP/UDP	464	更改/设置密码
TCP/UDP	389	轻型目录访问协议 (LDAP)
UDP	123	网络时间协议 (NTP)
TCP	135	分布式计算环境/端点映射器（DCE/EPMAP）

协议	端口	角色
TCP	445	目录服务 SMB 文件共享
TCP	636	基于 TLS/SSL 的轻量级目录访问协议 (LDAPS)
TCP	3268	微软全球目录
TCP	3269	SSL 上的微软全球目录
TCP	5985	WinRM 2.0（微软视窗远程管理）

协议	端口	角色
TCP	9389	微软 AD DS Web 服务，PowerSh
TCP	49152 - 65535	RPC 的临时端口

Important

单可用区 2 和所有多可用区文件系统部署都需要允许 TCP 端口 9389 上的出站流量。

Note

如果您使用的是 VPC 网络 ACL，则还必须允许来自 FSx 文件系统的动态端口 (49152-65535) 上的出站流量。

- 如果您要将亚马逊 FSx 文件系统连接到Amazon在其他 VPC 或账户中管理 Microsoft AD，然后确保该 VPC 和要在其中创建文件系统的 Amazon VPC 之间的连接。有关更多信息，请参阅 使用 Amazon FSxAmazon Managed Microsoft AD在不同 VPC 或账户中 (p. 28)。

  Important

  虽然 Amazon VPC 安全组要求仅在启动网络流量的方向上打开端口，但 VPC 网络 ACL 要求端口在两个方向上打开。

使用亚马逊 FSx 网络验证工具 (p. 28)以验证与 Active Directory 域控制器的连接。

使用资源林隔离模型

你将文件系统加入到Amazon Managed Microsoft AD设置。然后你建立单向森林信任关系Amazon Managed Microsoft AD您创建的域以及现有的自我管理 AD 域。对于 Amazon FSx 中的 Windows 身份验证，您只需要单向定向林信任，其中Amazon托管林信任公司域林。

您的公司域名扮演受信任域的角色，Amazon Directory Service托管域承担信任域的角色。经过验证的身份验证请求只能沿一个方向在域之间传输，允许公司域中的帐户根据托管域中共享的资源进行身份验证。在这种情况下，Amazon FSx 仅与托管域进行交互。然后，托管域将身份验证请求传递到您的公司域。

测试 Active Directory 配置

在创建 Amazon FSx 文件系统之前，我们建议您使用 Amazon FSx 网络验证工具验证与 Active Directory 域控制器的连接。有关更多信息，请参阅 验证与 Active Directory 域控制器的连接 (p. 28)。

下列相关资源在您使用的过程中会有所帮助：Amazon Directory Service for Microsoft Active Directory针对 Windows File Server 使用 FSx：

- 什么是AmazonDirectory Service中的Amazon Directory Service管理指南

- 创建您的Amazon托管 AD 目录中的Amazon Directory Service管理指南
- 何时创建信任关系中的Amazon Directory Service管理指南
- 演练 1：开始使用的先决条件 (p. 145)

使用 Amazon FSxAmazon Managed Microsoft AD在不同 VPC 或账户中

您可以将 FSx for Windows File Server 文件系统加入Amazon Managed Microsoft AD使用 VPC 对等互连，位于同一账户内不同 VPC 中的目录。您还可以将文件系统加入Amazon Managed Microsoft AD不同的目录Amazon使用目录共享帐户。

将文件系统加入到Amazon Managed Microsoft AD在不同 VPC 中的操作涉及以下步骤：

1. 设置您的网络环境。
2. 共享您的目录。
3. 将文件系统加入共享目录。

有关更多信息，请参阅 。共享您的目录中的Amazon Directory Service管理指南.

要设置网络环境，您可以使用Amazon Transit Gateway或 Amazon VPC，然后创建 VPC 对等连接。此外，请确保允许两个 VPC 之间的网络流量。

中转网关 是网络中转中心，您可用它来互连 VPC 和本地网络。有关使用 VPC 中转网关的更多信息，请参阅中转网关入门中的Amazon VPC 中转网关指南.

VPC 对等连接 是两个 VPC 之间的网络连接。使用此连接，您能够使用专用 Internet 协议版本 4 (IPv4) 或 Internet 协议版本 6 (IPv6) 地址，在它们之间路由流量。您可以使用 VPC 对等来连接位于相同的 VPCAmazon在区域或之间Amazon地区。有关 VPC 对等连接的更多信息，请参阅什么是 VPC 对等？中的Amazon VPC Peering Guide.

将文件系统加入到Amazon Managed Microsoft AD位于与文件系统不同的账户中的目录。你还需要与另一个帐户共享你的 Microsoft AD 目录。要执行此操作，您可以使用Amazon托管微软活动目录的目录共享功能。要了解更多信息，请参阅共享您的目录中的Amazon Directory Service管理指南.

验证与 Active Directory 域控制器的连接

在创建加入到 Active Directory 的 Windows 文件服务器文件系统之前，请使用 Amazon FSx 活动目录验证工具验证与 Active Directory 域的连接。您可以使用此测试是否将 FSx for Windows File Server 与Amazon 托管 Microsoft Active Directory 或使用自我管理的 Active Directory 配置。域控制器网络连接测试（Test-fsxadController Connection）不会针对域中的每个域控制器运行全套网络连接检查。相反，使用此测试对一组特定的域控制器运行网络连接验证。

验证与 Active Directory 域控制器的连接

1. 在同一子网中启动 Amazon EC2 Windows 实例，并且使用您将用于 Windows 文件服务器文件系统的 FSx 的相同 Amazon VPC 安全组。对于多可用区部署类型，请使用首选活动文件服务器的子网。
2. 将 EC2 Windows 实例加入您的活动目录。有关更多信息，请参阅 。手动加入 Windows 实例中的Amazon Directory Service管理指南.
3. 连接到您的 EC2 实例。有关更多信息，请参阅适用于 Windows 实例的 Amazon EC2 用户指南中的连接您的 Windows 实例。
4. 打开窗口 PowerShell 窗口（使用运行管理员身份）在 EC2 实例上。

测试是否需要适用于 Windows 的活动目录模块 PowerShell 已安装，请使用以下测试命令。

```
PS C:\> Import-Module ActiveDirectory
```

如果以上返回错误，请使用以下命令进行安装。

```
PS C:\> Install-WindowsFeature RSAT-AD-PowerShell
```

5. 使用以下命令下载网络验证工具。

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

6. 使用以下命令展开 zip 文件。

```
PS C:\> Expand-Archive -Path "AmazonFSxADValidation.zip"
```

7. 将 AmazonFSxCAD 验证模块添加到当前会话。

```
PS C:\> Import-Module .\AmazonFSxADValidation
```

8. 设置 Active Directory 域控制器 IP 地址的值，然后使用以下命令运行连接测试：

```
$ADControllerIp = '10.0.75.243'
$Result = Test-FSxADControllerConnection -ADControllerIp $ADControllerIp
```

9. 以下示例演示了检索测试输出，以及成功的连通性测试的结果。

```
PS C:\AmazonFSxADValidation> $Result

Name                           Value
----                           -----
TcpDetails                     {@{Port=88; Result=Listening; Description=Kerberos
 authentication}, @{Port=135; Resul...
Server                         10.0.75.243
UdpDetails                     {@{Port=88; Result=Timed Out; Description=Kerberos
 authentication}, @{Port=123; Resul...
Success                        True


PS C:\AmazonFSxADValidation> $Result.TcpDetails

Port Result    Description
---- ------    -----------
  88 Listening Kerberos authentication
 135 Listening DCE / EPMAP (End Point Mapper)
 389 Listening Lightweight Directory Access Protocol (LDAP)
 445 Listening Directory Services SMB file sharing
 464 Listening Kerberos Change/Set password
 636 Listening Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
3268 Listening Microsoft Global Catalog
3269 Listening Microsoft Global Catalog over SSL
9389 Listening Microsoft AD DS Web Services, PowerShell
```

以下示例显示了运行测试并获得失败的结果。

```
PS C:\AmazonFSxADValidation> $Result = Test-FSxADControllerConnection -ADControllerIp
 $ADControllerIp
WARNING: TCP 9389 failed to connect. Required for Microsoft AD DS Web Services,
 PowerShell.
Verify security group and firewall settings on both client and directory controller.
WARNING: 1 ports failed to connect to 10.0.75.243. Check pre-requisites in
https://docs.aws.amazon.com/fsx/latest/WindowsGuide/self-managed-AD.html#self-manage-
prereqs

PS C:\AmazonFSxADValidation> $Result

Name                           Value
----                           -----
TcpDetails                     {@{Port=88; Result=Listening; Description=Kerberos
 authentication}, @{Port=135; Resul...
Server                         10.0.75.243
UdpDetails                     {@{Port=88; Result=Timed Out; Description=Kerberos
 authentication}, @{Port=123; Resul...
Success                        False
FailedTcpPorts                 {9389}


PS C:\AmazonFSxADValidation> $Result.FailedTcpPorts
9389
```

Windows socket error code mapping

https://msdn.microsoft.com/en-us/library/ms740668.aspx

将 Amazon FSx 与自主管理的 Microsoft Active Directory 结合使用

您的组织可能会在自我管理的 Active Directory（本地或云中）上管理身份和设备。如果是这样，您可以将 Amazon FSx 文件系统直接加入现有的自我管理 AD 域。要将亚马逊 FSx 与您的Amazon Managed Microsoft AD设置后，您可以使用 Amazon FSx 控制台。在控制台中创建新 FSx for Windows File Server 文件系统时，选择自行管理的 Microsoft Active Directory在Windows 身份验证部分。提供自行管理的 AD 的以下详细信息：

- 自主管理目录的完全限定域名

  Note

  域名不得采用单一标签域 (SLD) 格式。Amazon FSx 目前不支持 SLD 域。

  Note

  对于单可用区 2 和所有多可用区文件系统，Active Directory 域名不能超过 47 个字符。

- 域的 DNS 服务器的 IP 地址

  DNS 服务器 IP 地址、AD 域控制器 IP 地址和客户端网络必须满足以下要求：

对于 2020 年 12 月 17 日之前创建的文件系统	对于 2020 年 12 月 17 日之后创建的文件系统
中的 IP 地址RFC 1918私有 IP 地址范围：	任何 IP 地址范围，但：

对于 2020 年 12 月 17 日之前创建的文件系统	对于 2020 年 12 月 17 日之后创建的文件系统
• 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	• 与亚马逊 Web 服务拥有的 IP 地址冲突的 IP 地址Amazon区域。列表Amazon按地区拥有的 IP 地址，请参阅AmazonIP 地址范围. • 以下 CIDR 区块范围内的 IP 地址：198.19.0.0/16

Note

您的 AD 域控制器必须可写。

- AD 域中服务帐户的用户名和密码，供 Amazon FSx 将文件系统加入 AD 域
- （可选）要加入文件系统的域中的组织单位 (OU)
- （可选）要向其委派权限以在文件系统上执行管理操作的域组。例如，此域组可以管理 Windows 文件共享、管理文件系统根文件夹上的 ACL、获取文件和文件夹的所有权等。如果您没有指定此组，默认情况下，Amazon FSx 将此权限委派给 AD 域中的域管理员组。

有关更多信息，请参阅 加入 Amazon FSx 文件系统 (p. 39)。

Important

如果您使用微软 DNS 作为默认 DNS 服务，则 Amazon FSx 仅为文件系统注册 DNS 记录。如果您使用的是第三方 DNS，则需要在创建 Amazon FSx 文件系统后手动设置 DNS 条目。

当您将文件系统直接加入到自我管理的 AD 时，您的 FSx for Windows File Server 位于同一 AD 林（包含域、用户和计算机的 AD 配置中最顶层的逻辑容器），并与用户和现有资源（包括现有资源）位于同一 AD 域中文件服务器)。

Note

如果您想从资源林隔离模型中受益，在此模型中，将资源（包括 Amazon FSx 文件系统）隔离到与用户所在的单独的 AD 林中，则可以选择将文件系统加入到Amazon管理 AD 并建立单向林信任关系Amazon您创建的托管广告和现有的自我管理的广告。

主题

使用自行管理的 Microsoft AD 的先决条件

在创建加入自我管理的 Microsoft AD 域的 Amazon FSx 文件系统之前，请确保您已创建并设置以下要求：

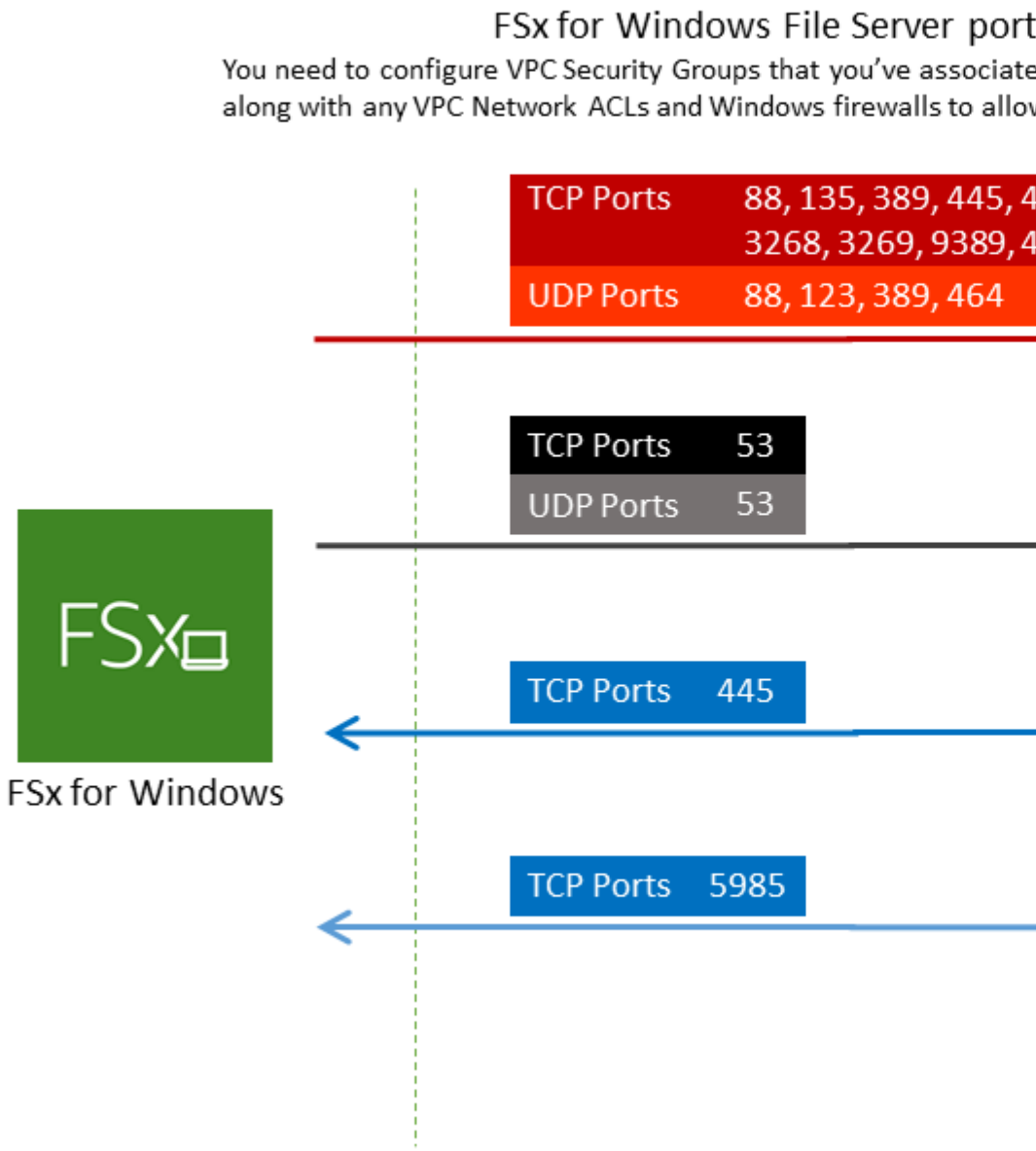
- Amazon FSx 文件系统要加入的本地或其他自我管理的 Microsoft AD，具有以下配置：
  - AD 域控制器的域功能级别为 Windows Server 2008 R2 或更高版本。
  - DNS 服务器 IP 地址和 AD 域控制器 IP 地址如下，具体取决于文件系统的创建时间：

对于 2020 年 12 月 17 日之前创建的文件系统	对于 2020 年 12 月 17 日之后创建的文件系统
中的 IP 地址RFC 1918私有 IP 地址范围： • 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	任何 IP 地址范围，但： • 与亚马逊 Web 服务拥有的 IP 地址冲突的 IP 地址Amazon区域。列表Amazon按地区拥有的 IP 地址，请参阅AmazonIP 地址范围. • 以下 CIDR 区块范围内的 IP 地址：198.19.0.0/16

如果您需要访问 2020 年 12 月 17 日之前使用非私有 IP 地址范围创建的 FSx for Windows 文件服务器文件系统，则可以通过还原文件系统的备份来创建新的文件系统。有关更多信息，请参阅 使用备份 (p. 71)。

- 不是单一标签域 (SLD) 格式的域名。亚马逊 FSx 不支持 SLD 域名。
- 对于单可用区 2 和所有多可用区文件系统，Active Directory 域名不能超过 47 个字符。
- 如果您已定义 Active Directory 站点，您必须确保在 Active Directory 站点中您 Amazon FSx 文件系统关联的 VPC 内定义了子网，并且 VPC 中的子网与您其他站点中的子网之间不存在冲突。

- 以下网络配置：
  - 在要创建文件系统的 Amazon VPC 与自我管理的 Active Directory 之间配置了连接。您可以使用设置连接Amazon Direct Connect、Amazon VPN、VPC 对等互连，或Amazon Transit Gateway.
  - 适用于VPC 安全组，您的默认 Amazon VPC 的默认安全组已添加到控制台中的文件系统。请确保在其中创建 FSx 文件系统的子网的安全组和 VPC 网络 ACL 允许端口上以及下图所示的说明中的流量。



下表确定了每个端口的角色。

协议	端口	角色
TCP/UDP	53	域名系统 (DNS)

协议	端口	角色
TCP/UDP	88	Kerberos 身份验证
TCP/UDP	464	更改/设置密码
TCP/UDP	389	轻型目录访问协议 (LDAP)
UDP	123	网络时间协议 (NTP)
TCP	135	分布式计算环境/端点映射器（DCE/EPMAP）
TCP	445	目录服务 SMB 文件共享
TCP	636	基于 TLS/SSL 的轻量级目录访问协议 (LDAPS)
TCP	3268	微软全球目录
TCP	3269	SSL 上的微软全球目录
TCP	5985	WinRM 2.0（微软视窗远程管理）
TCP	9389	微软 AD DS Web 服务，PowerShell
TCP	49152 - 65535	RPC 的临时端口

Important

单可用区 2 和所有多可用区文件系统部署都需要允许 TCP 端口 9389 上的出站流量。

Note

如果您使用的是 VPC 网络 ACL，则还必须允许来自 FSx 文件系统的动态端口 (49152-65535) 上的出站流量。

- 确保这些流量规则也镜像在适用于每个 AD 域控制器、DNS 服务器、FSx 客户端和 FSx 管理员的防火墙上。

  Important

  尽管 Amazon VPC 安全组要求仅在启动网络流量的方向上打开端口，但大多数 Windows 防火墙和 VPC 网络 ACL 都要求端口双向打开。

使用亚马逊 FSx 活动目录验证工具 (p. 36)在尝试将文件系统加入自我管理的 AD 之前测试这些网络设置。

- 具有将计算机加入域的委派权限的自主管理 Microsoft AD 中的服务帐户。一个服务账户是自我管理的 Microsoft AD 中已委派某些任务的用户帐户。

  至少还需要在您加入文件系统的 OU 中向服务帐户授予以下权限：

  - 能够重置密码
  - 能够限制帐户读取和写入数据
  - 已验证写入 DNS 主机名的能力
  - 已验证写入服务主体名称的能力
  - 授权创建和删除计算机对象的控制权
  - 验证读写账户限制的能力

  这些代表将计算机对象加入 Active Directory 所需的最低权限集。有关更多信息，请参阅 Microsoft Windows Server 文档主题。Error: 当被委派控制权的非管理员用户尝试将计算机加入域控制器时，访问将被拒绝.

要了解有关创建具有正确权限的服务帐户的更多信息，请参阅 将权限委派给您的 Amazon FSx 服务账户 (p. 35).

Note

亚马逊 FSx 在您的亚马逊 FSx 文件系统的整个生命周期内都要求有效的服务账户。Amazon FSx 必须能够使用完全管理文件系统并执行需要取消加入和重新加入 AD 域的任务，例如更换出现故障的文件服务器或修补 Windows Server 软件。请使用 Amazon FSx 保持您的 Active Directory 配置（包括服务帐户凭证）更新。要了解如何操作，请参阅使用 Amazon FSx 保持您的 Active Directory 配置更新 (p. 36)。

Note

Amazon FSx 要求连接到 AD 环境中的所有域控制器。如果您有多个域控制器，请确保所有域控制器都满足上述要求，并确保对服务帐户的任何更改都传播到所有域控制器。您可以使用亚马逊 FSx 活动目录验证工具 (p. 36).

如果这是您首次使用Amazon和 FSx for Windows File Server，请务必在启动之前进行设置。有关更多信息，请参阅 设置 (p. 5)。

Important

创建文件系统后，请勿移动 Amazon FSx 在 OU 中创建的计算机对象。这样做将导致文件系统配置错误。

将 FSx for Windows File Server 系统加入自管理的 Microsoft Active Directory 域的最佳实践

在将 FSx for Windows File Server 系统加入自管理的 Microsoft Active Directory 时，您应该考虑以下建议和准则。请注意，推荐使用这些做法作为最佳实践，但不是必需的。

将权限委派给您的 Amazon FSx 服务账户

确保使用所需的最低权限配置您向 Amazon FSx 提供的服务账户。此外，将组织单位 (OU) 与其他域控制器问题分开。

要将 Amazon FSx 文件系统加入您的域，请确保服务帐户具有委派的权限。的成员Domain Admins组有足够的权限来执行此任务。但是根据最佳实践，请使用仅具有执行此操作所需的最小权限的服务账户。以下过程演示了如何仅将加入 Amazon FSx 文件系统所需的权限委派给您的域。

在已加入到目录且已安装 Active Directory User and Computers MMC 管理单元的计算机上执行此过程。

为 Active Directory 域创建服务帐户

1. 确保您以 Active Directory 域的域管理员身份登录。
2. 打开Active Directory 用户和计算机MMC 管理单元。
3. 在任务窗格中，展开域节点。
4. 找到并打开要修改的 OU 的上下文 (右键单击) 菜单，然后选择委托控制.
5. 在存储库的控制委派向导选择页面，下一步.
6. 选择Add添加特定用户或特定组选定的用户和组选择，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. 选择仅在文件夹中的以下对象选择，然后选择Computer 对象.
9. 选择在这个文件夹中创建所选对象和删除此文件夹中的所选对象. 然后选择下一步。
10. 适用于Permissions (权限)选择以下选项：

    - 重置密码

- 读取和写入账户限制s
- 已验证写入 DNS 主机名
- 已验证写入服务委托方名称

11. 选择下一步，然后选择完成。
12. 关闭 Active Directory 用户和计算机 MMC 管理单元。

Important

创建文件系统后，请勿移动 Amazon FSx 在 OU 中创建的计算机对象。这样做将导致文件系统配置错误。

使用 Amazon FSx 保持您的 Active Directory 配置更新

为了帮助确保 Amazon FSx 文件系统的持续、不间断的可用性，请在更改自我管理的 AD 设置时随时更新文件系统的自管 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，一旦重置密码，请务必使用 Amazon FSx 更新服务账户密码。为此，请使用亚马逊 FSx 控制台、亚马逊 FSx API 或Amazon CLI. 同样，如果 Active Directory 域的 DNS 服务器 IP 地址发生更改，一旦发生更改，就立即使用 Amazon FSx 更新 DNS 服务器 IP 地址。同样，使用 Amazon FSx 控制台、API 或 CLI 执行此操作。

当您更新 Amazon FSx 文件系统的自我管理 AD 配置时，文件系统的状态将从Available到正在更新同时应用更新。验证状态是否切换回到Available应用更新后 — 请注意，更新可能需要几分钟才能完成。有关更多信息，请参阅 更新自行管理的 Active Directory 配置 (p. 46)。

如果更新的自我管理 AD 配置存在问题，则文件系统状态将切换为配置错误. 此状态在控制台、API 和 CLI 中的文件系统描述旁边显示错误消息和建议的纠正措施。在采取建议的纠正措施后，验证文件系统的状态最终更改为Available.

要详细了解如何排查可能的自我管理 AD 配置错误，请参阅文件系统处于错误配置状态 (p. 195).

使用安全组限制 VPC 内的流量

要限制虚拟私有云 (VPC) 中的网络流量，您可以在 VPC 中实施最小权限的原则。换言之，您可以将权限限限制为所需的最小权限。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 (p. 163)。

为文件系统的网络接口创建出站安全组规则

为了提高安全性，请考虑使用出站流量规则配置安全组。这些规则应只允许出站流量发送到自我管理的 Microsoft AD 域控制器或子网或安全组内。将此安全组应用于与 Amazon FSx 文件系统的 elastic network interface 关联的 VPC。要了解更多信息，请参阅“使用 Amazon VPC 进行文件系统访问控制 (p. 163)”。

验证 Active Directory 配置

在创建加入到 Active Directory FSx for Windows File Server 文件系统之前，我们建议您使用 Amazon FSx Active Directory 验证工具验证您的 Active Directory 配置。

验证 Active Directory 配置

1. 在同一子网中启动 Amazon EC2 Windows 实例，并且使用您将用于 Windows 文件服务器文件系统的 FSx 的相同 Amazon VPC 安全组。请确保 EC2 实例具有所需`AmazonEC2ReadOnlyAccess`IAM 权限。您可以使用 IAM 策略模拟器验证 EC2 实例角色权限。有关更多信息，请参阅 。使用 IAM 策略模拟器测试 IAM 策略中的IAM 用户指南.
2. 将 EC2 Windows 实例加入您的活动目录。有关更多信息，请参阅 。手动加入 Windows 实例中的Amazon Directory Service管理指南.

3. 连接到您的 EC2 实例。有关更多信息，请参阅适用于 Windows 实例的 Amazon EC2 用户指南中的连接您的 Windows 实例。
4. 打开窗口 PowerShell 窗口（使用运行管理员身份）在 EC2 实例上。

   测试是否需要适用于 Windows 的活动目录模块 PowerShell 已安装，请使用以下测试命令。

   ```
   PS C:\> Import-Module ActiveDirectory
   ```

   如果以上返回错误，请使用以下命令进行安装。

   ```
   PS C:\> Install-WindowsFeature RSAT-AD-PowerShell
   ```
5. 使用以下命令下载网络验证工具。

   ```
   PS C:\> Invoke-WebRequest "https://docs.aws.amazon.com/fsx/latest/WindowsGuide/samples/
   AmazonFSxADValidation.zip" -OutFile "AmazonFSxADValidation.zip"
   ```
6. 使用以下命令展开 zip 文件。

   ```
   PS C:\> Expand-Archive -Path "AmazonFSxADValidation.zip"
   ```
7. 添加AmazonFSxADValidation模块到当前会话。

   ```
   PS C:\> Import-Module .\AmazonFSxADValidation
   ```
8. 通过在以下命令中替换您的命令来设置所需的参数：

   - Active Directory 域名 (*DOMAINNAME.COM*)
   - 准备$Credential使用以下选项之一，将对象用于服务帐户密码。
     - 要以交互方式生成凭据对象，请使用以下命令。

       ```
       $Credential = Get-Credential
       ```
     - 使用生成凭据对象Amazon Secrets Manager资源，请使用以下命令。

       ```
       $Secret = ConvertFrom-Json -InputObject (Get-SECSecretValue -SecretId
        $AdminSecret).SecretString
       $Credential = (New-Object PSCredential($Secret.UserName,(ConvertTo-SecureString
        $Secret.Password -AsPlainText -Force)))
       ```
   - DNS 服务器 IP 地址 (*IP_ADDRESS _1*、*IP_ADDRESS _2*)
   - 计划在其中创建 Amazon FSx 文件系统的子网 ID (*SUBNET_1*、*SUBNET_2*，例如，subnet-04431191671ac0d19)。

   ```
   PS C:\>
   $FSxADValidationArgs = @{
       # DNS root of ActiveDirectory domain
       DomainDNSRoot = 'DOMAINNAME.COM'

       # IP v4 addresses of DNS servers
       DnsIpAddresses = @('IP_ADDRESS_1', 'IP_ADDRESS_2')

       # Subnet IDs for Amazon FSx file server(s)
   ```

```
    SubnetIds = @('SUBNET_1', 'SUBNET_2')

    Credential = $Credential
}
```

9. （可选）设置组织单位、委派管理员组、domainControllersMaxCount，并按照随附README.md文件之前运行验证工具。

   Note

   内置Domain Admins如果操作系统不是英文，则组的名称不同。例如，该组被命名为Administrateurs du domaine在法国操作系统版本中。如果不指定值，则默认值Domain Admins使用组名称，文件系统创建失败。

10. 使用此命令运行验证工具。

```
PS C:\> $Result = Test-FSxADConfiguration @FSxADValidationArgs
```

11. 以下是成功测试结果的示例。

```
Test 1 - Validate EC2 Subnets ...
...
Test 17 - Validate 'Delete Computer Objects' permission ...

Test computer object amznfsxtestd53f deleted!
...
SUCCESS - All tests passed! Please proceed to creating an Amazon FSx file system.
 For your convenience, SelfManagedActiveDirectoryConfiguration of result can be used
 directly in CreateFileSystemWindowsConfiguration for New-FSXFileSystem
PS C:\AmazonFSxADValidation> $Result.Failures.Count
0
PS C:\AmazonFSxADValidation> $Result.Warnings.Count
0
```

以下是出错测试结果的示例。

```
Test 1 - Validate EC2 Subnets ...
...
Test 7 - Validate that provided EC2 Subnets belong to a single AD Site ...

Name          DistinguishedName
 Site
----          -----------------
 ----
10.0.0.0/19   CN=10.0.0.0/19,CN=Subnets,CN=Sites,CN=Configuration,DC=test-ad,DC=local
 CN=SiteB,CN=Sites,CN=Configu...
10.0.128.0/19 CN=10.0.128.0/19,CN=Subnets,CN=Sites,CN=Configuration,DC=test-ad,DC=local
 CN=Default-First-Site-Name,C...
10.0.64.0/19  CN=10.0.64.0/19,CN=Subnets,CN=Sites,CN=Configuration,DC=test-ad,DC=local
 CN=SiteB,CN=Sites,CN=Configu...



Best match for EC2 subnet subnet-092f4caca69e360e7 is AD site CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=te
st-ad,DC=local
Best match for EC2 subnet subnet-04431191671ac0d19 is AD site
 CN=SiteB,CN=Sites,CN=Configuration,DC=test-ad,DC=local
WARNING: EC2 subnets subnet-092f4caca69e360e7 subnet-04431191671ac0d19 matched to
 different AD sites! Make sure they
are in a single AD site.
...
9 of 16 tests skipped.
```

```
FAILURE - Tests failed. Please see error details below:

Name                           Value
----                           -----
SubnetsInSeparateAdSites       {subnet-04431191671ac0d19, subnet-092f4caca69e360e7}



Please address all errors and warnings above prior to re-running validation to confirm
 fix.
PS C:\AmazonFSxADValidation> $Result.Failures.Count
1
PS C:\AmazonFSxADValidation> $Result.Failures

Name                           Value
----                           -----
SubnetsInSeparateAdSites       {subnet-04431191671ac0d19, subnet-092f4caca69e360e7}


PS C:\AmazonFSxADValidation> $Result.Warnings.Count
0
```

如果在运行验证工具时收到警告或错误，请参阅验证工具包中包含的故障排除指南（`TROUBLESHOOTING.md`）和Amazon FSx 故障排除 (p. 187).

加入 Amazon FSx 文件系统

当你创建适用于 Windows 文件服务器的新 FSx 文件系统时，你可以配置 Microsoft Active Directory 集成，以便它加入你自我管理的微软 Active Directory 域。为此，请为Microsoft AD 提供以下信息：

- 本地的 Microsoft AD D Directory 的完全限定域名

  Note

  亚马逊 FSx 目前不支持单一标签域 (SLD) 域。
- 域的 DNS 服务器的 DNS 服务器的 IP 地址。
- 本地的 Microsoft AD D D D D D 域中服务帐户的凭证。Amazon FSx 使用这些凭证加入您的自我管理广告。

或者，您也可以指定以下内容：

- 您希望 Amazon FSx 文件系统加入的域中的特定组织单位 (OU)。
- 为成员授予 Amazon FSx 文件系统管理权限的域组的名称。

指定此信息后，Amazon FSx 会使用您提供的服务账户将您的新文件系统加入到自我管理的 AD 域。

Important

只有在您加入文件系统的 AD 域使用 Microsoft DNS 作为默认 DNS 时，亚马逊 FSX 才会为该文件系统注册 DNS 记录。如果您使用的是第三方 DNS，则需要在创建文件系统后为 Amazon FSx 文件系统手动设置 DNS 条目。有关为文件系统选择正确 IP 地址的详细信息，请参阅获取用于 DNS 的正确文件系统 IP 地址 (p. 46).

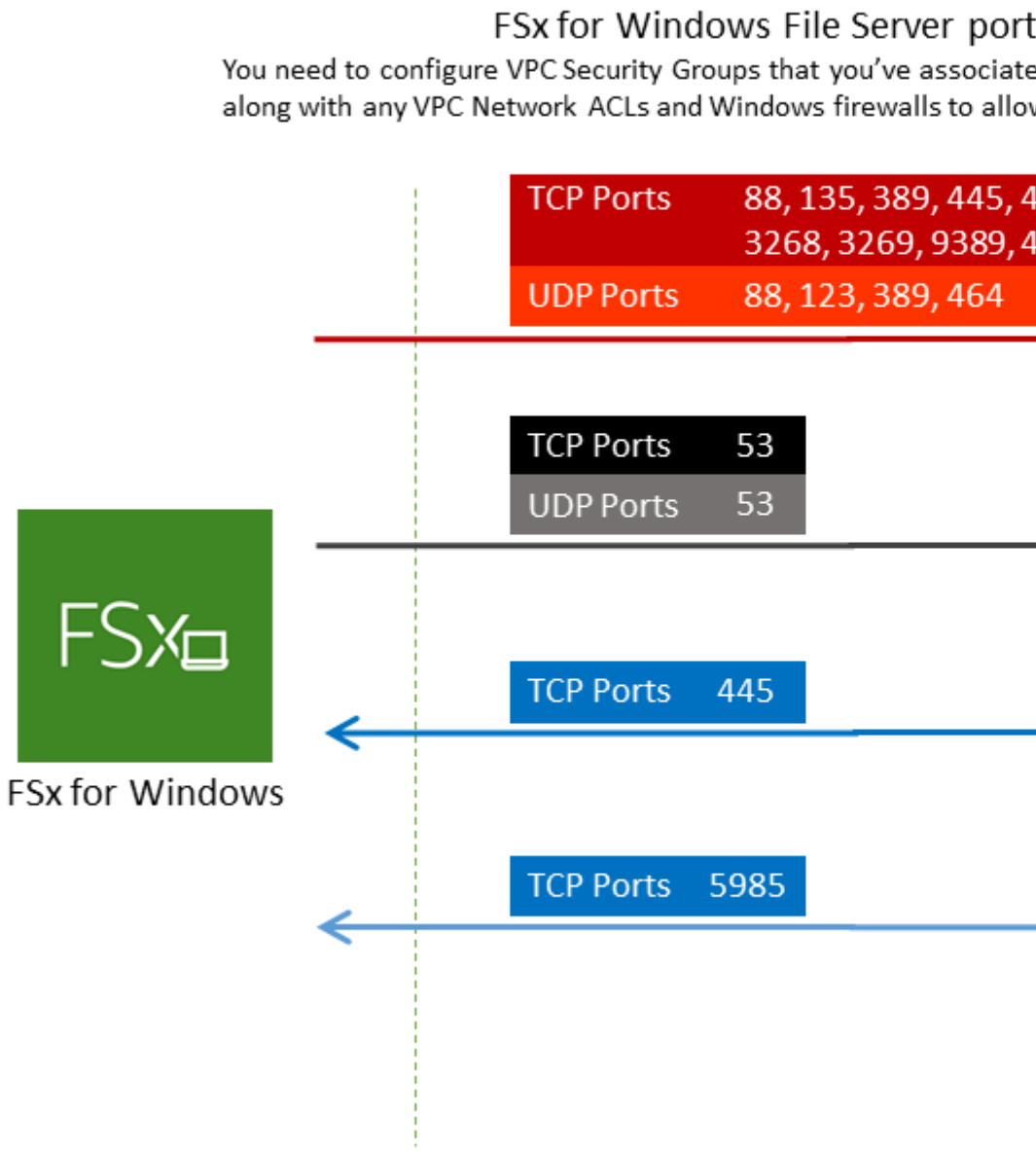
开始前的准备工作

请确保您已完成了使用自行管理的 Microsoft AD 的先决条件 (p. 31)在将 Amazon FSx 与自主管理的 Microsoft Active Directory 结合使用 (p. 30).

创建 FSx for Windows File Server 文件系统（控制台）

1. 从打开 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. 选择FSx for Windows File Server然后选择下一步. 显示创建文件系统 页面。
4. 为您的文件系统提供名称。最多可使用 256 个 Unicode 字母、空格和数字，以及特殊字符 +、-、=、_、:、_、:、:、:、.、_、:、:、:、:、.
5. 适用于存储容量中，输入文件系统的存储容量（以 GiB 为单位）的存储容量（以 GiB 为单位） 如果您使用的是 SSD 存储，请输入 32—65,536 范围内的任意整数。如果您使用的是硬盘存储，请输入 2,000—65,536 范围内的任何整数。创建文件系统后，您可以随时根据需要增加存储容量。有关更多信息，请参阅 管理存储容量 (p. 112)。
6. 保持吞吐量容量设置为原定设置。吞吐量能力是承载文件系统的文件服务器提供数据的持续速度。这些区域有：建议吞吐量容量量设置基于您选择的存储容量。如果您需要的容量超过建议的吞吐容量，请选择指定吞吐量容量量，然后选择一个值。有关更多信息，请参阅 FSx for Windows File Server 性能 (p. 141)。

   创建文件系统后，您可以随时根据需要修改吞吐量容量。有关更多信息，请参阅 管理吞吐量容量 (p. 122)。
7. 选择要与您的文件系统关联的 VPC。出于本入门练习的目的，请选择与您的 VPC 相同的 VPCAmazon Directory Service目录和Amazon EC2 实例。
8. 选择任意值可用区和子网.
9. 适用于VPC 安全组，您的默认 Amazon VPC 的默认安全组已添加到控制台中的文件系统中。请确保您在其中创建 FSx 文件系统的子网的安全组和 VPC 网络 ACL 允许端口和和的流量，如下图所示。



下表列出了每个端口的角色。

协议	端口	角色
TCP/UDP	53	域名系统 (DNS)
TCP/UDP	88	Kerberos 身份验证
TCP/UDP	464	更改/设置密码
TCP/UDP	389	轻型目录访问协议 (LDAD)
UDP	123	网络时间协议 (NTP)
TCP	135	分布式计算环境/端点映射器 (DCE/EPMAP)

协议	端口	角色
TCP	445	目录服务 SMB 文件共享
TCP	636	基于 TLS/SSL 的轻型目录访问协议 (LDAPS)
TCP	3268	Microsoft
TCP	3269	基于 SSL 的微软全球目录
TCP	5985	WinRM 2.0（微软 Windows 远程管理）

协议	端口	角色
TCP	9389	微软 AD DS 网络服务，PowerShell
TCP	49152 - 65535	RPC 的临时端口

Important

单可用区 2 和所有多可用区文件系统部署都需要允许 TCP 端口 9389 上的出站流量。

Note

如果您使用的是 VPC 网络 ACL，则还必须允许来自您的 FSx 文件系统的动态端口 (49152-65535) 上的出站流量。

- 出站规则，允许所有流量流向与自我管理的 Microsoft AD 域的 DNS 服务器和域控制器关联的 IP 地址。有关更多信息，请参阅 。微软关于为活动目录通信配置防火墙的文档.
- 确保这些流量规则也镜像到适用于每个 AD 域控制器、DNS 服务器、FSx 客户端和 FSx 管理员的防火墙上。

Note

如果已定义 Active Directory 站点，您必须确保在 Active Directory 站点中与您Amazon FSx 文件系统关联的 VPC 内定义了子网，并且 VPC 中的子网与您其他站点中的子网之间不存在冲突。您可以使用 Active Directory 站点和服务 MMC 管理单元查看和更改这些设置。

Important

虽然 Amazon VPC 安全组要求只在启动网络流量的方向打开端口，但大多数 Windows 防火墙和 VPC 网络 ACL 都要求双向打开端口。

10. 适用于Windows 身份验证，选择自行管理的 Microsoft A.
11. 为... 输入值完全限定域名自管理的 Microsoft AD D D D D D

Note

域名不得为单标签域 (SLD) 格式。Amazon FSx 目前不支持 SLD 域名。

Important

对于单可用区 2 和所有多可用区文件系统，Active Directory 域名不能超过 47 个字符。

12. 为... 输入值组织部门自管理的 Microsoft AD D D D D D

Note

确保您提供的服务帐号具有委派给您在此处指定的 OU 或默认 OU（如果未指定 OU）的权限。

13. 输入至少一个（不超过两个）的值DNS 服务器 IP 地址自管理的 Microsoft AD D D D D D
14. 为... 输入字符串值服务账户用户名用于自管理 AD 域中的帐户，例如`ServiceAcct`. 亚马逊 FSx 使用此用户名加入你的微软 AD 域。

    Important

    请勿包含域名前缀 (`corp.com\ServiceAcct`) 或域后缀 (`ServiceAcct@corp.com`) 在输入服务账户用户名.
    请勿在输入服务账户用户名(`CN=ServiceAcct,OU=example,DC=corp,DC=com`)。
15. 为... 输入值服务账户密码用于自管理 AD 域中的帐户。亚马逊 FSx 使用此密码加入你的微软 AD 域。
16. 重新输入密码以在确认密码.
17. 适用于委派文件系统管理员组，请指定`Domain Admins`组或自定义委派的文件系统管理员组（如果已创建）。您指定的组应具有在文件系统上执行管理任务的授权。如果未提供值，Amazon FSx 将使用内置的`Domain Admins`组中)。请注意，亚马逊 FSx 不支持`Delegated file system administrators group`（要么是`Domain Admins`组或您指定的自定义组）位于内置容器中。

    Important

    如果未提供委派文件系统管理员组，默认情况下 Amazon FSx 会尝试使用内置的`Domain Admins`组位于您的 AD 域中。如果此内置组的名称已更改，或者您正在使用其他组进行域管理，则必须在此处为该组提供该名称。

    Important

    请勿包含域前缀 (corp.com\ FSxAdmins) 或域后缀 (F)SxAdmins@corp .com) 提供组名参数时。
    请勿对组使用唯一判别名 (DN)。可分辨名称的示例是 CN=FSxAdmins，OU=example, DC=com。

创建 FSx for Windows File Server 文件系统，它加入自管理 AD (Amazon CLI)

以下示例创建 FSx for Windows File Server 文件系统`SelfManagedActiveDirectoryConfiguration`中的`us-east-2`可用区。

```
aws fsx --region us-east-2 \
create-file-system \
--file-system-type WINDOWS \
--storage-capacity 300 \
--security-group-ids security-group-id \
--subnet-ids subnet-id\
--windows-configuration
 SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",FileSystemAdministrators
 \
UserName="FSxService",Password="password", \
   DnsIps=["10.0.1.18"]}',ThroughputCapacity=8
```

Important

创建文件系统后，请勿移动 Amazon FSx 在 OU 中创建的计算机对象。这样做会导致文件系统配置错误。

获取用于 DNS 的正确文件系统 IP 地址

如果您使用微软 DNS 作为默认 DNS 服务，则 Amazon FSx 仅为文件系统注册 DNS 记录。如果您使用的是第三方 DNS，则需要为 Amazon FSx 文件系统手动设置 DNS 条目。本节介绍如果必须手动将文件系统添加到 DNS 中，如何获取要使用的正确的文件系统 IP 地址。

如何获取用于 DNS A 条目的文件系统 IP 地址

1. 在https://console.aws.amazon.com/fsx/中，选择要获取 IP 地址以显示文件系统详细信息页面的文件系统。
2. 在网络和安全选项卡执行以下操作之一：

   - 对于单可用区 1 文件系统：
     - 在子网面板中，选择下方显示的 elastic network interface网络接口以打开网络接口Amazon EC2 控制台中的页面。
     - 要使用的单可用区 1 文件系统的 IP 地址如主要私有 IPv4 IP 地址column.
   - 对于单可用区 2 或多可用区域文件系统：
     - 在首选子网面板中，选择下方显示的 elastic network interface网络接口以打开网络接口Amazon EC2 控制台中的页面。
     - 要使用的首选子网的 IP 地址显示在辅助私有 IPv4 IP 地址column.
     - 在 Amazon FSx备用子网面板中，选择下方显示的 elastic network interface网络接口以打开网络接口Amazon EC2 控制台中的页面。
     - 要使用的备用子网的 IP 地址显示在辅助私有 IPv4 IP 地址column.

更新自行管理的 Active Directory 配置

您可以使用Amazon Web Services Management Console、亚马逊 FSx API，或Amazon CLI以更新服务帐户的用户名和密码以及自管 Active Directory 配置的 Active Directory DNS 服务器的 IP 地址。您可以随时使用Amazon Web Services Management ConsoleAPI、CLI 和 API。有关更多信息，请参阅 监控自托管的 Active Directory 更新 (p. 47)。

更新自主管理的 Active Directory 配置 (控制台)

1. 打开 Amazon FSx 控制台https://console.aws.amazon.com/fsx/.
2. 导航到文件系统，然后选择要更新自主管理 AD 配置的 Windows 文件系统。
3. 在网络和安全选项卡，然后选择更新(对于)DNS 服务器 IP 地址，或服务帐户用户名，具体取决于您要更新的 Active Directory 属性。
4. 在显示的对话框中输入新的 DNS 服务器 IP 地址或新的服务帐户凭据。
5. 选择更新以启动 Active Directory 配置更新。

   您可以监控更新进度 (p. 47)使用Amazon Web Services Management Console或者Amazon CLI.

要更新自主管理的 Active Directory 配置 (CLI)

- 要更新 FSx for Windows File Server 文件系统的自主管理 Active Directory 配置，请使用Amazon CLI命令更新文件系统. 设置以下参数：

  - `--file-system-id`转到您要更新的文件系统的 ID。
  - `UserName`自管 AD 服务帐户的新用户名。
  - `Password`自管 AD 服务帐户的新密码。
  - `DnsIps`自管 AD DNS 服务器的 IP 地址。

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --windows-configuration
 SelfManagedActiveDirectoryConfiguration={UserName=username,Password=password,DnsIps=[192.0.2.0,192
```

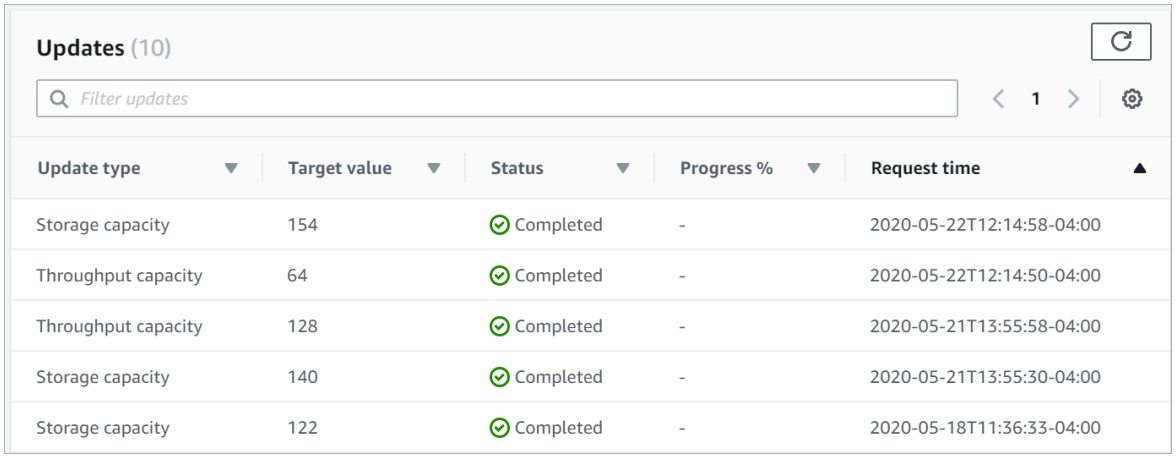
如果更新操作成功，则该服务将会发送回 HTTP 200 响应。这些区域有： AdminstrativeActions 响应中的数据描述了请求及其状态。有关更多信息，请参阅 监控自托管的 Active Directory 更新 (p. 47)。

监控自托管的 Active Directory 更新

您可以使用Amazon Web Services Management Console、API 或Amazon CLI.

在控制台中监控更新

在更新在中的选项卡文件系统详情窗口中，您可以查看每种更新类型的 10 个最近更新。



对于自主管理的 Active Directory 更新，您可以查看以下信息。

更新类型

支持的类型如下：

- DNS 服务器 IP 地址
- 服务帐户凭证

Target value (目标值)

将文件系统属性更新到的所需值。适用于服务帐户凭证更新，仅显示用户名，服务帐户密码永远不会包含在此字段中。

状态

更新的当前状态。对于自我管理的 Active Directory 更新，可能的值如下：

- Pending— 亚马逊 FSx 已收到更新请求，但尚未开始处理。
- 正在进行中— 亚马逊 FSx 正在处理更新请求。
- 已完成— 文件系统更新已成功完成。
- 已失败— 文件系统更新失败。选择问号 (?) 以查看失败的详细信息。

进度%

将文件系统更新进度显示为完成百分比。

请求时间

亚马逊 FSx 收到更新操作请求的时间。

使用Amazon CLI和 API

您可以使用描述文件系统 Amazon CLI命令和DescribeFileSystemsAPI 操作。这些区域有：`AdministrativeActions`阵列列出了每种管理操作类型的 10 个最近更新操作。

以下示例展示了响应摘录describe-file-systemsCLI 命令显示两个自我管理的 AD 文件系统更新。

```
    {
        "OwnerId": "111122223333",
        .
        .
        .
        "StorageCapacity": 1000,
        "AdministrativeActions": [
            {
                "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                "RequestTime": 1581694766.757,
                "Status": "PENDING",
                "TargetFileSystemValues": {
                    "WindowsConfiguration": {
                        "SelfManagedActiveDirectoryConfiguration": {
                            "UserName": "serviceUser",
                        }
                    }
                }
            },
            {
                "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                "RequestTime": 1619032957.759,
                "Status": "FAILED",
                "TargetFileSystemValues": {
                    "WindowsConfiguration": {
                        "SelfManagedActiveDirectoryConfiguration": {
                        "DnsIps": [
                                "10.0.138.161"
                            ]
                        }
                    }
                },
                "FailureDetails": {
                    "Message": "Failure details message."
                }
            }
        ],
.
.
.
```

使用微软 Windows 文件共享

Microsoft Windows文件共享是文件系统中的特定文件夹。它包括该文件夹的子文件夹，您可以使用服务器消息块 (SMB) 协议向计算实例访问该文件夹的子文件夹。你的文件系统附带默认的 Windows 文件共享，名为`share`. 您可以使用名为的 Windows 图形用户界面 (GUI) 工具创建和管理任意数量的其他 Windows 文件共享共享文件夹.

访问文件共享

要访问文件共享，您可以使用 Windows Map Network Drive 功能将计算实例上的驱动器盘符映射到 Amazon FSx 文件共享。将文件共享映射到计算实例上的驱动器的过程称为安装中Linux 中的文件共享。此过程因计算实例的类型和操作系统而异。映射文件共享后，应用程序和用户可以访问文件共享上的文件和文件夹，就像它们是本地文件和文件夹一样。

以下是在不同支持的计算实例上映射文件共享的过程。

主题

在 Amazon EC2 Windows 实例上映射文件共享

您可以使用 Windows 文件资源管理器或命令提示符在 EC2 Windows 实例上映射文件共享。

将文件共享映射到 Amazon EC2 Windows 实例（控制台）

1. 启动 EC2 Windows 实例并将其连接到您加入了 Amazon FSx 文件系统的微软 Active Directory。为此，请从Amazon Directory Service管理指南：
   - 无缝加入 Windows EC2 实例
   - 手动加入 Windows 实例
2. 连接到您的 EC2 Windows 实例。有关更多信息，请参阅《适用于 Windows 实例的 Amazon EC2 用户指南》中的连接您的 Windows 实例。
3. 连接后，请打开文件资源管理器。
4. 在导航窗格中，打开的上下文 (右键单击) 菜单网络，然后选择映射网络驱动器.
5. 适用于Drive，选择驱动器盘符。
6. 适用于文件夹中，输入文件系统的 DNS 名称或与文件系统关联的 DNS 别名，以及共享名称。

   您可以在Amazon FSx 控制台通过选择Windows 文件 Server、网络 & 安全. 或者，您可以在响应中找到它们CreateFileSystem要么DescribeFileSystemsAPI 操作。有关使用 DNS 别名的更多信息，请参阅。管理 DNS 别名 (p. 82).

   - 对于加入到的单可用区文件系统Amazon托管微软活动目录，DNS 名称如下所示。

```
fs-0123456789abcdef0.ad-domain.com
```

- 对于加入到自管 Active Directory 的单可用区文件系统以及任何多可用区文件系统，DNS 名称如下所示。

```
amznfsxaa11bb22.ad-domain.com
```

例如，要使用单可用区文件系统的 DNS 名称，请为文件夹.

```
\\fs-0123456789abcdef0.ad-domain.com\share
```

要使用多可用区文件系统的 DNS 名称，请输入以下文件夹.

```
\\famznfsxaa11bb22.ad-domain.com\share
```

要使用与文件系统关联的 DNS 别名，请为文件夹.

```
\\fqdn-dns-alias\share
```

7. 选择一个选项登录时重新连接，表示文件共享是否应在登录时重新连接，然后选择Finish.

在 Amazon EC2 Windows 实例上映射文件共享（命令提示符）

1. 启动 EC2 Windows 实例并将其连接到您加入了 Amazon FSx 文件系统的微软 Active Directory。为此，请从Amazon Directory Service管理指南：
   - 无缝加入 Windows EC2 实例
   - 手动加入 Windows 实例
2. 以用户身份 Connect 到 EC2 Windows 实例Amazon Managed Microsoft AD目录。有关更多信息，请参阅《适用于 Windows 实例的 Amazon EC2 用户指南》中的连接您的 Windows 实例。
3. 连接后，请打开命令提示符窗口。
4. 使用您选择的驱动器盘符、文件系统的 DNS 名称和共享名称挂载文件共享。你可以使用Amazon FSx 控制台通过选择Windows 文件 Server、网络 & 安全. 或者，您可以在响应中找到它们`CreateFileSystem`要么`DescribeFileSystems`API 操作。
   - 对于加入到的单可用区文件系统Amazon托管微软活动目录，DNS 名称如下所示。

```
fs-0123456789abcdef0.ad-domain.com
```

   - 对于加入到自管 Active Directory 的单可用区文件系统以及任何多可用区文件系统，DNS 名称如下所示。

```
amznfsxaa11bb22.ad-domain.com
```

下面是挂载文件共享的示例命令。

```
$ net use H: \\amzfsxaa11bb22.ad-domain.com\share /persistent:yes
```

而不是`net use`命令，你也可以使用任何受支持的 PowerShell 命令来挂载文件共享。

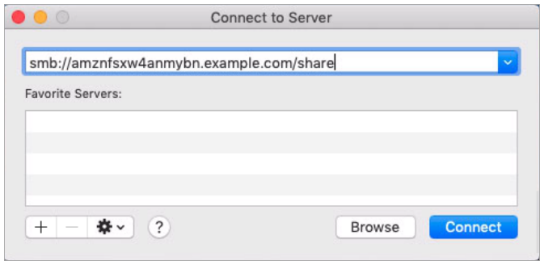
在 Amazon EC2 Mac 实例上挂载文件共享

您可以在已加入 Active Directory 或未加入的 Amazon EC2 Mac 实例上挂载文件共享。如果实例未加入您的 Active Directory，请务必更新为实例所在的 Amazon Virtual Private Cloud (Amazon VPC) 设置的 DHCP 选项，以包括您的 Active Directory 域的 DNS 名称服务器。然后重新启动实例。

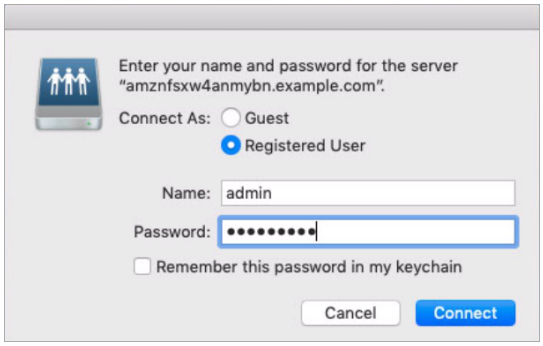
在 Amazon EC2 Mac 实例上装载文件共享 (GUI)

1. 启动 EC2 Mac 实例。为此，请从适用于 Linux 实例的 Amazon EC2 用户指南：
   - 使用控制台启动 Mac 实例
   - 使用启动 Mac 实例Amazon CLI
2. 使用虚拟网络计算 (VNC) Connect 到 EC2 Mac 实例。有关更多信息，请参阅 。使用 VNC 连接到您的实例。中的适用于 Linux 实例的 Amazon EC2 用户指南.
3. 在 EC2 Mac 实例上，连接到您的 Amazon FSx 文件共享，如下所示：
   a. 打开 Finder，选择转到，然后选择Connect 到 Server.
   b. 在Connect 到 Server对话框中，输入文件系统的 DNS 名称或与文件系统关联的 DNS 别名，以及共享名称。然后选择 Connect（连接）。

      您可以在Amazon FSx 控制台通过选择Windows 文件 Server、网络 & 安全. 或者，您可以在响应中找到它们CreateFileSystem要么DescribeFileSystemsAPI 操作。有关使用 DNS 别名的更多信息，请参阅。管理 DNS 别名 (p. 82).

   c. 在下一个屏幕上，选择Connect (连接)以继续。
   d. 输入 Amazon FSx 服务帐户的 Microsoft Active Directory (AD) 凭据，如以下示例所示。然后选择 Connect（连接）。

   e. 如果连接成功，您可以在下面看到 Amazon FSx 共享Locations在 “访达” 窗口中。

在 Amazon EC2 Mac 实例上挂载文件共享（命令行）

1. 启动 EC2 Mac 实例。为此，请从适用于 Linux 实例的 Amazon EC2 用户指南：

- 使用控制台启动 Mac 实例
- 使用启动 Mac 实例Amazon CLI

2. 使用虚拟网络计算 (VNC) Connect 到 EC2 Mac 实例。有关更多信息，请参阅 。使用 VNC 连接到您的实例。中的适用于 Linux 实例的 Amazon EC2 用户指南.
3. 使用以下命令挂载文件共享。

```
mount_smbfs //file_system_dns_name/file_share mount_point
```

你可以在Amazon FSx 控制台通过选择Windows 文件 Server、网络 & 安全. 或者，您可以在响应中找到它们`CreateFileSystem`要么`DescribeFileSystems`API 操作。

- 对于加入到的单可用区文件系统Amazon托管微软活动目录，DNS 名称如下所示。

```
fs-0123456789abcdef0.ad-domain.com
```

- 对于加入到自管 Active Directory 的单可用区文件系统以及任何多可用区文件系统，DNS 名称如下所示。

```
amznfsxaa11bb22.ad-domain.com
```

此过程中使用的 mount 命令在给定时间点执行以下操作：

- *//file_system_dns_name/file_share*— 指定要挂载的文件系统的 DNS 名称和共享。
- *mount_point*— 要装载文件系统的 EC2 实例上的目录。

在 Amazon EC2 Linux 实例上装载文件共享

您可以在已加入 Active Directory 或未加入的 Amazon EC2 Linux 实例上装载 FSx for Windows 文件服务器文件共享。

Note

以下命令仅指定参数，例如 SMB 协议、缓存以及读写缓冲区大小作为示例。Linux 的参数选择`cifs`命令以及使用的 Linux 内核版本可能会影响客户端和 Amazon FSx 文件系统之间网络操作的吞吐量和延迟。有关更多信息，请参阅 。`cifs`您正在使用的 Linux 环境的文档。

在加入到 Active Directory 的 Amazon EC2 Linux 实例上挂载文件共享

1. 如果你还没有将正在运行的 EC2 Linux 实例加入到你的 Microsoft Active Directory 中，请参阅手动加入 Linux 实例中的Amazon Directory Service管理指南为此，请按照指示操作。
2. Connect 到 EC2 Linux 实例。有关更多信息，请参阅适用于 Linux 实例的 Amazon EC2 用户指南中的连接到您的 Linux 实例。
3. 运行以下命令以下命令来安装`cifs-utils`程序包。此软件包用于在 Linux 上挂载诸如 Amazon FSx 之类的网络文件系统。

```
$ sudo yum install cifs-utils
```

4. 创建挂载点目录**`/mnt/fsx`**. 您将在这里挂载 Amazon FSx 文件系统。

```
$ sudo mkdir -p /mnt/fsx
```

5. 使用以下命令使用 kerberos 进行身份验证。

```
$ kinit
```

6. 使用以下命令挂载文件共享。

```
$ sudo mount -t cifs //file_system_dns_name/file_share mount_point --verbose -o
 vers=SMB_version,sec=krb5,cruid=ad_user,rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize,cache=none,ip=pr
file-server-Ip
```

   你可以在Amazon FSx 控制台通过选择Windows 文件 Server、网络 & 安全. 或者，您可以在响应中找到它们`CreateFileSystem`要么`DescribeFileSystems`API 操作。

   - 对于加入到的单可用区文件系统Amazon托管微软活动目录，DNS 名称如下所示。

     ```
     fs-0123456789abcdef0.ad-domain.com
     ```

   - 对于加入到自管 Active Directory 的单可用区文件系统以及任何多可用区文件系统，DNS 名称如下所示。

     ```
     amznfsxaa11bb22.ad-domain.com
     ```

   Replace*CIFSMaxBufSize*具有内核允许的最大值。运行以下命令以下命令以获取此值。

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

   输出显示最大缓冲区大小为 130048。

7. 通过运行以下命令验证文件系统是否已装载，该命令仅返回普通 Internet 文件系统 (CIFS) 类型的文件系统。

```
$ mount -l -t cifs
//fs-0123456789abcdef0/share on /mnt/fsx type cifs
 (rw,relatime,vers=SMB_version,sec=krb5,cache=cache_mode,username=user1@CORP.NETWORK.COM,uid=0,nofo
```

此过程中使用的 mount 命令在给定时间点执行以下操作：

- `//`*file_system_dns_name*`/`*file_share*— 指定要挂载的文件系统的 DNS 名称和共享。
- *mount_point*— 要装载文件系统的 EC2 实例上的目录。
- `-t cifs vers=`*SMB_version*— 将文件系统的类型指定为 CIFS 和 SMB 协议版本。适用于 Windows 文件服务器的亚马逊 FSx 支持中小型企业 2.0 至 3.1.1 版本。
- `sec=krb5`— 指定使用 Kerberos 版本 5 进行身份验证。
- `cache=`*cache_mode*— 设置缓存模式。CIFS 缓存的此选项可能会影响性能，您应该测试哪些设置最适合内核和工作负载（并查看 Linux 文档）。选项`strict`和`none`是推荐的，因为`loose`由于协议语义较宽松，可能会导致数据不一致。
- `cruid=`*ad_user*— 将凭据缓存所有者的 uid 设置给 AD 目录管理员。
- */mnt/fsx*— 指定 Amazon FSx 文件共享在 EC2 实例上的挂载点。
- `rsize=`*CIFSMaxBufSize*`,wsize=`*CIFSMaxBufSize*— 将读取和写入缓冲区大小指定为 CIFS 协议允许的最大值。Replace*CIFSMaxBufSize*具有内核允许的最大值。确定`CIFSMaxBufSize`通过运行以下命令。

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default: 16384
 Range: 8192 to 130048 (uint)
```

输出显示最大缓冲区大小为 130048。

- ip=*preferred-file-server-Ip*— 将目标 IP 地址设置为文件系统首选文件服务器的 IP 地址。

  您可以按如下方式检索文件系统的首选文件服务器 IP 地址：

  - 使用亚马逊 FSx 控制台，在网络 & 安全的选项卡文件系统详情页.
  - 在回应中`describe-file-systems`CLI 命令或等效命令DescribeFileSystemsAPI 命令。

在未加入活动目录的 Amazon EC2 Linux 实例上装载文件共享

以下过程将 Amazon FSx 文件共享装载到未加入您的 Active Directory (AD) 的 Amazon EC2 Linux 实例。对于 EC2 Linux 实例不加入活动目录后，只能使用其私有 IP 地址挂载 FSx for Windows 文件服务器文件共享。你可以使用Amazon FSx 控制台，在网络 & 安全选项卡，首选的文件服务器 IP 地址.

此示例使用 NTLM 身份验证。要执行此操作，您可以作为已加入 FSx for Windows 文件服务器文件系统的 Microsoft Active Directory 域的成员的用户挂载文件系统。用户账户的凭证在您在 EC2 实例上创建的文本文件中提供，`creds.txt`. 此文件包含用户的用户名、密码和域。

```
$ cat creds.txt
username=user1
password=Password123
domain=EXAMPLE.COM
```

启动和配置 Amazon Linux EC2 实例

1. 使用Amazon EC2 控制台. 有关更多信息，请参阅 。启动实例中的适用于 Linux 实例的 Amazon EC2 用户指南.
2. Connect 到 Amazon Linux EC2 实例。有关更多信息，请参阅适用于 Linux 实例的 Amazon EC2 用户指南中的连接到您的 Linux 实例。
3. 运行以下命令以下命令来安装`cifs-utils`程序包。此软件包用于在 Linux 上挂载诸如 Amazon FSx 之类的网络文件系统。

   ```
   $ sudo yum install cifs-utils
   ```

4. 创建挂载点**`/mnt/fsxx`**您计划在哪里挂载 Amazon FSx 文件系统。

   ```
   $ sudo mkdir -p /mnt/fsx
   ```

5. 创建`creds.txt`中的凭证文件`/home/ec2-user`目录，使用之前显示的格式。
6. 设置`creds.txt`文件权限，以便只有您（所有者）可以通过运行以下命令对文件进行读写。

   ```
   $ chmod 700 creds.txt
   ```

挂载文件系统

1. 您可以使用 Active Directory 的私有 IP 地址挂载未加入到 Active Directory 的文件共享。你可以使用Amazon FSx 控制台，在网络 & 安全选项卡，在首选文件 Server IP 地址.
2. 使用以下命令挂载文件系统：

```
$ sudo mount -t cifs //file-system-IP-address/file_share /mnt/fsx
 --verbose -o vers=SMB_version,sec=ntlmsspi,cred=/home/ec2-user/
creds.txt,rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize,cache=none
```

Replace*CIFSMaxBufSize*具有内核允许的最大值。运行以下命令以下命令以获取此值。

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

输出显示最大缓冲区大小为 130048。

3. 通过运行以下命令验证文件系统是否已装载，该命令仅返回 CIFS 文件系统。

```
$ mount -l -t cifs
//file-system-IP-address/file_share on /mnt/fsx type cifs
 (rw,relatime,vers=SMB_version,sec=ntlmsspi,cache=cache_mode,username=user1,domain=CORP.EXAMPLE.COM
```

此过程中使用的 mount 命令在给定时间点执行以下操作：

- *//file-system-IP-address/file_share*— 指定要挂载的文件系统的 IP 地址和共享。
- `-t cifs vers=`*SMB_version*— 将文件系统的类型指定为 CIFS 和 SMB 协议版本。适用于 Windows 文件服务器的亚马逊 FSx 支持中小型企业 2.0 至 3.1.1 版本。
- `sec=ntlmsspi`— 指定使用 NT 局域网管理器安全 Support 提供程序接口 (NTLMSSPI) 进行身份验证。
- `cache=`*cache_mode*— 设置缓存模式。CIFS 缓存的此选项可能会影响性能，您应该测试哪些设置最适合内核和工作负载（并查看 Linux 文档）。选项`strict`和`none`是推荐的，因为`loose`由于协议语义较宽松，可能会导致数据不一致。
- `cred=/home/ec2-user/creds.txt`— 指定在哪里获取用户凭据。
- */mnt/fsx*— 指定 Amazon FSx 文件共享在 EC2 实例上的挂载点。
- `rsize=`*CIFSMaxBufSize*`,wsize=`*CIFSMaxBufSize*— 将读取和写入缓冲区大小指定为 CIFS 协议允许的最大值。Replace*CIFSMaxBufSize*具有内核允许的最大值。确定`CIFSMaxBufSize`通过运行以下命令。

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default: 16384
 Range: 8192 to 130048 (uint)
```

输出显示最大缓冲区大小为 130048。

在未加入 Active Directory 的 Amazon Linux EC2 实例上自动挂载文件共享

只要装载到的 Amazon EC2 Linux 实例重新启动，您就可以自动装载您的 fSx for Windows 文件服务器文件共享。为此，请将条目添加到`/etc/fstab`文件在 EC2 实例上。`/etc/fstab` 文件包含有关文件系统的信息。该命令`mount -a`，在实例启动期间运行，用于挂载`/etc/fstab`文件。

对于未加入 Active Directory 的 Amazon Linux EC2 实例，您只能使用私有 IP 地址挂载 FSx for Windows 文件服务器文件共享。你可以使用Amazon FSx 控制台，在网络 & 安全选项卡，首选的文件服务器 IP 地址.

以下过程使用微软 NTLM 身份验证。您以作为 Microsoft Active Directory 域的成员的用户挂载文件系统，而 FSx for Windows File Server 系统已加入该域。文本文件中提供了用户帐户的凭据`creds.txt`. 此文件包含用户的用户名、密码和域。

```
$ cat creds.txt
username=user1
password=Password123
domain=EXAMPLE.COM
```

在未加入 Active Directory 的 Amazon Linux EC2 实例上自动挂载文件共享

启动和配置 Amazon Linux EC2 实例

1. 使用Amazon EC2 控制台. 有关更多信息，请参阅 。启动实例中的适用于 Linux 实例的 Amazon EC2 用户指南.
2. 连接到您的实例。有关更多信息，请参阅适用于 Linux 实例的 Amazon EC2 用户指南中的连接到您的 Linux 实例。
3. 运行以下命令以下命令来安装`cifs-utils`程序包。此软件包用于在 Linux 上挂载诸如 Amazon FSx 之类的网络文件系统。

   ```
   $ sudo yum install cifs-utils
   ```
4. 创建 `/mnt/fsx` 目录。您将在这里挂载 Amazon FSx 文件系统。

   ```
   $ sudo mkdir /mnt/fsx
   ```
5. 创建`creds.txt`中的凭证文件`/home/ec2-user`目录。
6. 设置文件权限，以便只有您（所有者）可以通过运行以下命令读取文件。

   ```
   $ sudo chmod 700 creds.txt
   ```

自动挂载文件系统

1. 您可以使用 Active Directory 的私有 IP 地址自动挂载未加入到 Active Directory 的文件共享。您可以从Amazon FSx 控制台，在网络 & 安全选项卡，首选的文件服务器 IP 地址.
2. 要使用文件共享的私有 IP 地址自动挂载文件共享，请将以下行添加到`/etc/fstab`文件。

   ```
   //file-system-IP-address/file_share /mnt/fsx cifs vers=SMB_version,sec=ntlmsspi,cred=/
   home/ec2-user/creds.txt,rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize,cache=none
   ```

   Replace*CIFSMaxBufSize*具有内核允许的最大值。运行以下命令以下命令以获取此值。

   ```
   $ modinfo cifs | grep CIFSMaxBufSize
   parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
    16384 Range: 8192 to 130048 (uint)
   ```

   输出显示最大缓冲区大小为 130048。
3. 测试`fstab`通过使用`mount`带 “fake” 选项的命令与 “all” 和 “verbose” 选项结合使用。

   ```
   $ sudo mount -fav
   home/ec2-user/fsx      : successfully mounted
   ```
4. 要挂载文件共享，请重新启动 Amazon EC2 实例。

5. 实例再次可用时，请通过运行以下命令验证文件系统是否已挂载。

```
$ sudo mount -l -t cifs
//file-system-IP-address/file_share on /mnt/fsx type cifs
 (rw,relatime,vers=SMB_version,sec=ntlmsspi,cache=cache_code,username=user1,domain=CORP.EXAMPLE.COM
```

添加到/etc/fstab在此过程中的文件在给定时刻执行以下操作：

- //*file-system-IP-address*/*file_share*— 指定您要安装的 Amazon FSx 文件系统的 IP 地址和共享。
- /mnt/fsx— 指定 Amazon FSx 文件系统在 EC2 实例上的挂载点。
- cifs vers=*SMB_version*— 将文件系统的类型指定为 CIFS 和 SMB 协议版本。适用于 Windows 文件服务器的亚马逊 FSx 支持中小型企业 2.0 至 3.1.1 版本。
- sec=ntlmsspi— 指定使用 NT LAN Manager 安全 Support 提供商界面来促进 NTLM 质询-响应身份验证。
- cache=*cache_mode*— 设置缓存模式。CIFS 缓存的此选项可能会影响性能，您应该测试哪些设置最适合内核和工作负载（并查看 Linux 文档）。选项strict和none是推荐的，因为loose由于协议语义较宽松，可能会导致数据不一致。
- cred=/home/ec2-user/creds.txt— 指定在哪里获取用户凭据。
- _netdev— 向操作系统指示文件系统位于需要网络访问的设备上。使用此选项禁止实例挂载文件系统，直到在客户端上启用了网络服务。
- 0— 表示应由备份文件系统dump，如果它是非零值。对于亚马逊 FSx，此值应为0.
- 0— 指定顺序fsck启动时检查文件系统。对于 Amazon FSx 文件系统，此值应为0来表明fsck不应该在启动时运行。

将现有文件存储迁移到 Amazon FSx

FSx for Windows File Server 具有功能、性能和兼容性，可帮助您轻松提升企业应用程序并将其转移到 Amazon Web Services 科技云。迁移到 FSx for Windows File Server 的过程包括以下步骤：

1. 将您的文件迁移到 FSx for Windows File Server。有关更多信息，请参阅 将现有文件存储迁移到 FSx for Windows File Server (p. 58)。
2. 将您的文件共享配置迁到 FSx for Windows File Server。有关更多信息，请参阅 将文件共享配置迁移到 Amazon FSx (p. 62)。
3. 将您现有的 DNS 名称关联为 Amazon FSx 文件系统的 DNS 别名。有关更多信息，请参阅 。将 DNS 别名与亚马逊 FSx 关联 (p. 63).
4. 切换到 FSx for Windows File Server。有关更多信息，请参阅 切入亚马逊 FSX (p. 65)。

您可以在以下章节找到有关流程中每个步骤的详细信息。

主题

将现有文件存储迁移到 FSx for Windows File Server

要将现有文件迁移到 FSx for Windows File Server 文件系统，我们建议使用Amazon DataSync，这是一项在线数据传输服务，旨在简化、自动化和加速向、复制大量数据的过程，并加快从复制大量数据的过程Amazon存储服务。 DataSync 通过 Internet 复制数据或Amazon Direct Connect. 作为一项完全托管服务，DataSync 无需修改应用程序、开发脚本或管理基础设施。有关更多信息，请参阅 使用以下命令将现有文件迁到 FSx for Windows File Server 使用Amazon DataSync (p. 59)。

作为替代解决方案，你可以使用 Robocopy 或 Robocopy，后者是适用于 Microsoft Windows 的命令行目录和文件复制命令集。有关如何使用 Robocopy 将文件存储迁移到 FSx for Windows File Server 的详细过程，请参阅使用 Robocopy 将现有文件迁移到 FSx for Windows File Server (p. 59).

将现有文件存储迁移到 FSx for Windows File Server 的最佳实践

要尽快将大量数据迁移到 FSx for Windows File Server，请使用配置了固态硬盘 (SSD) 存储的 Amazon FSx 文件系统。迁移完成后，您可以使用硬盘驱动器 (HDD) 存储将数据移动到 Amazon FSx 文件系统（如果这是最适合您的应用程序的解决方案）。

要将数据从使用 SDD 存储的 Amazon FSx 文件系统移动到 HDD 存储，您可以执行以下步骤。（请注意，HDD 文件系统至少有 2TB 的存储容量，从备份还原时无法更改存储容量。）

1. 备份 SSD 文件系统。有关更多信息，请参阅 创建用户启动的备份 (p. 72)。
2. 使用 HDD 存储将备份还原到文件系统。有关更多信息，请参阅 还原备份 (p. 75)。

使用以下命令将现有文件迁到 FSx for Windows File Server 使用Amazon DataSync

我们建议使用Amazon DataSync在 FSx for Windows File Server 文件系统之间传输数据。 DataSync 是一项数据传输服务，可以简化、自动完成并加快在本地存储系统与其他Amazon通过 Internet 或Amazon 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，例如，所有权、时间戳和访问权限。

DataSync 支持复制 NTFS 访问控制列表 (ACL)，还支持复制文件审核控制信息（也称为 NTFS 系统访问控制列表 (SACL)），管理员使用这些信息来控制用户尝试访问文件的审核日志记录。

您可以使用 DataSync 在两个 FSx for Windows File Server 文件系统之间传输文件，并将数据移动到不同文件系统中的文件系统Amazon Web Services 区域要么Amazonaccount. 您可以使用 DataSync 使用 FSx for Windows File Server 文件系统用于其他任务。例如，您可以执行一次性数据迁移，定期提取分布式工作负载的定期数据，以及安排复制以实现数据保护与恢复。

InAmazon DataSync，a位置for FSx for Windows 文件服务器是FSx for Windows File Server 的端点。您可以在 FSx for Windows File Server 的位置与其他文件系统的位置之间传输文件。想要了解有关信息，请参阅使用位置中的Amazon DataSync用户指南.

DataSync 使用服务器消息块 (SMB) 协议访问您的 FSx for Windows File Server。它使用您在中配置的用户名和密码来进行身份验证Amazon DataSync控制台或Amazon CLI.

先决条件

要将数据迁移到 Amazon FSx for Windows File Server 设置中，您需要一台服务器和网络满足 DataSync 要求。要了解更多信息，请参阅的 要求 DataSync中的Amazon DataSync用户指南.

如果正在使用 HDD 存储，并且将使用 DataSync，我们建议您切换到 SSD 存储。有关更多信息，请参阅 将现有文件存储迁移到 FSx for Windows File Server 的最佳实践 (p. 58)。

当你有 DataSync 要求到位，您可以按照以下讨论开始转移。

使用迁移文件的基本步骤 DataSync

使用源位置将文件从源位置传输到目标位置，使用使用源位置使用 DataSync, 执行以下基本步骤:

- 在您的环境中下载并部署代理，然后激活。
- 创建并配置源和目标位置。
- 创建并配置任务。
- 运行任务，将文件从源传输到目标。

如需了解如何将文件从现有的本地文件系统传输到 FSx for Windows File Server 中，请参阅，请参阅在自我管理的存储和之间传输数据Amazon、为 SMB 创建位置, 和为 Amazon FSx for Windows File Server 创建位置中的Amazon DataSync用户指南.

如需了解如何将文件从现有云端文件系统传输到 FSx for Windows File Server，请参阅，请参阅将您的代理部署为 Amazon EC2 实例中的Amazon DataSync用户指南.

使用 Robocopy 将现有文件迁移到 FSx for Windows File Server

适用于 Windows 文件服务器的 Amazon FSx 基于微软 Windows Server 构建，使您能够将现有数据集完全迁移到亚马逊 FSx 文件系统中。您可以迁移每个文件的数据。您还可以迁移所有相关的文件元数据，包括属

性、时间戳、访问控制列表 (ACL)、所有者信息和审核信息。借助这种全面的迁移支持，Amazon FSx 可以将基于 Windows 的工作负载和依赖这些文件数据集的应用程序迁移到Amazon Web Services 科技云。

以下主题可指导您完成复制现有文件数据的过程。在执行此复制时，您将保留来自本地数据中心或 Amazon EC2 上自管理文件服务器的所有文件元数据。

先决条件

开始之前，请确保您已执行以下操作：

- 建立网络连接（通过使用Amazon Direct Connect或者 VPN）在您的本地活动目录和要在其中创建 Amazon FSx 文件系统的 VPC 之间。
- 在 Active Directory 上创建具有将计算机加入域的委派权限，创建服务账户。有关更多信息，请参阅 。将权限委派给您的服务账户中的Amazon Directory Service管理指南.
- 创建一个 Amazon FSx 文件系统，将其加入到自管理（本地）Microsoft AD 目录中。
- 记下位置（例如，`\\Source\Share`）的文件共享（本地或在Amazon)，其中包含您要转移到 Amazon FSx 的现有文件。
- 记下位置（例如，`\\Target\Share`)，您希望通过现有文件传输到的 Amazon FSx 文件系统上的文件共享。

下表总结了三种迁移用户访问模式的源文件系统和目标文件系统可访问性要求。

迁移用户访问模型	源文件系统可访问性要求	目标 FSx 文件服务器可访问性要求
直接读/写权限模型	用户需要至少对要迁移的文件和文件夹具有读取权限 (NTFS ACL)。	用户至少需要对要迁移的文件和文件夹具有写入权限 (NTFS ACL)。
用于覆盖访问权限的备份/还原权限模型	用户需要是本地 Active Directory 的Backup 操作员组的成员，并将 /b 标志与 RoboCopy.	用户必须是 Amazon FSx 文件系统的成员管理员组*，并将 /b 标志与 RoboCopy.
覆盖访问权限的域管理员（完全）权限模型	用户需要是内部部署活动目录的域管理员组的成员。	用户必须是 Amazon FSx 文件系统的成员管理员组*，并将 /b 标志与 RoboCopy

Note

* 对于已加入的文件系统Amazon管理微软 AD，亚马逊 FSx 文件系统管理员组是Amazon委派的 FSx 管理员. 在你自行管理的 Microsoft AD 中，Amazon FSx 文件系统管理员组是Domain Admins或在创建文件系统时为管理指定的自定义组。

如何使用 Robocopy 将现有文件迁移到亚马逊 FSX

您可以使用以下过程将现有文件迁移到 Amazon FSx。

将现有文件迁移到 Amazon FSx

1. 在与亚马逊 FSX 文件系统相同的亚马逊 VPC 中启动 Windows Server 2016 Amazon EC2 实例。
2. 连接到您的 Amazon EC2 实例。有关更多信息，请参阅适用于 Windows 实例的 Amazon EC2 用户指南中的连接您的 Windows 实例。
3. 打开命令提示符并将源文件共享映射到现有文件服务器上（本地或在Amazon) 转换为驱动器号（例如*Y*:) 如下所示。作为其中的一部分，您需要为内部部署 Active Directory 的成员提供凭据域管理员组中)。

```
C:\>net use Y: \\fileserver1.mydata.com\localdata /user:mydata.com\Administrator
Enter the password for 'fileserver1.mydata.com': _

Drive Y: is now connected to \\fileserver1.mydata.com\localdata.

The command completed successfully.
```

4. 将 Amazon FSx 文件系统上的目标文件共享映射到不同的驱动器号（例如，Z在您的 Amazon EC2 实例上使用：作为其中的一部分，您需要为属于本地 Active Directory 的域管理员组和 Amazon FSx 文件系统的管理员组成员的用户账户提供凭证。对于已加入的文件系统Amazon管理微软 AD，该组是**Amazon Delegated FSx Administrators**. 在你自我管理的 Microsoft AD 中，该群组是**Domain Admins**或在创建文件系统时为管理指定的自定义组。

   有关更多信息，请参阅表源文件系统和目标文件系统可访问性要求 (p. 60)中的先决条件 (p. 60).

```
C:\>net use Z: \\amznfsxabcdef1.mydata.com\share /user:mydata.com\Administrator
Enter the password for 'amznfsxabcdef1.mydata.com': _

Drive Z: is now connected to \\amznfsxabcdef1.mydata.com\share.

The command completed successfully.
```

5. 选择以管理员身份运行从上下文菜单上。打开命令提示符要么Windows PowerShell并运行以下 Robocopy 命令将文件从源共享复制到目标共享。

   这些区域有：ROBOCOPYcommand 是一个灵活的文件传输实用程序，具有多个选项来控制数据传输过程。正因为如此ROBOCOPY命令执行时，源共享中的所有文件和目录都将复制到 Amazon FSx 目标共享。副本会保留文件和文件夹的 NTFS ACL、属性、时间戳、所有者信息和审核信息。

```
robocopy Y:\ Z:\ /copy:DATSOU /secfix /e /b /MT:8
```

   前面的示例命令使用以下元素和选项：

   - Y — 指位于本地 Active Directory 林 mydata.com 中的源共享。
   - Z — 指亚马逊 FSX 上的目标份额\\ amznfsxabcdef1.mydata.com\ 共享。
   - /copy — 指定要复制的以下文件属性：
     - D — data
     - A — 属性
     - T — 时间戳
     - S — NTFS ACL
     - O — 所有者信息
     - U — 审计信息。
   - /secfix — 修复了所有文件的文件安全性，甚至是跳过的文件。
   - /e — 复制子目录，包括空的子目录。
   - /b — 在 Windows 中使用备份和还原权限复制文件，即使它们的 NTFS ACL 拒绝当前用户的权限。
   - /MT: 8 — 指定用于执行多线程复制的线程的数目。

   Note

   如果您通过缓慢或不可靠的连接复制大文件，则可以使用/zb选项与robocopy代替/b选项。在可重启模式下，如果大文件的传输中断，则可以在传输过程中执行后续的 Robocopy 操作，而不必从头开始重新复制整个文件。启用可重启模式会降低数据传输速度。

将文件共享配置迁移到 Amazon FSx

您可以使用以下过程将现有文件共享配置迁移到 Amazon FSx。在此过程中，源文件服务器是您要将其文件共享配置迁移到 Amazon FSx 的文件服务器。

Note

在迁移文件共享配置之前，请先将文件迁移到 Amazon FSx。有关更多信息，请参阅 将现有文件存储迁移到 FSx for Windows File Server (p. 58)。

将现有文件共享迁移到 FSx for Windows File Server

1. 在源文件服务器上，选择以管理员身份运行从上下文菜单上。打开Windows PowerShell作为管理员。
2. 将源文件服务器的文件共享导出到名为的文件`SmbShares.xml`通过以下命令命令命令命令命令命令命令命令命令的 PowerShell. 将本示例中的 F: 替换为要从中导出文件共享的文件服务器上的驱动器号。

```
$shareFolder = Get-SmbShare -Special $false | ? { $_.Path -like “F:\*” }
$shareFolder | Export-Clixml -Path F:\SmbShares.xml
```

3. 编辑`SmbShares.xml`文件，将所有对 F: (您的驱动器号) 的引用替换为 D:，因为 Amazon FSx 文件系统驻留在 D: 上。
4. 将现有文件共享配置到 FSx for Windows File Server 中。在有权访问目标 Amazon FSx 文件系统和源文件服务器的客户端上，复制保存的文件共享配置。通过以下命令将它导入变量中，使用以下命令中。

```
$shares = Import-Clixml -Path F:\SmbShares.xml
```

5. 使用以下选项之一准备在 FSx for Windows File Server 上创建文件共享所需的凭据对象。

   要以交互方式生成凭据对象，请使用以下命令。

```
$credential = Get-Credential
```

   使用生成凭据对象Amazon Secrets Manager资源，请使用以下命令。

```
$credential = ConvertFrom-Json -InputObject (Get-SECSecretValue -SecretId
 $AdminSecret).SecretString
$FSxAdminUserCredential = (New-Object PSCredential($credential.UserName,(ConvertTo-
SecureString $credential.Password -AsPlainText -Force)))
```

6. 使用以下脚本将文件共享配置迁移到您的 Amazon FSx 文件服务器。

```
$FSxAcceptedParameters = ("ContinuouslyAvailable", "Description",
 "ConcurrentUserLimit", "CATimeout", "FolderEnumerationMode", "CachingMode",
 "FullAccess", "ChangeAccess", "ReadAccess", "NoAccess", "SecurityDescriptor", "Path",
 "Name", "EncryptData")
ForEach ($item in $shares) {
    $param = @{};
    Foreach ($property in $item.psObject.properties) {
        if ($property.Name -In $FSxAcceptedParameters) {
            $param[$property.Name] = $property.Value
        }
    }
    Invoke-Command -ConfigurationName FSxRemoteAdmin -ComputerName
 amznfsxxxxxxxxx.corp.com -ErrorVariable errmsg -ScriptBlock { New-FSxSmbShare -
Credential $Using:credential @Using:param }
}
```

迁移 DNS 配置以使用亚马逊 FSx

FSx for Windows File Server 为每个文件系统提供一个默认的域名系统 (DNS) 名称，您可以使用该名称访问文件系统上的数据。通过将备用 DNS 名称配置为 Amazon FSx 文件系统的 DNS 别名，您也可以使用自己选择的任何 DNS 名称访问文件系统。

借助 DNS 别名，在将文件系统存储从本地迁移到 Amazon FSx 时，您可以继续使用现有的 DNS 名称来访问存储在 Amazon FSx 上的数据。这有助于在迁移到 Amazon FSx 时无需更新任何使用您的 DNS 名称的工具或应用程序。在创建新文件系统以及从备份创建新文件系统时，您可以将 DNS 别名与现有 FSx for Windows File Server 文件系统相关联。您可以同时将最多 50 个 DNS 别名与文件系统关联。有关更多信息，请参阅管理 DNS 别名 (p. 82)。

DNS 别名必须满足以下要求：

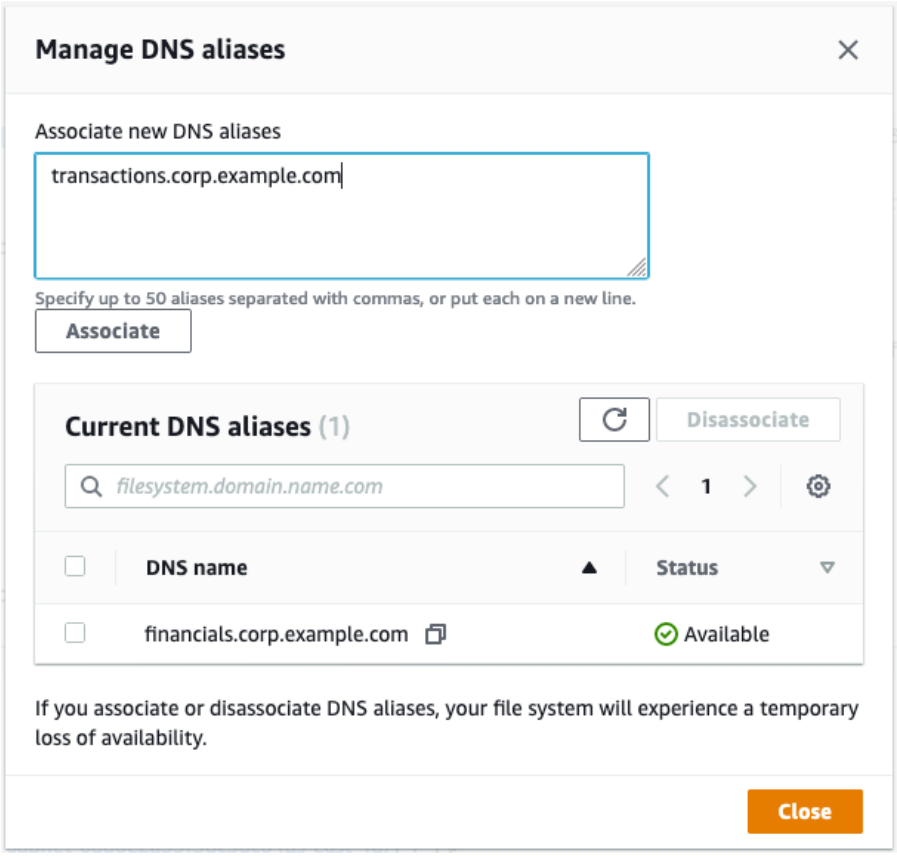
- 必须将格式化为完全限定域名 (FQDN)，例如，`accounting.example.com`.
- 可以包含字母数字字符和连字符 (-)。
- 不得以连字符开头或结尾。
- 可以使用数字开头。

对于 DNS 别名，Amazon FSx 会将字母字符存储为小写字母 (a-z)，无论您指定将其存储为大写字母、小写字母还是转义码中的对应字母。

以下过程介绍如何使用 Amazon FSx 控制台、CLI 和 API 将 DNS 别名与现有 FSx for Windows 文件服务器文件系统关联。有关在创建新文件系统（包括从备份创建新文件系统）时关联 DNS 别名的详细信息，请参见创建新文件系统时关联 DNS 别名 (p. 83).

将 DNS 别名与现有文件系统关联（控制台）（控制台）（控制台）

1. 从打开 Amazon FSx 控制台https://console.aws.amazon.com/fsx/.
2. 导航到文件系统，然后选择要与 DNS 别名关联的 Windows 文件系统。
3. 在存储库的网络和安全选项卡上，选择Manage为了DNS 别名以打开管理 DNS 别名对话框。



4. 在关联新别名框中，输入要关联的 DNS 别名。
5. 选择Ass向文件系统添加别名。

   您可以监控刚刚在当前别名list。当状态显示为Available，则别名与文件系统相关联（这个过程可能需要长达 2.5 分钟）。

将 DNS 别名与现有文件系统关联 (CLI) (CLI)

- 使用`associate-file-system-aliases`CLI 命令或AssociateFileSystemAliases将 DNS 别名与现有文件系统关联的 API 操作。

  以下命令将两个别名与指定的文件系统关联。

```
aws fsx associate-file-system-aliases \
    --file-system-id fs-0123456789abcdef0 \
    --aliases financials.corp.example.com transfers.corp.example.com
```

  响应显示 Amazon FSx 正在与文件系统关联的别名的状态。

```
{
      "Aliases": [
          {
              "Name": "financials.corp.example.com",
              "Lifecycle": CREATING
          },
          {
```

```
            "Name": "transfers.corp.example.com",
            "Lifecycle": CREATING
        }
    ]
}
```

要监控正在关联的别名的状态，请使用`describe-file-system-aliases`CLI 命令 (DescribeFileSystemAliases是等效的 API 操作）。何时`Lifecycle`如果别名值为 AVAILABLE，则可以使用它来访问文件系统（此过程最多需要 2.5 分钟）。

切入亚马逊 FSX

要切换到 FSx for Windows File Server 文件系统，您需要执行以下步骤，请执行以下步骤：

- 准备剪裁。
  - 暂时断开 SMB 客户端与原始文件系统的连接。
  - 执行最终的文件和文件共享配置同步。
- 为您的 Amazon FSx 文件系统配置服务主体名称 (SPN)。
- 更新 DNS CNAME 记录以指向您的亚马逊 FSx 文件系统。

每个步骤的执行以下步骤的过程。

主题

为切换到亚马逊 FSx 做准备

要准备切换到 Amazon FSx 文件系统，您必须执行以下操作：

- 断开所有写入原始文件系统的客户端。
- 使用执行最终文件同步Amazon DataSync或者 Robocopy。有关更多信息，请参阅 将现有文件存储迁移到 FSx for Windows File Server (p. 58)。
- 执行最终的文件共享配置同步。有关更多信息，请参阅 将文件共享配置迁移到 Amazon FSx (p. 62)。

为 Kerberos 身份配置的 SPN

我们建议您在 Amazon FSx 中使用基于 Kerberos 的身份验证和加密。Kerberos 为访问文件系统的客户端提供最安全的身份验证。要为使用 DNS 别名访问 Amazon FSX 的客户端启用 Kerberos 身份验证，您必须添加与 Amazon FSx 文件系统的 Active Directory 计算机对象上的 DNS 别名相对应的服务主体名称 (SPN)。

对 Kerberos 身份验证有两个必需的 SPN。

```
HOST/alias
HOST/alias.domain
```

举个例子，如果别名是`finance.domain.com`，两个必需的 SPN 如下所示。

```
HOST/finance
```

```
HOST/finance.domain.com
```

SPN 同时只能与一个 Active Directory 计算机对象关联。如果为原始文件系统的 Active Directory 计算机对象配置的 DNS 名称存在现有 SPN，则必须在为 Amazon FSx 文件系统创建 SPN 之前将其删除。

以下过程介绍如何为您的 Amazon FSx 文件系统的 Active Directory 计算机对象查找任何现有 SPN、删除它们以及创建新的 SPN。

安装所需的 PowerShell Active Di

1. 登录加入您的 Amazon FSx 文件系统所加入的活动目录的 Windows 实例。
2. 打开 PowerShell 作为管理员。
3. 安装 PowerShell 使用以下命令命令命令使用以下命令命令命令命令命令命令命令命令命令命令将

```
Install-WindowsFeature RSAT-AD-PowerShell
```

查找和删除原始文件系统的 Active Directory 计算机对象上的现有 DNS 别名 SPN

1. 使用以下命令查找任何现有的 SPN。Replace*alias_fqdn*使用与文件系统关联的 DNS 别名迁移 DNS 配置以使用亚马逊 FSx (p. 63).

```
## Find SPNs for original file system's AD computer object
$ALIAS = "alias_fqdn"
SetSPN /Q ("HOST/" + $ALIAS)
SetSPN /Q ("HOST/" + $ALIAS.Split(".")[0])
```

2. 使用以下示例脚本删除上一步中返回的现有 HOST SPN。

   - Replace*alias_fqdn*使用与文件系统关联的完整 DNS 别名迁移 DNS 配置以使用亚马逊 FSx (p. 63).
   - Replace*file_system_DNS_name*使用原始文件系统的 DNS 名称。

```
## Delete SPNs for original file system's AD computer object
$Alias = "alias_fqdn"
$FileSystemDnsName = "file_system_dns_name"
$FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})

SetSPN /D ("HOST/" + ${Alias}) ${FSxAdComputer}.Name
SetSPN /D ("HOST/" + ${Alias}.Split(".")[0]) ${FSxAdComputer}.Name
```

3. 对与中的文件系统关联的每个 DNS 别名重复这些步骤迁移 DNS 配置以使用亚马逊 FSx (p. 63).

在 Amazon FSx 文件系统的 Active Directory 计算机对象上设置 SPN

1. 通过运行以下命令为您的 Amazon FSx 文件系统设置新的 SPN。

   - Replace*file_system_DNS_name*使用 Amazon FSx 分配给文件系统的 DNS 名称。

     要在 Amazon FSx 控制台上查找文件系统的 DNS 名称，请选择文件系统，然后选择您的文件系统。选择网络和安全文件系统详细信息页面的窗格。你也可以在响应中获取 DNS 名称DescribeFileSystemsAPI 操作。
   - Replace*alias_fqdn*使用与文件系统关联的完整 DNS 别名迁移 DNS 配置以使用亚马逊 FSx (p. 63).

```
## Set SPNs for FSx file system AD computer object
$FSxDnsName = "file_system_DNS_name"
$Alias = "alias_fqdn"
$FileSystemHost = (Resolve-DnsName $FSxDnsName | Where Type -eq 'A')[0].Name.Split(".")
[0]
$FSxAdComputer = (Get-AdComputer -Identity $FileSystemHost)

Set-AdComputer -Identity $FSxAdComputer -Add @{"msDS-AdditionalDnsHostname"="$Alias"}
SetSpn /S ("HOST/" + $Alias.Split('.')[0]) $FSxAdComputer.Name
SetSpn /S ("HOST/" + $Alias) $FSxAdComputer.Name
```

Note

如果原始文件系统的计算机对象的 AD 中存在 DNS 别名的 SPN，则为 Amazon FSx 文件系统设置 SPN 将失败。有关查找和删除现有 SPN 的信息，请参阅查找和删除原始文件系统的 Active Directory 计算机对象上的现有 DNS 别名 SPN (p. 66).

2. 使用以下示例脚本验证是否为 DNS 别名配置了新 SPN。确保响应中包含两个 HOST SPN，`HOST/alias`和`HOST/alias_fqdn`.

   Replace*file_system_DNS_name*使用 Amazon FSx 分配给您的文件系统的 DNS 名称。要在 Amazon FSx 控制台上查找文件系统的 DNS 名称，请选择文件系统，选择您的文件系统，然后选择网络和安全”窗格位于文件系统详细信息页面上。

   你也可以在响应中获取 DNS 名称DescribeFileSystemsAPI 操作。

```
## Verify SPNs on FSx file system AD computer object
$FileSystemDnsName = "file_system_dns_name"
$FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})
SetSpn /L ${FSxAdComputer}.Name
```

3. 对与中的文件系统关联的每个 DNS 别名重复上步骤 DNS 别名，重复上述步骤迁移 DNS 配置以使用亚马逊 FSx (p. 63).

Note

通过在 Active Directory 中设置以下组策略对象 (GPO)，可以在客户端使用 DNS 别名连接到文件系统的过程中强制执行 Kerberos 身份验证和加密：

- 限制 NTLM：向远程服务器传出 NTLM 流量
- 限制 NTLM：为 NTLM 身份验证添加远程服务器例外

有关更多信息，请参阅 。使用 GPO 强制执行 Kerberos 身份验证 (p. 157)在演练 5：使用 DNS 别名访问文件系统.

更新亚马逊 FSx 文件系统的 DNS CNAME 记录

为文件系统正确配置 SPN 后，您可以将解析到原始文件系统的每个 DNS 记录替换为解析为 Amazon FSx 文件系统的默认 DNS 名称的 DNS 记录，从而切换到 Amazon FSx。

安装所需的 PowerShell cmdlet

1. 以具有 DNS 管理权限的组成员的身份登录到加入您的 Amazon FSx 文件系统的 Active Directory 的 Windows 实例（Amazon域名系统委托管理员在Amazon管理Microsoft ActiveDomain Admins或您在自己管理的 Active Directory 中委派了 DNS 管理权限的其他组）

   有关更多信息，请参阅适用于 Windows 实例的 Amazon EC2 用户指南中的连接您的 Windows 实例。
2. 打开 PowerShell 作为管理员。
3. 这些区域有： PowerShell 需要使用 DNS 服务器模块来执行此过程中的说明。使用以下命令安装它。

```
Install-WindowsFeature RSAT-DNS-Server
```

更新现有的 DNS 别名记录的步骤

1. 以下脚本更新所有现有的 DNS CNAME 记录*alias_fqdn*到您的 Amazon FSx 文件系统的计算机对象。如果未找到，则会为 DNS 别名创建一个新的 DNS 别名记录*alias_fqdn*它会解析为您的 Amazon FSx 文件系统的默认 DNS 名称。

   要运行脚本，请执行以下操作：

   - Replace*alias_fqdn*使用与文件系统关联的 DNS 别名。
   - Replace*file_system_DNS_name*使用 Amazon FSx 已分配给文件系统的默认 DNS 名称。

```
$Alias="alias_fqdn"
$FSxDnsName="file_system_dns_name"
$AliasHost=$Alias.Split('.')[0]
$ZoneName=((Get-WmiObject Win32_ComputerSystem).Domain)
$DnsServerComputerName = (Resolve-DnsName $ZoneName -Type NS | Where Type -eq 'A' |
 Select -ExpandProperty Name)[0]

Add-DnsServerResourceRecordCName -Name $AliasHost -ComputerName $DnsServerComputerName
 -HostNameAlias $FSxDnsName -ZoneName $ZoneName
```

2. 对与中的文件系统关联的每个 DNS 别名重复上步骤 DNS 别名，重复上步骤。迁移 DNS 配置以使用亚马逊 FSx (p. 63).

将 FSx for Windows File Server 与 Microsoft

高可用性 (HA) Microsoft SQL Server 通常部署在 Windows 服务器故障转移群集 (WSFC) 中的多个数据库节点上，每个节点都可以访问共享文件存储。你可以通过两种方式将 FSx for Windows File Server 用作高可用性 (HA) Microsoft SQL Server 部署的共享存储：用作活动数据文件的存储空间和作为 SMB 文件共享见证。

Note

目前，亚马逊 FSX 不支持微软 SQL Server IFI（即时文件初始化）功能。

建议将固态硬盘存储用于 SQL 服务器。SSD 存储专为性能最高、延迟最敏感的工作负载（包括数据库）而设计。

有关使用 Amazon FSx 降低 SQL Server 高可用性部署的复杂性和成本的信息，请参阅Amazon存储博客：

- 使用适用于 Windows File Server 的 Amazon File Server 高可用性部署
- 优化高可用性 SQL Server 部署的成本Amazon
- 使用AmazonLaunch Wizard 和亚马逊 FSx

将 Amazon FSx 用于活动 SQL Server 数据文件

Microsoft SQL Server 可以使用 SMB 文件共享作为活动数据文件的存储选项进行部署。Amazon FSx 经过优化，通过支持持续可用 (CA) 文件共享，为 SQL Server 数据库提供共享存储。这些文件共享专为需要不间断访问共享文件数据的 SQL Server 之类的应用程序而设计。虽然您可以在单可用区 2 文件系统上创建 CA 共享，但对于所有 SQL Server 部署，无论是否高可用区，都需要在多可用区文件系统上使用 CA 共享。

创建持续可用的共享

您可以在上使用用于远程管理的 Amazon FSx CLI 创建 CA 共享 PowerShell. 要指定共享为持续可用的共享，请使用`New-FSxSmbShare`用`-ContinuouslyAvailable`选项设置为`$True`. 要了解有关创建新 CA 共享的更多信息，请参阅创建持续可用的共享 (p. 88).

配置 SMB 超时设置

如中所述FSx or Windows File Server (p. 18)，多可用区的故障转移和回切可能会导致 I/O 暂停，通常在 30 秒内完成。您的 SQL Server 应用程序对超时设置的敏感度可能不同，具体取决于其配置方式。

您可以调整 SMB 客户端配置会话超时，以确保您的应用程序对多可用区文件系统故障转移具有弹性。您可以通过更新文件系统的吞吐容量来测试应用程序在故障转移期间的行为，这将启动自动故障切换和回切。

使用 Amazon FSx 作为 SMB 文件共享见证

Windows 服务器故障转移群集部署通常会部署 SMB 文件共享见证，以维护群集资源的仲裁。见证文件共享只需要少量存储法定信息。Amazon FSx 文件系统可用作 Windows 服务器故障转移群集部署的 SMB 文件共享见证。

将 FSx for Windows File Server 与 Amazon Kendra 结合使用

Amazon Kendra 是一项高度准确且智能的搜索服务。适用于 Windows 文件服务器文件系统的 FSx 可用作 Amazon Kendra 的数据源，允许您索引和智能搜索文件系统中存储的文档中包含的信息。

- 有关 Amazon Kendra 的更多信息，请参阅什么是 Amazon Kendra中的Amazon Kendra 开发者指南.
- 有关如何将文件系统添加为 Amazon Kendra 数据源的更多信息，请参阅。开始使用 Amazon FSx 数据源（控制台）中的Amazon Kendra 开发者指南.
- 有关 Amazon Kendra 的概述信息，请参阅Amazon Kendra 网站.
- 有关如何使用 Amazon Kendra 搜索文件系统的演练，请参阅。使用 Amazon Kendra 连接器在 Windows 文件系统上安全地搜索非结构化数据，以获取适用于 Windows 文件服务器的 Amazon FSx在AmazonMachine Learning 博客.

文件系统性能

当您将 FSx for Windows File Server 系统添加为数据源时，Amazon Kendra 会按常规同步频率抓取文件系统上的文件和文件夹，以创建和维护其搜索索引。（您可以在建立集成时选择同步频率。）Amazon Kendra 的此文件访问活动将消耗文件系统资源，类似于您自己的工作负载访问文件系统的活动。

确保文件系统配置了足够的资源，以免您的工作负载性能受到影响。具体来说，如果您计划为大量文件编制索引，我们建议使用具有 SSD 存储类型的文件系统，该文件系统可为需要访问存储卷的请求提供更高的最大吞吐量和 IOPS 级别。

有关 Amazon FSx 绩效模型的更多信息，请参阅FSx for Windows File Server 性能 (p. 141).

使用备份、卷影副本和定时复制保护您的数据

除了自动复制文件系统的数据以确保高持久性之外，Amazon FSx 还为您提供以下选项，以进一步保护存储在文件系统上的数据：

- Amazon FSx 原生备份支持您在 Amazon FSx 中的备份保留和合规性需求。
- Amazon Backup您的 Amazon FSx 文件系统的备份是集中式自动备份解决方案的一部分Amazon云端和本地服务。
- Windows 卷影副本使用户能够通过将文件还原到以前的版本来轻松撤消文件更改并比较文件版本。
- Amazon DataSync按计划将 Amazon FSx 文件系统复制到第二个文件系统可提供数据保护和恢复。

主题

使用备份

有了 Amazon FSx，备份 file-system-consistent、高度耐用、增量。为了确保文件系统的一致性，Amazon FSX 在微软 Windows 中使用了卷影复制服务 (VSS)。为了确保高持久性，Amazon FSx 将备份存储在亚马逊Simple Storage Service (Amazon S3) 中。

Amazon FSx 备份是增量备份，无论是使用每日自动备份还是用户启动的备份功能生成。这意味着只在文件系统上保存在最新备份后更改的数据。由于无需复制数据，这将最大限度缩短创建备份所需的时间和节省存储成本。（请注意，如果文件系统中的数据频繁更改，您的总备份使用量可能会大于文件系统的已用存储容量。）删除备份，只删除该备份特有的数据。

每个 FSx for Windows File Server 备份都包含从备份创建新文件系统所需的所有信息，从而有效地还原 point-in-time 文件系统快照。

为文件系统创建常规备份是一种最佳实践，可以补充 Amazon FSx for Windows File Server 对文件系统执行的复制。Amazon FSx 备份有助于满足您的备份保留和合规性需求。使用 Amazon FSx 备份非常简单，无论是创建备份、复制备份、从备份还原文件系统还是删除备份。

主题

使用每日自动备份

默认情况下，Amazon FSx 每天自动备份您的文件系统。这些每日自动备份发生在创建文件系统时确定的每日备份窗口内。在每日备份时段中的某个时刻，启动备份 I/O 可能会短时间暂停存储 I/O (通常不到几秒)。当

您选择每日备份时段时，我们建议您选择一天中方便的时间。对于使用该文件系统的应用程序来说，此时间最好超出正常工作时间。

每日自动备份会保留一段时间，即保留期。每日自动备份的默认保留期为 7 天。您可以将保留期设置为在 0-90 天之间。将保留期设置为 0（零）天会关闭每日自动备份。删除文件系统后，将删除每日自动备份。

> Note
>
> 将保留期设置为 0 天意味着永远不会自动备份您的文件系统。我们强烈建议您对具有任何级别的关键功能的文件系统使用每日自动备份。

您可以使用Amazon CLI或者其中一个Amazon用于更改文件系统的备份时段和备份保留期的 SDK。使用`UpdateFileSystem`API 操作或`update-file-system`CLI 命令。有关更多信息，请参阅 演练 3：更新现有文件系统 (p. 149)。

使用用户启动的备份

借助 Amazon FSx，您可以随时手动备份文件系统。您可以使用 Amazon FSx 控制台、API 或Amazon Command Line Interface(Amazon CLI)。用户启动的 Amazon FSx 文件系统备份永不过期，只要您想保留这些备份，它们就可以使用。即使删除了已备份的文件系统，用户启动的备份也会保留。您只能通过使用 Amazon FSx 控制台、API 或 CLI 删除用户启动的备份。它们永远不会被 Amazon FSx 自动删除。有关更多信息，请参阅 删除备份 (p. 75)。

如果在修改文件系统时（例如在更新吞吐容量期间或在文件系统维护期间）启动备份，则备份请求将排入队列，并在活动完成后恢复。

创建用户启动的备份

以下过程将指导您如何在 Amazon FSx 控制台中为现有文件系统创建用户启动的备份。

创建用户启动的文件系统备份

1. 从打开 Amazon FSx 控制台https://console.aws.amazon.com/fsx/.
2. 从控制台控制台控制台控制台，选择要备份的文件系统的名称。
3. 从操作，选择创建备份.
4. 在创建备份对话框中，提供备份的名称。Backup 名称最多可以包含 256 个 Unicode 字符，包括字母、空格、数字和特殊字符。+-= _:/
5. 选择 Create backup (创建备份)。

现在，您已创建文件系统备份。您可以在 Amazon FSx 控制台中找到所有备份的表，方法是选择备份在右侧导航栏中。您可以搜索为备份提供的名称，表筛选器以仅显示匹配的结果。

当您按照此过程所述创建用户启动的备份时，其类型为`USER_INITIATED`，它有`CREATING`状态，直到它完全可用。

使用Amazon Backup使用Amazon FSx

Amazon Backup是一种简单且经济高效的方法，可通过备份 Amazon FSx 文件系统来保护您的数据。Amazon Backup统一备份服务，旨在简化备份的创建、复制、还原和删除，同时提供改进的报告和审核。Amazon Backup可以更轻松地为法律法规和专业合规性制定集中式备份战略。Amazon Backup也让保护你的Amazon提供集中位置让您完成以下操作，从而简化存储卷、数据库和文件系统：

- 配置和审计Amazon要备份的资源。
- 计划自动备份。
- 设置保留策略。
- 拷贝备份Amazon区域和跨区域Amazon账户。

- 监控所有最近的备份、复制和还原活动。

Amazon Backup使用 Amazon FSx 的内置备份功能。备份取自Amazon Backup控制台具有与通过 Amazon FSx 控制台执行的备份相同级别的文件系统一致性和性能以及相同的还原选项。如果您使用Amazon Backup要管理这些备份，您可以获得其他功能，例如无限保留选项和每小时创建一次定时备份的能力。此外，Amazon Backup即使删除了源文件系统，也会保留不可变的备份。这样可以防止意外或恶意删除。

备份由Amazon Backup被视为用户启动的备份，并计入 Amazon FSx 用户启动的备份配额。您可以查看和还原由Amazon Backup在 Amazon FSx 控制台、CLI 和 API 中。但是，您无法删除备份Amazon Backup在 Amazon FSx 控制台、CLI 或 API 中。有关如何使用的更多信息Amazon Backup要备份您的 Amazon FSx 文件系统，请参阅使用亚马逊 FSx 文件系统中的Amazon Backup开发人员指南.

复制备份

您可以使用 Amazon FSx 在同一版本中手动复制备份Amazon账户转到另一个Amazon区域（跨区域副本）或同一区域内Amazon区域（区域内副本）。你只能在同一个区域内制作跨区域副本AmazonPartite 您可以使用 Amazon FSx 控制台创建用户启动的备份副本，Amazon CLI，或 API。创建用户启动的备份副本时，其类型为`USER_INITIATED`.

您还可以使用Amazon Backup复制备份Amazon区域和跨区域Amazon账户。Amazon Backup是一项完全托管的备份管理服务，为基于策略的备份计划提供了一个中央接口。借助跨账户管理，您可以自动使用备份策略跨组织内的账户应用备份计划。

跨区域备份副本对于跨区域灾难恢复特别有用。您进行备份并将其复制到另一个Amazon区域，以便在发生灾难时在主要Amazon区域，您可以从备份中恢复并在另一个区域快速恢复可用性Amazon区域。您还可以使用备份副本将文件数据集克隆到另一个Amazon区域或在同一个区域内Amazon区域。你在同一个里面制作备份副本Amazon账户（跨区域或区域内）使用 Amazon FSx 控制台，Amazon CLI，或亚马逊 FSx API。您还可以使用Amazon Backup执行按需或基于策略的备份拷贝。

跨账户备份副本对于满足将备份复制到独立帐户的法规遵从性要求非常有用。它们还提供了额外的数据保护层，以帮助防止意外或恶意删除备份、丢失凭据或泄露Amazon KMS钥匙。跨账户备份支持扇入（将多个主帐户的备份复制到一个独立的备份副本帐户）和扇出（将备份从一个主帐户复制到多个独立的备份副本帐户）。

您可以使用创建跨账户备份副本Amazon Backup和Amazon Organizations支持。跨账户副本的账户界限由Amazon Organizations政策。有关的更多信息，使用Amazon Backup要制作跨账户备份副本，请参阅创建备份副本Amazon Web Services 账户中的Amazon Backup开发人员指南.

Backup 副本限制

复制备份时，存在以下一些限制：

- 跨区域备份副本仅在任意两个商业版之间受支持Amazon中国（北京）和中国（宁夏）区域之间，以及在Amazon GovCloud （US-East）和Amazon GovCloud （美国西部）区域，但不能跨越这些区域组。
- 选择加入区域不支持跨区域备份副本。
- 你可以在任何地方制作区域内备份副本Amazon区域。
- 源备份的状态必须为`AVAILABLE`然后你才能复制它。
- 如果正在复制源备份，则无法将其删除。目标备份可用和允许您删除源备份之间可能会有短暂的延迟。如果重试删除源备份，则应记住此延迟。
- 最多可以同时进行到同一目标的五个备份副本请求Amazon每账户区域。

跨区域备份副本

您可以使用 IAM 策略语句授予执行备份复制操作的权限。与消息来源沟通Amazon区域要请求跨区域备份副本，请求者（IAM 角色或 IAM 用户）必须有权访问源备份和源Amazon区域。

您可使用策略授予权限CopyBackup备份复制操作的操作。请在策略的中指定该操作Action字段，并在策略的Resource字段，如下面的示例所示。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "fsx:CopyBackup",
            "Resource": "arn:aws:fsx:*:111111111111:backup/*"
        }
    ]
}
```

有关有关有关 IAM 策略的有关的更多信息，IAM 中的策略和权限。中的IAM 用户指南.

完整和增量拷贝

将备份复制到其他Amazon来自源备份的区域，第一个副本是完整备份副本。在第一个备份副本后，所有后续备份副本到同一目标区域内的相同目标区域Amazon账户是增量的，前提是您尚未删除该区域中以前复制的所有备份，并且一直在使用相同的备份Amazon KMS键。如果两个条件都不满足，则复制操作会生成完整（非增量）备份副本。

使用控制台在同一账户（跨区域或区域内）中复制备份

1. 从打开 Amazon FSx 控制台https://console.aws.amazon.com/fsx/.
2. 在导航窗格中，选择 Backups。
3. 在备份表，选择要复制的备份，然后选择复制备份.
4. 在设置部分中，执行以下操作：
   - 在目标区域列表中，选择一个目的地Amazon要将备份复制到的区域。目标可能在另一个Amazon区域（跨区域复制）或同一区域内Amazon区域（区域内复制）。
   - （可选）选择复制标签将标记从源备份复制到目标备份。如果您选择复制标签并在步骤 6 中添加标签，所有标签都将合并。
5. 适用于加密，选择Amazon KMS加密密钥来加密复制的备份。
6. 适用于标签-可选输入键和值以添加复制的备份的标签。如果您在此处添加标签并且还选择了复制标签在第 4 步中，所有标记都将合并。
7. 选择 Copy backup (复制备份)。

你的备份被复制到同一Amazon账户到选定的Amazon区域。

使用 CLI 在同一账户（跨区域或区域内）中复制备份

- 使用copy-backupCLI 命令或CopyBackupAPI 操作以复制备份Amazon账户，要么跨一个Amazon区域或在Amazon区域。

  以下命令复制 ID 为的备份backup-0abc123456789cba7来自 的us-east-1区域。

  ```
  aws fsx copy-backup \
    --source-backup-id backup-0abc123456789cba7 \
    --source-region us-east-1
  ```

  响应显示复制备份。

  您可以在 Amazon FSx 控制台或以编程方式使用describe-backupsCLI 命令或DescribeBackupsAPI 操作。

还原备份

您可以使用可用备份来创建新的文件系统，从而有效地恢复 point-in-time 另一个文件系统的快照。您可以使用控制台还原备份，Amazon CLI，或者其中一个Amazon开发工具包。将备份恢复到新文件系统所花费的时间与创建新文件系统的时间相同。从备份还原的数据延迟加载到文件系统中，在此期间，您将遇到稍高的延迟。

为确保用户可以继续访问已恢复的文件系统，请确保与已还原文件系统关联的 Active Directory 域与原始文件系统关联的 Active Directory 域相同，或者受原始文件系统的 AD 域信任。有关有关 Active Directory 有关的更多信息，在 FSx for Windows File Server 中使用 Microsoft Active Directory (p. 22).

以下过程将指导您如何使用控制台还原备份，以创建新的文件系统。

> Note
>
> 您只能将备份还原到与原始文件具有相同部署类型和存储容量的文件系统。在恢复的文件系统可用后，您可以增加其存储容量。有关更多信息，请参阅 管理存储容量 (p. 112)。

从备份还原文件系统

1. 从打开 Amazon FSx 控制台https://console.aws.amazon.com/fsx/.
2. 在控制台控制面板中，选择备份从左侧导航栏。
3. 选择要从还原备份备份表，然后选择还原备份.

   这样做将打开文件系统创建向导。此向导与标准文件系统创建向导相同，只不过是Deployment type (部署类型)和存储容量已设置，无法更改。但是，您可以更改吞吐容量、关联的 VPC 和其他设置以及存储类型。存储类型设置为SSS默认情况下，但您可以将其更改为HDS在以下条件下：

   - 文件系统部署类型为多可用区要么单可用区 2.
   - 存储容量至少为 2,000 GiB。
4. 像创建新文件系统时一样完成向导。
5. 选择 Review and create。
6. 查看您为 Amazon FSx 文件系统选择的设置，然后选择创建文件系统.

您已从备份中恢复，现在正在创建一个新的文件系统。当其状态更改为`AVAILABLE`文件系统，您可以照常使用文件系统。

删除备份

删除备份是一项永久性的、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future 不再需要该备份，否则请勿删除该备份。您无法删除由创建的备份Amazon Backup，其中有类型Amazon备份Amazon FSx 控制台、CLI 或 API。

删除备份

1. 从打开 Amazon FSx 控制台https://console.aws.amazon.com/fsx/.
2. 在控制台控制面板中，选择备份从右侧导航。
3. 选择要从备份备份表，然后选择删除备份.
4. 在删除备份对话框中，确认备份 ID 标识您要删除的备份。
5. 确认已检查您要删除的备份对应的复选框。
6. 选择删除备份.

现在，您的备份和所有包含的数据都将被永久删除，且不可恢复。

使用卷影副本

Microsoft卷影复制是 Windows File 系统在某个时间点的快照。启用卷影副本后，用户可以在 Windows 文件资源管理器中轻松查看和还原早期快照中的单个文件或文件夹。这样做使用户可以轻松撤消更改并比较文件版本。使用 Amazon FSx 的存储管理员可以轻松地安排使用 Windows 定期制作卷影副本 PowerShell 命令。

卷影副本与文件系统的数据一起存储，因此会占用文件系统的存储容量。但是，卷影副本仅占用文件更改部分的存储容量。存储在文件系统中的所有卷影副本都包含在文件系统的备份中。

> Note
>
> 卷影副本是不FSx for Windows File Server 的默认启用。要在文件系统上运行卷影副本，必须启用卷影副本，并在文件系统上设置卷影复制时间表。有关更多信息，请参阅 使用默认设置设置卷影副本 (p. 77)。

> Note
>
> 卷影副本不能替代备份。如果启用卷影复制，请确保继续执行常规备份。

主题

卷影副本配置概述

您可以使用 Windows 在文件系统上启用和计划定期卷影复制 PowerShellAmazon FSx 定义的命令。卷影复制配置包含两个设置：

- 卷影副本可以在文件系统上使用的最大存储量
- （可选）按定义的时间和间隔（如每天、每周和每月）制作卷影拷贝的时间表

在任意时间点，每个文件系统最多可以存储 500 个卷影副本。达到此限制后，您创建的下一个卷影副本将替换最旧的卷影副本。同样，当达到最大卷影副本存储量时，将删除一个或多个最旧的卷影副本，以便为下一个卷影副本腾出足够的存储空间。

有关如何使用默认 Amazon FSx 设置快速启用和计划定期卷影复制的信息，请参阅使用默认设置设置卷影副本 (p. 77). 有关如何自定义卷影副本配置的信息，请参阅卷影副本 (p. 107).

分配卷影副本存储的注意事项

卷影副本是自上次卷影副本以来所做的文件更改的块级副本。整个文件不会被复制，只复制更改。因此，以前版本的文件通常不会占用当前文件那么多的存储空间。用于更改的卷空间量可能因工作负载而异。修改文件时，卷影副本使用的存储空间取决于您的工作负载。在确定要为卷影副本分配多少存储空间时，应考虑工作负载的文件系统使用模式。

启用卷影副本时，可以指定卷影副本可在文件系统上使用的最大存储量。默认限制为 10% 的文件系统。如果您的用户经常添加或修改文件，我们建议您提高限制。如果将此限制设置得太小，可能会导致删除最旧的卷影副本的频率高于用户的预期。

您可以将卷影副本存储设置为 unbounding (`Set-FsxShadowStorage -Maxsize "UNBOUNDED"`)。但是，无限制的配置可能会导致大量卷影副本占用您的文件系统存储。这可能会导致您的工作负载没有足够的存储容量。如果设置了无限存储，请确保在达到卷影副本限制时扩展存储容量。有关将卷影副本存储配置为特定大小或无界大小的信息，请参阅设置卷影副本存储 (p. 107).

启用卷影副本后，您可以监视卷影副本占用的存储空间量。有关更多信息，请参阅 查看您的卷影副本存储 (p. 108)。

卷影副本的文件系统建议

以下是使用卷影副本的文件系统建议。

- 确保在文件系统上为工作负载需求预置足够的性能容量。亚马逊 FSX 提供了微软 Windows Server 提供的卷影副本功能。从设计上讲，微软视窗使用的是 copy-on-write 方法来记录自最近的卷影复制点以来的更改，还有这个 copy-on-write 活动可能导致每个文件写入操作最多执行三个 I/O 操作。如果 Windows 无法跟上每秒 I/O 操作的传入速率，它可能会导致所有卷影副本都被删除，因为它无法再通过以下方式维护卷影副本 copy-on-write. 因此，必须为文件系统上的工作负载需求配置足够的 I/O 性能容量（确定文件服务器 I/O 性能的吞吐容量维度，以及决定存储 I/O 性能的存储类型和容量）。
- 我们通常建议您在启用卷影副本时使用配置了 SSD 存储而不是 HDD 存储的文件系统，这是因为 Windows 需要更高的 I/O 性能来维护卷影副本，而且 HDD 存储为 I/O 操作提供的性能容量较低。
- 除了配置的最大卷影副本存储容量外，您的文件系统还应至少有 320 MB 的可用空间（`MaxSpace`）。例如，如果您分配了 5 GB`MaxSpace`对于卷影副本，除了 5 GB 之外，您的文件系统应始终至少有 320 MB 的可用空间`MaxSpace`.

  Warning

  配置卷影复制计划时，请确保在迁移数据或计划运行重复数据消除作业时不要安排卷影复制。在预期文件系统处于空闲状态时，应安排卷影复制。有关配置自定义卷影复制计划的信息，请参阅创建自定义卷影复制时间表 (p. 109).

使用默认设置设置卷影副本

您可以使用卷影副本存储和计划的默认设置，在文件系统上快速设置卷影副本。默认的卷影副本存储设置允许卷影副本最多占用文件系统的 10%。如果增加文件系统的存储容量（以百分比或绝对值表示），则当前分配的卷影副本存储量不会同样增加。

默认计划在世界标准时间每周一、周二、周三、周四和周五的上午 7:00 和下午 12:00 自动制作卷影副本。

设置卷影副本存储的默认级别

1. 连接到与文件系统有网络Connect 的 Windows 计算实例。
2. 以文件系统管理员组成员身份登录到 Windows 计算实例。InAmazon Managed Microsoft AD，那组是Amazon委派的 FSx 管理员. 在你自我管理的 Microsoft AD 中，该群组是Domain Admins或在创建文件系统时为管理指定的自定义组。有关更多信息，请参阅适用于 Windows 实例的 Amazon EC2 用户指南中的连接您的 Windows 实例。
3. 使用以下命令设置默认的卷影存储量。Replace*`FSxFileSystem-Remote-PowerShell-Endpoint`*使用 Windows 遥控器 PowerShell 要管理的文件系统的端点。您可以找到 Windows 遥控器 PowerShell 终端节点在 Amazon FSx 控制台中网络和安全文件系统详细信息窗口的部分，或者在`DescribeFileSystem`API 操作。

   ```
   PS C:\Users\delegateadmin> Invoke-Command -ComputerName FSxFileSystem-Remote-
   PowerShell-Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {Set-
   FsxShadowStorage -Default}
   ```

   响应看起来与以下内容类似。

   ```
   FSx Shadow Storage Configuration
   ```

```
AllocatedSpace UsedSpace     MaxSpace
-------------- ---------     --------
             0          0  32530536858
```

创建默认卷影复制计划

- 通过输入以下命令来设置默认的卷影复制计划。

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName FSxFileSystem-Remote-
PowerShell-Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {Set-
FsxShadowCopySchedule -Default}
```

响应将显示现在设置的默认计划。

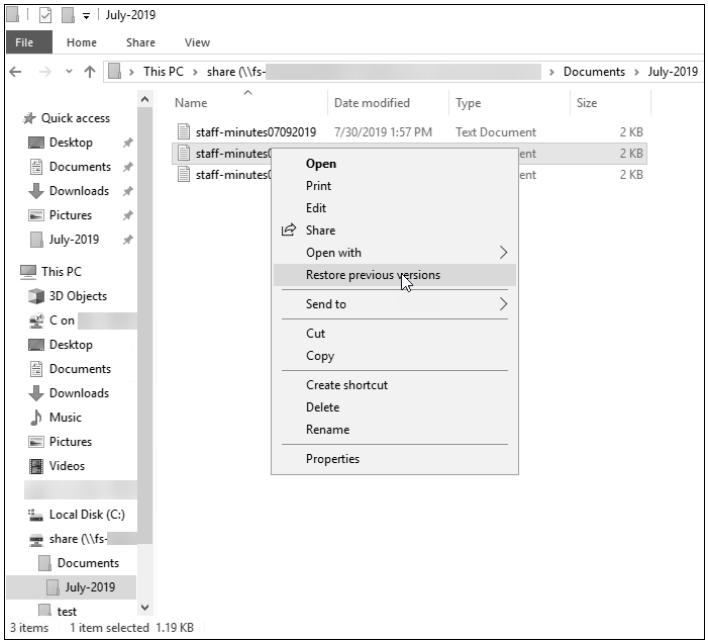
```
FSx Shadow Copy Schedule

Start Time                 Days of week                              WeeksInterval
----------                 ------------                              -------------
2019-07-16T07:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday              1
2019-07-16T12:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday              1
```

要了解其他选项和创建自定义卷影复制计划，请参阅创建自定义卷影复制时间表 (p. 109).

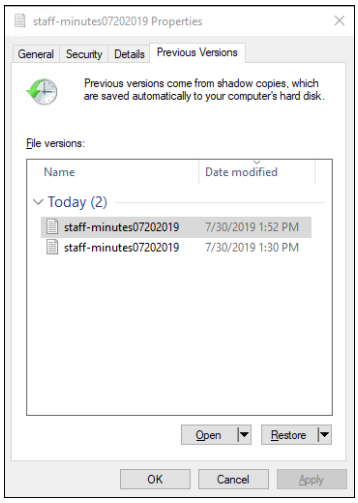
还原单个文件和文件夹

在 Amazon FSx 文件系统上配置卷影副本后，您的用户可以快速恢复单个文件或文件夹的先前版本。这样做可以使他们恢复存储在共享文件系统上的已删除或更改的文件。他们直接在桌面上以自助方式执行此操作，无需管理员协助。这种自助服务方法提高了工作效率并减少了管理工作量。

用户使用熟悉的 Windows 文件资源管理器界面将文件还原到以前的版本。要还原文件，请选择要还原的文件，然后选择还原早期版本(右键单击) 菜单中的。



然后，用户可以从中查看和还原以前的版本先前版本list。



要了解全套自定义 PowerShell 用于管理 FSx for Windows 文件服务器共享上的卷影副本的命令，请参阅卷影副本 (p. 107).

使用的已安排复制Amazon DataSync

您可以使用Amazon DataSync计划将 FSx for Windows File Server 文件系统的定期复制计划到第二个文件系统。此功能适用于区域内和跨区域部署。要了解更多信息，请参阅使用以下命令将现有文件迁到 FSx for Windows File Server 使用Amazon DataSync (p. 59)本指南中的数据传输Amazon存储服务中的Amazon DataSync用户指南.

管理文件系统

您可以使用自定义远程管理管理您的 FSx for Windows File Server 文件系统 PowerShell 命令，或者在某些情况下使用 Microsoft Windows — 本机图形用户界面 (GUI)。在下文中，您可以找到所有自定义的说明 PowerShell 每个可用的文件系统管理类别中的命令。

主题

开始使用 Amazon FSx CLI 进行远程管理 PowerShell

用于远程管理的 Amazon FSx CLI PowerShell 为文件系统管理员组中的用户启用文件系统管理。启动遥控器 PowerShell FSx for Windows File Server 文件系统上的会话，请首先满足以下先决条件：

- 能够连接到与文件系统有网络连接的 Windows 计算实例。
- 以文件系统管理员组成员身份登录到 Windows 计算实例。InAmazon Managed Microsoft AD，那组是 Amazon委派的 FSx 管理员。在自我管理的 Microsoft AD 中，该组是域管理员或在创建文件系统时为管理指定的自定义组。有关更多信息，请参阅 自我管理的 AD 最佳实践 (p. 35)。
- 确保文件系统的安全组入站规则允许端口 5985 上的流量。

安全性和用于远程管理的 CLI PowerShell

用于远程管理的 Amazon FSx CLI PowerShell 使用以下安全功能：

- 用户登录使用 Kerberos 身份验证进行身份验证。
- 管理会话通信使用 Kerberos 进行加密。

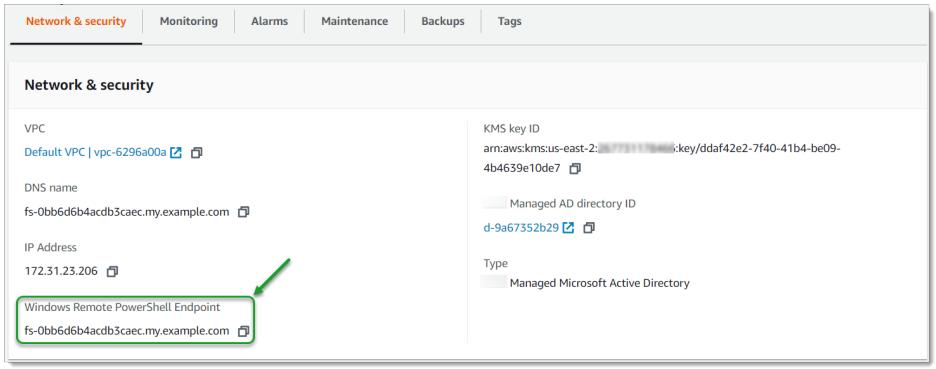
在上使用 CLI 进行远程管理 PowerShell

您可以通过两种方式在 Amazon FSx 文件系统上运行远程管理命令。你可以建立一个长时间运行的远程 PowerShell 会话并在会话中运行命令。或者，您也可以使用`Invoke-Command`在不建立长时间运行的 Remote 的情况下运行单个命令或单个命令块 PowerShell 会话。如果要设置变量并将其作为参数传递给远程管理命令，则需要使用`Invoke-Command`.

> **Note**
>
> 对于多可用区文件系统，您只能在文件系统位于其首选文件服务器上时使用 Amazon FSx CLI 进行远程管理。有关更多信息，请参阅 可用性与持久性：单可用区和多可用区文件系统 (p. 18)。

要运行这些命令，必须知道Windows 远程 PowerShell端点您的文件系统。要找到此终端节点，请执行以下步骤：

1. 从打开 Amazon FSx 控制台https://console.aws.amazon.com/fsx/.
2. 选择您的文件系统。在存储库的网络与安全选项卡上，找到Windows 远程 PowerShell 终端节点，如下所示。



启动遥控器 PowerShell 您的文件系统上的会话

1. 以您在置备文件系统时选择的委派 FSx 管理员组成员的身份连接到与您的文件系统具有网络Connect 的计算实例。
2. 打开窗户 PowerShell 窗口。
3. 使用以下命令在 Amazon FSx 文件系统上打开远程会话。Replace*FSxFileSystem-Remote-PowerShell-Endpoint*使用 Windows 遥控器 PowerShell 要管理的文件系统的终端节点。

```
PS C:\Users\delegateadmin> enter-pssession -ComputerName FSxFileSystem-Remote-
PowerShell-Endpoint -ConfigurationName FsxRemoteAdmin
[fs-0123456789abcdef0]: PS>
```

如果您的实例不属于 Amazon FSx AD 域，系统会在弹出窗口中提示您输入用户凭证。如果您的实例已加入域，则不会要求您提供证书。

您也可以在上运行 Amazon FSx CLI 进行远程管理 CLI PowerShell 文件系统上的命令使用`Invoke-Command`cmdlet，下面介绍的。

以下示例演示在使用`Invoke-Command`cmdlet PowerShell FSx for Windows File Server 文件系统上的命令。

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FSxRemoteAdmin -scriptblock { fsx-command}
```

管理 DNS 别名

FSx for Windows File Server 为每个文件系统提供一个默认的域名系统 (DNS) 名称，您可以使用该名称访问文件系统上的数据。您还可以使用自己选择的 DNS 别名访问文件系统。借助 DNS 别名，在将文件系统存储从本地迁移到 Amazon FSx 时，您可以继续使用现有 DNS 名称访问存储在 Amazon FSx 上的数据，而无需更新任何工具或应用程序。有关更多信息，请参阅 将现有文件存储迁移到 Amazon FSx (p. 58)。

Note

美国东部时间 2020 年 11 月 9 日中午 12:00 之后创建的适用于 Windows 文件服务器文件系统的 FSx 上提供了对 DNS 别名的Support。要在东部时间 2020 年 11 月 9 日下午 12:00 之前创建的文件系统上使用 DNS 别名，请执行以下操作：

1. 对现有文件系统进行备份。有关更多信息，请参阅 使用用户启动的备份 (p. 72)。
2. 将备份还原到新的文件系统。有关更多信息，请参阅 还原备份 (p. 75)。

一旦新文件系统可用，您就可以使用本节中提供的信息使用 DNS 别名来访问它。

Note

此处提供的信息假定您完全在 Active Directory 中工作，并且没有使用外部 DNS 提供程序。第三方 DNS 提供商可能会导致意外行为。
只有在您加入文件系统的 AD 域使用 Microsoft DNS 作为默认 DNS 时，亚马逊 FSX 才会为该文件系统注册 DNS 记录。如果您使用的是第三方 DNS，则需要在创建文件系统后为 Amazon FSx 文件系统手动设置 DNS 条目。有关为文件系统选择正确 IP 地址的详细信息，请参阅获取用于 DNS 的正确文件系统 IP 地址 (p. 46).

在创建新文件系统以及从备份创建新文件系统时，您可以将 DNS 别名与现有 FSx for Windows File Server 文件系统相关联。您可以同时将最多 50 个DNS 别名与文件系统关联。

除了将 DNS 别名与文件系统关联外，要使客户端使用 DNS 别名连接到文件系统，还必须执行以下操作：

- 为 Kerberos 身份验证和加密配置服务主体名称 (SPN)。
- 为解析为 Amazon FSx 文件系统的默认 DNS 名称的 DNS 别名记录配置 DNS 别名记录。

有关更多信息，请参阅 演练 5：使用 DNS 别名访问文件系统 (p. 152)。

DNS 别名必须满足以下要求：

- 必须格式化为完全限定域名 (FQDN)。
- 可以包含字母数字字符和连字符 (-)。
- 不得以连字符开头或结尾。
- 可以使用数字开头。

对于 DNS 别名，Amazon FSx 会将字母字符存储为小写字母 (a-z)，无论您指定将其存储为大写字母、小写字母还是转义码中的对应字母。

如果您尝试关联已与文件系统关联的别名，则不会产生任何影响。如果您尝试取消别名与文件系统无关的文件系统的关联，则 Amazon FSx 会以错误的请求错误作出响应。

Note

当 Amazon FSx 在文件系统上添加或删除别名时，连接的客户端会暂时断开连接，并将自动重新连接到文件系统。在断开连接时由映射非连续可用（非 CA）共享的客户端打开的任何文件都必须由客户端重新打开。

主题

将 DNS 别名与 Keros 身份验证使用

我们建议您在 Amazon FSx 中使用基于 Kerberos 的身份验证和加密。Kerberos 为访问文件系统的客户端提供最安全的身份验证。要为使用 DNS 别名访问您的 Amazon FSx 文件系统的客户端启用 Kerberos 身份验证，您必须配置与 Amazon FSx 文件系统的 Active Directory 计算机对象上的 DNS 别名相对应的服务主体名称 (SPN)。

如果您为分配给 Active Directory 中计算机对象上的另一个文件系统的 DNS 别名配置了 SPN，则必须先删除这些 SPN，然后才能将 SPN 添加到文件系统的计算机对象。有关更多信息，请参阅 演练 5：使用 DNS 别名访问文件系统 (p. 152)。

查看与文件系统和备份关联的 DNS 别名

您可以使用 Amazon FSx 控制台查看当前与文件系统和备份关联的 DNS 别名AmazonCLI，以及亚马逊 FSx API 和软件开发工具包。

要查看与文件系统关联的 DNS 别名，请执行以下操作：

- 使用控制台 — 选择一个文件系统以查看文件系统详情页面。选择网络与安全选项卡以查看DNS 别名.
- 使用 CLI 或 API — 使用`describe-file-system-aliases`CLI 命令或DescribeFileSystemAliasesAPI 操作。

要查看与备份关联的 DNS 别名，请执行以下操作：

- 使用控制台 — 在导航窗格中，选择备份，然后选择要查看的备份。在摘要” 窗格中，查看DNS 别名字段中返回的子位置类型。
- 使用 CLI 或 API — 使用`describe-backups`CLI 命令或DescribeBackupsAPI 操作。

DNS 别名状态

DNS 别名可能具有下列值之一：

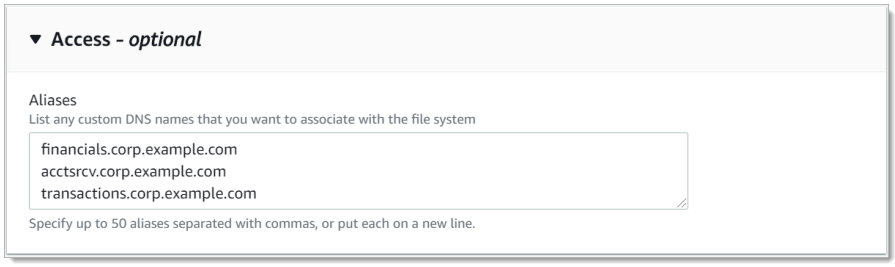
- 可用 — DNS 别名与 Amazon FSx 文件系统相关联。
- 正在创建 — Amazon FSx 正在创建 DNS 别名并将其与文件系统关联。
- 删除 — Amazon FSx 正在解除 DNS 别名与文件系统的关联并将其删除。
- 创建失败 — Amazon FSx 无法将 DNS 别名与文件系统关联。
- 删除失败 — Amazon FSx 无法解除 DNS 别名与文件系统的关联。

创建新文件系统时关联 DNS 别名

在从头开始创建新文件系统或从备份创建文件系统时，可以关联 DNS 别名。

在创建新的 Amazon FSx 文件系统时关联 DNS 别名（控制台）

1. 从打开 Amazon FSx 控制台https://console.aws.amazon.com/fsx/.
2. 按照中所述的创建新文件系统的过程进行操作第 1 步：创建文件系统 (p. 7)“入门” 一节中的。
3. 在访问权限-可选的 部分创建文件系统向导中，输入要与您的文件系统关联的 DNS 别名。



4. 当文件系统为Available，则可以通过配置服务主体名称 (SPN) 以及更新或创建别名的 DNS 别名记录来使用 DNS 别名记录来访问它。有关更多信息，请参阅 演练 5：使用 DNS 别名访问文件系统 (p. 152)。

在创建新的 Amazon FSx 文件系统时关联 DNS 别名 (CLI)

1. 在创建新的文件系统时，使用别名属性与CreateFileSystem将 DNS 别名与新文件系统关联的 API 操作。

```
aws fsx create-file-system \
  --file-system-type WINDOWS \
  --storage-capacity 2000 \
  --storage-type SSD \
  --subnet-ids subnet-123456 \
  --windows-configuration Aliases=[financials.corp.example.com,accts-
rcv.corp.example.com]
```

2. 当文件系统为Available，则可以通过配置服务主体名称 (SPN) 以及更新或创建别名的 DNS 别名记录来使用 DNS 别名记录来访问它。有关更多信息，请参阅 演练 5：使用 DNS 别名访问文件系统 (p. 152)。

在从备份创建新的 Amazon FSx 文件系统时关联或取消关联 DNS 别名 (CLI)

1. 从现有文件系统的备份中创建新的文件系统时，您可以使用别名属性与CreateFileSystemFromBackupAPI 操作如下所示：

   - 默认情况下，与备份关联的所有别名都与新文件系统相关联。
   - 要创建文件系统而不保留备份中的任何别名，请使用`Aliases`属性具有一个空集合。

     要关联其他 DNS 别名，请使用`Aliases`属性，同时包含与备份关联的原始别名和要关联的新别名。

   以下 CLI 命令将两个别名与 Amazon FSx 通过备份创建的文件系统相关联。

```
aws fsx create-file-system-from-backup \
  --backup-id backup-0123456789abcdef0
  --storage-capacity 2000 \
  --storage-type HDD \
  --subnet-ids subnet-123456 \
  --windows-configuration Aliases=[transactions.corp.example.com,accts-
rcv.corp.example.com]
```

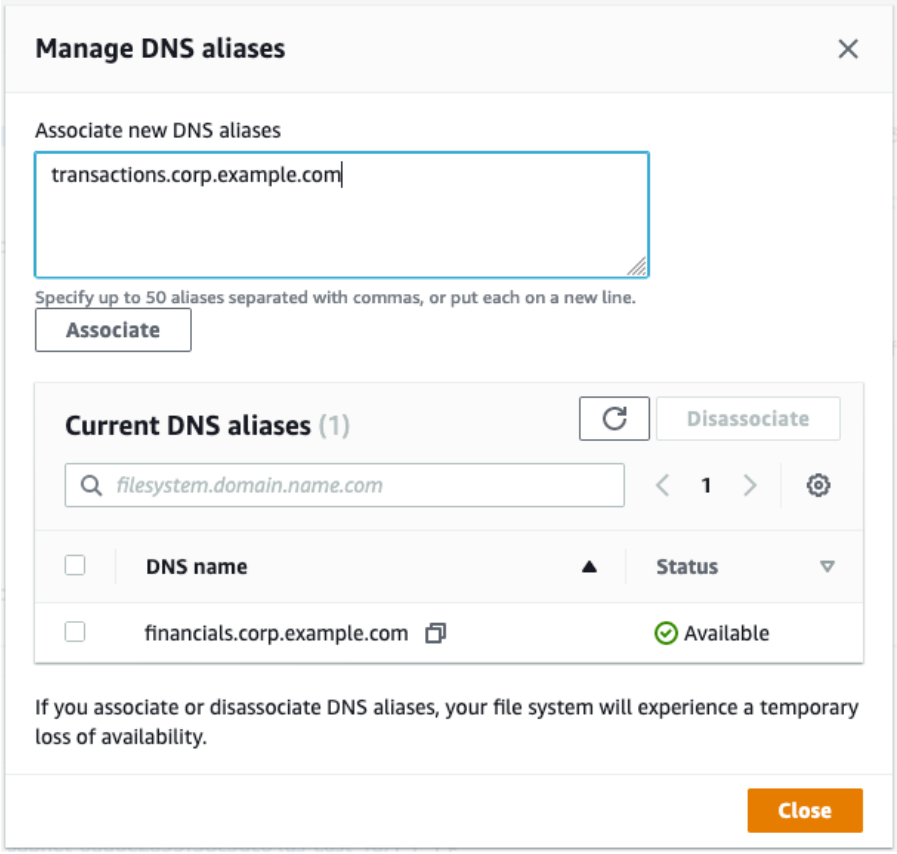
2. 当文件系统为Available，则可以通过配置服务主体名称 (SPN) 以及更新或创建别名的 DNS 别名记录来使用 DNS 别名记录来访问它。有关更多信息，请参阅 演练 5：使用 DNS 别名访问文件系统 (p. 152)。

管理现有文件系统上的 DNS 别名

您可以在现有文件系统上添加和删除别名。

在现有文件系统上管理 DNS 别名（控制台）

1. 从打开 Amazon FSx 控制台https://console.aws.amazon.com/fsx/.
2. 导航到文件系统，然后选择要管理其的 DNS 别名的 Windows 文件系统。
3. 在存储库的网络与安全选项卡上，选择Manage为了DNS 别名，显示管理 DNS 别名对话框。



   - 要关联 DNS 别名 — 在关联新别名框中，输入要关联的 DNS 别名。选择 Associate。
   - 取消关联 DNS 别名 — 在当前别名列表中，选择要解除关联的别名。选择取消关联。

   您可以在中监控您管理的别名状态当前别名list。刷新列表以更新状态。将别名与文件系统关联或取消关联最多需要 2.5 分钟。
4. 当别名是Available，您可以使用 DNS 别名访问文件系统，方法是配置服务主体名称 (SPN) 并更新或创建别名的 DNS CNAME 记录。有关更多信息，请参阅 演练 5：使用 DNS 别名访问文件系统 (p. 152)。

将 DNS 别名与现有的文件系统关联 (CLI)

1. 使用`associate-file-system-aliases`CLI 命令或AssociateFileSystemAliases将 DNS 别名与现有的文件系统关联的 API 操作。

   以下 CLI 请求将两个别名与指定的文件系统关联。

   ```
   aws fsx associate-file-system-aliases \
     --file-system-id fs-0123456789abcdef0 \
     --aliases financials.corp.example.com transfers.corp.example.com
   ```

   响应显示 Amazon FSx 正在与文件系统关联的别名的状态。

   ```
   {
       "Aliases": [
           {
               "Name": "financials.corp.example.com",
               "Lifecycle": CREATING
           },
           {
               "Name": "transfers.corp.example.com",
               "Lifecycle": CREATING
           }
       ]
   }
   ```

2. 使用`describe-file-system-aliases`CLI 命令 (DescribeFileSystemAliases是等效的 API 操作）来监视您正在关联的别名的状态。
3. 当`Lifecycle`的值为 AVAILABLE（该过程最多需要 2.5 分钟），则可以通过配置服务主体名称 (SPN) 以及更新或创建别名的 DNS 别名记录来使用 DNS 别名记录来访问文件系统。有关更多信息，请参阅 演练 5：使用 DNS 别名访问文件系统 (p. 152)。

解除 DNS 别名与文件系统的关联 (CLI)

- 使用`disassociate-file-system-aliases`CLI 命令或DisassociateFileSystemAliasesAPI 操作，用于将 DNS 别名从现有的文件系统解除关联。

  以下命令解除一个别名与文件系统的关联。

  ```
  aws fsx disassociate-file-system-aliases \
    --file-system-id fs-0123456789abcdef0 \
    --aliases financials.corp.example.com
  ```

  响应显示 Amazon FSx 正在与文件系统解除关联的别名的状态。

  ```
  {
      "Aliases": [
          {
              "Name": "financials.corp.example.com",
              "Lifecycle": DELETING
          }
      ]
  }
  ```

  使用`describe-file-system-aliases`CLI 命令 (DescribeFileSystemAliases是等效的 API 操作），用于监控别名状态。删除别名最多需要 2.5 分钟。

文件共享

您可以管理文件共享并执行以下任务。

- 创建新的文件共享
- 修改文件共享
- 移除文件共享

您可以使用 Windows 原生共享文件夹 GUI 和 Amazon FSx CLI 进行远程管理 PowerShell 管理FSx for Windows File Server 文件系统上的文件共享。

> Warning
>
> Amazon FSx 要求系统用户具有完全控制对您创建 SMB 文件共享的每个文件夹的 NTFS ACL 权限。请勿更改此用户对文件夹的 NTFS ACL 权限，因为这样做会使您的文件共享不可访问。

使用 GUI 管理文件共享

要管理 Amazon FSx 文件系统上的文件共享，您可以使用共享文件夹 GUI。共享文件夹 GUI 为管理 Windows 服务器上的所有共享文件夹提供了一个中心位置。以下流程详细介绍了如何管理您的文件共享。

将共享文件夹连接到 FSx 文件系统

1. 启动您的 Amazon EC2 实例，并将其连接到您的 Amazon FSx 文件系统所加入的微软活动目录。为此，请从Amazon Directory Service管理指南：
   - 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身份Connect 您的实例。InAmazon托管微软活动目录，这个组被称为Amazon委派的 FSx 管理员。在自我管理的 Microsoft Active Directory 中，此组称为域管理员或您在创建过程中提供的管理员组的自定义名称。有关更多信息，请参阅适用于 Windows 实例的 Amazon EC2 用户指南中的连接您的 Windows 实例。
3. 打开启动菜单并运行fsmgmt.msc使用以管理员身份运行. 执行此操作将打开共享文件夹 GUI 工具。
4. 适用于操作，选择Connect 另一台计算机.
5. 适用于另一台计算机中，输入 Amazon FSx 文件系统的域名系统 (DNS) 名称，例如**`amznfsxabcd0123.corp.example.com`**.

   要在 Amazon FSx 控制台上查找文件系统的 DNS 名称，请选择文件系统，选择您的文件系统，然后选中网络与安全部分，位于文件系统详细信息页面的。你也可以在响应中获取 DNS 名称DescribeFileSystemsAPI 操作。
6. 选择 OK（确定）。然后，Amazon FSx 文件系统的条目将出现在共享文件夹工具的列表中。

现在，共享文件夹已连接到您的 Amazon FSx 文件系统，您可以管理文件系统上的 Windows 文件共享。默认共享称为`\share`. 可执行以下操作来做到这一点：

- 创建新的文件共享— 在 “共享文件夹” 工具中，选择共享在左窗格中查看您的 Amazon FSx 文件系统的活动共享。选择新共享并完成 “创建共享文件夹” 向导。

  必须先创建本地文件夹，然后才能创建新的文件共享。可执行如下所示：
  - 使用共享文件夹工具：指定本地文件夹路径时单击 “浏览”，然后单击 “创建新文件夹” 以创建本地文件夹。
  - 使用命令行：

```
New-Item -Type Directory -Path \\amznfsxabcd0123.corp.example.com\D$\share\MyNewShare
```

- 修改文件共享— 在 Shared Folders 工具中，在右侧窗格中打开您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.
- 移除文件共享— 在 Shared Folders 工具中，在右侧窗格中打开您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

  对于单可用区 2 和多可用区文件系统，使用共享文件夹 GUI 工具删除文件共享或修改文件共享（包括更新权限、用户限制和其他属性）只有在连接到fsmgmt.msc使用 Amazon FSx 文件系统的 DNS 名称。如果您使用文件系统的 IP 地址或 DNS 别名进行连接，则共享文件夹 GUI 工具不支持这些操作。

使用 PowerShell 管理文件共享

您可以使用自定义远程管理命令来管理文件共享 PowerShell. 这些命令可以帮助您更轻松地自动执行以下任务：

- 将现有文件服务器上的文件共享迁移到 Amazon FSx
- 同步文件共享Amazon灾难恢复区域
- 以编程方式管理持续工作流的文件共享，例如团队文件共享配置

要了解如何使用 Amazon FSx CLI 进行远程管理，请访问 PowerShell，请参阅开始使用 Amazon FSx CLI 进行远程管理 PowerShell (p. 80).

创建持续可用的共享

您可以使用用于远程管理的 Amazon FSx CLI 创建持续可用 (CA) 共享 PowerShell. 在 FSx for Windows 文件服务器多可用区文件系统上创建的 CA 共享具有很高的持久性和高可用性。Amazon FSx 单可用区文件系统是在单节点群集上构建的。因此，在单可用区文件系统上创建的 CA 共享具有很高的持久性，但可用性不高。使用`New-FSxSmbShare`命令使用`-ContinuouslyAvailable`选项设置为`$True`以指定共享为持续可用的共享。以下是创建 CA 共享的示例命令。

```
New-FSxSmbShare -Name "New CA Share" -Path "D:\share\new-share" -Description "CA share" -
ContinuouslyAvailable $True
```

您可以修改`-ContinuouslyAvailable`选项在现有的文件共享上使用`Set-FSxSmbShare`命令。

以下是自定义远程管理 PowerShell 您可以使用的命令。

共享管理命令	描述
New-FSxSmbShare	创建新的文件共享。
Remove-FSxSmbShare	移除文件共享。
Get-FSxSmbShare	检索现有文件共享。
Set-FSxSmbShare	设置共享的属性。
Get-FSxSmbShareAccess	检索共享的访问控制列表 (ACL)。

共享管理命令	描述
Grant-FSxSmbShareAccess	将受托人的允许访问控制条目 (ACE) 添加到共享的安全描述符中。
Revoke-FSxSmbShareAccess	从共享的安全描述符中删除受托人的所有 allow ACE。
Block-FSxSmbShareAccess	将受托人的拒绝 ACE 添加到共享的安全描述符中。
Unblock-FSxSmbShareAccess	从共享的安全描述符中删除受托人的所有拒绝 ACE。

每个命令的联机帮助提供了所有命令选项的参考。要访问此帮助，请运行命令`-?`，例如`New-FSxSmbShare -?`.

将证书传递给 New-FSxSmbShare

你可以将证书传递给 New-FSxSmbShare 这样你就可以循环运行它来创建成百上千个共享，而不必每次都重新输入凭据。

使用以下选项之一准备在 FSx for Windows File Server 上创建文件共享所需的凭据对象。

- 要以交互方式生成凭据对象，请使用以下命令。

```
$credential = Get-Credential
```

- 使用生成凭据对象Amazon Secrets Manager资源，请使用以下命令。

```
$credential = ConvertFrom-Json -InputObject (Get-SECSecretValue -SecretId
 $AdminSecret).SecretString
$FSxAdminUserCredential = (New-Object PSCredential($credential.UserName,(ConvertTo-
SecureString $credential.Password -AsPlainText -Force)))
```

审计文件访问

适用于 Windows 文件服务器的 Amazon FSx 支持审核最终用户对文件、文件夹和文件共享的访问权限。你可以选择将审计事件日志发送给一组丰富的其他Amazon支持查询、处理、存储和存档日志、发出通知和触发操作的服务，以进一步推进安全性和合规性目标。

主题

文件访问审核概述

通过文件访问审计，您可以根据定义的审计控制来记录最终用户对单个文件、文件夹和文件共享的访问权限。审计控制也称为 NTFS 系统访问控制列表 (SACL)。如果您已经对现有文件数据设置了审计控制，则可以通过创建一个新的 Amazon FSx for Windows 文件服务器文件系统并迁移数据来利用文件访问审核。

Amazon FSx 支持 Windows 为文件、文件夹和文件共享访问提供的以下审计事件：

- 对于文件访问，它支持：全部、Traverse 文件夹/执行文件、列表文件夹/读取数据、读取属性、创建文件/写入数据、创建文件夹/追加数据、写入属性、删除子文件夹和文件、删除、读取权限、更改权限和获取所有权。
- 对于文件共享访问，它支持：Connect 到文件共享。

在文件、文件夹和文件共享访问中，Amazon FSx 支持记录成功尝试（例如具有足够权限的用户成功访问文件或文件共享）、失败尝试或两者兼有。

您可以配置是仅对文件和文件夹、仅对文件共享还是两者进行访问审核。您还可以配置应记录哪些类型的访问（仅限成功尝试、仅失败尝试或两者兼而有）。您也可以随时关闭文件访问审核。

> Note
>
> 文件访问审计仅记录最终用户访问数据自启用时起。也就是说，文件访问审核不会生成启用文件访问审核之前发生的最终用户文件、文件夹和文件共享访问活动的审核事件日志。

支持的访问审计事件的最高速率为每秒 5,000 个事件。不会为每个文件读取和写入操作生成访问审计事件，而是在每个文件元数据操作（例如用户创建、打开或删除文件时）生成一次访问审计事件。

审核事件日志目标

启用后，文件访问审核功能必须配置AmazonAmazon FSx 将审计事件日志发送到的服务。此审核事件日志目标必须是亚马逊 CloudWatch 将日志流记录到 CloudWatch 记录日志组或 Amazon Kinesis Data Firehose 传输流。您可以在创建 Amazon FSx for Windows File Server 文件系统时或之后通过更新该文件系统选择审核事件日志目标。有关更多信息，请参阅 管理文件访问审计 (p. 92)。

以下是一些可能有助于您决定要选择哪个审计事件日志目标的建议：

- 选择 CloudWatch 日志是否要在亚马逊中存储、查看和搜索审计事件日志 CloudWatch 控制台，使用对日志运行查询 CloudWatch 记录见解并触发 CloudWatch 警报或 Lambda 函数。
- 如果要将事件持续流式传输到 Amazon S3 中的存储、Amazon Redshift 中的数据库和亚马逊，请选择 Kinesis Data Firehose OpenSearch 服务，或者Amazon用于进一步分析的合作伙伴解决方案（例如 Splunk 或 Datadog）。

默认情况下，Amazon FSx 将创建并使用默认值 CloudWatch 将您账户中的日志组记录为审核事件日志目标。如果您希望使用自定义 CloudWatch 日志日志组或使用 Kinesis Data Firehose 作为审核事件日志目标，以下是审核事件日志目标的名称和位置的要求：

- 的名称 CloudWatch 日志日志组必须以`/aws/fsx/`prefix. 如果您没有现有 CloudWatch 记录日志组在控制台上创建或更新文件系统时，Amazon FSx 可以在 CloudWatch 日志`/aws/fsx/windows`日志组。如果您不想使用默认日志组，配置 UI 允许您创建一个 CloudWatch 在控制台上创建或更新文件系统时记录日志组。
- Kinesis Data Firehose 传输流的名称必须以`aws-fsx-`prefix. 如果您没有现有的 Kinesis Data Firehose 传输流，则可以在控制台创建或更新文件系统时创建一个。
- 必须将 Kinesis Data Firehose 传输流配置为使用`Direct PUT`作为它的来源。您不能将现有的 Kinesis 数据流用作交付流的数据源。
- 目标（无论是） CloudWatch 必须位于同一个日志组或 Kinesis Data Firehose 传输流中）Amazon分区，Amazon Web Services 区域, 和Amazon Web Services 账户作为您的 Amazon FSx 文件系统。

您可以随时更改审计事件日志目标（例如，从 CloudWatch 将日志记录到 Kinesis Data Firehose）。执行此操作时，新的审计事件日志将仅发送到新目标。

尽力审计事件日志交付

通常，审计事件日志记录在几分钟内交付，但有时可能需要更长的时间。在极少数情况下，审核事件日志记录可能遗漏。如果您的使用案例需要特定的语义（例如，确保不遗漏审核事件），建议您在设计工作流程时对遗漏的事件加以说明。您可以通过扫描文件系统上的文件和文件夹结构以审核遗漏的事件。

审核文件和文件夹的访问权限

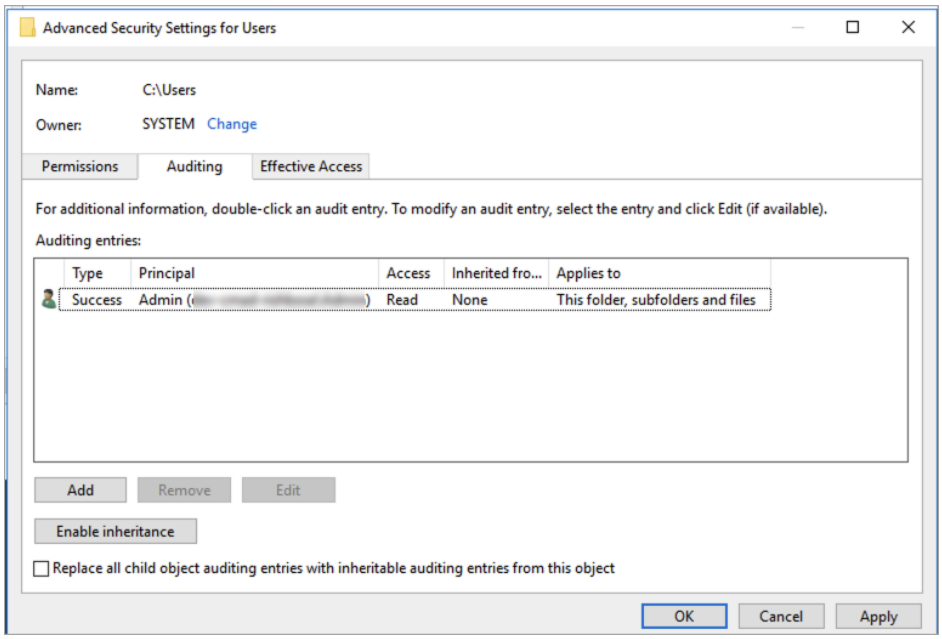
您需要对要审计用户访问尝试的文件和文件夹设置审计控制。审计控制也称为 NTFS 系统访问控制列表 (SACL)。

您可以使用 Windows 原生 GUI 界面或以编程方式使用 Windows 配置审计控制 PowerShell 命令。如果启用继承，则通常只需要在要记录访问权限的顶级文件夹上设置审计控制。

使用 Windows GUI 设置审核访问权限

要使用 GUI 设置文件和文件夹的审计控制，请使用 Windows 文件资源管理器。在给定的文件或文件夹上，打开 Windows 文件资源管理器，然后选择属性 > 安全 > 高级 > 审计选项卡。

以下审计控制示例审计文件夹的成功事件。只要管理员用户成功读取该句柄，就会发出 Windows 事件日志条目。



这些区域有：类型字段指示要审核哪些操作。将此字段设置为成功为了审计成功的尝试，Fail审计失败的尝试，或者全部审计成功和失败的尝试。

有关审核条目字段的更多信息，请参阅对文件或文件夹应用基本审计策略在微软文档中。

使用 PowerShell 设置审计访问权限的命令

您可以使用 Microsoft Windows`Set-Acl`命令在任何文件或文件夹上设置审计 SACL。有关此命令的信息，请参阅 MicrosoftSet-Ac文档中）。

以下是使用一系列 PowerShell 命令和变量来设置成功尝试的审计访问权限。您可以调整这些示例命令以满足文件系统的需求。

```
$path = "C:\Users\TestUser\Desktop\DemoTest\"
```

```
$ACL = Get-Acl $path

$ACL | Format-List

$AuditUser = "TESTDOMAIN\TestUser"

$AuditRules = "FullControl"

$InheritType = "ContainerInherit,ObjectInherit"

$AuditType = "Success"

$AccessRule = New-Object System.Security.AccessControl.FileSystemAuditRule($AuditUser,
$AuditRules,$InheritType,"None",$AuditType)

$ACL.SetAuditRule($AccessRule)

$ACL | Set-Acl $path

Get-Acl $path -Audit | Format-List
```

管理文件访问审计

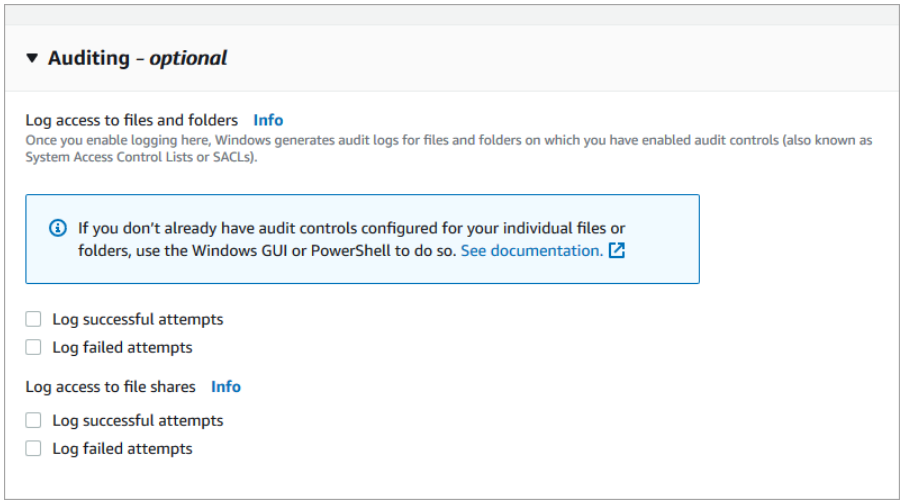
您可以在创建新的 Amazon FSx for Windows File Server 文件系统时启用文件访问审核。当您从 Amazon FSx 控制台创建文件系统时，默认情况下，文件访问审核处于关闭状态。

在已启用文件访问审核的现有文件系统上，您可以更改文件访问审核设置，包括更改文件和文件共享访问的访问尝试类型以及审计事件日志目标。您可以使用 Amazon FSx 控制台执行这些任务，Amazon CLI，或者 API。

> Note
>
> 对于吞吐量为 32 MB/s 或更高的 Windows 文件服务器文件系统，只有 Amazon FSx 才支持文件访问审核。如果启用了文件访问审核，则无法创建或更新吞吐量小于 32 MB/s 的文件系统。您可以在创建文件系统后随时修改吞吐量容量。有关更多信息，请参阅 管理吞吐量容量 (p. 122)。

创建文件系统时启用文件访问审核（控制台）

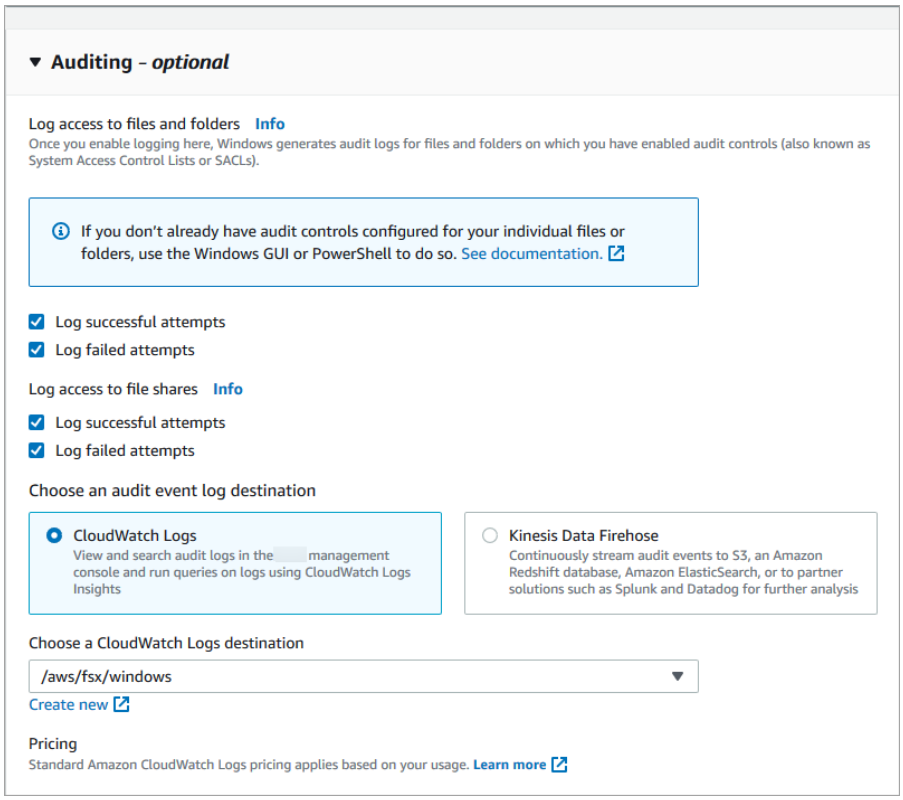
1. 从打开 Amazon FSx 控制台https://console.aws.amazon.com/fsx/.
2. 按照中所述的创建新文件系统的过程进行操作第 1 步：创建文件系统 (p. 7)在 “入门” 章节中。
3. 打开审核-可选部分。默认情况下，禁用文件访问审核。



4. 要启用和配置文件访问审核，请执行以下操作。

   - 适用于日志访问文件和文件夹中，选择成功和/或失败尝试的记录。如果没有进行选择，文件和文件夹的日志记录将被禁用。
   - 适用于记录对文件共享的访问中，选择成功和/或失败尝试的记录。如果您没有进行选择，文件共享将禁用日志记录。
   - 适用于选择审核事件日志目标，选择CloudWatch Logs (CloudWatch 日志)要么Kinesis Data Firehose. 然后选择现有日志或传输流或创建新的流。适用于 CloudWatch 日志，Amazon FSx 可以在 CloudWatch 日志`/aws/fsx/windows`日志组。

   以下是一个文件访问审计配置的示例，该配置将审计最终用户对文件、文件夹和文件共享的成功和失败的访问尝试。审计事件日志将发送到默认值 CloudWatch 日志`/aws/fsx/windows`日志组目标。



5. 继续操作文件系统创建向导的下一部分。

当文件系统处于Available，启用了文件访问审核功能。

创建文件系统时启用文件访问审核 (CLI)

1. 创建新的文件系统时，请使用`AuditLogConfiguration`房地产与CreateFileSystem用于启用新文件系统的文件访问审核的 API 操作。

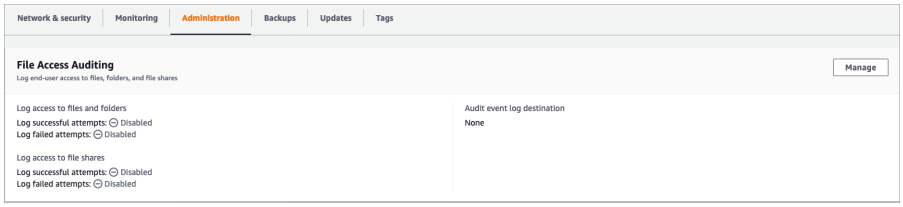
```
aws fsx create-file-system \
  --file-system-type WINDOWS \
  --storage-capacity 300 \
  --subnet-ids subnet-123456 \
  --windows-configuration
 AuditLogConfiguration='{FileAccessAuditLogLevel="SUCCESS_AND_FAILURE", \
    FileShareAccessAuditLogLevel="SUCCESS_AND_FAILURE", \
```

```
    AuditLogDestination="arn:aws:logs:us-east-1:123456789012:log-group:/aws/fsx/my-
customer-log-group"}'
```

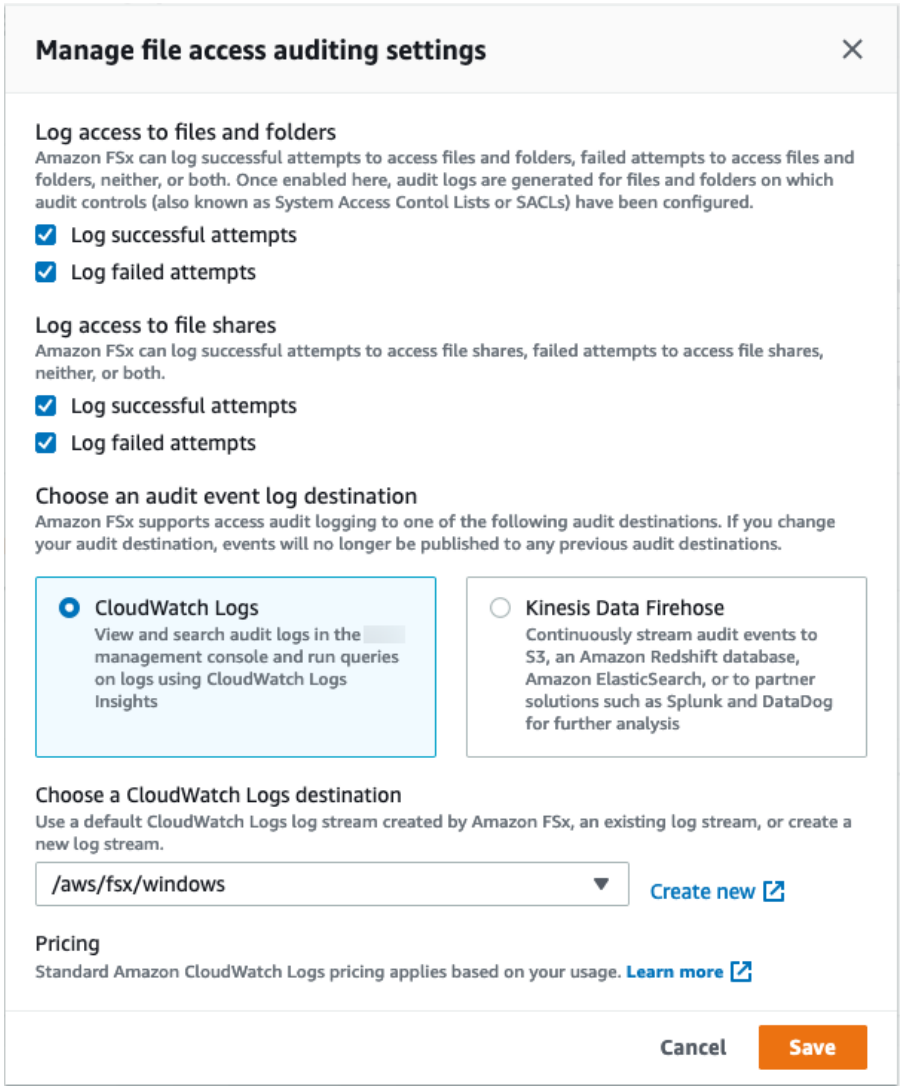
2. 当文件系统处于Available，启用了文件访问审核功能。

更改文件访问审核配置（控制台）

1. 从打开 Amazon FSx 控制台https://console.aws.amazon.com/fsx/.
2. 导航到文件系统，然后选择要管理其文件访问审核的 Windows 文件系统。
3. 选择管理选项卡。
4. 在存储库的审核文件访问面板中，选择Manage.



5. 在存储库的管理文件访问审核设置对话框中，更改所需的设置。



- 适用于日志访问文件和文件夹中，选择成功和/或失败尝试的记录。如果没有进行选择，文件和文件夹的日志记录将被禁用。
- 适用于记录对文件共享的访问中，选择成功和/或失败尝试的记录。如果您没有进行选择，文件共享将禁用日志记录。
- 适用于选择审核事件日志目标，选择CloudWatch Logs (CloudWatch 日志)要么Kinesis Data Firehose. 然后选择现有日志或传输流或创建新的流。

6. 选择 Save（保存）。

更改文件访问审核配置 (CLI)

- 使用`update-file-system`CLI 命令或等效命令`UpdateFileSystem`API 操作。

```
aws fsx update-file-system \
  --file-system-id fs-0123456789abcdef0 \
  --windows-configuration
 AuditLogConfiguration='{FileAccessAuditLogLevel="SUCCESS_ONLY", \
    FileShareAccessAuditLogLevel="FAILURE_ONLY", \
```

```
    AuditLogDestination="arn:aws:logs:us-east-1:123456789012:log-group:/aws/fsx/my-
customer-log-group"}'
```

迁移审核控制

如果您已经对现有文件数据设置了审计控制 (SACL)，则可以创建 Amazon FSx 文件系统并将数据迁移到新的文件系统。我们建议使用Amazon DataSync将数据和关联的 SACL 传输到您的 Amazon FSx 文件系统。作为替代解决方案，你可以使用 Robocopy（强大的文件副本）。有关更多信息，请参阅 将现有文件存储迁移到 Amazon FSx (p. 58)。

查看事件日志

在 Amazon FSx 开始发布审计事件日志后，您可以查看审计事件日志。查看日志的位置和方式取决于审计事件日志目标：

- 您可以查看 CloudWatch 通过转到记录日志 CloudWatch 控制台，然后选择将审计事件日志发送到的日志组和日志流。有关更多信息，请参阅 。查看发送到的日志数据 CloudWatch 日志中的亚马逊 CloudWatch 日志用户指南.

  您可以使用 CloudWatch 记录 Insights 以交互方式搜索和分析您的日志数据。有关更多信息，请参阅 。使用 分析日志数据 CloudWatch 日志见解，在亚马逊 CloudWatch 日志用户指南.

  您还可以将审核事件日志导出到 Amazon S3。有关更多信息，请参阅 。将日志数据导出到 Amazon S3，也在中亚马逊 CloudWatch 日志用户指南.
- 您无法在 Kinesis Data Firehose 上查看审计事件日志。但是，您可以将 Kinesis Data Firehose 配置为将日志转发到可以从中读取的目标。目标包括 Amazon S3、Amazon Redshift、Amazon OpenSearch 服务和合作伙伴解决方案，例如 Splunk 和 Datadog，有关详细信息，请参阅选择目标中的Amazon Kinesis Data Firehose 开发人员指南.

审核事件字段

本节介绍了审计事件日志中的信息以及审计事件的示例。

以下是 Windows 审计事件中的突出字段的说明。

- EventId是指微软定义的 Windows 事件日志事件 ID。有关以下信息，请参阅 Microsoft 文档文件系统事件和文件共享事件.
- 主题用户名指执行访问权限的用户。
- objectName指已访问的目标文件、文件夹或文件共享。
- SharenName适用于为文件共享访问而生成的事件。例如，`EventID 5140`是在访问网络共享对象时生成的。
- IpAddress指为文件共享事件启动事件的客户端。
- 关键词，如果可用，请参阅文件访问是成功还是失败。对于成功访问，该值将为`0x8020000000000000`. 对于失败的访问，值为`0x8010000000000000`.
- TimeCreated System Time是指在系统中生成事件并以 <YYYY-MM-DDThh:mm:ss.s>Z 格式显示的时间。
- Computer指文件系统的 DNS 名称 Windows Remote PowerShell 终端节点和可用于标识文件系统。
- Access Mask（如果可用）是指执行的文件访问类型（例如 ReadData、WriteData）。
- 访问列表指请求或授予对对象的访问权限。有关详细信息，请参阅下表和 Microsoft 文档（例如事件 4556)。

访问类型	访问掩码	值
读取数据或列表目录	0x1	%%4416
写数据或添加文件	0x2	%%4417
追加数据或添加子目录	0x4	%%4418
阅读扩展属性	0x8	%%4419
写入扩展属性	0x10	%%4420
执行/Traverse	0x20	%%4421
删除子级	0x40	%%4422
阅读属性	0x80	%%4423
写入属性	0x100	%%4424
删除	0x10000	%%1537
阅读 ACL	0x20000	%%1538
写入 ACL	0x40000	%1539
写入拥有者	0x80000	%%1540
同步	0x100000	%1541
访问安全 ACL	0x1000000	%%1542

以下是带示例的一些关键事件。请注意，XML 设置了格式以便于阅读。

事件 ID 4660删除对象时将记录该对象。

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4660</EventID><Version>0</Version><Level>0</Level>
<Task>12800</Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-05-18T04:51:56.916563800Z'/>
<EventRecordID>315452</EventRecordID><Correlation/>
<Execution ProcessID='4' ThreadID='5636'/><Channel>Security</Channel>
<Computer>amznfsxgyzohmw8.example.com</Computer><Security/></System><EventData>
<Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x50932f71</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='HandleId'>0x12e0</Data><Data Name='ProcessId'>0x4</Data><Data
 Name='ProcessName'></Data>
<Data Name='TransactionId'>{00000000-0000-0000-0000-000000000000}</Data></EventData></
Event>
```

事件 ID 4659已登录删除文件的请求。

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4659</EventID><Version>0</Version><Level>0</Level><Task>12800</Task><Opcode>0</
Opcode>
```

```
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-0603T19:18:09.951551200Z'/>
<EventRecordID>308888</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='5540'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/></
System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device\HarddiskVolume8\shar
\event.txt</Data>
<Data Name='HandleId'>0x0</Data><Data
 Name='TransactionId'>{00000000-0000-0000-0000-000000000000}</Data>
<Data Name='AccessList'>%%1537
    %%4423
    </Data><Data Name='AccessMask'>0x10080</Data><Data Name='PrivilegeList'>-</Data>
<Data Name='ProcessId'>0x4</Data></EventData></Event>
```

事件 ID 4663在对象执行特定操作时记录。以下示例显示从文件中读取数据，可以从AccessList %%4416.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4663< /EventID><Version>1</Version><Level>0</Level><Task>12800</Task><Opcode>0</
Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:10:13.887145400Z'/>
<EventRecordID>308831</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='6916'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/></
System>
<EventData>< Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113< /
Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device\HarddiskVolume8\share
\event.txt</Data>
<Data Name='HandleId'>0x101c</Data><Data Name='AccessList'>%%4416
    </Data>
<Data Name='AccessMask'>0x1</Data><Data Name='ProcessId'>0x4</Data>
<Data Name='ProcessName'></Data><Data Name='ResourceAttributes'>S:AI</Data>
</EventData></Event>
```

以下示例显示了从文件中写入/附加数据，可以从AccessList %%4417.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4663</EventID><Version>1</Version><Level>0</Level><Task>12800</Task><Opcode>0</
Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:12:16.813827100Z'/>
<EventRecordID>308838</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='5828'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/></
System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device\HarddiskVolume8\share
\event.txt</Data>
<Data Name='HandleId'>0xa38</Data><Data Name='AccessList'>%%4417
    </Data><Data Name='AccessMask'>0x2</Data><Data Name='ProcessId'>0x4</Data>
```

```
<Data Name='ProcessName'></Data><Data Name='ResourceAttributes'>S:AI</Data></EventData></
Event>
```

事件 ID 4656表示请求了对象的特定访问权限。在以下示例中，已启动读取请求 ObjectName “permtest” 并且是失败的尝试，如0x8010000000000000.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4656</EventID><Version>1</Version><Level>0</Level><Task>12800</Task><Opcode>0</
Opcode>
<Keywords>0x8010000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:22:55.113783500Z'/>
<EventRecordID>308919</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='4924'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/></
System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device\HarddiskVolume8\share
\permtest</Data>
<Data Name='HandleId'>0x0</Data><Data
 Name='TransactionId'>{00000000-0000-0000-0000-000000000000}</Data>
<Data Name='AccessList'>%%1541
    %%4416
    %%4423
    </Data><Data Name='AccessReason'>%%1541: %%1805
    %%4416: %%1805
    %%4423: %%1811 D:(A;OICI;0x1301bf;;;AU)
    </Data><Data Name='AccessMask'>0x100081</Data><Data Name='PrivilegeList'>-</Data>
<Data Name='RestrictedSidCount'>0</Data><Data Name='ProcessId'>0x4</Data><Data
 Name='ProcessName'></Data>
<Data Name='ResourceAttributes'>-</Data></EventData></Event>
```

事件 ID 4670在对象的权限发生更改时记录。以下示例显示用户 “admin” 修改了上的权限 ObjectName “许可” 向 SID “S-1-5-21-658495921-4185342820-3824891517-1113” 添加权限。有关如何解释权限的更多信息，请参阅 Microsoft 文档。

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4670</EventID><Version>0</Version><Level>0</Level>
<Task>13570</Task><Opcode>0</Opcode><Keywords>0x8020000000000000</Keywords>
<TimeCreated SystemTime='2021-06-03T19:39:47.537129500Z'/><EventRecordID>308992</
EventRecordID>
<Correlation/><Execution ProcessID='4' ThreadID='2776'/><Channel>Security</Channel>
<Computer>amznfsxgyzohmw8.example.com</Computer><Security/></System><EventData>
<Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device\HarddiskVolume8\share
\permtest</Data>
<Data Name='HandleId'>0xcc8</Data>
<Data Name='OldSd'>D:PAI(A;OICI;FA;;;SY)
(A;OICI;FA;;;S-1-5-21-658495921-4185342820-3824891517-2622)</Data>
<Data Name='NewSd'>D:PARAI(A;OICI;FA;;;S-1-5-21-658495921-4185342820-3824891517-1113)
(A;OICI;FA;;;SY)(A;OICI;FA;;;
S-1-5-21-658495921-4185342820-3824891517-2622)</Data><Data Name='ProcessId'>0x4</Data>
<Data Name='ProcessName'></Data></EventData></Event>
```

事件 ID 5140每次访问文件共享时都会记录。

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>5140</EventID><Version>1</Version><Level>0</Level><Task>12808</Task><Opcode>0</
Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:32:07.535208200Z'/>
<EventRecordID>308947</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='3120'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/></
System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-2620</Data>
<Data Name='SubjectUserName'>EC2AMAZ-1GP4HMN$</Data><Data
 Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2d4ca529</Data><Data Name='ObjectType'>File</Data><Data
 Name='IpAddress'>172.45.6.789</Data>
<Data Name='IpPort'>49730</Data><Data Name='ShareName'>\\AMZNFSXCYDKLDZZ\share</Data>
<Data Name='ShareLocalPath'>\??\D:\share</Data><Data Name='AccessMask'>0x1</Data><Data
 Name='AccessList'>%%4416
    </Data></EventData></Event>
```

事件 ID 5145在文件共享级别拒绝访问时记录。下面的示例演示了访问权限 ShareName “demoshare01” 被拒绝。

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>5145</EventID><Version>0</Version><Level>0</Level>
<Task>12811</Task><Opcode>0</Opcode><Keywords>0x8010000000000000</Keywords>
<TimeCreated SystemTime='2021-05-19T22:30:40.485188700Z'/><EventRecordID>282939</
EventRecordID>
<Correlation/><Execution ProcessID='4' ThreadID='344'/><Channel>Security</Channel>
<Computer>amznfsxtmn9autz.example.com</Computer><Security/></System><EventData>
<Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-
1113</Data><Data Name='SubjectUserName'>Admin</Data><Data
 Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x95b3fb7</Data><Data Name='ObjectType'>File</Data>
<Data Name='IpAddress'>172.31.7.112</Data><Data Name='IpPort'>59979</Data>
<Data Name='ShareName'>\\AMZNFSXDPNTE0DC\demoshare01</Data><Data Name='ShareLocalPath'>\??
\D:\demoshare01</Data>
<Data Name='RelativeTargetName'>Desktop.ini</Data><Data Name='AccessMask'>0x120089</Data>
<Data Name='AccessList'>%%1538 %%1541 %%4416 %%4419 %%4423 </Data><Data
 Name='AccessReason'>%%1538:
%%1804 %%1541: %%1805 %%4416: %%1805 %%4419: %%1805 %%4423: %%1805 </Data></EventData></
Event>
```

如果您使用 CloudWatch 记录 Insights 要搜索日志数据，您可以对事件字段运行查询，如以下示例所示：

- 查询特定事件 ID：

```
fields @message
   | filter @message like /4660/
```

- 要查询与特定文件名匹配的所有事件：

```
fields @message
   | filter @message like /event.txt/
```

有关 CloudWatch Logs Insights 查询语言，请参阅使用 分析日志数据 CloudWatch 日志见解，在亚马逊 CloudWatch 日志用户指南.

用户会话和打开的文件

您可以使用共享文件夹工具监控已连接的用户会话并在 FSx for Windows File Server 文件系统上打开文件。“共享文件夹” 工具提供了一个中央位置来监视谁连接到文件系统，以及哪些文件被打开和由谁打开。您可以使用此工具执行以下操作：

- 恢复对锁定文件的访问权限。
- 断开用户会话连接，这将关闭该用户打开的所有文件。

您可以使用 Windows 原生共享文件夹 GUI 工具和 Amazon FSx CLI 进行远程管理 PowerShell 管理用户会话并在 FSx for Windows File Server 文件系统上打开文件。

使用 GUI 管理用户和会话

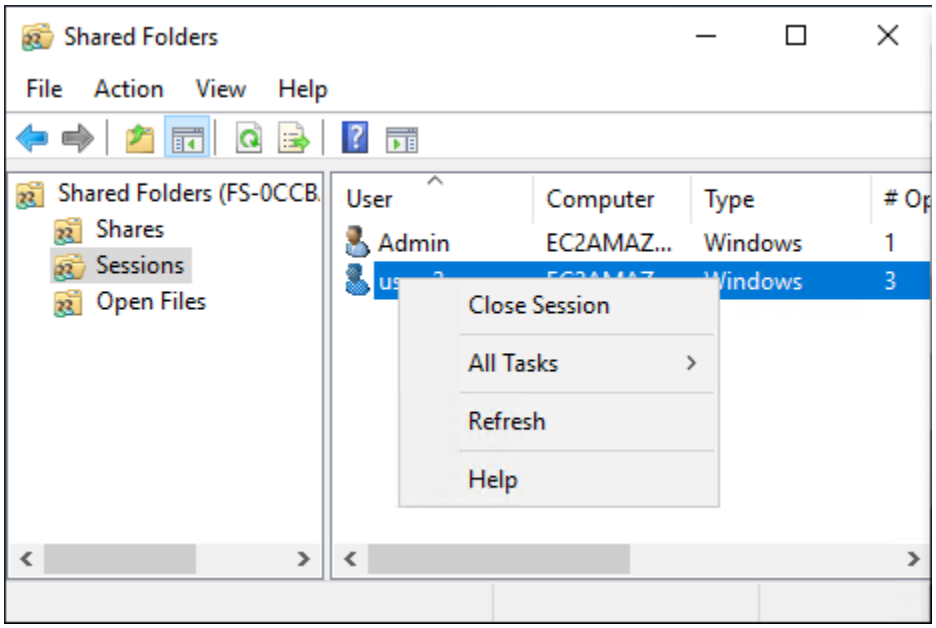
以下过程详细说明了如何在 Amazon FSx 文件系统上管理用户会话和打开文件。

启动共享文件夹工具

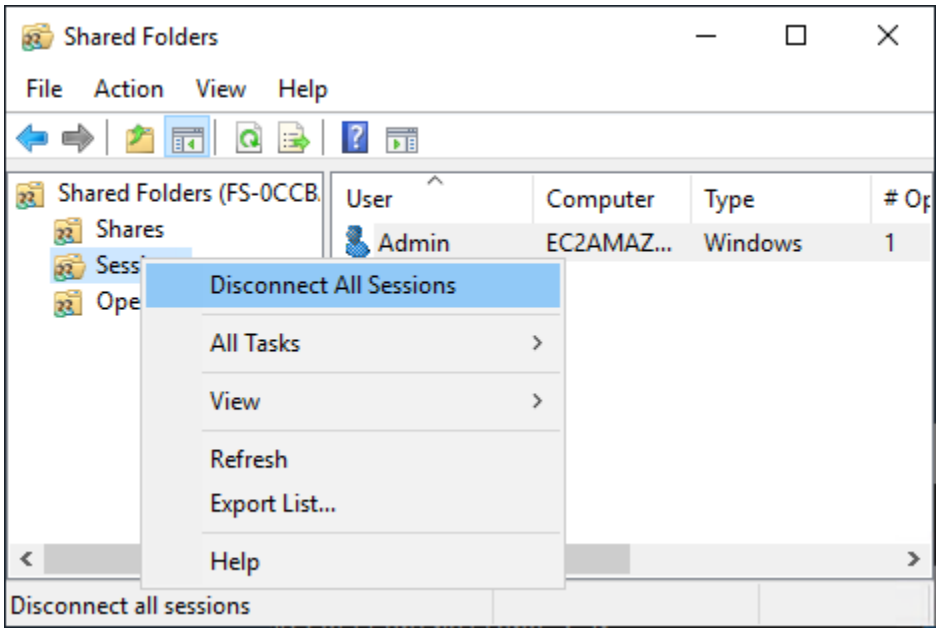
1. 启动您的 Amazon EC2 实例，并将其连接到您的 Amazon FSx 文件系统所加入的微软活动目录。为此，请从Amazon Directory Service管理指南：
   - 无缝加入 Windows EC2 实例
   - 手动加入 Windows 实例
2. 以文件系统管理员组成员身份Connect 您的实例。InAmazon托管微软活动目录，这个组被称为Amazon委派的 FSx 管理员。在自我管理的 Microsoft Active Directory 中，此组称为域管理员或您在创建过程中提供的管理员组的自定义名称。有关更多信息，请参阅适用于 Windows 实例的 Amazon EC2 用户指南中的连接您的 Windows 实例。
3. 打开启动菜单并运行fsmgmt.msc使用`Run As Administrator`. 执行此操作将打开共享文件夹 GUI 工具。
4. 适用于操作，选择Connect 另一台计算机.
5. 适用于另一台计算机，例如，输入 Amazon FSx 文件系统的 DNS 名称`fs-`*`012345678901234567`*`.`*`ad-domain`*`.com`.
6. 选择 OK（确定）。然后，Amazon FSx 文件系统的条目将出现在共享文件夹工具的列表中。

管理用户会话

在 “共享文件夹” 工具中，选择会话查看连接到 FSx for Windows File Server 文件系统的所有用户会话。如果用户或应用程序正在访问您的 Amazon FSx 文件系统上的文件共享，此管理单元将向您显示其会话。您可以通过以下方式断开会话的连接 (右键单击) 菜单，然后选择关闭会话.

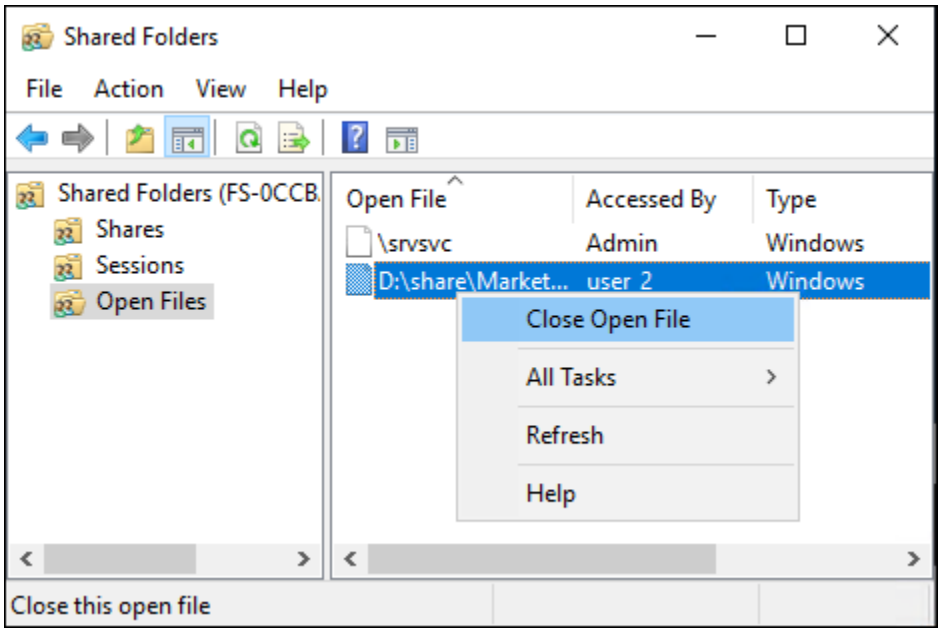


要断开所有打开的会话的连接，请打开 context (右键单击) 菜单会话，选择断开所有会话连接，并确认你的行动。

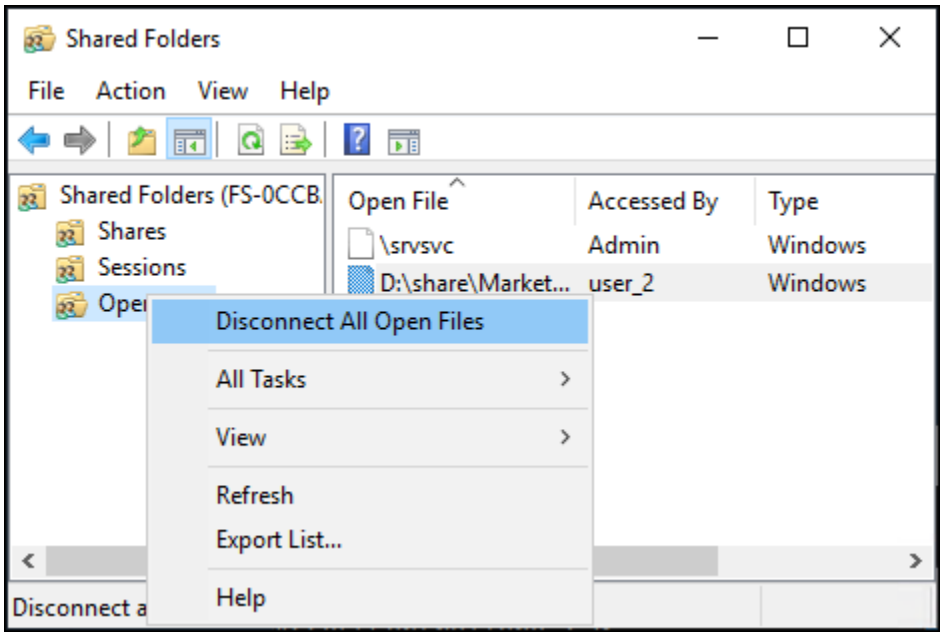


管理打开的文件

在 “共享文件夹” 工具中，选择Open Files（打开的文件）查看系统上当前处于打开状态的所有文件。该视图还显示哪些用户打开了文件或文件夹。此信息有助于追踪其他用户无法打开某些文件的原因。您可以关闭任何用户打开的文件，只需在列表中打开该文件条目的上下文 (右键单击) 菜单，然后选择Close（关闭）.



要断开文件系统中所有打开的文件，请使用上下文 (右键单击) 菜单Open Files（打开的文件）然后选择断开所有打开的文件，并确认你的行动。



使用 PowerShell 管理用户会话和打开文件

您可以使用 Amazon FSx CLI 管理活动用户会话和打开文件系统上的文件，以便在上进行远程管理 PowerShell. 要了解如何使用此 CLI，请参阅开始使用 Amazon FSx CLI 进行远程管理 PowerShell (p. 80).

以下是可用于用户会话和打开文件管理的命令。

命令	描述
Get-FSxSmbSession	检索有关当前在文件系统和关联客户端之间建立的服务器消息块 (SMB) 会话的信息。
Close-FSxSmbSession	结束 SMB 会话。
Get-FSxSmbOpenFile	检索有关为连接到文件系统的客户端打开的文件的信息。
Close-FSxSmbOpenFile	关闭为 SMB 服务器的其中一个客户端打开的文件。

每个命令的联机帮助提供了所有命令选项的参考。要访问此帮助，请运行命令-?，例如Get-FSxSmbSession -?.

重复数据删除

大型数据集通常具有冗余数据，这增加了数据存储成本。例如，对于用户文件共享，多个用户可以存储同一文件的多个副本或版本。对于软件开发份额，许多二进制文件在构建之间保持不变。

您可以通过为文件系统启用重复数据删除功能来降低数据存储成本。重复数据删除通过仅存储数据集的重复部分一次来减少或消除冗余数据。默认情况下，当您使用重复数据删除时，会启用数据压缩，通过在重复数据删除后压缩数据，进一步减少数据存储量。重复数据消除作为后台进程运行，持续自动扫描和优化您的文件系统，并且对您的用户和连接的客户端是透明的。

使用重复数据删除可以节省多少存储空间取决于数据集的性质，包括跨文件存在多少重复。一般用途文件共享的典型节约率平均为 50-60%。在份额范围内，节省的费用从用户文档的 30-50% 到软件开发数据集的 70-80% 不等。您可以使用`Measure-FSxDedupFileMetadata`命令如下所述。

您还可以自定义重复数据删除以满足特定的存储需求。例如，您可以将重复数据消除配置为仅在某些文件类型上运行，也可以创建自定义作业时间表。由于重复数据消除作业会消耗文件服务器资源，因此我们建议使用`Get-FSxDedupStatus`命令如下所述。

有关重复数据删除的更多信息，请参阅 Microsoft了解重复数据删除文档中）。

> Note
>
> 如果您在成功运行重复数据消除作业时遇到问题，请参阅重复数据删除故障排除 (p. 201).
>
> Warning
>
> 不建议使用重复数据删除功能运行某些 Robocopy 命令，因为这些命令可能会影响区块存储的数据完整性。有关更多信息，请参阅 Microsoft重复数据删除互操作性文档中）。

启用重复数据删除

您可以使用 Amazon FSx for Windows File Server 文件共享启用重复数据删除`Enable-FSxDedup`命令，如下所示。

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FSxRemoteAdmin -ScriptBlock {Enable-FsxDedup }
```

启用重复数据删除后，将创建默认时间表和配置。您可以使用以下命令创建、修改和删除时间表和配置。

请注意，创建新的自定义重复数据消除作业时间表不会覆盖或删除现有的默认计划。在创建自定义重复数据消除作业之前，如果不需要默认作业，则可能需要禁用它。

您可以使用`Disable-FSxDedup`命令在文件系统上完全禁用重复数据消除。

Note

当您增加文件系统的存储容量时，Amazon FSx 会在将数据从旧磁盘迁移到新的更大磁盘的存储优化过程中取消现有的重复数据消除任务。在此期间，OptimizedFilesSavingsRate值为 0。存储容量增加优化任务完成后，Amazon FSx 将恢复重复数据删除。有关增加存储容量和优化存储的更多信息，请参阅管理存储容量 (p. 112).

制定重复数据消除计划

尽管默认计划在大多数情况下都能正常工作，但您可以使用New-FsxDedupSchedule命令，如下所示。重复数据删除计划使用 UTC 时间。

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FSxRemoteAdmin -ScriptBlock {
New-FSxDedupSchedule -Name "CustomOptimization" -Type Optimization -Days Mon,Wed,Sat -Start
 08:00 -DurationHours 7
}
```

完成后，此命令将创建一个名为的计划CustomOptimization在星期一、星期三和星期六运行，作业在每天上午 8:00 (UTC) 启动，最长持续时间为 7 小时，如果作业仍在运行，则在此之后，作业将停止。

修改重复数据消除计划

您可以使用修改现有的重复数据删除计划Set-FsxDedupSchedule命令，如下所示。

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FSxRemoteAdmin -ScriptBlock {
Set-FSxDedupSchedule -Name "CustomOptimization" -Type Optimization -Days Mon,Tues,Wed,Sat -
Start 09:00 -DurationHours 9
}
```

此命令修改现有的CustomOptimization计划在星期一至星期三和星期六的某天运行，在每天上午 9:00 (UTC) 启动作业，最长持续时间为 9 小时，如果作业仍在运行，则在此之后将停止作业。

要修改优化前的最短文件保存期限设置，请使用Set-FSxDedupConfiguration命令。

查看节省的空间量

要查看通过运行重复数据消除节省的磁盘空间量，请使用Get-FSxDedupStatus命令，如下所示。

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FsxRemoteAdmin -ScriptBlock {
Get-FSxDedupStatus } | select
 OptimizedFilesCount,OptimizedFilesSize,SavedSpace,OptimizedFilesSavingsRate

OptimizedFilesCount OptimizedFilesSize SavedSpace OptimizedFilesSavingsRate
------------------- ------------------ ---------- -------------------------
              12587           31163594   25944826                        83
```

Note

以下参数的命令响应中显示的值不可靠，您不应使用这些值：容量， FreeSpace、 UsedSpace、 UnoptimizedSize, 和 SavingsRate.

管理重复数据删除

您可以使用 Amazon FSx CLI 管理文件系统上的重复数据消除，以便在上进行远程管理 PowerShell. 要了解如何使用此 CLI，请参阅开始使用 Amazon FSx CLI 进行远程管理 PowerShell (p. 80).

以下是可用于重复数据删除的命令。

重复数据删除命令	描述
Enable-FSxDedup	在文件共享上启用重复数据消除。启用重复数据删除后，默认启用重复数据消除后的数据压缩。
Disable-FSxDedup	在文件共享上禁用重复数据消除。
Get-FSxDedupConfiguration	检索重复数据消除配置信息，包括用于优化的最小文件大小和期限、压缩设置以及排除的文件类型和文件夹。
Set-FSxDedupConfiguration	更改重复数据消除配置设置，包括最小文件大小和优化期限、压缩设置以及排除的文件类型和文件夹。
Get-FSxDedupStatus	检索重复数据消除状态，并包含只读属性，这些属性描述了文件系统上的优化节省和状态、时间以及文件系统上最后作业的完成状态。
Get-FSxDedupMetadata	检索重复数据消除优化元数据。
Update-FSxDedupStatus	计算和检索更新的重复数据消除节省信息。
Measure-FSxDedupFileMetadata	测量并检索在删除一组文件夹后可以在文件系统上回收的潜在存储空间。文件通常包含在其他文件夹之间共享的区块，重复数据消除引擎会计算出哪些区块是唯一的，哪些区块将被删除。
Get-FSxDedupSchedule	检索当前定义的重复数据消除计划。
New-FSxDedupSchedule	创建和自定义重复数据消除计划。
Set-FSxDedupSchedule	更改现有重复数据消除计划的配置设置。
Remove-FSxDedupSchedule	删除重复数据删除计划。
Get-FSxDedupJob	获取当前正在运行或排队的所有重复数据消除作业的状态和信息。
Stop-FSxDedupJob	取消一个或多个指定的重复数据消除作业。

每个命令的联机帮助提供了所有命令选项的参考。要访问此帮助，请运行命令-?，例如Enable-FSxDedup -?.

存储配额

您可以在文件系统上配置用户存储配额，以限制用户可以使用的数据存储量。设置配额后，您可以跟踪配额状态以监控使用情况并查看用户何时超过配额。

您还可以通过阻止达到配额的用户写入存储空间来强制执行配额。强制执行配额时，超出配额的用户会收到“磁盘空间不足”错误消息。

您可以为配额设置设置以下阈值：

- 警告-用于跟踪用户或组是否正在接近其配额限制，仅与跟踪相关。
- Limit-用户或组的存储配额限制。

您可以配置应用于访问文件系统的新用户的默认配额，以及应用于特定用户或组的默认配额。您还可以查看每个用户或组正在消耗多少存储空间以及他们是否超过配额的报告。

用户级别的存储消耗是根据文件所有权进行跟踪的。存储消耗量是使用逻辑文件大小计算的，而不是文件占用的实际物理存储空间。在将数据写入文件时跟踪用户存储配额。

更新多个用户的配额需要为每个用户运行一次 update 命令，或者将这些用户组织到一个组中并更新该组的配额。

管理用户存储配额

您可以使用 Amazon FSx CLI 管理文件系统上的用户存储配额，以便在上进行远程管理 PowerShell. 要了解如何使用此 CLI，请参阅开始使用 Amazon FSx CLI 进行远程管理 PowerShell (p. 80).

以下是可以用来管理用户存储配额的命令。

用户存储配额命令	描述
Enable-FSxUserQuotas	开始跟踪或强制实施用户存储配额，或两者兼而有之。
Disable-FSxUserQuotas	停止对用户存储配额的跟踪和强制执行。
Get-FSxUserQuotaSettings	检索文件系统的当前用户存储配额设置。
Get-FSxUserQuotaEntries	检索文件系统上各个用户和组的当前用户存储配额条目。
Set-FSxUserQuotas	为单个用户或组设置用户存储配额。以字节为单位指定配额值。

每个命令的联机帮助提供了所有命令选项的参考。要访问此帮助，请运行命令-?，例如Enable-FSxUserQuotas -?.

卷影副本

使用一组自定义 PowerShell 命令中，您可以在 FSx fFSx for Windows File Server 系统上管理卷影副本的所有方面。

主题

设置卷影副本存储

卷影副本占用了创建卷影副本的同一文件系统上的存储空间。配置卷影副本存储时，您可以使用`Set-FsxShadowStorage`自定义 PowerShell 命令。您可以使用指定卷影副本可以增长到的最大大小`-Maxsize`或者`-Default`命令选项。

使用`-Maxsize`，您可以定义影子副本存储，如下所示：

- 以字节为单位：`Set-FsxShadowStorage -Maxsize 2500000000`
- 以千字节、兆字节、千兆字节或其他单位为单位：`Set-FsxShadowStorage -Maxsize (2500MB)`要么`Set-FsxShadowStorage -Maxsize (2.5GB)`
- 占总存储空间的百分比：`Set-FsxShadowStorage -Maxsize "20%"`
- 如无界限：`Set-FsxShadowStorage -Maxsize "UNBOUNDED"`

使用`-Default`要将卷影存储设置为最多使用 10% 的文件系统: `Set-FsxShadowStorage -Default`. 要了解有关使用默认选项的更多信息，请参阅。使用默认设置设置卷影副本 (p. 77).

设置 FSx for Windows File Server 文件系统上的卷影副本存储量

1. 以文件系统管理员组成员的身份连接到与您的文件系统具有网络Connect 的计算实例。InAmazon Managed Microsoft AD，那组是Amazon委派的 FSx 管理员. 在你自我管理的 Microsoft AD 中，该群组是Domain Admins或在创建您的文件系统时为管理指定的自定义组。有关更多信息，请参阅适用于 Windows 实例的 Amazon EC2 用户指南中的连接您的 Windows 实例。
2. 打开窗户 PowerShell ” 窗口。
3. 使用以下命令开启一个遥控器 PowerShell 在您的 Amazon Fsx 文件系统上的会话。Replace*FSxFileSystem-Remote-PowerShell-Endpoint*使用 Windows 遥控器 PowerShell 要管理的文件系统的端点。您可以找到 Windows 遥控器 PowerShell 终端节点位于 Amazon FSx 控制台中的网络与安全文件系统详细信息窗口的部分，或者在`DescribeFileSystem`API 操作。

```
PS C:\Users\delegateadmin> enter-pssession -computername FSxFileSystem-Remote-
PowerShell-Endpoint -configurationname fsxremoteadmin
```

4. 使用以下命令验证未在文件系统上配置卷影副本存储。

```
[fs-1234567890abcef12]: PS>Get-FsxShadowStorage
No Fsx Shadow Storage Configured
```

5. 使用将卷影存储量设置为卷的 10%`-Default`选项。

```
[fs-1234567890abcef12]: PS>Set-FsxShadowStorage -Default
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace     MaxSpace
-------------- ---------     --------
             0         0  32530536858
```

查看您的卷影副本存储

您可以使用以下命令查看文件系统上卷影副本当前占用的存储量`Get-FsxShadowStorage`遥控器中的命令 PowerShell 您的文件系统上的会话。有关启动遥控器的说明 PowerShell 您的文件系统上的会话，请参阅开始使用 Amazon FSx CLI 进行远程管理 PowerShell (p. 80).

```
[fs-1234567890abcef12]: PS>Get-FsxShadowStorage
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace     MaxSpace
-------------- ---------     --------
    1619869696  14417920  32530536858
```

输出显示了卷影存储配置，如下所示：

- `AllocatedSpace`— 文件系统上当前分配给卷影副本的存储量（以字节为单位）。最初，此值为 0。

- `UsedSpace`— 卷影副本当前使用的存储量（以字节为单位）。最初，此值为 0。
- `MaxSpace`— 影子存储可增长到的最大存储量（以字节为单位）。这是您为设置的值卷影副本存储 (p. 107)使用`Set-FsxShadowStorage`命令。

当`UsedSpace`数量达到配置的最大卷影副本存储量 (`MaxSpace`），则您创建的下一个卷影副本将替换最旧的卷影副本。如果您不想丢失最旧的卷影副本，请监视卷影副本存储，以确保有足够的存储空间来存储新的卷影副本。如果您需要更多空间，您可以删除现有的卷影副本 (p. 111)或者增加最大金额卷影副本存储 (p. 107).

Note

自动或手动创建卷影副本时，它们会将您配置的卷影副本存储量用作存储限制。卷影副本不使用显示的可用存储空间 CloudWatch `FreeStorageCapacity`指标作为存储限制。

删除卷影副本存储、计划和所有卷影副本

您可以删除卷影副本配置，包括所有现有的卷影副本，以及卷影复制计划。同时，您可以释放文件系统上的卷影副本存储。

为此，请输入`Remove-FsxShadowStorage`遥控器中的命令 PowerShell您的文件系统上的会话。有关启动遥控器的说明 PowerShell 您的文件系统上的会话，请参阅开始使用 Amazon FSx CLI 进行远程管理 PowerShell (p. 80).

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowStorage

Confirm
Are you sure you want to perform this action?
Performing the operation "Remove-FsxShadowStorage" on target "Removing all Shadow Copies,
 Shadow Copy Schedule, and Shadow Storage".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y": Y
FSx Shadow Storage Configuration
Removing Shadow Copy Schedule
Removing Shadow Copies
All shadow copies removed.
Removing Shadow Storage
Shadow Storage removed successfully.
```

创建自定义卷影复制时间表

卷影复制计划使用 Microsoft Windows 中的计划任务触发器来指定何时自动制作卷影副本。卷影拷贝计划可以有多个触发器，这为您提供了很大的时间安排灵活性。一次只能有一个卷影复制时间表存在。在创建卷影复制时间表之前，您必须先设置卷影副本存储 (p. 107).

当你运行`Set-FsxShadowCopySchedule`命令时，将覆盖任何现有的卷影复制时间表。如果您的客户端计算机处于 UTC 时区，则还可以使用 Windows 时区和`-TimezoneId`选项。有关 Windows 时区列表，请参阅微软的默认时区文档或在 Windows 命令提示符处运行以下命令：`tzutil /l`. 要了解有关 Windows 任务触发器的更多信息，请参阅。任务触发器在微软 Windows 开发人员中心文档中。

您也可以使用`-Default`选项以快速设置默认的卷影复制时间表。要了解更多信息，请参阅 使用默认设置设置卷影副本 (p. 77)。

创建自定义卷影复制时间表

1. 创建一组 Windows 计划任务触发器，以定义在卷影复制计划中创建卷影副本的时间。使用`new-scheduledTaskTrigger`命令在 PowerShell在本地计算机上设置多个触发器。

   以下示例创建了一个自定义卷影复制计划，该计划在世界标准时间每周一至周五的上午 6:00 和下午 6:00 进行卷影复制。默认情况下，时间采用 UTC，除非您在创建的 Windows 计划任务触发器中指定时区。

```
PS C:\Users\delegateadmin> $trigger1 = new-scheduledTaskTrigger -weekly -DaysOfWeek
 Monday,Tuesday,Wednesday,Thursday,Friday -at 06:00
PS C:\Users\delegateadmin> $trigger2 = new-scheduledTaskTrigger -weekly -DaysOfWeek
 Monday,Tuesday,Wednesday,Thursday,Friday -at 18:00
```

2. 使用invoke-command运行scriptblock命令。这样做会编写一个脚本，该脚本使用new-scheduledTaskTrigger您刚刚创建的值。Replace*FSxFileSystem-Remote-PowerShell-Endpoint*使用 Windows 遥控器 PowerShell 要管理的文件系统的端点。您可以找到 Windows 遥控器 PowerShell 终端节点位于 Amazon FSx 控制台中的网络与安全文件系统详细信息窗口的部分，或者在DescribeFileSystemAPI 操作。

```
PS C:\Users\delegateadmin> invoke-command -ComputerName FSxFileSystem-Remote-
PowerShell-Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {
```

3. 在以下位置输入以下行>>提示使用设置卷影复制时间表set-fsxshadowcopyschedule命令。

```
>> set-fsxshadowcopyschedule -scheduledtasktriggers $Using:trigger1,$Using:trigger2 -
Confirm:$false }
```

响应将显示您在文件系统上配置的卷影复制计划。

```
FSx Shadow Copy Schedule


Start Time:     : 2019-07-16T06:00:00+00:00
Days of Week    : Monday,Tuesday,Wednesday,Thursday,Friday
WeeksInterval   : 1
PSComputerName : fs-0123456789abcdef1
RunspaceId      : 12345678-90ab-cdef-1234-567890abcde1

Start Time:     : 2019-07-16T18:00:00+00:00
Days of Week    : Monday,Tuesday,Wednesday,Thursday,Friday
WeeksInterval   : 1
PSComputerName : fs-0123456789abcdef1
RunspaceId      : 12345678-90ab-cdef-1234-567890abcdef
```

查看您的卷影复制计划

要查看文件系统上现有的卷影复制计划，请在远程 PowerShell 您的文件系统上的会话。有关启动遥控器的说明 PowerShell 您的文件系统上的会话，请参阅开始使用 Amazon FSx CLI 进行远程管理 PowerShell (p. 80).

```
[fs-0123456789abcdef1]PS> Get-FsxShadowCopySchedule
FSx Shadow Copy Schedule

Start Time                Days of week                              WeeksInterval
----------                ------------                              -------------
2019-07-16T07:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday              1
2019-07-16T12:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday              1
```

删除影子复制时间表

要删除文件系统上现有的卷影复制计划，请在远程 PowerShell 您的文件系统上的会话。有关启动遥控器的说明 PowerShell 您的文件系统上的会话，请参阅开始使用 Amazon FSx CLI 进行远程管理 PowerShell (p. 80).

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowCopySchedule

Confirm
Are you sure you want to perform this action?
Performing the operation "Remove-FsxShadowCopySchedule" on target "Removing FSx Shadow Copy
 Schedule".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y"): Y
[fs-0123456789abcdef1]PS>
```

创建影子副本

要手动创建卷影副本，请在远程 PowerShell 您的文件系统上的会话。有关启动遥控器的说明 PowerShell 您的文件系统上的会话，请参阅开始使用 Amazon FSx CLI 进行远程管理 PowerShell (p. 80).

```
[fs-0123456789abcdef1]PS>New-FsxShadowCopy

Shadow Copy {ABCDEF12-3456-7890-ABCD-EF1234567890} taken successfully
```

查看现有的卷影副本

要查看文件系统上现有的卷影副本集，请在远程 PowerShell 您的文件系统上的会话。有关启动遥控器的说明 PowerShell 您的文件系统上的会话，请参阅开始使用 Amazon FSx CLI 进行远程管理 PowerShell (p. 80).

```
[fs-0123456789abcdef1]PS>Get-FsxShadowCopies
FSx Shadow Copies: 2 total

Shadow Copy ID                          Creation Time
--------------                          -----------------
{ABCDEF12-3456-7890-ABCD-EF1234567890} 6/17/2019 7:11:09 AM
{FEDCBA21-6543-0987-0987-EF3214567892} 6/19/2019 11:24:19 AM
```

删除影子副本

您可以使用删除您的文件系统上的一个或多个现有的卷影副本。`Remove-FsxShadowCopies`遥控器中的命令 PowerShell 您的文件系统上的会话。有关启动遥控器的说明 PowerShell 您的文件系统上的会话，请参阅开始使用 Amazon FSx CLI 进行远程管理 PowerShell (p. 80).

使用以下所需选项之一指定要删除的卷影副本：

- `-Oldest`删除最早的卷影副本
- `-All`删除所有现有的卷影副本
- `-ShadowCopyId`按 ID 删除特定的卷影副本。

在命令中只能使用一个选项。如果未指定要删除的卷影副本、指定了多个卷影副本 ID 或者指定了无效的卷影副本 ID，则会发生错误。

要删除文件系统上最旧的卷影副本，请在远程 PowerShell 您的文件系统上的会话。

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowCopies -Oldest
Confirm
Are you sure you want to perform this action?
Performing the operation "Remove-FSxShadowCopies" on target "Removing oldest shadow copy".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y": Y
Shadow Copy {ABCDEF12-3456-7890-ABCD-EF1234567890} deleted
```

要删除文件系统上的特定卷影副本，请在远程 PowerShell 您的文件系统上的会话。

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowCopies -ShadowCopyId "{ABCDEF12-3456-7890-ABCD-EF1234567890}"
Are you sure you want to perform this action?
Performing the operation "Remove-FSxShadowCopies" on target "Removing shadow copy
 {ABCDEF12-3456-7890-ABCD-EF1234567890}".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y":>Y
Shadow Copy \\AMZNFSXABCDE123\root\cimv2:Wind32_ShadowCopy.ID{ABCDEF12-3456-7890-ABCD-EF1234567890}".ID deleted.
```

管理传输中加密

你可以使用一套自定义 PowerShell 控制在 FSx for Windows File Server 文件系统和客户端之间传输中数据加密。您可以将文件系统访问权限限制为仅支持 SMB 加密的客户端，以便 data-in-transit 始终加密。启用强制以加密 data-in-transit，则从不支持 SMB 3.0 加密的客户端访问文件系统的用户将无法访问已启用加密的文件共享。

您还可以控制的加密 data-in-transit 在文件共享级别，而不是文件服务器级别。如果要对某些包含敏感数据的文件共享强制执行传输中的加密，并允许所有用户访问其他文件共享，则可以使用文件共享级别的加密控制在同一个文件系统上混合使用加密和未加密的文件共享。服务器范围的加密优先于共享级加密。如果启用了全局加密，则无法有选择地禁用某些共享的加密。

您可以使用 Amazon FSx CLI 管理文件系统上的用户传输中加密，以便在上进行远程管理 PowerShell. 要了解如何使用此 CLI，请参阅开始使用 Amazon FSx CLI 进行远程管理 PowerShell (p. 80).

以下是可用于在文件系统上管理用户传输中加密的命令。

传输命令中加密	描述
Get-FSxSmbServerConfiguration	检索服务器消息块 (SMB) 服务器配置。
Set-FSxSmbServerConfiguration	此命令有两个选项可用于配置传输中加密： • `-EncryptData $True\|$False`— 启用或关闭传输中数据加密。 • `-RejectUnencryptedAccess $True\|$False`— 允许或禁止访问不支持加密的客户端。

每个命令的联机帮助提供了所有命令选项的参考。要访问此帮助，请运行命令-?，例如Get-FSxSmbServerConfiguration -?.

管理存储容量

由于需要额外存储容量，可以增加 FSx for Windows File Server 文件系统上配置的存储容量。您可以使用亚马逊 FSx 控制台、亚马逊 FSx API 或Amazon Command Line Interface(Amazon CLI)。

Note

您只能增加文件系统的存储容量；不能减少存储容量。

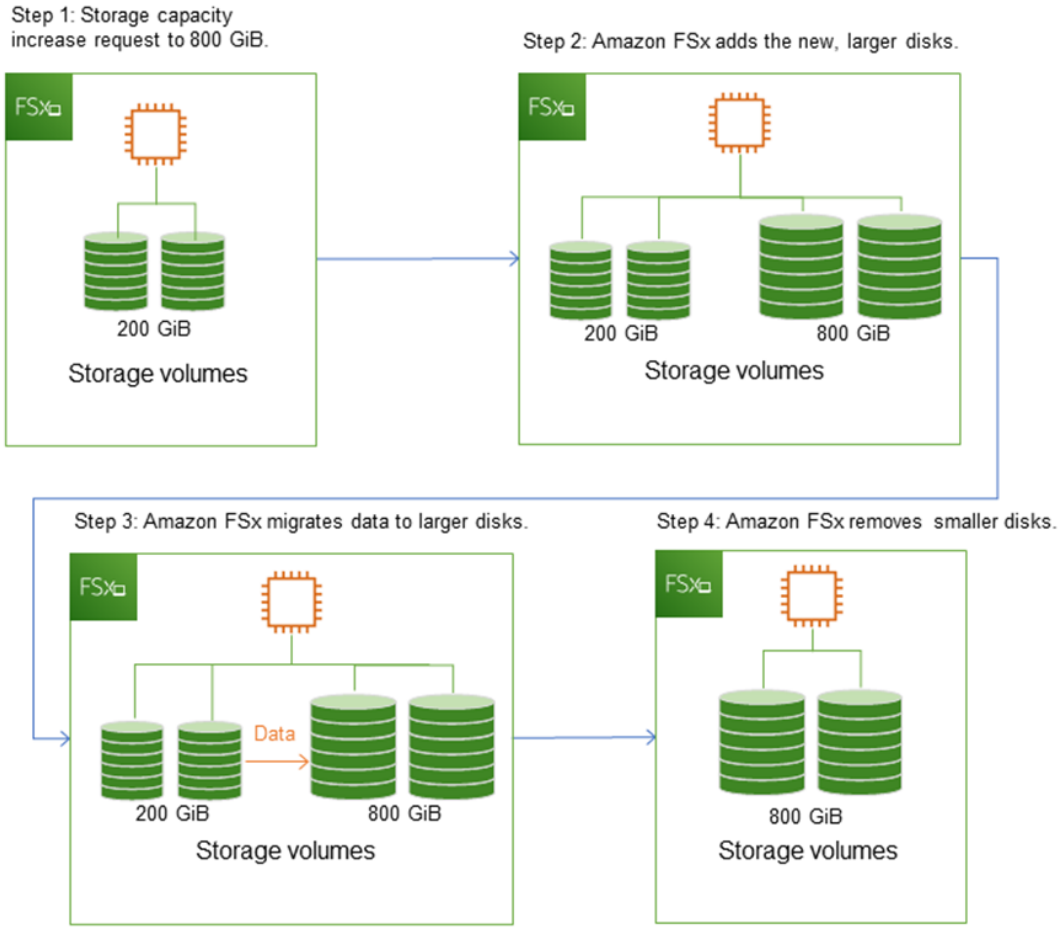
Note

增加存储容量不适用于 2019 年 6 月 23 日之前创建的文件系统或从属于 2019 年 6 月 23 日之前创建的文件系统的备份还原的文件系统。

当您在后台增加 Amazon FSx 文件系统的存储容量时，Amazon FSx 会向您的文件系统添加一组新的、更大的磁盘。在几分钟内可供使用新容量。当新的存储容量可用时，您只需为新的存储容量付费。

Amazon FSx 在后台运行存储优化流程，以透明方式将数据从旧磁盘迁移到新的更大的磁盘。对于大多数文件系统，存储优化需要几个小时至几天，对工作负载性能的明显影响最小。

下图显示了 Amazon FSx 在增加文件系统存储容量时使用的四个主要步骤。



您可以随时使用 Amazon FSx 控制台、CLI 和 API 跟踪存储优化进度。有关更多信息，请参阅 监控存储容量的增加 (p. 115)。

主题

- 增加存储容量时需要知道的重要点 (p. 114)
- 何时增加存储容量 (p. 114)
- 存储容量增加和文件系统性能 (p. 114)
- 如何增加存储容量 (p. 114)
- 监控存储容量的增加 (p. 115)
- 动态增加 FSx for Windows File Server 文件系统的存储容量 (p. 118)

增加存储容量时需要知道的重要点

以下是增加存储容量时需要考虑的几个重要事项：

- 仅增加— 您只能增加文件系统的存储容量；不能减少存储容量。
- 最小增加— 每次增加存储容量必须至少为文件系统当前存储容量的 10%，最大允许值为 65,536 GiB。
- 最小吞吐量容量— 要增加存储容量，文件系统的最低吞吐容量必须为 16 MB/s。这是因为存储优化步骤是吞吐量密集型的过程。
- 增长之间的时间— 在请求最后一次增加后 6 个小时或存储优化过程完成之前，无法在文件系统上进一步增加存储容量，以较长的时间为准。存储优化可能需要几个小时到几天才能完成。为了最大限度地缩短完成存储优化所需的时间，我们建议在增加存储容量之前增加文件系统的吞吐量容量（在存储扩展完成后可以缩小吞吐容量），并在流量最少的情况下增加存储容量文件系统。

何时增加存储容量

当文件系统的可用存储容量不足时，请增加文件系统的存储容量。使用`FreeStorageCapacity` CloudWatch 用于监控文件系统上可用的可用存储空间量的指标。您可以创建亚马逊 CloudWatch 针对此指标发出警报，并在其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 CloudWatch 监控 (p. 134)。

当可用存储容量低于指定的阈值时，您可以自动增加文件系统的存储容量。使用Amazon-开发自定义 Amazon CloudFormation模板来部署实施自动化解决方案所需的所有组件。有关更多信息，请参阅 动态增加存储容量 (p. 118)。

存储容量增加和文件系统性能

大多数工作负载对性能的影响最小，而 Amazon FSx 将在新存储容量可用后在后台运行存储优化过程。具有大量活动数据集的写入密集型应用程序可能会暂时降低多达一半的写入性能。对于这些情况，您可以首先增加文件系统的吞吐量容量以前增加存储容量。这使您能够继续提供相同级别的吞吐量，以满足应用程序的性能需求。有关更多信息，请参阅 管理吞吐量容量 (p. 122)。

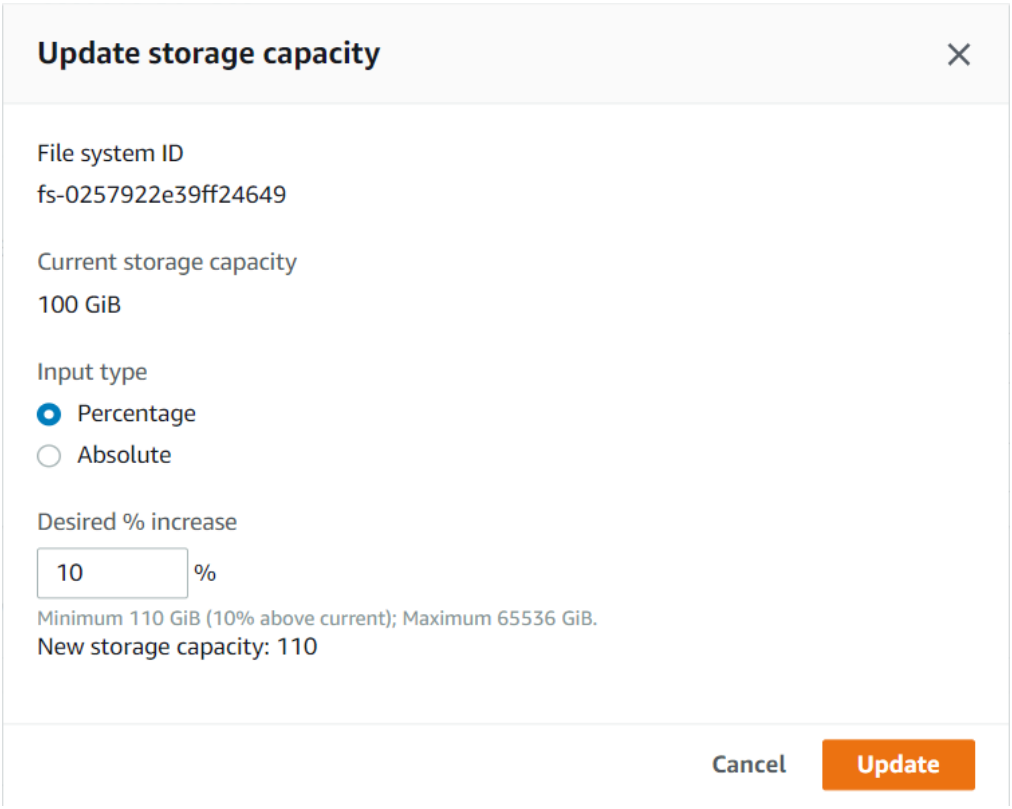
如何增加存储容量

您可以使用 Amazon FSx 控制台来增加文件系统的存储容量Amazon CLI，或者亚马逊 FSx API。

增加文件系统的存储容量（控制台）

1. 在打开 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存储容量的 Windows 文件系统。
3. 适用于操作，选择更新存储. 或者，在摘要面板中，选择更新旁边的文件系统存储容量.

   这些区域有：更新存储容量此时显示窗口。



4. 适用于输入类型，选择百分比以与当前值相比的百分比变化输入新存储容量，或者选择绝对以 GiB 为单位输入新值。
5. 输入所需存储容量.

   Note

   所需容量值必须至少比当前值大 10%，最大值为 65,536 GiB。
6. 选择更新以启动存储容量更新。
7. 您可以在文件系统详情页面，在更新选项卡。

增加文件系统的存储容量 (CLI)

要增加 FSx for Windows File Server 文件系统的存储容量，请使用Amazon CLI命令更新文件系统. 设置以下参数：

- `--file-system-id`到您要更新的文件系统的 ID。
- `--storage-capacity`至少比当前值大 10% 的值。

您可以使用Amazon CLI命令描述文件系统. 查找`administrative-actions`在输出中。

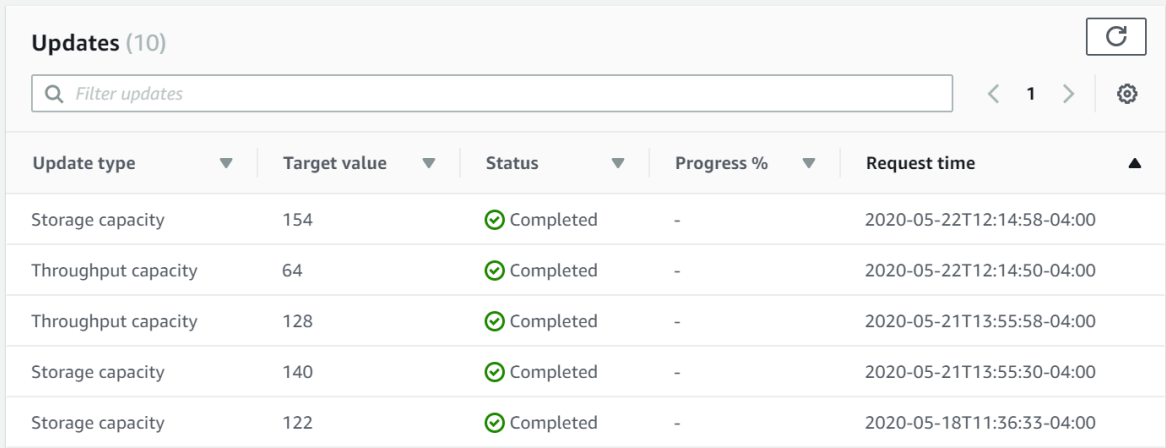
有关更多信息，请参阅 。管理操作.

监控存储容量的增加

您可以使用 Amazon FSx 控制台、API 或Amazon CLI.

在控制台中监控增加

在更新在 “” 选项卡中文件系统细节窗口中，您可以查看每种更新类型的 10 个最近更新。



对于存储容量更新，您可以查看以下信息。

更新类型

支持的类型包括存储容量、存储优化, 和吞吐量容量.

Target value (目标值)

将文件系统的存储容量更新为的所需值。

状态

更新的当前状态。对于存储容量更新，可能的值如下所示：

- Pending— 亚马逊 FSx 已收到更新请求，但尚未开始处理。
- 正在进行中— 亚马逊 FSx 正在处理更新请求。
- 更新优化— Amazon FSx 增加了文件系统的存储容量。存储优化过程现在正在将文件系统数据移动到新的较大磁盘上。
- 已完成— 存储容量增加已成功完成。
- 已失败— 存储容量增加失败。选择问号 (?) 以查看有关存储更新失败原因的详细信息。

进程%

将存储优化过程的进度显示为完成百分比。

请求时间

亚马逊 FSx 收到更新操作请求的时间。

监控随着Amazon CLI和 API

您可以使用描述文件系统 Amazon CLI命令和DescribeFileSystemsAPI 操作。这些区域有：`AdministrativeActions`阵列列出了每种管理操作类型的 10 个最近更新操作。当你增加文件系统的存储容量时，`AdministrativeActions`生成：a`FILE_SYSTEM_UPDATE`和`STORAGE_OPTIMIZATION`action.

以下示例显示了响应摘录describe-file-systemsCLI 命令。文件系统的存储容量为 300 GB，还有待执行将存储容量增加到 1000 GB 的管理措施。

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 300,
            "AdministrativeActions": [
                {
                     "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                     "RequestTime": 1581694764.757,
                     "Status": "PENDING",
                     "TargetFileSystemValues": {
                         "StorageCapacity": 1000
                     }
                },
                {
                    "AdministrativeActionType": "STORAGE_OPTIMIZATION",
                    "RequestTime": 1581694764.757,
                    "Status": "PENDING",
                }
            ]
```

Amazon FSx 处理FILE_SYSTEM_UPDATE首先操作，将新的较大的存储磁盘添加到文件系统中。当新存储空间可用于文件系统时，FILE_SYSTEM_UPDATE状态将更改为UPDATED_OPTIMIZING. 存储容量显示了新的更大价值，Amazon FSx 开始处理STORAGE_OPTIMIZATION行政操作。以下摘录显示了这一点：describe-file-systemsCLI 命令。

这些区域有：ProgressPercent属性显示存储优化过程的进度。存储优化过程成功完成后，FILE_SYSTEM_UPDATE操作更改为COMPLETED，以及STORAGE_OPTIMIZATION动作不再出现。

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 1000,
            "AdministrativeActions": [
                {
                    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                    "RequestTime": 1581694764.757,
                    "Status": "UPDATED_OPTIMIZING",
                    "TargetFileSystemValues": {
                        "StorageCapacity": 1000
                }
                },
                {
                    "AdministrativeActionType": "STORAGE_OPTIMIZATION",
                    "RequestTime": 1581694764.757,
                    "Status": "IN_PROGRESS",
                    "ProgressPercent": 50,
                }
            ]
```

如果存储容量增加失败，则FILE_SYSTEM_UPDATE操作更改为FAILED. 这些区域有：FailureDetails属性提供了有关故障的信息，如以下示例所示。

```
{
```

```
"FileSystems": [
    {
        "OwnerId": "111122223333",
        .
        .
        .
        "StorageCapacity": 300,
        "AdministrativeActions": [
            {
                "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                "FailureDetails": {
                    "Message": "string"
                },
                "RequestTime": 1581694764.757,
                "Status": "FAILED",
                "TargetFileSystemValues":
                    "StorageCapacity": 1000
            }
        ]
```

有关解决失败操作的信息，请参阅存储或吞吐量容量更新失败 (p. 199).

动态增加 FSx for Windows File Server 文件系统的存储容量

当可用存储容量低于指定的阈值时，可以使用以下解决方案动态增加 FSx for Windows File Server 文件系统的存储容量。该Amazon CloudFormation模板会自动部署定义可用存储容量阈值所需的所有组件、基于此阈值的 Amazon CloudWatch 警报以及Amazon Lambda函数，可增加文件系统的存储容量。

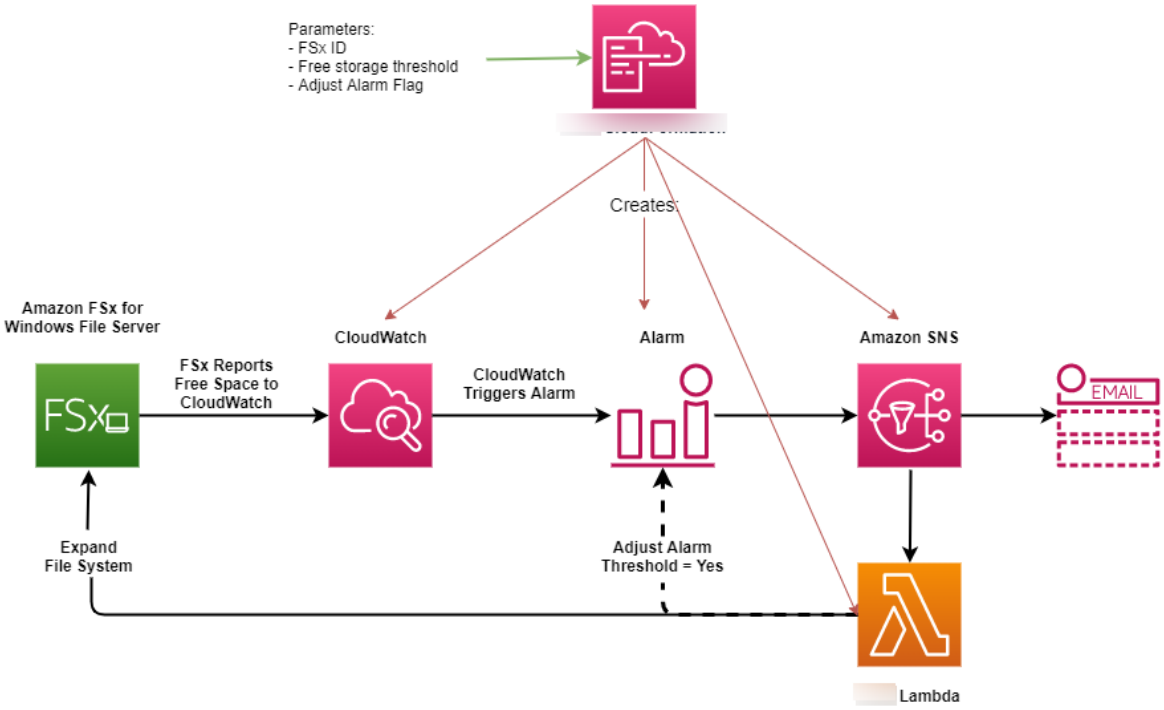
该解决方案会自动部署所有需要的组件，并采用以下参数：

- 文件系统 ID
- 可用存储容量阈值（数值）
- 计量单位（百分比 [默认] 或 GiB）
- 增加存储容量的百分比 (%)
- SNS 订阅的电子邮件地址
- 调整警报阈值（是/否）

主题

架构概述

部署此解决方案将在Amazon云。



下图说明了以下步骤：

1. 这些区域有：Amazon CloudFormation模板部署 CloudWatch 警报，Amazon Lambda函数、Amazon Simple Notification Service (Amazon SNS) 队列以及所有必需的Amazon Identity and Access Management(IAM) 角色。IAM 角色授予 Lambda 函数调用 Amazon FSx API 操作的权限。
2. 当文件系统的可用存储容量低于指定阈值时，CloudWatch 会触发警报，并向 Amazon SNS 队列发送消息。
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 函数可以选择性地调整可用存储容量阈值，使其等于文件系统新存储容量的指定百分比。
6. 最初的 CloudWatch Lambda 函数操作的警报状态和结果将发送到 Amazon SNS 队列。

接收有关作为响应而执行的操作的通知 CloudWatch 警报，Amazon SNS 必须按照订阅确认电子邮件。

Amazon CloudFormation 模板

此解决方案使用Amazon CloudFormation以自动部署用于自动增加 FSx for Windows File Server 文件系统存储容量的组件。要使用此解决方案，请下载增加 FSX 大小 Amazon CloudFormation。模板。

该模板使用参数的描述如下。查看模板参数及其默认值，然后根据文件系统的需要对其进行修改。

FileSystemId

无默认值。要自动增加存储容量的文件系统的 ID。

低可用数据存储容量阈值

无默认值。指定触发警报并自动增加文件系统的存储容量的初始可用存储容量阈值，以 GiB 或文件系统当前存储容量的百分比 (%) 指定。如果以百分比形式表示，则 CloudFormation 模板重新计算到 GiB 以匹配 CloudWatch 警报设置。

低可用数据存储容量阈值单元

默认值为%. 指定的单位`LowFreeDataStorageCapacityThreshold`，以 GiB 为单位或当前存储容量的百分比。

警报修改通知

默认值为是. 如果设置为 “是”，则初始`LowFreeDataStorageCapacityThreshold`，按比例增加`PercentIncrease`用于后续的警报阈值。

例如，什么时候`PercentIncrease`设置为 20，并且 AlarmModificationNotification 设置为 “是”，可用可用空间阈值 (`LowFreeDataStorageCapacityThreshold`) 对于随后的存储容量增加事件，在 GiB 中指定的将增加 20%。

EmailAddress

无默认值。指定用于 SNS 订阅的电子邮件地址，并将接收存储容量阈值警报。

百分比增加

无默认值。指定增加存储容量的数量，以当前存储容量的百分比表示。

通过自动部署Amazon CloudFormation

以下过程配置和部署Amazon CloudFormation堆栈以自动增加 FSx for Windows File Server 文件系统的存储容量。部署大约需要 5 分钟时间。

Note

实施此解决方案需要对相关的Amazon服务。有关更多信息，请参阅这些服务的定价详细信息页面。

在开始之前，您必须在您的 Amazon FSx 文件系统中运行在 Amazon Virtual Private Cloud (Amazon VPC) 中运行的 Amazon FSx 文件系统的 IDAmazonaccount. 有关创建 Amazon FSx 资源的更多信息，请参阅开始使用 Amazon FSx (p. 7).

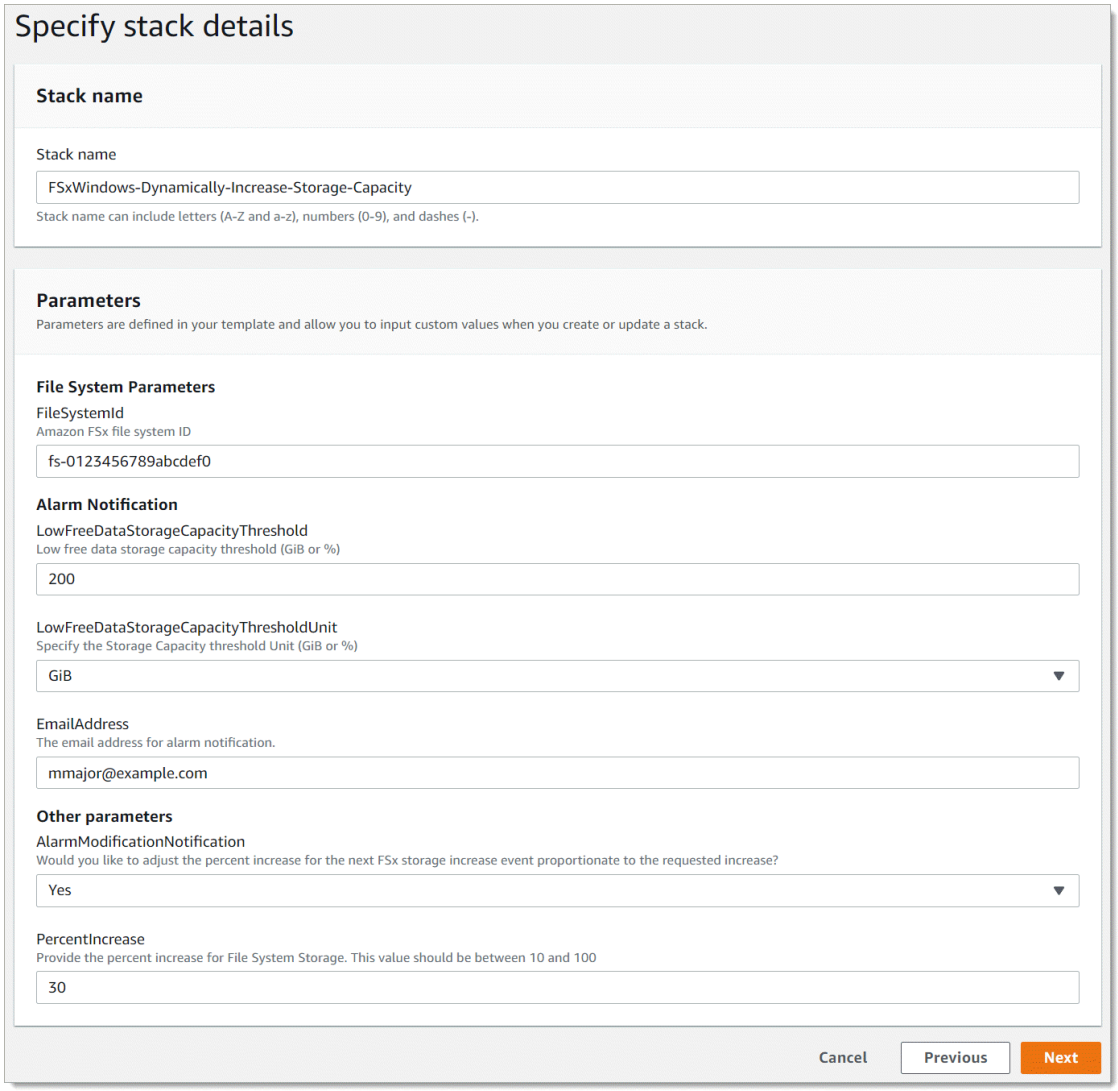
启动自动增加存储容量解决方案堆栈

1. 下载增加 FSX 大小 Amazon CloudFormation。模板。有关创建 CloudFormation 堆栈，请参阅在 Amazon CloudFormation 控制台中的Amazon CloudFormation用户指南.

   Note

   Amazon FSx 目前仅在特定情况下可用Amazon地区。你必须在Amazon亚马逊 FSx 可用的地区。有关更多信息，请参阅 。Amazon FSx 终端节点和配额中的Amazon一般参考.

2. In指定栈详细信息中，输入自动存储容量增加解决方案的值。



3. 输入堆栈名称.
4. 适用于参数，请查看模板的参数并根据文件系统的需要对其进行修改。然后选择下一步。
5. 输入任何选项选择您想要的自定义解决方案的设置，然后选择下一步.
6. 适用于审核，查看并确认解决方案设置。您必须选中确认模板创建 IAM 资源的复选框。
7. 选择 Create (创建) 以部署堆栈。

您可以在 Amazon CloudFormation 控制台的 Status (状态) 列中查看堆栈的状态。您应看到的状态创建_COMPLETE在大约 5 分钟内。

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来更新堆栈。有关更多信息，请参阅 。直接更新堆栈中的Amazon CloudFormation用户指南.

管理吞吐量容量

Windows File Server 的每个 FSx 文件系统都具有在创建文件系统时配置的吞吐量容量。您可以根据需要随时修改文件系统的吞吐量容量。吞吐量是决定托管文件系统的文件服务器提供文件数据的速度的一个因素。更高的吞吐量容量还包括更高的每秒 I/O 操作 (IOPS) 以及用于缓存文件服务器上的数据的更多内存。有关更多信息，请参阅 FSx for Windows File Server 性能 (p. 141)。

当您修改文件系统的吞吐量时，在幕后，Amazon FSx 会切换文件系统的文件服务器。对于多可用区文件系统，在 Amazon FSx 切换首选文件服务器和辅助文件服务器时，它会导致自动故障切换和故障恢复。对于单可用区系统，在吞吐量扩展期间，文件系统将在几分钟内不可用。文件系统可用后，您需要为新的吞吐量量收取费用。

> Note
>
> 在后端进行维护操作期间，系统修改（例如对吞吐量的修改）可能会延迟。维护可能会导致这些更改排队列直到下一步处理。

主题

何时修改吞吐量容量

Amazon FSx 与 Amazon CloudWatch 集成，使您能够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量、存储容量和存储类型之外，您可以在文件系统中驱动的性能（吞吐量和 IOPS）取决于特定工作负载的特征。您可以使用 CloudWatch 用于确定为提高绩效而要更改其中哪个维度的指标。有关更多信息，请参阅 使用 Amazon CloudWatch 监控 (p. 134)。

对于多可用区文件系统，吞吐量扩展会导致自动故障切换和故障恢复，而 Amazon FSX 切换首选文件服务器和辅助文件服务器，此期间的任何数据更改都需要在文件服务器之间同步。在此期间，您的文件系统将继续可用，但为了缩短数据同步的持续时间，我们建议您在文件系统负载最小的空闲期间修改吞吐量容量。

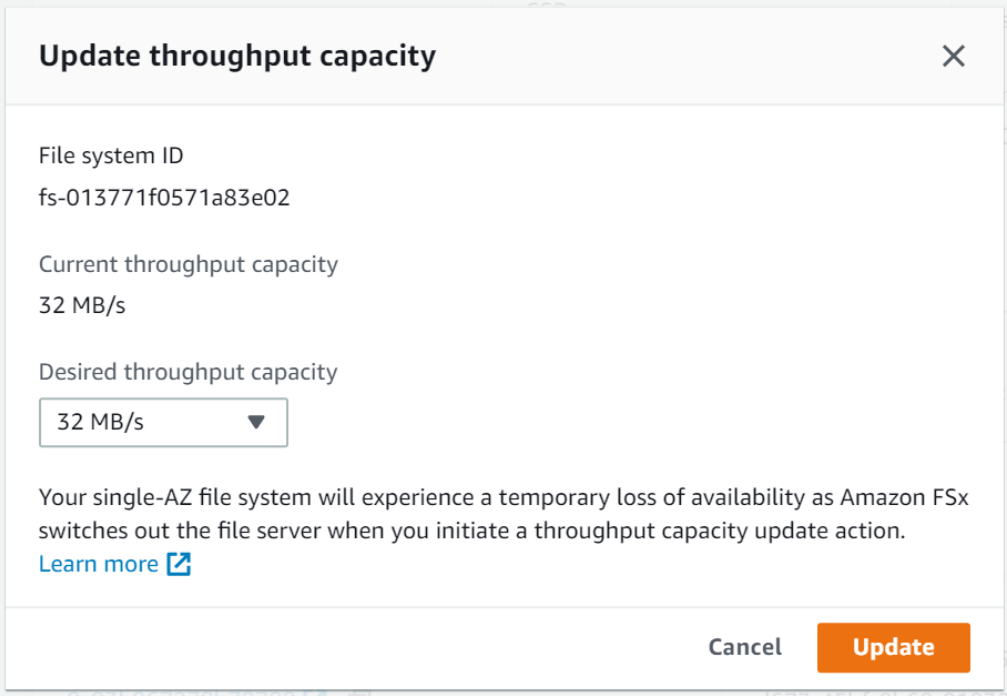
如何修改吞吐量容量

您可以使用 Amazon FSx 控制台修改文件系统的吞吐量容量，Amazon Command Line Interface(Amazon CLI) 或者亚马逊 FSx API。

修改文件系统的吞吐量容量（控制台）

1. 在以下位置打开 Amazon FSx 控制台https://console.aws.amazon.com/fsx/.
2. 导航到文件系统，然后选择要增加吞吐量容量的 Windows 文件系统。
3. 适用于操作，选择更新吞吐量. 或者，在摘要面板中，选择更新旁边的文件系统吞吐量容量.

   这些区域有：更新吞吐量容量窗口将出现。
4. 选择新值吞吐量容量从列表中。



5. 选择更新以启动吞吐量容量更新。

   Note

   多可用区文件系统在更新吞吐量扩展时进行故障切换和故障恢复，并且完全可用。在更新期间，单可用区文件系统经历了非常短的时间不可用。

6. 您可以在文件系统详情页面，在更新选项卡。

   您可以使用 Amazon FSx 控制台（Amazon CLI，以及 API。有关更多信息，请参阅 监控吞吐量容量变化 (p. 123)。

修改文件系统的吞吐量 (CLI)

要修改文件系统的吞吐量容量，请使用Amazon CLI命令更新文件系统. 设置以下参数：

- `--file-system-id`转换为要更新的文件系统的 ID。
- `ThroughputCapacity`到要将文件系统更新到的所需值。

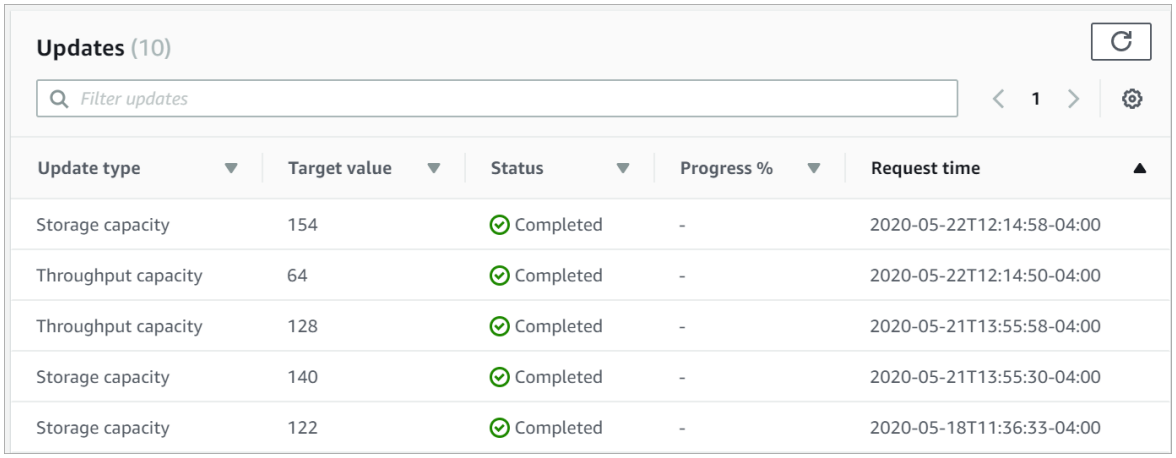
您可以使用 Amazon FSx 控制台（Amazon CLI，以及 API。有关更多信息，请参阅 监控吞吐量容量变化 (p. 123)。

监控吞吐量容量变化

您可以使用 Amazon FSx 控制台、API 和Amazon CLI.

在控制台中监控吞吐量容量变化

在更新选项卡中的文件系统详情窗口中，您可以查看每种更新操作类型的 10 个最近更新操作。



对于吞吐量容量更新操作，您可以查看以下信息。

更新类型

支持的类型有：吞吐量容量、存储容量, 和存储优化.

Target value (目标值)

将文件系统的吞吐量更改为的所需值。

状态

更新的当前状态。对于吞吐量容量，可能的值如下所示：

- Pending— 亚马逊 FSx 已收到更新请求，但尚未开始处理。
- 正在进行中— 亚马逊 FSx 正在处理更新请求。
- 已完成— 吞吐量容量更新已成功完成。
- 已失败— 吞吐量容量更新失败。选择问号 (?) 以查看有关吞吐量更新失败的原因的详细信息。

请求时间

亚马逊 FSx 收到更新请求的时间。

使用监控更改Amazon CLI和 API

您可以使用描述文件系统CLI 命令和DescribeFileSystemsAPI 操作。这些区域有：`AdministrativeActions`阵列列出了每种管理操作类型的 10 个最近更新操作。当您修改文件系统的吞吐量容量时，`FILE_SYSTEM_UPDATE`已生成管理操作。

以下示例显示了一个响应摘录`describe-file-systems`CLI 命令。文件系统的吞吐量为 8 MB/s，目标吞吐量为 256 MB/s。

```
.
.
.
    "ThroughputCapacity": 8,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "PENDING",
        "TargetFileSystemValues": {
          "WindowsConfiguration": {
```

```
            "ThroughputCapacity": 256
          }
        }
    }
]
```

当 Amazon FSx 成功处理操作后，状态将变为COMPLETED. 然后，文件系统可以使用新的吞吐量容量，并显示在ThroughputCapacity财产。以下响应摘录显示了一个describe-file-systemsCLI 命令。

```
.
.
.
    "ThroughputCapacity": 256,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "COMPLETED",
        "TargetFileSystemValues": {
          "WindowsConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

如果吞吐量容量修改失败，则状态将变为FAILED，以及FailureDetails属性提供了有关失败的信息。有关解决失败操作的信息，请参阅存储或吞吐量容量更新失败 (p. 199).

标记 Amazon FSx 资源

为了帮助您管理文件系统和其他 Amazon FSx 资源，您可通过标签的形式为每个资源分配元数据。标签可让您按各种标准（例如用途、所有者或环境）对 Amazon 资源进行分类。这在您具有相同类型的很多资源时会很有用—您可以根据分配给特定资源的标签快速识别该资源。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 Amazon 资源分配的标记。每个标签都包含您定义的一个键 和一个可选值。

标签可让您按各种标准 (例如用途、所有者或环境) 对 Amazon 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。有关如何实施有效的资源标记策略的更多信息，请参阅 Amazon 白皮书标记最佳实践。

标签对 Amazon FSx 没有任何语义意义，应严格按字符串进行解析。同时，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

其设为空值。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，则AmazonCLI 或AmazonSDK，您可以使用`TagResource`将标签应用到现有资源的 API 操作。此外，某些资源创建操作允许您在创建资源时为其指定标签。如果无法在资源创建期间应用标签，系统会回滚资源创建过程。这样可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。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。有关允许用户在创建时标记资源的更多信息，请参阅 在创建过程中授予标记资源的权限 (p. 167)。

给您的 资源加标签

您可以标记账户中存在的 Amazon FSx 资源。如果您使用的是 Amazon FSx 控制台，则可以使用相关资源屏幕上的 Tags (标签) 选项卡对资源应用标签。创建资源时，可以使用值应用 Name 键，也可以在创建新文件系统时应用自己选择的标签。控制台可能根据 Name (名称) 标签对资源进行组织，但此标签对 Amazon FSx 服务没有任何语义意义。

对于支持在创建时标记的 Amazon FSx API 操作，您可以在 IAM 策略中应用基于标签的资源级权限，以对可在创建时标记资源的用户和组实施精细控制。您的资源从创建开始会受到适当的保护 — 标签会立即用于您的资源，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。

您也可以将资源级权限应用于`TagResource`和`UntagResource`标记 IAM 策略中的 Amazon FSx API 操作，以控制对现有资源设置哪些标签键和值。

有关标记资源以便于计费的更多信息，请参阅 Amazon Billing 用户指南中的使用成本分配标签。

标签限制

下面是适用于标签的基本限制：

- 每个资源的标签数上限 – 50
- 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。
- 最大键长度 – 128 个 Unicode 字符 (采用 UTF-8 格式)
- 最大值长度 – 256 个 Unicode 字符 (采用 UTF-8 格式)
- 允许使用 Amazon FSx 标签的字符包括：可以使用 UTF-8 表示的字母、数字和空格以及以下字符：+-=. _:/@。
- 标签键和值区分大小写。
- `aws:` 前缀专门预留供 Amazon 使用。如果某个标签具有带有此标签键，则您无法编辑该标签的键或值。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；必须指定资源的标识符。例如，要删除使用名为的标签键标记的文件系统，请运行以下命令：`DeleteMe`，必须使用`DeleteFileSystem`具有文件系统资源标识符的操作，例如 fs-1234567890abcdef0。

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Amazon Web Services 账户; 没有其他Amazon Web Services 账户将有权访问这些标签。为了对共享资源进行基于标签的访问控制，Amazon Web Services 账户必须分配自己的一组标签来控制对资源的访问。

权限和标签

有关在创建时标记 Amazon FSx 资源所需的权限的更多信息，请参阅在创建过程中授予标记资源的权限 (p. 167). 有关使用标签限制对 IAM 策略中 Amazon FSx 资源的访问的更多信息，请参阅使用标签控制对 Amazon FSx 资源的访问 (p. 170).

使用亚马逊 FSx 维护窗口

适用于 Windows 文件服务器的亚马逊 FSx 为它管理的微软 Windows 服务器软件执行例行软件修补。维护时段是您控制软件修补程序一周中哪一天和时间的机会。

修补程序很少发生，通常每几周进行一次。修补程序应该只需要 30 分钟的维护时段的一小部分。在这几分钟内，您应该期望单可用区文件系统将不可用，并且多可用区文件系统将自动进行故障切换和故障恢复。

您可以在创建文件系统期间选择维护时段。如果没有时间偏好，则会分配一个 30 分钟的默认窗口。

> Note
>
> 为了确保维护活动期间的数据完整性，Amazon FSx for Windows File Server 会在维护开始之前完成对托管文件系统的底层存储卷的任何待处理写入操作。

您可以使用 Amazon FSx 管理控制台，Amazon CLI、AmazonAPI，或者其中一个Amazon可更改文件系统的维护时段的 SDK。

要更改每周维护时段（控制台）

1. 打开 Amazon FSx 控制台https://console.aws.amazon.com/fsx/.
2. 选择文件系统在左侧导航栏中。
3. 选择要更改每周维护时段的文件系统。将显示文件系统详细信息页面。
4. 选择管理显示文件系统管理设置面板。
5. 选择更新显示更改维护时段窗口。
6. 输入希望每周维护时段开始的新日期和时间。
7. 选择 Save (保存) 以保存您的更改。新的维护开始时间显示在管理设置面板。

要使用 CLI 或 API 更改每周维护时段，请使用更新文件系统操作，请参阅演练 3：更新现有文件系统 (p. 149).

管理 Amazon FSx 文件系统的最佳实践

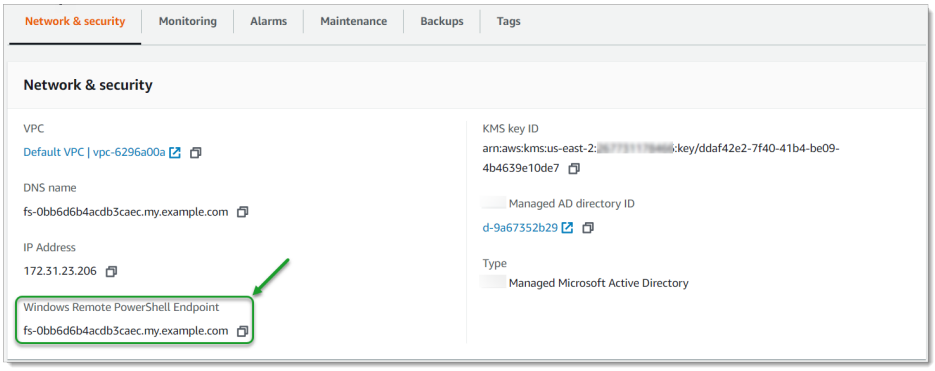
Amazon FSx 提供了多项功能，可帮助您实施管理文件系统的最佳做法，包括：

- 优化存储消耗
- 使最终用户能够将文件和文件夹恢复到以前的
- 为所有连接客户端强制加密

在 PowerShell 上使用以下 Amazon FSx CLI 进行远程管理，在文件系统上快速实施这些最佳做法。

要运行这些命令，您必须了解Windows 远程 PowerShell 终端节点为您的文件系统。要查找此终端节点，请执行以下步骤：

1. 在以下位置打开 Amazon FSx 控制台https://console.aws.amazon.com/fsx/.
2. 选择您的文件系统。在存储库的网络与安全选项卡中，找到Windows 远程 PowerShell 端点，如下所示。



有关更多信息，请参阅 管理文件系统 (p. 80) 和 开始使用 Amazon FSx CLI 进行远程管理 PowerShell (p. 80)。

主题

- 一次性管理设置任务 (p. 128)
- 监控文件系统的持续管理任务 (p. 129)

一次性管理设置任务

以下是您可以为文件系统快速设置一次的任务。

管理存储消耗

使用以下命令管理文件系统存储空间消耗。

- 要使用默认计划启用重复数据消除，请运行以下命令。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Enable-FsxDedup }
```

或者，使用以下命令在文件创建后立即在文件上运行重复数据消除，而不需要任何最短文件期限。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FSxDedupConfiguration -MinimumFileAgeDays 0 }
```

有关更多信息，请参阅 重复数据删除 (p. 104)。

- 使用以下命令在 “跟踪” 模式下启用用户存储配额，该模式仅用于报告目的，而不是用于强制执行。

```
$QuotaLimit = Quota limit in bytes
$QuotaWarningLimit = Quota warning threshold in bytes
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Enable-FSxUserQuotas -Track -DefaultLimit
 $Using:QuotaLimit -DefaultWarningLimit $Using:QuotaWarningLimit }
```

有关更多信息，请参阅 存储配额 (p. 106)。

打开卷影副本以使最终用户能够将文件和文件夹恢复到以前的版本

使用默认时间表（平日早上 7 点和中午 12 点）打开卷影副本，如下所示。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FsxShadowStorage -Default }

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FsxShadowCopySchedule -Default -Confirm:$False}
```

有关更多信息，请参阅 卷影副本 (p. 107)。

传输过程中强制加密

以下命令对连接到文件系统的客户端强制加密。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FsxSmbServerConfiguration -EncryptData $True -
RejectUnencryptedAccess $True -Confirm:$False}
```

您可以关闭所有打开的会话，并使用加密强制当前连接的客户端重新连接。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Close-FSxSmbSession -Confirm:$False}
```

有关更多信息，请参阅 管理传输中加密 (p. 112) 和 用户会话和打开的文件 (p. 101)。

监控文件系统的持续管理任务

以下正在执行的任务可帮助您监控文件系统的磁盘使用情况、用户配额和打开的文件。

监控重数据删除状态

监控重复数据消除状态，包括在文件系统上实现的节省率，如下所示。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -
ConfigurationName FsxRemoteAdmin -ScriptBlock { Get-FSxDedupStatus } | select
 OptimizedFilesCount,OptimizedFilesSize,SavedSpace,OptimizedFilesSavingsRate
```

监控用户级存储消耗

获取有关当前用户存储配额条目的报告，包括他们消耗的空间量以及他们是否违反了限制和警告阈值。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Get-FSxUserQuotaEntries }
```

监控和关闭打开的文件

通过查找已打开的文件并关闭它们来管理打开的文件。使用以下命令检查打开的文件。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Get-FSxSmbOpenFile}
```

使用以下命令关闭打开的文件。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Close-FSxSmbOpenFile -Confirm:$false}
```

使用 DFS 命名空间对多个文件系统进行分组

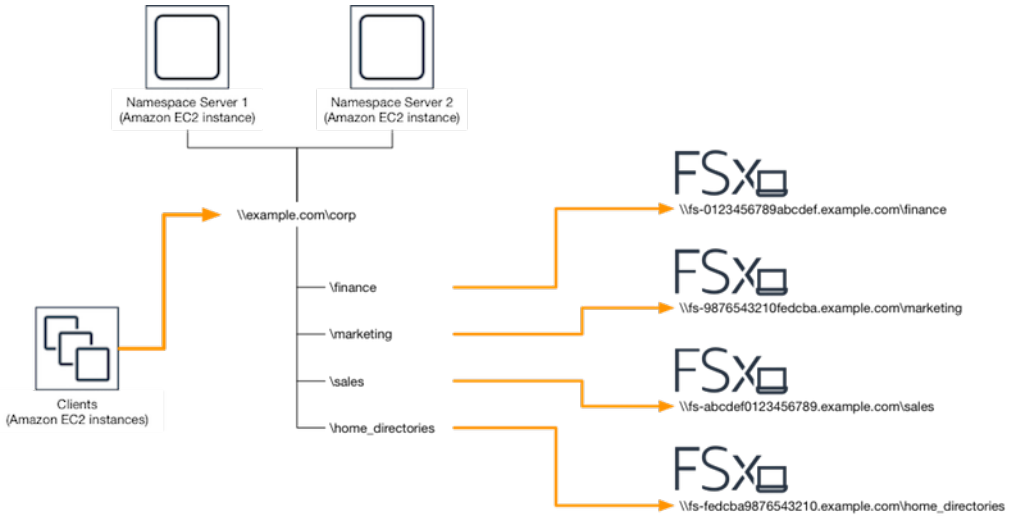
适用于 Windows 文件服务器的 Amazon FSx 支持使用微软的分布式文件系统 (DFS) 命名空间。您可以使用 DFS 命名空间将多个文件系统上的文件共享分组到一个用于访问整个文件数据集的通用文件夹结构（命名空间）中。DFS 命名空间可以帮助您组织和统一跨多个文件系统对文件共享的访问权限。DFS 命名空间还可以帮助扩展文件数据存储空间，超出每个文件系统对大型文件数据集的支持范围（64 TB），最多可达数百 PB。

设置 DFS 命名空间以对多个文件系统进行分组

您可以使用 DFS 命名空间将多个文件系统分组到一个命名空间下。在下面的示例中，基于域的命名空间 (example.com\ corp) 是在两个命名空间服务器上创建的，整合了存储在多个 Amazon FSx 文件系统（财务、营销、销售、home_目录）上的文件共享。这允许您的用户使用通用命名空间访问文件共享。鉴于此，他们不需要为托管文件共享的每个文件系统指定文件系统 DNS 名称。

> **Note**
>
> 无法将亚马逊 FSx 添加到 DFS 共享路径的根目录中。

这些步骤将指导您在两个命名空间服务器上创建单个命名空间（example.com\ corp）。您还可以在命名空间下设置四个文件共享，每个共享都以透明方式将用户重定向到托管在不同 Amazon FSx 文件系统上的共享。



将多个文件系统分组到一个共同的 DFS 命名空间

1. 如果您尚未运行 DFS 命名空间服务器，则可以使用设置-dfsn-Server。模板 Amazon CloudFormationTemplate。有关创建Amazon CloudFormation堆栈，请参阅在上创建堆栈Amazon CloudFormation 控制台中的Amazon CloudFormation用户指南.
2. 以用户身份 Connect 到在上一步中启动的 DFS 命名空间服务器之一Amazon委托管理员组中)。有关更多信息，请参阅适用于 Windows 实例的 Amazon EC2 用户指南中的连接您的 Windows 实例。
3. 打开以访问 DFS 管理控制台。打开启动然后运行菜单dfsmgmt.msc. 这将打开 DFS 管理 GUI 工具。

4. 选择操作然后命名空间中，键入您为其启动的第一个 DFS 命名空间服务器的计算机名称服务器然后选择下一步.
5. 适用于名称，键入你正在创建的命名空间（例如，Corp)。
6. 选择编辑设置并根据您的要求设置适当的权限。选择 Next（下一步）。
7. 保留默认值基于域的命名空间选择选项，请保留启用 Windows Server 2008选项已选中，然后选择下一步.

   Note

   Windows Server 2008 模式是命名空间的最新可用选项。
8. 查看命名空间设置并选择Create.
9. 在下面选择了新创建的命名空间命名空间在导航栏中，选择操作然后添加命名空间 Server.
10. 输入您为其启动的第二个 DFS 命名空间服务器的计算机名称命名空间 Server.
11. 选择编辑设置，根据您的要求设置适当的权限，然后选择确定.
12. 打开刚刚创建的命名空间的上下文 (右键单击) 菜单，选择。新文件夹，键入文件夹的名称（例如，`finance`为了名称，然后选择确定.
13. 键入希望 DFS 命名空间文件夹以 UNC 格式指向的文件共享的 DNS 名称（例如，`\\fs-0123456789abcdef0.example.com\finance`) 对于文件夹目标的路径然后选择确定.
14. 如果该份额不存在：
    a. 选择是来创建它。
    b. 从创建共享对话框中，选择浏览.
    c. 在下面选择现有文件夹，或在下面创建一个文件夹D$，然后选择确定.
    d. 设置适当的共享权限，然后选择确定.
15. 从新文件夹对话框中，选择确定. 新文件夹将在命名空间下创建。
16. 对于要在同一命名空间中共享的其他文件夹，重复最后四个步骤。

监控 FSx for Windows File Server

监控是保持 Amazon FSx 和您的 Amazon FSx 的可靠性、可用性和性能的重要环节。Amazon解决方案。你应该从你的所有部分收集监控数据Amazon解决方案，以便更轻松地调试出现的多点故障。不过，在开始监控 Amazon FSx 之前，您应制定一个监控计划并在计划中回答下列问题：

- 监控目的是什么？
- 您将监控哪些资源？
- 监控这些资源的频率如何？
- 您将使用哪些监控工具？
- 谁负责执行监控任务？
- 出现错误时应通知谁？

下一步，通过在不同时间和不同负载条件下测量性能，在您的环境中建立正常 Amazon FSx 性能的基准。监控 Amazon FSx 时，您应考虑存储历史监控数据。此存储数据为您提供与当前性能数据进行比较的基准，确定正常性能模式和性能异常，以及设计解决问题的方法。

例如，使用 Amazon FSx，您可监控网络吞吐量、读写 I/O 和元数据操作以及文件系统的可用存储容量。如果性能低于您所建立的基准，则您可能需要更改文件系统的大小，以便针对工作负载优化文件系统。

要建立基准，您至少应监控以下各项：

- 文件系统的网络吞吐量。
- 每个文件系统操作的字节数，包括数据读取、数据写入和元数据操作。

监控工具

Amazon提供各种可以用来监控 Amazon FSx 的工具。您可以配置其中的一些工具来为您执行监控任务，但有些工具需要手动干预。建议您尽可能实现监控任务自动化。

自动监控工具

您可以使用以下自动化监控工具来监控 Amazon FSx 并在出现错误时进行报告：

- 亚马逊 CloudWatch Alarms— 监控您指定的时间段内的单个指标，并根据相对于给定阈值的指标值在若干时间段内执行一项或多项操作。操作是一个发送到 Amazon Simple Notification Service (Amazon SNS) 主题或 Amazon EC2 Auto Scaling 策略的通知。 CloudWatch 警报将不会调用操作，因为这些操作处于特定状态，该状态必须改变并在指定数量的时间段内一直保持。有关更多信息，请参阅 使用 Amazon CloudWatch 监控 (p. 134)。
- 亚马逊 CloudWatch 日志— 监控、存储和访问日志文件Amazon CloudTrail或其他源。有关更多信息，请参阅 。什么是 Amazon CloudWatch 日志？中的亚马逊 CloudWatch 日志用户指南.
- Amazon CloudTrail日志监控— 在账户间共享日志文件，监控 CloudTrail 通过将文件发送到来实时登录文件 CloudWatch 日志、使用 Java 编写日志处理应用程序，以及验证您的日志文件是否在由 CloudTrail 传送后未发生更改。有关更多信息，请参阅 。使用 CloudTrail 日志文件中的Amazon CloudTrail用户指南.

手动监控工具

监控 Amazon FSx 的另一个重要环节是手动监控 Amazon FSx 的那些商品。 CloudWatch 警报不包括在内。亚马逊 FSx、CloudWatch 和其他Amazon控制台仪表板提供 at-a-glance 查看您的状态Amazon环境。建议还要查看文件系统上的日志文件。

- 您可以从 Amazon FSx 控制台找到文件系统的以下项目：
  - 免费存储容量
  - 总吞吐量（字节/秒）
  - 总 IOPS（操作/秒）
- 这些区域有： CloudWatch 主页显示：
  - 当前告警和状态
  - 告警和资源图表
  - 服务运行状况

  此外，您还可以使用 CloudWatch 执行以下操作：
  - Create控制面板监控您使用的服务。
  - 绘制指标数据图，以排除问题并弄清楚趋势。
  - 搜索并浏览您所有的 Amazon 资源指标。
  - 创建和编辑告警接收有关问题的通知。

使用 Amazon CloudWatch 监控

您可以使用 Amazon CloudWatch 监控文件系统，此工具可从 FSx for Windows File Server 收集原始数据，并将数据处理为易读的近乎实时的指标。这些统计数据将保留 15 个月，从而使您能够访问历史信息，并能够更好地了解您的 Web 应用程序或服务的运行情况。默认情况下，Amazon FSx for Windows File Server 指标数据将自动发送到 CloudWatch 在 1 分钟期间。有关 CloudWatch 的更多信息，请参阅什么是 Amazon CloudWatch？中的亚马逊 CloudWatch 用户指南.

Amazon FSx CloudWatch 指标作为原始指标报告为字节. 字节数不会舍入到十进制或二进制单位倍数。

Amazon FSx for Windows File Server 发布以下指标：`AWS/FSx`CloudWatch 中的命名空间。对于每个指标，FSx for Windows File Server 每分钟每个文件系统发出一个数据点。

指标	描述
`DataReadBytes`	文件系统读取操作的字节数。 这些区域有：`Sum`统计数据是该时段内与读取操作关联的总字节数。要计算某个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`	文件系统写入操作的字节数。 这些区域有：`Sum`统计数据是该时段内与写入操作关联的总字节数。要计算某个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`	读取操作数。 这些区域有：`Sum`统计数据是该时段内的读取操作数。要计算某个时段内的平均读取操作数（每秒操作数），请将`Sum`统计数据按该时段的秒数计算。

指标	描述
	单位：计数 有效统计数据：Sum
DataWriteOperations	写入操作数。 这些区域有：Sum统计数据是该时段内的写入操作数。要计算某个时段内的平均写入操作数（每秒操作数），请将Sum统计数据按该时段的秒数计算。 单位：计数 有效统计数据：Sum
MetadataOperations	元数据操作数。 这些区域有：Sum统计数据是该时间段内元数据操作的计数。要计算某个时段内的元数据操作数（每秒操作数），请将Sum统计数据按该时段的秒数计算。 单位：计数 有效统计数据：Sum
FreeStorageCapacity	可用存储容量的大小。 单位：字节 有效统计数据：Average、Minimum

FSx for Windows File Server 维度

FSx for Windows File Server 指标使用FSx命名空间并为单个维度提供指标，FileSystemId. 你可以使用描述文件系统 Amazon CLI命令或DescribeFileSystemsAPI 命令。文件系统 ID 采用以下格式：*fs-0123456789abcdef0*.

如何将 FSx for Windows File Server 指标使用

Amazon FSx 报告的指标提供可通过不同方式分析的信息。以下列表显示了这些指标的一些常见用途。这些是入门建议，并不全面。

如何确定...	相关指标
我的文件系统的 IOPS？	总 IOPS = SUM（数据交易操作 + DataWriteOperations + 元数据操作）/周期（以秒为单位）
我的文件系统的吞吐量？	SUM（datareadBytes + DataWriteBytes）/周期（以秒为单位）

> **Note**
>
> 我们建议您将平均吞吐量利用率保持在 50% 以下，以确保有足够的备用吞吐量容量来应对工作负载的意外峰值，以及任何后台 Windows 存储操作（例如存储同步、重复数据删除或卷影副本）。

访问 CloudWatch 指标

你可以查看亚马逊 FSx 指标 CloudWatch 通过以下方式。

- 亚马逊 FSx 控制台。
- 这些区域有： CloudWatch 控制台。
- 这些区域有： CloudWatch CLI（命令行界面）。
- 这些区域有： CloudWatch API。

以下步骤向您介绍了如何使用这些不同工具访问指标。

使用 Amazon FSx 控制台查看指标

1. 从打开 Amazon FSx 控制台https://console.aws.amazon.com/fsx/.
2. 从导航窗格中，选择文件系统，然后选择要查看其指标的文件系统。
3. 选择操作然后选择查看详细信息.
4. 在存储库的摘要页面上，选择监控以查看您的文件系统的指标。

使用 查看指标 CloudWatch 控制台

1. 打开 CloudWatch 控制台。
2. 在导航窗格中，选择 Metrics (指标)。
3. 选择FSx命名空间。
4. （可选）要查看某个指标，请在搜索字段中输入其名称。
5. （可选）要按维度筛选，请选择 FileSystemId。

从 Amazon CLI 访问指标

- 使用`list-metrics`命令使用`--namespace "AWS/FSx"`命名空间。有关更多信息，请参阅 Amazon CLI 命令参考。

使用 CloudWatch API

从 访问指标 CloudWatch API

- 调用 `GetMetricStatistics`。有关更多信息，请参阅 。亚马逊 CloudWatch API 参考.

创建 CloudWatch 监控 Amazon FSx

您可以创建 CloudWatch 警报，以在警报改变状态时发送 Amazon SNS 消息。警报会每隔一段时间 (由您指定) 监控一个指标，并根据相对于给定阈值的指标值每隔若干个时间段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。

警报只会调用操作进行持续的状态变更。 CloudWatch 警报不会仅仅因为处于特定状态而调用操作；该状态必须已发生变化，并在指定数量的时间段内保持该状态。您可以从亚马逊 FSx 控制台或 CloudWatch 控制台。

以下过程介绍了如何使用控制台为 Amazon FSx 创建警报，Amazon CLI和 API。

使用 Amazon FSx 控制台设置警报

1. 从打开 Amazon FSx 控制台https://console.aws.amazon.com/fsx/.
2. 从导航窗格中，选择文件系统，然后选择要为其创建警报的文件系统。
3. 选择操作菜单，然后选择查看详细信息.

4. 在存储库的摘要页面上，选择Alarms.
5. 选择Create CloudWatch 警报. 随后您将被重定向至 CloudWatch 控制台。
6. 选择选择指标，然后选择下一步.
7. 在指标部分，选择FSX.
8. 选择文件系统指标中，选择要为其设置警报的指标，然后选择。选择指标.
9. 在条件部分中，选择你想要的警报条件，然后选择下一步.

   Note

   单可用区文件系统的文件系统维护期间可能不会发布指标。要防止不必要和误导性的警报状况更改，并配置警报以使其能够抵御丢失的数据点，请参阅配置方式 CloudWatch 警报处理缺失数据中的亚马逊 CloudWatch 用户指南.
10. 如果您想 CloudWatch 要在警报状态触发操作时向您发送一封电子邮件或 SNS 通知，请为每当此警报状态下，.

    适用于选择 SNS 主题中，选择一个现有 SNS 主题。如果您选择 Create topic (创建主题)，那么您就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 Next（下一步）。

    Note

    如果您使用 Create topic (创建主题) 创建一个新 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。当警报进入警报状态时，才会发送电子邮件。如果在验证电子邮件地址之前警报状态发生了变化，那么它们不会接收到通知。
11. 填写名称、说明, 和Whenever指标的值，然后选择下一步.
12. 在存储库的创建预览和创建页面上，查看您将要创建的警报，然后选择。创建警报.

使用设置警报 CloudWatch 控制台

1. 登录到Amazon Web Services Management Console然后打开 CloudWatch 控制台在https://console.aws.amazon.com/cloudwatch/.
2. 选择创建警报启动创建警报向导.
3. 选择FSx 指标，并滚动 Amazon FSx 指标以找到要为其设置警报的指标。要在此对话框中仅显示 Amazon FSx 指标，请搜索文件系统的文件系统 ID。选择要创建警报的指标，然后选择。下一步.
4. 填写指标的 Name、Description 和 Whenever 值。
5. 如果您想 CloudWatch 要在达到警报状态时向您发送一封电子邮件，请为每当此警报，选择状态是警报. 对于发送通知到，选择一个现有 SNS 主题。如果您选择 Create topic (创建主题)，那么您就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。

   Note

   如果您使用 Create topic (创建主题) 创建一个新 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。当警报进入警报状态时，才会发送电子邮件。如果在验证电子邮件地址之前警报状态发生了变化，那么它们不会接收到通知。
6. 此时，警报预览区域将为您提供一次机会来预览即将创建的警报。选择 Create Alarm（创建告警）。

使用 Amazon CLI 设置警报

- 调用 `put-metric-alarm`。有关更多信息，请参阅 Amazon CLI Command Reference。

使用 设置警报 CloudWatch API

- 调用 `PutMetricAlarm`。有关更多信息，请参阅 。亚马逊 CloudWatch API 参考.

使用记录 FSx for Windows File Server API 调用 Amazon CloudTrail

亚马逊 FSx 与Amazon CloudTrail，提供用户、角色或者执行操作的记录的服务。Amazon亚马逊 FSx 中的服务。 CloudTrail 将 Amazon FSx 的所有 API 调用作为事件捕获。捕获的调用包括来自 Amazon FSx 控制台的调用和对 Amazon FSx API 操作的代码调用。

如果您创建跟踪，则可以使 CloudTrail 一个 Amazon S3 FSx 的事件，包括 Amazon FSx 的事件。如果您不配置跟踪，则仍可在 CloudTrail 控制台事件历史. 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《Amazon CloudTrail 用户指南》。

CloudTrail 中的 Amazon FSx 信息

在您创建 Amazon 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 活动以及其他Amazon中的服务事件事件历史. 您可以在 Amazon 账户中查看、搜索和下载最新事件。有关更多信息，请参阅 。使用查看事件 CloudTrail 事件历史.

要持续记录您的事件Amazon要创建跟踪记录（包括 Amazon FSx 的事件）。一个踪迹启用 CloudTrail 将日志文件传送至 Amazon S3 存储桶。预设情况下，在控制台中创建跟踪时，此跟踪应用于所有 Amazon 区域。此跟踪记录来自 Amazon 分区中的所有 Amazon 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，您还可以配置其他Amazon服务用于进一步分析在中收集的事件数据并采取措施 CloudTrail 日志。有关更多信息，请参阅 Amazon CloudTrail 用户指南 中的以下主题：

- 创建跟踪概览
- CloudTrail 支持的服务和集成
- 为 CloudTrail 配置 Amazon SNS 通知
- 接收 CloudTrail 多个区域中的日志文件和从多个账户接收 CloudTrail 日志文件

所有 Amazon FSxAPI 调用由 CloudTrail 记录。例如，对`CreateFileSystem`和`TagResource`操作在 CloudTrail 日志文件。

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 Amazon 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 Amazon 服务发出。

有关更多信息，请参阅 Amazon CloudTrail 用户指南中的 CloudTrail userIdentity 元素。

了解 Amazon FSx 日志文件条目

一个踪迹是一种配置，可用于将事件作为日志文件传送到您指定的 Amazon S3 存储桶。 CloudTrail 日志文件包含一个或多个日志条目。网络 ACL 和安全组都允许 (因此可到达您的实例) 的发起 ping 的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 CloudTrail 说明`TagResource`从控制台为文件系统创建标签时执行操作。

```
{
    "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 CloudTrail 说明`UntagResource`从控制台删除文件系统标签时执行操作。

```
{
    "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"
}
```

FSx for Windows File Server 性能

FSx for Windows File Server 提供满足各种性能需求的文件系统。以下是 Amazon FSx 文件系统性能的概述，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

概览

文件系统性能是通过其延迟、吞吐量和每秒 I/O 操作数 (IOPS) 来衡量的。

延迟

适用于 Windows File Server 文件服务器的 FSx 使用快速内存缓存，为主动访问的数据实现一致的亚毫秒级延迟。对于不在内存缓存中的数据，即需要通过在底层存储卷上执行 I/O 来完成的文件操作，Amazon FSx 通过固态驱动器 (SSD) 存储提供亚毫秒级的文件操作延迟，使用硬盘驱动器 (HDD) 提供个位数毫秒的延迟存储。

吞吐量和 IOPS

Amazon FSx 文件系统提供高达数 GB/s 的吞吐量和数十万的 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 取决于文件系统的吞吐容量和存储容量配置，以及工作负载的性质，包括活动工作集的大小。

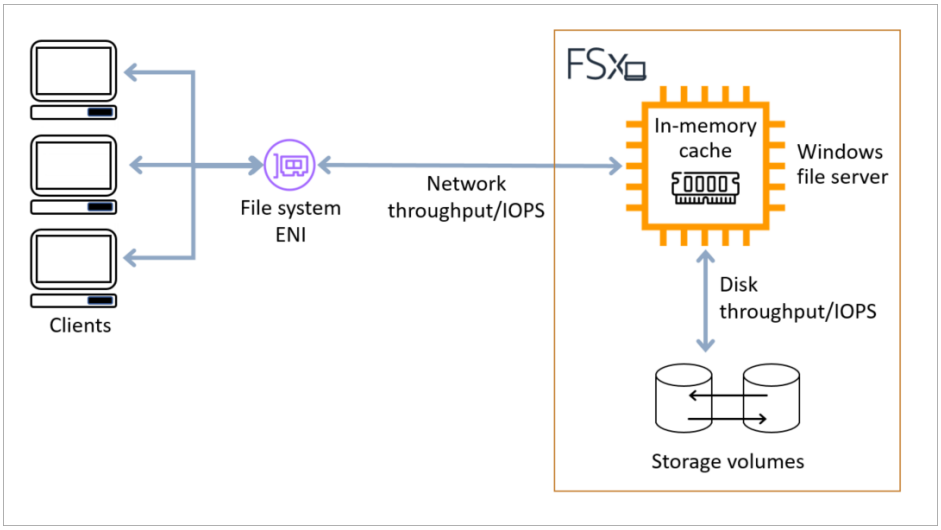
单客户机性能

使用 Amazon FSx，您可以通过访问文件系统的单个客户端获得文件系统的全部吞吐量和 IOPS 级别。Amazon FSx 支持中小型企业多渠道. 此功能使它能够为访问您的文件系统的单个客户端提供高达数GB/s的吞吐量和数十万的IOPS。SMB Multichannel 同时使用客户端和服务器之间的多个网络连接来聚合网络带宽，以最大限度地提高利用率。

性能详细信息

要详细了解 Amazon FSx 性能模型，您可以检查 Amazon 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Amazon或本地，通过elastic network interface (ENI) 访问您的文件系统。此网络接口位于您与文件系统关联的 Amazon VPC 中。文件系统 ENI 的背后是 Windows 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 在文件服务器上提供快速内存缓存，以增强最常访问数据的性能。文件服务器后面是托管文件系统数据的存储卷或磁盘。

下图说明这些组件。



与这些架构组件（网络接口、内存缓存和存储容量）相对应的是 FSx for Windows File Server 文件系统的三个主要性能特征，它们决定了总体吞吐量和 IOPS 性能。

- 网络 I/O 性能：客户端和文件服务器之间请求的吞吐量/IOPS（聚合）
- 文件服务器上的内存缓存大小：可容纳用于缓存的活动工作集的大小
- 磁盘 I/O 性能：文件服务器和存储卷之间请求的吞吐量/IOPS

有两个因素决定了您的文件系统的这些性能特征：存储容量和您为其配置的吞吐容量。前两个性能特征（网络 I/O 性能和内存缓存大小）完全由吞吐量容量决定，而第三个特征（磁盘 I/O 性能）由吞吐容量和存储容量的组合决定。

基于文件的工作负载通常是尖峰的，其特点是高 I/O 时间短而密集，两次突发之间有充足的空闲时间。为了支持高峰工作负载，除了文件系统可以全天候维持的基准速度外，Amazon FSx 还提供了在一段时间内为网络 I/O 和磁盘 I/O 操作突增至更高速度的功能。Amazon FSx 使用网络 I/O 积分机制根据平均利用率分配吞吐量和 IOPS — 文件系统在吞吐量和 IOPS 使用量低于基准限制时累积积分，并且可以在执行 I/O 操作时使用这些积分。

存储容量对性能的影响

存储容量的类型和数量会影响文件系统的性能。您需要配置文件系统所需的存储容量类型和容量，以便为您的工作负载提供所需的性能级别。

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：

- 您的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
- 由您为文件系统选择的存储容量类型和容量提供的磁盘性能级别

您的文件系统的存储提供以下级别的磁盘吞吐量和 IOPS：

存储类型	磁盘吞吐量（每 TiB 存储的兆字节/秒）	磁盘 IOPS（每 TiB 存储的 IOPS）
SSD	750	3000
HDD	12 个基准；80 个突发（每个文件系统最大 1 GB/s）	12 个基线；80 个爆发

您可以随时增加文件系统的存储容量。有关更多信息，请参阅 管理存储容量 (p. 112)。

吞吐量容量对性能的影响

每个 Amazon FSx 文件系统都有您在创建文件系统时配置的吞吐容量。吞吐量容量决定了网络 I/O 性能的级别，也就是说，托管您的文件系统的文件服务器通过网络向访问它的客户端提供文件数据的速度。更高级别的吞吐容量伴随着用于在文件服务器上缓存数据的更多内存，以及文件服务器支持的更高级别的磁盘 I/O 性能。

当您使用 Amazon Web Services 管理控制台创建文件系统时，Amazon FSx 会根据您选择的存储容量自动为您的文件系统选择建议的吞吐容量级别。虽然推荐的吞吐容量应该足以满足大多数工作负载，但您可以选择覆盖建议并选择特定的吞吐容量级别来满足应用程序的需求。创建吞吐容量后，您可以随时增加或减少吞吐容量。有关更多信息，请参阅 管理吞吐量容量 (p. 122)。

下表显示了吞吐容量的全套规格以及基准和突增级别以及文件服务器上的内存量（可用于缓存和用于执行重复数据删除和卷影复制等后台活动的内存）。

Note

下表显示了您在使用 Amazon FSx 控制台时为文件系统选择吞吐容量时可以选择的一组选项。虽然在使用 Amazon FSX API 或 CLI 时，您可以为吞吐容量选择较低级别（8 Mbps 或 16 Mbps），但请记住，8 Mbps 和 16 Mbps 级别适用于测试和开发工作负载，而不是生产工作负载。8 Mbps 和 16 Mbps 的吞吐容量不支持文件访问审计。

FSx 吞吐容量 (Mbps)	网络吞吐容量 (Mbps)		网络 IOPS	内存 (GB)	磁盘吞吐量 (Mbps)		磁盘 IOPS	
	基准	Burst（每天持续几分钟）			基准	爆发（每天 30 分钟）	基准	爆发（每天 30 分钟）
32	32	600	千	4	32	260	2K	12K
64	64	600	数十万	8	64	350	4K	16K
128	150	1,250		8	128	600	6K	20K
256	300	1,250	几十万	16	256	600	10K	20K
512	600	1,250		32	512	–	20K	–
1024	1,500	–		72	1,024	–	40K	–
2,048	3,125	–		144	2,048	–	80K	–

示例：存储容量和吞吐容量

以下示例说明了存储容量和吞吐量容量如何影响文件系统性能。

配置有 2 TiB HDD 存储容量和 32 Mbps 吞吐容量的文件系统具有以下吞吐量级别：

- 网络吞吐量 — 32 Mbps 基准吞吐量和 600 Mbps 突发吞吐量（参见吞吐
- 磁盘吞吐量 — 24 Mbps 基准吞吐量和 160 Mbps 突发吞吐量，这是文件服务器支持的磁盘吞吐量水平 32 Mbps 基准和 260 Mbps 突发吞吐量（基于吞吐容量）以及 24 Mbps 基线（12 Mbps /TB）和 160 Mbps 突发（每 TB 80 Mbps）中的较低值* 2 TB）受存储容量支持。

因此，您访问文件系统的工作负载将能够为文件服务器内存缓存中缓存的正在访问的数据执行的文件操作提高高达 32 Mbps 的基准吞吐量和 600 Mbps 的突增吞吐量，对于需要执行的文件操作，基准吞吐量最高可达 24 Mbps 和 160 Mbps 的突增吞吐量一直到磁盘，例如，由于缓存丢失。

使用以下方法衡量性能 CloudWatch 指标

你可以使用亚马逊 CloudWatch 测量和监控文件系统的吞吐量和 IOPS。有关更多信息，请参阅如何将 FSx for Windows File Server 指标使用 (p. 135)。

Amazon FSx 演练

接下来，你可以找到许多面向任务的演练，指导你完成各种流程。

主题

演练 1：开始使用的先决条件

在完成入门练习之前，您必须已将基于 Microsoft Windows 的 Amazon EC2 实例加入到Amazon Directory Service目录。还必须以目录的管理员用户身份通过 Windows 远程桌面协议登录到实例。以下演练说明了如何执行这些必要的先决条件操作。

主题

第 1 步：设置活动目录

借助 Amazon FSx，您可以为基于 Windows 的工作负载运行完全托管的文件存储。同样，Amazon Directory Service提供完全托管的目录，以便在工作负载部署中使用 如果您在中运行现有的公司 AD 域Amazon在使用 EC2 实例的虚拟私有云 (VPC) 中，您可以启用基于用户的身份验证和访问控制。为此，您可以在您的组织之间建立信任关系。Amazon托管微软 AD 和你的公司域。对于 Amazon FSx 中的 Windows 身份验证，您只需要单向定向林信任，其中Amazon托管林信任公司域林。

您的公司域名扮演受信任域的角色，Amazon Directory Service托管域承担信任域的角色。经过验证的身份验证请求只能沿一个方向在域之间传输，允许公司域中的帐户根据托管域中共享的资源进行身份验证。在这种情况下，Amazon FSx 仅与托管域进行交互。然后，托管域将身份验证请求传递到您的公司域。

> Note
>
> 您还可以将外部信任类型与 Amazon FSx 结合使用来处理受信任域。

您的 Active Directory 安全组必须启用来自 Amazon FSx 文件系统安全组的入站访问权限。

创建Amazon适用于 Microsoft AD 的目录服务

- 如果您还没有，请使用Amazon Directory Service创建Amazon托管的 Microsoft AD 目录。有关更多信息，请参阅 。创建您的Amazon托管的 Microsoft AD 目录中的Amazon Directory Service管理指南.

Important

记住您分配给管理员用户的密码；在本入门练习稍后需要密码。如果忘记了密码，则需要重复本练习中的步骤使用新的Amazon Directory Service目录和管理员用户。

- 如果您有现有 AD，请在您的Amazon管理微软 AD 和你现有的广告。有关更多信息，请参阅 。何时创建信任关系中的Amazon Directory Service管理指南。

第 2 步：在 Amazon EC2 控制台中启动 Windows 实例

可以使用Amazon Web Services Management Console如以下过程所述。这旨在帮助您快速启动第一个实例，因此无法涵盖所有可能的选项。有关高级选项的更多信息，请参阅启动实例。

启动实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从控制台控制面板中，选择启动实例。
3. Choose an Amazon Machine Image (AMI) 页面显示一组称为 Amazon Machine Image (AMI) 的基本配置，作为您的实例的模板。选择适用于 Windows Server 2016 Base 的 AMI 或 Windows Server 2012 R2 Base。请注意，这些 AMI 标记为“Free tier eligible”(符合条件的免费套餐)。
4. 在 Choose an Instance Type (选择实例类型) 页面上，您可以选择实例的硬件配置。选择 `t2.micro` 类型 (预设情况下的选择)。请注意，此实例类型适用免费套餐。
5. 选择 Review and Launch 让向导为您完成其它配置设置。
6. 在存储库的核查实例启动页面，下个安全组，将显示向导为您创建并选择的安全组。可以使用此安全组，也可以按照以下步骤选择您在设置时创建的安全组：

   a. 选择 Edit security groups。
   b. 在 Configure Security Group 页面上，确保 Select an existing security group 处于选中状态。
   c. 从现有安全组列表中选择您的安全组，然后选择 Review and Launch。
7. 在 Review Instance Launch 页面上，选择 Launch。
8. 当系统提示提供密钥时，选择 Choose an existing key pair，然后选择您在进行设置时创建的密钥对。

   另外，您也可以新建密钥对。选择 Create a new key pair，输入密钥对的名称，然后选择 Download Key Pair。这是您保存私有密钥文件的唯一机会，因此务必单击进行下载。将私有密钥文件保存在安全位置。当您启动实例时，您将需要提供密钥对的名称；当您每次连接到实例时，您将需要提供相应的私有密钥。

   Warning

   请勿选择在没有密钥对的情况下继续选项。如果您启动的实例没有密钥对，就不能连接到该实例。

   准备好后，选中确认复选框，然后选择 Launch Instances。
9. 确认页面会让您知道自己的实例已启动。选择 View Instances 以关闭确认页面并返回控制台。
10. 在实例屏幕上，您可以查看启动状态。启动实例只需很短的时间。启动实例时，其初始状态为 `pending`。实例启动后，其状态变为 `running`，并且会收到一个公有 DNS 名称。(如果 Public DNS (IPv4) 列已隐藏，请选择页面右上角的 Show/Hide Columns (齿轮状图标)，然后选择 Public DNS (IPv4)。)
11. 需要几分钟准备好实例，以便您能连接到实例。检查您的实例是否通过了状态检查；您可以在 Status Checks 列中查看此信息。

Important

记下启动此实例时创建的安全组的 ID。当您创建 Amazon FSx 文件系统时，您将需要此信息。

现在实例已启动，您可以连接到您的实例。

第 3 步：连接到您的实例

要连接到 Windows 实例，您必须检索初始管理员密码，然后在使用远程桌面连接到实例时指定此密码。

管理员账户的名称取决于操作系统的语言。例如，英语为 Administrator，法语为 Administrator，葡萄牙语则为 Administrator。有关更多信息，请参阅 Microsoft TechNet Wiki 中的 Windows 管理员账户的本地化名称。

如果您将实例加入到域，则可以使用您在中定义的域凭证连接到您的实例。Amazon Directory Service. 在远程桌面登录屏幕上，不要使用本地计算机名称和生成的密码。相反，请使用管理员的完全限定用户名和此帐户的密码。示例是 **`corp.example.com\Admin`**。

出于管理目的，Windows Server 操作系统 (OS) 的许可证允许同时进行两个远程连接。适用于 Windows Server 的许可证包含在您的 Windows 实例的价格中。如果您需要同时进行两个以上的远程连接，则必须购买远程桌面服务 (RDS) 许可证。如果尝试第三个连接，将产生错误。有关更多信息，请参阅 。配置连接允许的同时远程连接数.

使用 RDP 客户端连接到 Windows 实例

1. 在 Amazon EC2 控制台中，选择实例，然后选择 Connect (连接)。
2. 在连接到您的实例对话框中，选择获取密码（密码在实例启动几分钟之后才可用）。
3. 选择 Browse 并导航至您启动实例时所创建的私有密钥文件。选择文件并选择 Open (打开)，以便将文件的全部内容复制到 Contents (内容) 字段。
4. 选择 Decrypt Password。控制台将在连接到您的实例对话框，将链接替换到获取密码之前用实际密码显示。
5. 记录下默认管理员密码，或将其复制到剪贴板。需要使用此密码连接实例。
6. 选择 Download Remote Desktop File。您的浏览器会提示您打开或保存 .rdp 文件。两种选择都可以。完成后，可以选择Close要解雇连接到您的实例对话框。

   - 如果已打开 .rdp 文件，您将看到 Remote Desktop Connection 对话框。
   - 如果已保存 .rdp 文件，请导航至下载目录，然后打开 .rdp 文件以显示该对话框。
7. 您可能看到一条警告，指出远程连接发布者未知。您可以继续连接到您的实例。
8. 当收到系统提示时，使用操作系统的管理员账户和您之前记录或复制的密码登录该实例。如果您的 Remote Desktop Connection (远程桌面连接) 已经设置了管理员账户，您可能需要选择 Use another account (使用其他账户) 选项，然后手动键入用户名和密码。

   Note

   有时复制和粘贴内容可能会损坏数据。如果您在登录时遇到“Password Failed (密码失败)”错误，请尝试手动键入密码。
9. 由于自签名证书的固有特性，您可能会看到一条警告，指出无法验证该安全证书。请使用以下步骤验证远程计算机的标识；或者，如果您信任该证书，则直接选择 Yes (是) 或 Continue (继续) 以继续操作。

   a. 如果您正在从 Windows PC 使用 Remote Desktop Connection，请选择 View certificate。如果您正在 Mac 上使用 Microsoft Remote Desktop，请选择 Show Certificate。
   b. 选择 Details (详细信息) 选项卡，并向下滚动到 Thumbprint (指纹) 条目（在 Windows PC 上）或 SHA1 Fingerprints (SHA1 指纹) 条目（在 Mac 上）。这是远程计算机的安全证书的唯一标识符。
   c. 在 Amazon EC2 控制台中，选择该实例，选择 Actions (操作)，然后选择 Get System Log (获取系统日志)。
   d. 在系统日志输出中，查找标记为 `RDPCERTIFICATE-THUMBPRINT` 的条目。如果此值与证书的指纹匹配，则表示您已验证了远程计算机的标识。
   e. 如果您正在从 Windows PC 使用 Remote Desktop Connection，请返回到 Certificate 对话框并选择 OK。如果您正在 Mac 上使用 Microsoft Remote Desktop，请返回到 Verify Certificate 并选择 Continue。

f. [Windows] 在 Remote Desktop Connection 窗口中选择 Yes 连接到您的实例。

现在您已连接到实例，可以将实例加入到Amazon Directory Service目录。

第 4 步：将你的实例加入你的Amazon Directory Servicedirectory

以下过程说明了如何将现有 Amazon EC2 Windows 实例手动加入到Amazon Directory Service目录。

将 Windows 实例加入Amazon Directory Servicedirectory

1. 使用任何远程桌面协议客户端连接到实例。
2. 在实例上打开 TCP/IPv4 属性对话框。
   a. 打开 Network Connections。

      Tip

      您可以在实例上从命令提示符运行以下命令，直接打开 Network Connections。

      ```
      %SystemRoot%\system32\control.exe ncpa.cpl
      ```

   b. 打开任何已启用网络连接的上下文 (右键单击) 菜单，然后选择属性.
   c. 在连接属性对话框中，打开 (双击) Internet Protocol Version 4。
3. （可选）选择使用以下 DNS 服务器地址，更改首选 DNS 服务器和备用 DNS 服务器的 IP 地址的地址 Amazon Directory Service— 提供 DNS 服务器，然后选择确定.
4. 打开系统属性对于实例的对话框，选择计算机名称选项卡，然后选择变更.

   Tip

   您可以在实例上从命令提示符运行以下命令，打开 System Properties 对话框。

   ```
   %SystemRoot%\system32\control.exe sysdm.cpl
   ```

5. 在成员框中，选择域中，输入完全限定的名称Amazon Directory Service目录，然后选择确定.
6. 当系统提示您输入域管理员的名称和密码时，输入 Admin 帐户的用户名和密码。

   Note

   您可以输入域的完全限定名称，也可以输入 NetBios name，后跟反斜杠 (\)，然后是用户名 (在此例中为)管理员. 例如，corp.example.com\Admin 或 corp\Admin。
7. 收到欢迎加入域的消息之后，重新启动实例使更改生效。
8. 通过 RDP 重新连接到您的实例，然后使用您的用户名和密码登录实例。Amazon Directory Service目录的管理员用户。

现在实例已加入域，您可以创建 Amazon FSx 文件系统。然后，你可以继续完成入门练习中的其他任务。有关更多信息，请参阅开始使用 Amazon FSx (p. 7)。

演练 2：从备份创建文件系统

使用 Amazon FSx，您可以从备份创建文件系统。执行此操作时，可以更改以下任意元素，以更好地适应新创建的文件系统的使用案例：

- 存储类型
- 吞吐量容量
- VPC
- 可用区：
- 子网
- VPC 安全组
- Active Directory 配置
- Amazon KMS加密密钥
- 每日自动备份开始时间
- 每周维护时段

以下过程将指导您完成从备份创建新文件系统的过程。在创建该文件系统之前，您必须拥有现有备份。有关更多信息，请参阅 。使用备份 (p. 71)

从现有备份创建文件系统

1. 从打开 Amazon FSx 控制台https://console.aws.amazon.com/fsx/.
2. 从右侧的导航列表中，选择备份.
3. 从仪表板上的表格中，选择要用于创建新文件系统的备份。

   Note

   您只能将备份还原到与原始备份具有相同存储容量的文件系统中。您可以在恢复的文件系统可用后增加它的存储容量。有关更多信息，请参阅 管理存储容量 (p. 112)。
4. 选择 Restore backup (还原备份)。这将开始创建文件系统向导。
5. 选择要为此新文件系统更改的设置。存储类型设置为SSD默认情况下，您可以将其更改为HDD在以下情况下：

   - 文件系统部署类型为多可用区要么单可用区 2.
   - 存储容量至少为 2,000 GiB。
6. 选择审阅摘要以便在创建文件系统之前查看您的设置。
7. 选择 Create file system。

现在，您已从现有备份中成功创建新文件系统。

演练 3：更新现有文件系统

您可以使用本演练中的步骤更新三个要素。可以更新的文件系统中的所有其他元素，可以从控制台执行此操作。这些过程假设你有Amazon CLI在本地计算机上安装并配置的。有关更多信息，请参阅 。安装和配置中的Amazon Command Line Interface用户指南.

- AutomaticBackupRetentionDays— 您希望自动备份保留文件系统自动备份的天数。
- DailyAutomaticBackupStartTime— 以协调世界时 (UTC) 表示的您希望每日自动备份启动时段的时间。从这个指定时间开始，窗口为 30 分钟。此时段不能与每周维护备份时段重叠。
- WeeklyMaintenanceStartTime— 您希望维护时段开始的一周中的时间。第 1 天是星期一，2 是星期二，依此类推。从这个指定时间开始，窗口为 30 分钟。此时段不能与每日自动备份时段重叠。

以下过程概述如何使用Amazon CLI.

更新文件系统的自动备份保留多长时间

1. 在计算机上打开命令提示符或终端。
2. 运行以下命令，将文件系统 ID 替换为文件系统的 ID 和要保留自动备份的天数。

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-
configuration AutomaticBackupRetentionDays=30
```

更新文件系统的每日备份窗口

1. 在计算机上打开命令提示符或终端。
2. 运行以下命令，将文件系统 ID 替换为文件系统的 ID 以及开始窗口的时间。

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-
configuration DailyAutomaticBackupStartTime=01:00
```

更新文件系统的每周维护时段

1. 在计算机上打开命令提示符或终端。
2. 运行以下命令，将文件系统 ID 替换为文件系统的 ID 以及开始窗口的日期和时间。

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-
configuration WeeklyMaintenanceStartTime=1:01:30
```

演练 4：在亚马逊上使用亚马逊 FSx AppStream 2.0

通过支持服务器消息块 (SMB) 协议，适用于 Windows 文件服务器的 Amazon FSx 支持从 Amazon EC2、VMware Cloud 上访问您的文件系统Amazon、Amazon WorkSpaces 和亚马逊 AppStream 2.0 个实例。 AppStream 2.0 是完全托管的应用程序流媒体服务。您在上集中管理桌面应用程序 AppStream 2.0 并将它们安全地传送到任何计算机上的浏览器。有关 AppStream 2.0，请参阅亚马逊 AppStream 2.0 管理指南.

使用此演练作为指南，了解如何使用 Amazon FSx AppStream 2.0 适用于两个用例：为每个用户提供个人持久存储空间，并在用户之间提供共享文件夹以访问通用文件。

为每个用户提供个人持久存储

您可以使用 Amazon FSx 为组织中的每位用户提供唯一的存储驱动器 AppStream 2.0 流会话。用户只有访问其文件夹的权限。驱动器会在流式传输会话开始时自动挂载，并且添加或更新到驱动器的文件将在流式传输会话之间自动保留。

要完成此任务，您需要执行三个过程。

使用 Amazon FSx 为域用户创建主文件夹

1. 创建 Amazon FSx 文件系统。有关更多信息，请参阅 开始使用 Amazon FSx (p. 7)。
2. 在文件系统可用后，为每个域创建一个文件夹。 AppStream 亚马逊 FSx 文件系统中的 2.0 个用户。以下示例使用用户的域用户名作为相应文件夹的名称。这样做意味着您可以使用 Windows 环境变量构建文件共享的 UNC 名称，以便轻松映射`%username%`.
3. 将这些文件夹中的每个文件夹共享为共享文件夹。有关更多信息，请参阅 文件共享 (p. 87)。

启动加入域的步骤 AppStream 2.0 映像生成器

1. 登录到 AppStream 2.0 控制台：https://console.aws.amazon.com/appstream2
2. 选择目录配置从导航菜单中创建一个目录 Config 对象。有关更多信息，请参阅 。将 Active Directory 与结合使用 AppStream 2.0中的亚马逊 AppStream 2.0 管理指南.
3. 选择映像、映像生成器，然后启动一个新映像生成器。
4. 选择在映像生成器启动向导中之前创建的目录配置对象，将映像生成器加入 Active Directory 域。
5. 在与 Amazon FSx 文件系统相同的 VPC 中启动映像构建器。确保将图像构建器与相同的图像构建器关联Amazon Managed Microsoft AD您的 Amazon FSx 文件系统已加入的目录。与映像构建器关联的 VPC 安全组必须允许访问 Amazon FSx 文件系统。
6. 映像构建器可用后，连接到映像构建器并使用域管理员帐户登录。
7. 安装应用程序。

将亚马逊 FSx 文件共享链接到 AppStream 2.0

1. 在映像构建器中，使用以下命令创建批处理脚本，然后将其存储在已知文件位置（例如：C:\Scripts\map-fs.bat）。以下示例使用 S: 作为驱动器盘符来映射 Amazon FSx 文件系统上的共享文件夹。您可以在此脚本中使用 Amazon FSx 文件系统的 DNS 名称或与文件系统关联的 DNS 别名，您可以从 Amazon FSx 控制台的文件系统详细信息视图中获取该名称。

   如果您使用文件系统的 DNS 名称：

   ```
   @echo off
   net use S: /delete
   net use S: \\file-system-DNS-name\users\%username%
   ```

   如果您使用的是与文件系统关联的 DNS 别名：

   ```
   @echo off
   net use S: /delete
   net use S: \\fqdn-DNS-alias\users\%username%
   ```

2. 打开 PowerShell 提示并运行`gpedit.msc`.
3. 从用户配置选择Windows 设置然后登录.
4. 导航到您在此过程的第一步中创建的批处理脚本，然后选择它。
5. 从计算机配置，选择Windows 管理模板、系统，然后组策略.
6. 选择策略配置登录脚本延迟. 启用策略并减少时间延迟0. 此设置有助于确保在用户启动流式传输会话时立即执行用户登录脚本。
7. 创建你的图片并将其分配给 AppStream 2.0 队列。确保你也加入 AppStream 2.0 队列与您用于映像构建器的同一 Active Directory 域。在 Amazon FSx 文件系统使用的同一 VPC 中启动队列。您与队列关联的 VPC 安全组必须提供对 Amazon FSx 文件系统的访问权限。
8. 使用 SAML SSO 启动串流会话。要连接到加入 Active Directory 的队列，请使用 SAML 提供程序配置单点登录联合身份验证。有关更多信息，请参阅 。访问单点登录访问 AppStream 2.0 使用 SAML 2.0中的亚马逊 AppStream 2.0 管理指南.
9. 您的 Amazon FSx 文件共享映射到串流会话中的 S: 驱动器盘符。

在用户之间提供共享文件夹

您可以使用 Amazon FSx 向组织中的用户提供共享文件夹。共享文件夹可用于维护所有用户所需的常用文件（例如演示文件、代码示例、说明手册等）。

要完成此任务，您需要执行三个过程。

使用 Amazon FSx 创建共享文件夹

1. 创建 Amazon FSx 文件系统。有关更多信息，请参阅 开始使用 Amazon FSx (p. 7)。
2. 默认情况下，每个 Amazon FSx 文件系统都包含一个共享文件夹，您可以使用地址*#### DNS #*\ 共享，或者*FQDN-DNS-##*\ 如果您使用的是 DNS 别名，请分享。您可以使用默认共享或创建其他共享文件夹。有关更多信息，请参阅 文件共享 (p. 87)。

启动 AppStream 2.0 映像生成器

1. 从 AppStream 2.0 控制台，启动新的映像构建器或连接到现有的映像构建器。在 Amazon FSx 文件系统使用的同一 VPC 中启动映像构建器。与映像构建器关联的 VPC 安全组必须允许访问 Amazon FSx 文件系统。
2. 映像构建器可用后，以管理员用户身份连接到映像构建器。
3. 以管理员身份安装或更新应用程序。

将共享文件夹链接到 AppStream 2.0

1. 创建批处理脚本（如上一过程中所述），以便在用户启动流会话时自动挂载共享文件夹。要完成脚本，您需要文件系统的 DNS 名称或与文件系统关联的 DNS 别名（您可以从 Amazon FSx 控制台的文件系统详细信息视图中获取）以及用于访问共享文件夹的凭据。

   如果您使用文件系统的 DNS 名称：

   ```
   @echo off
   net use S: /delete
   net use S: \\file-system-DNS-name\share /user:username password
   ```

   如果您使用的是与文件系统关联的 DNS 别名：

   ```
   @echo off
   net use S: /delete
   net use S: \\fqdn-DNS-alias\share /user:username password
   ```

2. 创建组策略以在每次用户登录时执行此批处理脚本。您可以按照上一部分中介绍的相同说明进行操作。
3. 创建你的映像并将其分配给你的车队。
4. 启动流会话。现在，您应该看到共享文件夹自动映射到驱动器盘符。

演练 5：使用 DNS 别名访问文件系统

FSx for Windows File Server 为每个文件系统提供一个默认的域名系统 (DNS) 名称，您可以使用该名称访问文件系统上的数据。您还可以使用自己选择的 DNS 别名访问文件系统。借助 DNS 别名，在将文件系统存储从本地迁移到 Amazon FSx 时，您可以继续使用现有 DNS 名称访问存储在 Amazon FSx 上的数据，而无需更新任何工具或应用程序。您可以同时将最多 50 个 DNS 别名与文件系统关联。

要使用 DNS 别名访问您的 Amazon FSx 文件系统，您必须执行以下三个步骤：

1. 将 DNS 别名与您的亚马逊 FSx 文件系统关联。
2. 为文件系统的计算机对象配置服务主体名称 (SPN)。（这是在使用 DNS 别名访问文件系统时获得 Kerberos 身份验证所必需的。）

3. 为文件系统和 DNS 别名更新或创建 DNS 别名记录。

主题

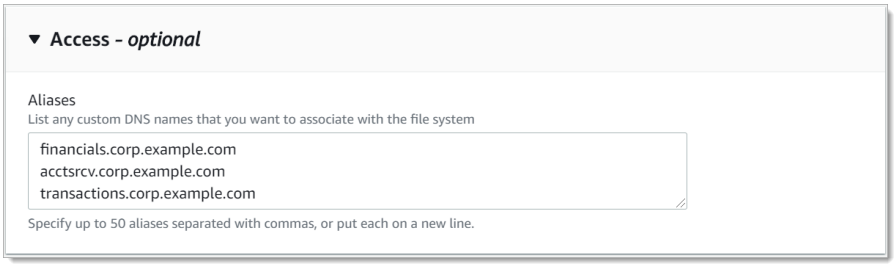
第 1 步：将 DNS 别名与您的亚马逊 FSx 文件系统关联

在创建新文件系统时，以及使用 Amazon FSx 控制台、CLI 和 API 从备份创建新文件系统时，您可以将 DNS 别名与现有 FSx for Windows 文件服务器文件系统相关联。如果要使用其他域名创建别名，请输入全名（包括父域）以关联别名。

此过程介绍在使用 Amazon FSx 控制台创建新文件系统时如何关联 DNS 别名。有关将 DNS 别名与现有文件系统关联的信息，以及有关使用 CLI 和 API 的详细信息，请参阅管理 DNS 别名 (p. 82).

在创建新文件系统时关联 DNS 别名

1. 从打开 Amazon FSx 控制台https://console.aws.amazon.com/fsx/.
2. 按照创建新文件系统的过程进行操作，如中所述第 1 步：创建文件系统 (p. 7)“入门” 一节中的。
3. 在访问-可选的 部分创建文件系统向导中，输入要与您的文件系统关联的 DNS 别名。



   指定 DNS 别名时遵循以下准则：

   - 必须格式化为完全限定域名 (FQDN)*hostname.domain*，例如，`accounting.example.com`.
   - 可以包含字母数字字符和连字符 (-)。
   - 不得以连字符开头或结尾。
   - 可以使用数字开头。

   对于 DNS 别名，Amazon FSx 会将字母字符存储为小写字母 (a-z)，无论您指定将其存储为大写字母、小写字母还是转义码中的对应字母。
4. 适用于维护偏好，执行所需的任何更改。
5. 在标签-可选部分中，添加所需的任何标签，然后选择下一步.
6. 检查创建文件系统页面上显示的文件系统配置。选择创建文件系统创建文件系统。

   当您的新文件系统变为可用时，请继续步骤 2。

第 2 步：为 Kerberos 配置服务主体名称 (SPN)

我们建议您在 Amazon FSx 中使用基于 Kerberos 的身份验证和加密。Kerberos 为访问文件系统的客户端提供最安全的身份验证。

要为使用 DNS 别名访问 Amazon FSX 的客户端启用 Kerberos 身份验证，您必须添加与 Amazon FSx 文件系统的 Active Directory 计算机对象上的 DNS 别名相对应的服务主体名称 (SPN)。SPN 同时只能与一个 Active Directory 计算机对象关联。如果您有为原始文件系统的 Active Directory 计算机对象配置的 DNS 名称的现有 SPN，则必须先将其删除。

Kerberos 身份验证有两个必需的 SPN：

```
HOST/alias
HOST/alias.domain
```

如果别名是`finance.domain.com`，以下是两个必需的 SPN：

```
HOST/finance
HOST/finance.domain.com
```

> **Note**
>
> 在为 Amazon FSx 文件系统的 Active Directory (AD) 计算机对象创建新的 HOST SPN 之前，您需要删除与 Active Directory 计算机对象上的 DNS 别名对应的所有现有 HOST SPN。如果 AD 中存在 DNS 别名的 SPN，则尝试为您的 Amazon FSx 文件系统设置 SPN 将失败。

以下过程介绍了如何执行以下操作：

- 在原始文件系统的 Active Directory 计算机对象上查找任何现有 DNS 别名 SPN。
- 删除找到的现有 SPN（如果有）。
- 为您的 Amazon FSx 文件系统的 Active Directory 计算机对象创建新的 DNS 别名 SPN。

安装所需的 PowerShell “Active D

1. 登录已加入您的 Amazon FSx 文件系统所加入的活动目录的 Windows 实例。
2. 打开 PowerShell 作为管理员。
3. 安装 PowerShell Active Directory 模块使用以下命令。

```
Install-WindowsFeature RSAT-AD-PowerShell
```

查找和删除原始文件系统的 Active Directory 计算机对象上的现有 DNS 别名 SPN

1. 使用以下命令查找任何现有的 SPN。Replace*alias_fqdn*使用您与中的文件系统关联的 DNS 别名步骤 1 (p. 153).

```
## Find SPNs for original file system's AD computer object
$ALIAS = "alias_fqdn"
SetSPN /Q ("HOST/" + $ALIAS)
SetSPN /Q ("HOST/" + $ALIAS.Split(".")[0])
```

2. 使用以下示例脚本删除上一步中返回的现有 HOST SPN。
   - Replace*alias_fqdn*使用您在中与文件系统关联的完整 DNS 别名步骤 1 (p. 153).
   - Replace*file_system_DNS_name*使用原始文件系统的 DNS 名称。

```
## Delete SPNs for original file system's AD computer object
$Alias = "alias_fqdn"
$FileSystemDnsName = "file_system_dns_name"
```

```
$FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})

SetSPN /D ("HOST/" + ${Alias}) ${FSxAdComputer}.Name
SetSPN /D ("HOST/" + ${Alias}.Split(".")[0]) ${FSxAdComputer}.Name
```

3. 对与中的文件系统关联的每个 DNS 别名重复上述步骤步骤 1 (p. 153).

在 Amazon FSx 文件系统的 Active Directory 计算机对象上设置 SPN

1. 通过运行以下命令为您的 Amazon FSx 文件系统设置新的 SPN。

   - Replace*file_system_DNS_name*使用 Amazon FSx 分配给文件系统的 DNS 名称。

     要在 Amazon FSx 控制台上查找文件系统的 DNS 名称，请选择文件系统，选择您的文件系统，然后选择网络和安全性”窗格位于文件系统详细信息页面上。

     你也可以在响应中获取 DNS 名称DescribeFileSystemsAPI 操作。
   - Replace*alias_fqdn*使用您在中与文件系统关联的完整 DNS 别名步骤 1 (p. 153).

```
## Set SPNs for FSx file system AD computer object
$FSxDnsName = "file_system_DNS_name"
$Alias = "alias_fqdn"
$FileSystemHost = (Resolve-DnsName $FSxDnsName | Where Type -eq 'A')[0].Name.Split(".")
[0]
$FSxAdComputer = (Get-AdComputer -Identity $FileSystemHost)

Set-AdComputer -Identity $FSxAdComputer -Add @{"msDS-AdditionalDnsHostname"="$Alias"}
SetSpn /S ("HOST/" + $Alias.Split('.')[0]) $FSxAdComputer.Name
SetSpn /S ("HOST/" + $Alias) $FSxAdComputer.Name
```

   Note

   如果原始文件系统的计算机对象的 AD 中存在 DNS 别名的 SPN，则为 Amazon FSx 文件系统设置 SPN 将失败。有关查找和删除现有 SPN 的信息，请参阅查找和删除原始文件系统的 Active Directory 计算机对象上的现有 DNS 别名 SPN (p. 154).

2. 使用以下示例脚本验证是否为 DNS 别名配置了新 SPN。确保响应中包含两个 HOST SPN，`HOST/`*alias*和`HOST/`*alias_fqdn*，如本过程前面的中所述。

   Replace*file_system_DNS_name*使用 Amazon FSx 分配给您的文件系统的 DNS 名称。要在 Amazon FSx 控制台上查找文件系统的 DNS 名称，请选择文件系统，选择您的文件系统，然后选择网络和安全性”窗格位于文件系统详细信息页面上。

   你也可以在响应中获取 DNS 名称DescribeFileSystemsAPI 操作。

```
## Verify SPNs on FSx file system AD computer object
$FileSystemDnsName = "file_system_dns_name"
$FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})
SetSpn /L ${FSxAdComputer}.Name
```

3. 对与中的文件系统关联的每个 DNS 别名重复上述步骤步骤 1 (p. 153).

有关如何强制客户端在连接到 Amazon FSx 文件系统时使用 Kerberos 身份验证和加密的信息，请参阅使用 GPO 强制执行 Kerberos 身份验证 (p. 157).

第 3 步：更新或创建文件系统的 DNS CNAME 记录

为文件系统正确配置 SPN 后，您可以将解析到原始文件系统的每个 DNS 记录替换为解析为 Amazon FSx 文件系统的默认 DNS 名称的 DNS 记录，从而切换到 Amazon FSx。

这些区域有：dnsserver和activedirectory运行本节中介绍的命令需要 Windows 模块。

安装所需的 PowerShell cmdlet

1. 以具有 DNS 管理权限的组成员的身份登录到加入您的 Amazon FSx 文件系统的 Active Directory 的 Windows 实例（AmazonAmazon域名系统委托管理员在AmazonManaged Active DiDomain Admins或您在自己管理的 Active Directory 中委派了 DNS 管理权限的其他组）。

   有关更多信息，请参阅适用于 Windows 实例的 Amazon EC2 用户指南中的连接您的 Windows 实例。
2. 打开 PowerShell 作为管理员。
3. 这些区域有： PowerShell DNS 服务器模块是执行本过程中的说明所必需的。使用以下命令安装它。

```
Install-WindowsFeature RSAT-DNS-Server
```

更新或创建您的 Amazon FSx 文件系统的自定义 DNS 名称

1. 以具有 DNS 管理权限的组成员的用户身份Connect 您的 Amazon EC2 实例（Amazon域名系统委托管理员在AmazonManaged Active DiDomain Admins或您在自己管理的 Active Directory 中委派了 DNS 管理权限的其他组）。

   有关更多信息，请参阅适用于 Windows 实例的 Amazon EC2 用户指南中的连接您的 Windows 实例。
2. 在命令提示符下，运行以下脚本。此脚本会将任何现有的 DNS CNAME 记录迁移到您的 Amazon FSx 文件系统。如果未找到，则会为 DNS 别名创建一个新的 DNS 别名记录*alias_fqdn*它会解析为您的 Amazon FSx 文件系统的默认 DNS 名称。

   要运行脚本，请执行以下操作：

   - Replace*alias_fqdn*使用您与文件系统关联的 DNS 别名。
   - Replace*file_system_DNS_name*使用 Amazon FSx 已分配给文件系统的 DNS 名称。

```
$Alias="alias_fqdn"
$FSxDnsName="file_system_dns_name"
$AliasHost=$Alias.Split('.')[0]
$ZoneName=((Get-WmiObject Win32_ComputerSystem).Domain)
$DnsServerComputerName = (Resolve-DnsName $ZoneName -Type NS | Where Type -eq 'A' |
 Select -ExpandProperty Name)

Add-DnsServerResourceRecordCName -Name $AliasHost -ComputerName $DnsServerComputerName
 -HostNameAlias $FSxDnsName -ZoneName $ZoneName
```

3. 对与中的文件系统关联的每个 DNS 别名重复上一步骤步骤 1 (p. 153).

现在，您已使用 DNS 别名为亚马逊 FSx 文件系统添加了 DNS 别名记录值。您现在可使用 DNS 别名访问您的数据。

> **Note**
>
> 更新 DNS CNAME 记录以指向先前指向另一个文件系统的 Amazon FSx 文件系统时，客户端可能在短时间内无法与文件系统连接。当客户端 DNS 缓存刷新时，它们应该能够使用 DNS 别名进行连接。有关更多信息，请参阅无法使用 DNS 别名访问文件系统 (p. 189)。

使用 GPO 强制执行 Kerberos 身份验证

在访问文件系统时，可以通过在 Active Directory 中设置以下组策略对象 (GPO) 来强制执行 Kerberos 身份验证：

- 限制 NTLM: 向远程服务器传出 NTLM 流量-使用此策略设置拒绝或审核从计算机到运行 Windows 操作系统的任何远程服务器的传出 NTLM 通信。
- 限制 NTLM: 为 NTLM 身份验证添加远程服务器例外-使用此策略设置创建允许客户端设备使用 NTLM 身份验证的远程服务器的例外列表，如果网络安全: 限制 NTLM: 向远程服务器传出 NTLM 流量策略设置已配置。

1. 登录已加入活动目录的 Windows 实例，您的 Amazon FSx 文件系统已以管理员身份加入该实例。如果您正在配置自我管理的 Active Directory，请将这些步骤直接应用于活动目录。
2. 选择启动，选择管理工具，然后选择组策略管理.
3. 选择组策略对象.
4. 如果您的组策略对象尚不存在，您可以创建它。
5. 找到现有的网络安全: 限制 NTLM: 向远程服务器传出 NTLM 流量政策。（如果没有现有策略，您可以创建新策略。）在本地安全设置选项卡，打开上下文 (右键单击) 菜单，然后选择属性.
6. 选择全部拒绝.
7. 选择Apply保存安全设置。
8. 要为客户端的特定远程服务器的 NTLM 连接设置例外，请找到网络安全: 限制 NTLM: 添加远程服务器例外.

   打开上下文 (右键单击) 菜单，然后选择属性中的本地安全设置选项卡。
9. 输入要添加到例外列表的任何服务器的名称。
10. 选择Apply保存安全设置。

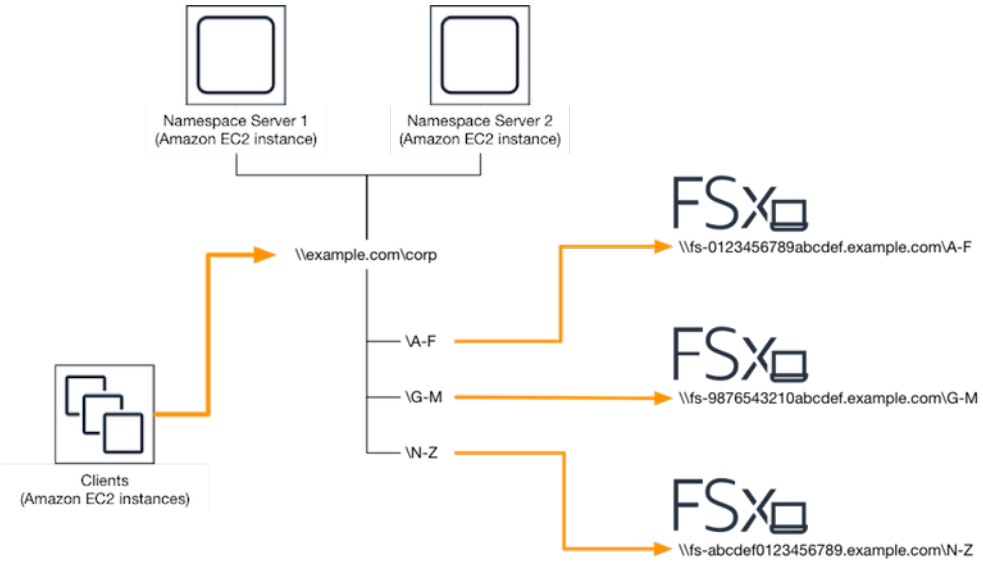
演练 6：利用分片扩展性能

适用于 Windows 文件服务器的亚马逊 FSx 支持使用微软分布式文件系统 (DFS)。通过使用 DFS 命名空间，您可以通过在多个 Amazon FSx 文件系统中传播文件数据来扩展性能（读取和写入）以服务 I/O 密集型工作负载。同时，您仍然可以在公共命名空间下向应用程序呈现统一视图。此解决方案涉及将文件数据划分为较小的数据集，或鞘翅并将它们存储在不同的文件系统中。从多个实例访问数据的应用程序可以通过并行读取和写入这些分片来实现高水 parallel 的性能。

当您的工作负载需要对文件数据进行均匀分布的读/写访问（例如，每个计算实例子集访问文件数据的不同部分）时，您可以使用此解决方案。

设置 DFS 命名空间以实现横向扩展性能

以下过程将指导您在 Amazon FSx 上创建 DFS 解决方案，以实现横向扩展性能。在此示例中，存储在*Corp*命名空间按字母顺序进行分片。数据文件 “A-F”、“G-M” 和 “N-Z” 都存储在不同的文件共享中。根据数据类型、I/O 大小和 I/O 访问模式，您应该决定如何在多个文件共享之间最好地分片数据。选择在计划使用的所有文件共享之间均匀分配 I/O 的分片约定。请记住，每个命名空间总共支持多达 50,000 个文件共享和数百 PB 的存储容量。



为横向扩展性能设置 DFS 命名空间

1. 如果您尚未运行 DFS 命名空间服务器，则可以使用设置-dfsn-Server。模板 Amazon CloudFormationTemplate。有关创建Amazon CloudFormation堆栈，请参阅在上创建堆栈Amazon CloudFormation 控制台中的Amazon CloudFormation用户指南.
2. 以用户身份 Connect 到在上一步中启动的 DFS 命名空间服务器之一Amazon委托管理员组中)。有关更多信息，请参阅适用于 Windows 实例的 Amazon EC2 用户指南中的连接您的 Windows 实例。
3. 访问 DFS 管理控制台。打开启动运行菜单并运行dfsmgmt.msc. 这将打开 DFS 管理 GUI 工具。
4. 选择操作然后新命名空间中，键入您为其启动的第一个 DFS 命名空间服务器的计算机名称服务器然后选择下一步.
5. 适用于名称，键入你正在创建的命名空间（例如，Corp)。
6. 选择编辑设置并根据您的要求设置适当的权限。选择 Next（下一步）。
7. 保留默认值基于域的命名空间选择选项，请保留启用 Windows Server 2008 模式选项已选中，然后选择下一步.

   Note

   Windows Server 2008 模式是命名空间的最新可用选项。
8. 查看命名空间设置并选择Create.
9. 在下面选择了新创建的命名空间命名空间在导航栏中，选择操作然后添加命名空间 Server.
10. 输入您为其启动的第二个 DFS 命名空间服务器的计算机名称命名空间 Server.
11. 选择编辑设置，根据要求设置适当的权限，然后选择。确定.
12. 打开刚刚创建的命名空间的上下文 (右键单击) 菜单，选择。新建文件夹，输入第一个分片的文件夹的名称 (例如，`A-F`为了名称)，然后选择Add.
13. 以 UNC 格式输入托管此分片的文件共享的 DNS 名称（例如，`\\fs-0123456789abcdef0.example.com\A-F`) 对于文件夹目标的路径然后选择确定.
14. 如果该份额不存在：

    a. 选择是来创建它。
    b. 从创建共享对话框，选择浏览.
    c. 在下选择现有文件夹，或在下面创建一个文件夹。D$，然后选择确定.
    d. 设置适当的共享权限，然后选择确定.
15. 现在为分片添加了文件夹目标，请选择确定.

16. 对要添加到同一命名空间的其他分片重复最后四个步骤。

演练 7：将备份复制到另一个备份Amazon Web Services 区域

使用 Amazon FSx，您可以在同一个备份中复制现有备份Amazon Web Services 账户到另一个Amazon Web Services 区域（跨区域备份副本）或同样的备份副本Amazon Web Services 区域（区域内备份副本）。

以下过程将指导您完成在同一个备份副本的过程。Amazon Web Services 账户. 在创建此备份副本之前，必须拥有现有备份。有关更多信息，请参阅 使用备份 (p. 71)。

复制同一个现有备份Amazon Web Services 账户（跨区域或区域内）

1. 从打开 Amazon FSx 控制台https://console.aws.amazon.com/fsx/.
2. 在导航窗格中，选择 Backups。
3. 在备份表中，选择要复制的备份。
4. 选择 Copy backup (复制备份)。这样做会打开复制备份向导。
5. 在目标区域列表中，选择目的地Amazon Web Services 区域将备份复制到。目标可能在另一个Amazon Web Services 区域或者在同样的范围内Amazon Web Services 区域.
6. （可选）选择复制标签将标签从源备份复制到目标备份。如果您选择复制标签并在步骤 8 中添加标签，所有标签都将合并。
7. 适用于加密，选择Amazon KMS加密密钥用于加密复制的备份。
8. 适用于标签-可选，输入键和值以为复制备份添加标签。如果你在这里添加标签并且还选择了复制标签在步骤 6 中，所有标签都将合并。
9. 选择 Copy backup (复制备份)。

您现在已成功复制同一个备份Amazon Web Services 账户到另一个Amazon Web Services 区域或者在同样的范围内Amazon Web Services 区域.

Amazon FSx 的安全性

Amazon 十分重视云安全性。作为 Amazon 客户，您将从专为满足大多数安全敏感型企业的要求而打造的数据中心和网络架构中受益。

安全性是 Amazon 和您的共同责任。责任共担模型将其描述为云的安全性和云中的安全性：

- 云的安全性–Amazon负责保护运行的基础设施AmazonAmazon Web Services 云中的服务。Amazon还向您提供可安全使用的服务。作为 Amazon 合规性计划的一部分，第三方审核人员将定期测试和验证安全性的有效性。要了解适用于 Amazon FSx for Windows File Server 的合规性计划，请参阅Amazon合规性计划范围内的服务.
- 云中的安全性 - 您的责任由您使用的 Amazon 服务决定。您还需要对其它因素负责，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 适用于 Windows 文件服务器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Amazon帮助您监控和保护 Amazon FSx for Windows File Server 资源。

您可以在下文中找到有关使用 Amazon FSx 的安全注意事项说明。

主题

亚马逊 FSx 中的数据加密

Amazon FSx for Windows File Server 支持两种形式的文件系统加密：传输中的数据加密和静态加密。对于映射在支持 SMB 协议 3.0 或更新版本的计算实例上的文件共享，支持对传输中的数据进行加密。创建 Amazon FSx 文件系统时，将自动启用静态数据加密。当您访问文件系统时，Amazon FSx 会使用 SMB 加密自动加密传输中的数据，而无需修改应用程序。

何时使用加密

如果您的组织的公司或监管策略要求静态加密数据和元数据，我们建议您创建加密的文件系统以挂载使用传输中的数据加密的文件系统。

有关使用 Amazon FSx 加密 Windows 文件服务器的更多信息，请参阅以下相关主题：

- 创建适用于 Windows 文件服务器文件系统的 Amazon FSx (p. 7)

- Amazon FSx API 权限：操作、资源和条件参考 (p. 168)

主题

- 静态加密 (p. 161)
- 传输中加密 (p. 162)

静态加密

所有 Amazon FSx 文件系统都进行静态加密，密钥使用Amazon Key Management Service(Amazon KMS)。在将数据写入到文件系统之前，将自动对其进行加密，并在读取时自动解密。Amazon FSx 透明处理这些过程，因此，您不必修改您的应用程序。

Amazon FSx 使用行业标准 AES-256 加密算法静态加密 Amazon FSx 数据和元数据。有关更多信息，请参阅 。加密基础知识中的Amazon Key Management Service开发人员指南.

> Note
>
> 这些区域有：Amazon密钥管理基础设施使用联邦信息处理标准 (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。

Amazon FSx 如何使用Amazon KMS

Amazon FSxAmazon KMS对于密钥管理。Amazon FSx 使用Amazon KMS key对文件系统进行加密。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。此 KMS 密钥可以是以下两种类型之一：

- Amazon 托管式密钥— 这是默认的 KMS 密钥，可以免费使用。
- 客户托管密钥— 这是使用最灵活的 KMS 密钥，因为您可以配置其密钥策略以及为多个用户或服务提供授权。有关创建客户托管密钥的更多信息，请参阅创建密钥中的 Amazon Key Management Service开发人员指南.

如果您使用客户托管密钥作为 KMS 密钥以加密和解密文件数据，您可以启用密钥轮换。在启用密钥轮换时，Amazon KMS 自动每年轮换一次您的密钥。此外，使用客户托管密钥，您可以随时选择何时禁用、重新启用、删除或撤销您的 KMS 密钥的访问权限。有关更多信息，请参阅 。旋转Amazon KMS keys中的Amazon Key Management Service开发人员指南 的第一个版本。

静态文件系统加密和解密是透明处理的。但是，Amazon Web Services 账户特定于亚马逊 FSx 的 ID 会显示在您的Amazon CloudTrail相关的日志Amazon KMS行动。

亚马逊 FSx 关键政策Amazon KMS

密钥策略是控制对 KMS 密钥访问的主要方法。有关密钥策略的更多信息，请参阅使用以下密钥策略Amazon KMS中的Amazon Key Management Service开发人员指南 的第一个版本。下面的列表介绍了所有Amazon KMSAmazon FSx 支持针对静态加密文件系统的相关权限：

- kms:Encrypt—（可选）将明文加密为密文。该权限包含在默认密钥策略中。
- kms:Decrypt—（必需）解密密文。密文是以前加密的明文。该权限包含在默认密钥策略中。
- kms: 重新加密—（可选）使用新的 KMS 密钥加密服务器端的数据，而不公开客户端的数据明文。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: 生成了没有纯文本的数据键—（必需）返回根据 KMS 密钥加密的数据加密密钥。该权限包含在默认密钥策略中的 kms:GenerateDataKey* 下面。

- kms:CreateGrant— （必需）为密钥添加授权以指定哪些用户可以在什么条件下使用密钥。授权是密钥策略的替代权限机制。有关授权的更多信息，请参阅使用授权中的Amazon Key Management Service开发人员指南 的第一个版本。该权限包含在默认密钥策略中。
- kms:DescribeKey— （必需）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。
- kms:ListAliases— （可选）列出账户中的所有密钥别名。当您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。

传输中加密

对于映射在支持 SMB 协议 3.0 或更新版本的计算实例上的文件共享，支持对传输中的数据进行加密。这包括从 Windows Server 2012 和 Windows 8 开始的所有 Windows 版本，以及所有带有 Samba 客户端 4.2 或更高版本的 Linux 客户端。Amazon FSx for Windows File Server 会在您访问文件系统时使用 SMB 加密自动加密传输中的数据，而无需修改应用程序。

SMB 加密使用 AES-128-GCM 或 AES-128-CCM（如果客户端支持 SMB 3.1.1，则选择 GCM 变体）作为其加密算法，并通过使用 SMB Kerberos 会话密钥进行签名提供数据完整性。例如，通过加密的 SMB 连接复制大文件时，使用 AES-128-GCM 可带来更好的性能提高 2 倍。

为了满足始终加密传输中数据的合规性要求，您可以将文件系统访问限制为仅允许访问支持 SMB 加密的客户端。您还可以启用或禁用每个文件共享或整个文件系统的传输中加密。这允许您在同一文件系统中混合使用加密和未加密的文件共享。了解有关管理的更多信息 encryption-in-transit 在文件系统中，请参阅管理传输中加密 (p. 112).

使用 Windows ACL 进行文件和文件夹级访问控制

适用于 Windows 文件服务器的 Amazon FSx 支持通过 Microsoft Active Directory 通过服务器消息块 (SMB) 协议进行基于身份的身份验证。Active Directory 是 Microsoft 目录服务，用于存储有关网络上对象的信息，并使管理员和用户轻松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帐户。要了解有关 Amazon FSx 中 Active Directory 支持的更多信息，请参阅在 FSx for Windows File Server 中使用 Microsoft Active Directory (p. 22).

您加入域的计算实例可以使用 Active Directory 凭据访问 Amazon FSx 文件共享。您可以使用标准 Windows 访问控制列表 (ACL) 进行精细的文件和文件夹级访问控制。Amazon FSx 文件系统会自动验证访问文件系统数据的用户的凭据以强制执行这些 Windows ACL。

每个亚马逊 FSx 文件系统都附带一个默认的 Windows 文件共享`share`. 此共享文件夹的 Windows ACL 配置为允许域用户进行读/写访问。它们还允许对 Active Directory 中委派的管理员组进行完全控制，该组被委派在文件系统上执行管理操作。如果你要将文件系统与Amazon管理微软 AD，这个组是Amazon委派的 FSx 管理员。如果你要将文件系统与自我管理的 Microsoft AD 设置集成，则此组可以是域管理员。或者，它可以是您在创建文件系统时指定的自定义委派管理员组。要更改 ACL，您可以将共享映射为委派管理员组成员的用户。

> **Warning**
>
> 亚马逊 FSx 要求 SYSTEM 用户拥有完全控制对文件系统中所有文件夹的 NTFS ACL 权限。不要更改此用户在文件夹上的 NTFS ACL 权限。这样做可以使文件共享无法访问，并防止文件系统备份可用。

相关链接

- 什么是AmazonDirectory Service？中的Amazon Directory Service管理指南。

- 创建您的Amazon托管 Microsoft AD 目录中的Amazon Directory Service管理指南.
- 何时创建信任关系中的Amazon Directory Service管理指南.
- 演练 1：开始使用的先决条件 (p. 145).

使用 Amazon VPC 进行文件系统访问控制

您可以通过 elastic network interface 访问 Amazon FSx 文件系统。该网络接口位于虚拟私有云 (VPC) 中，该网络接口基于您与您的文件系统关联的 Amazon Virtual Private Cloud (Amazon VPC) 服务。通过 Amazon FSx 域名服务 (DNS) 名称连接到 Amazon FSx 文件系统。DNS 名称映射到 VPC 中文件系统 elastic network interface 的私有 IP 地址。只有关联 VPC 内的资源，与关联 VPC 连接的资源Amazon Direct Connect或 VPN，或者对等 VPC 中的资源可以访问文件系统的网络接口。有关更多信息，请参阅 。Amazon VPC 是什么？中的Amazon VPC User Guide。

> Warning
>
> 不得修改或删除与文件系统关联的 elastic network interface。修改或删除网络接口可能会导致永久丢失您的 VPC 与您的文件系统之间的连接。

FSx for Windows File Server 支持 VPC 共享，这使您能够查看、创建、修改和删除另一个 VPC 中共享子网中的资源Amazonaccount. 有关更多信息，请参阅 Amazon VPC 用户指南 中的使用共享 VPC。

Amazon VPC 安全组

要进一步控制通过 VPC 内文件系统 elastic network interface 的网络流量，您可以使用安全组来限制对文件系统的访问。一个安全组是有状态防火墙，用于控制进出与其关联的网络接口的流量。在这种情况下，相关资源是文件系统的网络接口。

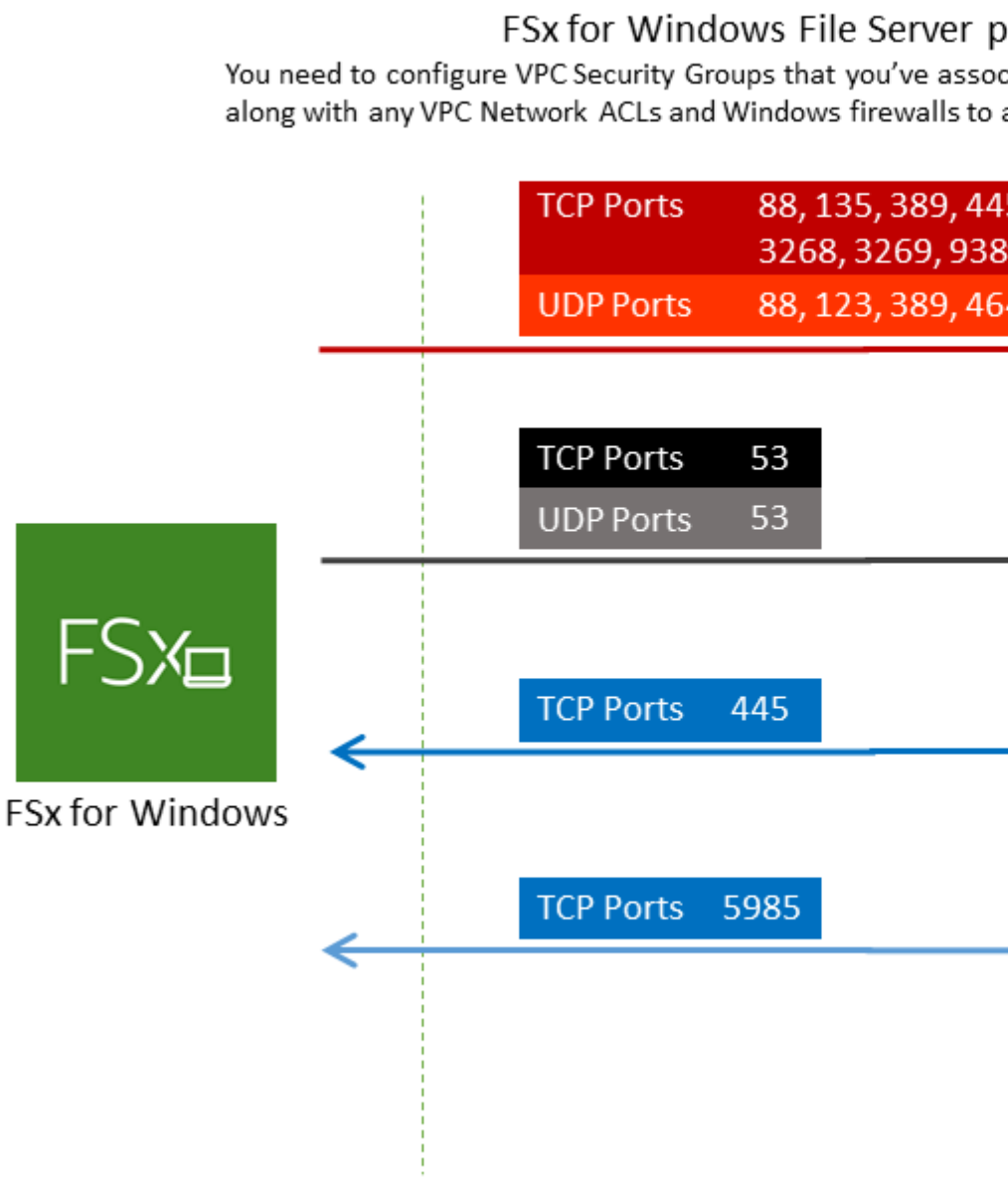
要使用安全组控制对 Amazon FSx 文件系统的访问，请添加入站和出站规则。入站规则控制传入流量，出站规则控制从您的文件系统传出的流量。确保您的安全组中有正确的网络流量规则，以便将 Amazon FSx 文件系统的文件共享映射到受支持的计算实例上的文件夹。

有关安全组规则的更多信息，请参阅安全组规则中的适用于 Linux 实例的 Amazon EC2 用户指南。

为 Amazon FSx 创建安全组

1. 在以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2.
2. 在导航窗格中，选择 Security Groups。
3. 选择 Create Security Group。
4. 为安全组指定名称和描述。
5. 适用于VPC中，选择与您的文件系统关联的 Amazon VPC 以在该 VPC 内创建安全组。
6. 添加以下规则以允许以下端口上的出站网络流量：

   a. 适用于VPC 安全组，您默认 Amazon VPC 的默认安全组已添加到控制台中的您的文件系统。请确保在其中创建 FSx 文件系统的子网的安全组和 VPC 网络 ACL 允许端口上以及下图所示的说明中的流量。



下表确定了每个端口的角色。

协议	端口	角色
TCP/UDP	53	域名系统 (DNS)

协议	端口	角色
TCP/UDP	88	Kerberos 身份验证
TCP/UDP	464	更改/设置密码
TCP/UDP	389	轻型目录访问协议 (LDAP)
UDP	123	网络时间协议 (NTP)
TCP	135	分布式计算环境/端点映射器（DCE/EPMAP）
TCP	445	目录服务 SMB 文件共享
TCP	636	基于 TLS/SSL 的轻量级目录访问协议 (LDAPS)
TCP	3268	Microsoft 全球目录
TCP	3269	SSL 上的微软全球目录
TCP	5985	WinRM 2.0（微软视窗远程管理）
TCP	9389	微软 AD DS Web 服务，PowerShell
TCP	49152 - 65535	RPC 的临时端口

Important

单可用区 2 和所有多可用区文件系统部署都需要允许 TCP 端口 9389 上的出站流量。

b. 确保这些流量规则也镜像在适用于每个 AD 域控制器、DNS 服务器、FSx 客户端和 FSx 管理员的防火墙上。

Important

尽管 Amazon VPC 安全组要求仅在启动网络流量的方向上打开端口，但大多数 Windows 防火墙和 VPC 网络 ACL 都要求端口双向打开。

Note

如果您已定义 Active Directory 站点，您必须确保在 Active Directory 站点中与 Amazon FSx 文件系统关联的 VPC 内定义了子网，并且 VPC 中的子网与您其他站点中的子网之间不存在冲突。您可以使用 Active Directory 站点和服务 MMC 管理单元查看和更改这些设置。

Note

在某些情况下，您可能修改了的规则Amazon Managed Microsoft AD默认设置中的安全组。如果是，请确保此安全组具有所需的入站规则，以允许来自 Amazon FSx 文件系统的流量。有关所需入站规则的更多信息，请参阅Amazon Managed Microsoft AD先决条件中的Amazon Directory Service管理指南.

现在您已经创建了安全组，可以将其与 Amazon FSx 文件系统的 elastic network interface 关联起来。

将安全组与您的 Amazon FSx 文件系统关联

1. 在以下网址打开 Amazon FSx 控制台：https://console.aws.amazon.com/fsx/.
2. 在控制面板上，选择您的文件系统以查看其详细信息。
3. 选择网络 & 安全选项卡，然后选择文件系统的网络接口 ID（例如，ENI-01234567890123456）。

4. 适用于操作，选择更改安全组.
5. 在更改安全组对话框中，选择要使用的安全组，然后选择Save（保存）.

禁止访问文件系统

要暂时禁止所有客户端对文件系统进行网络访问，您可以删除与文件系统 elastic network interface 关联的所有安全组，然后用没有入站/出站规则的组替换它们。

Amazon VPC 网络 ACL

确保对 VPC 内文件系统的访问安全的另一种选择是建立网络访问控制列表（网络 ACL）。网络 ACL 与安全组分开，但具有类似的功能，可以为 VPC 中的资源添加额外安全层。有关网络 ACL 的更多信息，请参阅网络 ACL中的Amazon VPC User Guide。

利用 IAM 对 Amazon FSx 进行资源管理访问控制

每个 Amazon 资源都归某个 Amazon Web Services 账户 账户所有，创建或访问资源的权限由权限策略进行管理。账户管理员可以向Amazon Identity and Access Management(IAM) 身份 (即：用户、组和角色)。有些服务（例如 Amazon Lambda）还支持向资源附加权限策略。

> Note
>
> 账户管理员（或管理员用户）是具有管理员权限的用户。有关更多信息，请参阅 IAM 用户指南中的 IAM 最佳实践。

在授予权限时，您要决定谁获得权限，获得对哪些资源的权限，以及您允许对这些资源执行的具体操作。

主题

Amazon FSx for Windows File Server 资源和操作

在 Amazon FSx for Windows File Server 中，主要资源是文件系统. Amazon FSx for Windows File Server 还支持其他子资源类型。备份. 您只能在现有文件系统范围内创建备份，或者通过复制现有备份来创建备份。

这些资源和子资源具有与其关联的唯一 Amazon Resource Name (ARN)，如下表所示。

Amazon FSx 提供一组操作用来处理 Amazon FSx 资源。有关可用操作的列表，请参阅Amazon FSx API 参考.

了解资源所有权

Amazon账户对在该账户下创建的资源具有所有权，而无论创建资源的人员是谁。具体而言，资源所有者是对资源创建请求进行身份验证的委托人实体（即根账户、IAM 用户或 IAM 角色）的Amazon账户。以下示例说明了它的工作原理：

- 如果使用您的根账户凭证Amazon创建文件系统的账户，Amazon账户就是该资源的所有者 (在 Amazon FSx 中，资源就是文件系统)。
- 如果在中创建 IAM 用户Amazon账户并向该用户授予创建文件系统的权限，则该用户可以创建文件系统。但是，您的Amazon账户 (即该用户所属的账户) 拥有该文件系统资源。
- 如果在中创建 IAM 角色Amazon具有文件系统创建权限的账户，则能够担任该角色的任何人都可以创建文件系统。您的Amazon账户 (即角色所属的账户) 拥有该文件系统资源。

在创建过程中授予标记资源的权限

某些资源创建 Amazon FSx API 操作允许您在创建资源时指定标签。您可以使用资源标签来实现基于属性的访问控制 (ABAC)。有关更多信息，请参阅 。什么是 ABAC 的用途Amazon中的IAM 用户指南.

为使用户能够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` 或 `fsx:CreateBackup`）的权限。如果在资源创建操作中指定了标签，则 Amazon 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。

例如，下面的策略允许用户创建文件系统并在特定文件系统中创建期间向文件系统应用标签。Amazon Web Services 账户.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateFileSystem",
         "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:region:account-id:file-system/*"
    }
  ]
}
```

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期间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操作中应用了标签时，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 (p. 125). 有关使用标签控制对 FSx 资源的访问的更多信息，请参阅使用标签控制对 Amazon FSx 资源的访问 (p. 170).

管理对 Amazon FSx 资源的访问

权限策略规定谁可以访问哪些内容。下一节介绍创建权限策略时的可用选项。

> Note
>
> 本节讨论如何在适用于 Windows File Server 的 Amazon FSx 范围内使用 IAM。这里不提供有关 IAM 服务的详细信息。有关完整的 IAM 文档，请参阅 IAM 用户指南中的什么是 IAM？。有关 IAM 策略语法和说明的信息，请参阅 IAM 用户指南中 Amazon IAM 策略参考。

附加到 IAM 身份的策略称作基于身份 的策略（IAM 策略），附加到资源的策略称作基于资源 的策略。Amazon FSx for Windows File Server 只支持基于身份的策略 (IAM 策略)。

Amazon FSx API 权限：操作、资源和条件参考

在设置访问控制并编写可附加到 IAM 身份的权限策略 (基于身份的策略) 时，可使用以下内容：作为参考。这些区域有：每个 Amazon FSx API 操作、您可授予执行该操作的权限的对应操作，Amazon资源，您可以授予权限。您可以在策略的 `Action` 字段中指定这些操作，并在策略的 `Resource` 字段中指定资源值。

您可以使用Amazon表达条件键在您的 Amazon FSx 策略中显示条件。有关 Amazon 范围内的键的完整列表，请参阅《IAM 用户指南》https://docs.amazonaws.cn/IAM/latest/UserGuide/reference_policies_elements.html#AvailableKeys中的可用键。

要指定操作，请在 API 操作名称之前使用 `fsx:` 前缀 (例如，`fsx:CreateFileSystem`)。每项操作都适用于单个 Amazon FSx 文件系统，也适用于由Amazon账户、单个备份或者属于Amazon Web Services 账户.

本部分仅包括这些操作所需的 Amazon FSx 权限。其他权限Amazon其中一些操作需要提供服务。

Amazon FSx API 和必需的操作权限

Amazon FSx API 操作	所需权限（API 操作）	资源
关联文件系统别名	`fsx:AssociateFileSystemAliases`	`arn:aws:fsx:region:account-id:file-system/file-system-id`
取消数据存储库任务	`fsx:CancelDataRepositoryTask`	`arn:aws:fsx:region:account-id:file-system/file-system-id`

COPYBackup	`fsx:CopyBackup`
	
	`fsx:CopyBackup`
	
	`fsx:TagResource`
		`arn:aws:fsx:region:account-id:backup/source-backup-id`— 源备份
		
		`arn:aws:fsx:region:account-id:backup/*`— 目标区域
		
		`arn:aws:fsx:region:account-id:backup/*`— 在备份副本上复制或创建标签所需

CreateBackup	FSX：创建备份
	
	FSX：创建备份
	
	`fsx:TagResource`
		`arn:aws:fsx:region:account-id:backup/*`
		
		`arn:aws:fsx:region:account-id:file-system/file-system-id`

Amazon FSx API 操作	所需权限（API 操作）	资源
		arn:aws:fsx:*region*:*account-id*:backup/*— 在新备份上创建标签所需
CreateFileSystem	fsx:CreateFileSystem fsx:TagResource	arn:aws:fsx:*region*:*account-id*:file-system/* arn:aws:fsx:*region*:*account-id*:file-system/*— 在文件系统上创建标签
从备份创建文件系统	fsx:CreateFileSystemFromBackup fsx:CreateFileSystemFromBackup fsx:TagResource	arn:aws:fsx:*region*:*account-id*:file-system/* arn:aws:fsx:*region*:*account-id*:backup/* arn:aws:fsx:*region*:*account-id*:file-system/*— 在文件系统上创建标签
DeleteBackup	fsx:DeleteBackup	arn:aws:fsx:*region*:*account-id*:backup/*backup-id*
DeleteFileSystem	fsx:DeleteFileSystem fsx:TagResource	arn:aws:fsx:*region*:*account-id*:file-system/*filesystem-id* arn:aws:fsx:*region*:*account-id*:backup/*— 如果已创建，则需要在最终备份上创建标签
DescribeBackups	fsx:DescribeBackups	arn:aws:fsx:*region*:*account-id*:backup/*
描述文件系统别名	fsx:DescribeFileSystemAliases	arn:aws:fsx:*region*:*account-id*:file-system/*file-system-id*
DescribeFileSystems	fsx:DescribeFileSystems	arn:aws:fsx:*region*:*account-id*:file-system/*
取消关联文件系统别名	fsx:DisassociateFileSystemAliases	arn:aws:fsx:*region*:*account-id*:file-system/*
ListTagsForResource	fsx:ListTagsForResource	arn:aws:fsx:*region*:*account-id*:backup/*backup-id* arn:aws:fsx:*region*:*account-id*:file-system/*filesystem-id* arn:aws:fsx:*region*:*account-id*:task/*task-id*

Amazon FSx API 操作	所需权限（API 操作）	资源
TagResource	fsx:TagResource	arn:aws:fsx:*region*:*account-id*:backup/*backup-id* arn:aws:fsx:*region*:*account-id*:file-system/*filesystem-id* arn:aws:fsx:*region*:*account-id*:task/*task-id*
UntagResource	fsx:UntagResource	arn:aws:fsx:*region*:*account-id*:backup/*backup-id* arn:aws:fsx:*region*:*account-id*:file-system/*filesystem-id* arn:aws:fsx:*region*:*account-id*:task/*task-id*
更新文件系统	fsx:UpdateFileSystem	arn:aws:fsx:*region*:*account-id*:file-system/*filesystem-id*

使用标签控制对 Amazon FSx 资源的访问

要控制对 Amazon FSx 资源和操作的访问，您可以使用Amazon Identity and Access Management(IAM) 基于标签的策略。您可以使用两种方法提供控制：

1. 根据 Amazon FSx 资源上的标签控制对这些资源的访问。
2. 控制可以在 IAM 请求条件中传递的标签。

有关如何使用标签控制对的访问的信息Amazon资源，请参阅使用标签控制访问中的IAM 用户指南. 有关在创建时为 Amazon FSx 资源添加标签的更多信息，请参阅在创建过程中授予标记资源的权限 (p. 167). 有关使用标签的更多信息，请参阅标记 Amazon FSx 资源 (p. 125).

根据资源上的标签控制访问

要控制用户或角色可以对 Amazon FSx 资源执行的操作，您可以使用该资源上的标签。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 示例策略 — 在提供特定标签时在上创建文件系统

此策略允许用户仅在使用特定的标签密钥值对标记文件系统时才能创建文件系统，在本示例中，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 示例策略 — 仅在具有特定标记的文件系统上创建备份

此策略允许用户仅在带有密钥值对标记的文件系统上创建备份key=Department, value=Finance，然后将使用标签创建备份Deparment=Finance.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:file-system/*",
            "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 示例策略 — 使用具有特定标记的备份创建具有特定标签的文件系统

此策略允许用户创建标记为的文件系统。Department=Finance仅来自标记的备份Department=Finance.

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

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

Example 示例策略 — 删除具有特定标签的文件系统

此策略只允许用户删除标记为的文件系统。Department=Finance. 如果他们创建了最终备份，那么必须使用Department=Finance.

```
{
    "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"
                }
            }
        }
    ]
}
```

对 Amazon FSx 使用服务相关角色

Amazon FSx for Windows File Server 使用Amazon 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，它与 Amazon FSx 直接相关。服务相关角色由 Amazon FSx 预定义，并包含该服务调用其他角色所需的所有权限。Amazon服务代表您。

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它 IAM 实体的权限策略。

只有在首先删除相关资源后，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它服务的信息，请参阅使用 IAM 的 Amazon 服务并查找 Service-Linked Role（服务相关角色）列中显示为 Yes（是）的服务。请选择 Yes 与查看该服务的服务相关角色文档的链接。

Amazon FSx 的服务相关角色权限

Amazon FSx 使用名为的服务相关角色AWSServiceRoleForAmazonFSx— 在您的账户中执行某些操作，例如为 VPC 中的文件系统创建弹性网络接口。

角色权限策略允许 Amazon FSx 对所有适用的对策略完成以下操作：Amazon资源：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData",
                "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",
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "AmazonFSx.FileSystemId"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
```

```
                "Null": {
                    "aws:ResourceTag/AmazonFSx.FileSystemId": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateRoute",
                "ec2:ReplaceRoute",
                "ec2:DeleteRoute"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/AmazonFSx": "ManagedByAmazonFSx"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/fsx/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "firehose:DescribeDeliveryStream",
                "firehose:PutRecord",
                "firehose:PutRecordBatch"
            ],
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
        }
    ]
}
```

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

无需手动创建服务相关角色。当您在中创建文件系统时Amazon Web Services Management Console、IAM CLI 或 IAM API，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 账户中出现新角色。

如果删除此服务相关角色，然后需要再次创建，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 将再次为您创建服务相关角色。

编辑适用于 Amazon FSx 的服务相关角色

Amazon FSx 不允许您编辑 AWSServiceRoleForAmazonFSx 服务相关角色。创建服务相关角色后，将无法更改角色名称，因为可能有多个实体引用该角色。但是可以使用 IAM 编辑角色说明。有关更多信息，请参见《IAM 用户指南》中的编辑服务相关角色。

删除适用于 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。这样您就没有未被主动监控或维护的未使用实体。但是，您必须先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

如果在您试图删除资源时 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，请参见 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 Amazon 区域和终端节点。

AmazonAmazon FSx 的托管式策略

要向用户、组和角色添加权限，与自己编写策略相比，使用 Amazon 托管策略更简单。创建仅为团队提供所需权限的 IAM 客户托管策略需要时间和专业知识。要快速入门，您可以使用我们的 Amazon 托管式策略。这些策略涵盖常见使用案例，可在您的 Amazon Web Services 账户 中使用。有关 Amazon 托管式策略的更多信息，请参阅 IAM 用户指南中的Amazon 托管式策略。

Amazon Web Services 负责维护和更新 Amazon 托管式策略。您无法更改 Amazon 托管式策略中的权限。服务偶尔会向 Amazon 托管式策略添加额外权限以支持新功能。此类更新会影响附加策略的所有身份（用户、组和角色）。当启动新功能或新操作可用时，服务最有可能会更新 Amazon 托管式策略。服务不会从 Amazon 托管式策略中删除权限，因此策略更新不会破坏您的现有权限。

此外，Amazon 还支持跨多种服务的工作职能的托管式策略。例如，`ViewOnlyAccess` Amazon 托管式策略提供对许多 Amazon Web Services 服务和资源的只读访问权限。当服务启动新功能时，Amazon 会为新操作和资源添加只读权限。有关工作职能策略的列表和说明，请参阅 IAM 用户指南中的适用于工作职能的 Amazon 托管策略。

Amazon托管策略：AmazonfXX 删除服务链接角色访问权限

您不能将 `AmazonFSxDeleteServiceLinkedRoleAccess` 附加到自己的 IAM 实体。此策略与服务相关角色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 对 Amazon FSx 使用服务相关角色 (p. 172)。

此策略授予管理权限，允许 Amazon FSx 删除其用于 Amazon S3 访问的服务关联角色，该角色仅由 Amazon FSx for Lustre 使用。

权限详细信息

此策略包括中的权限`iam`允许 Amazon FSx 查看、删除和查看 Amazon S3 访问的 FSx 服务关联角色的删除状态。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:GetServiceLinkedRoleDeletionStatus",
                "iam:GetRole"
            ],
            "Resource": "arn:*:iam::*:role/aws-service-role/s3.data-
source.lustre.fsx.amazonaws.com/AWSServiceRoleForFSxS3Access_*"
        }
    ]
}
```

Amazon托管策略：AmazonFSxFullAccess

您可以将 AmazonFSXFullAccess 附加到您的 IAM 实体。Amazon FSx 还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 的完全访问权限和访问相关的权限Amazon服务。

权限详细信息

此策略包含以下权限。

- `fsx`允许委托人完全访问权限，以执行所有 Amazon FSx 操作。
- `ds`— 允许委托人查看有关Amazon Directory Service目录。
- `iam`允许原则代表用户创建 Amazon FSx 服务关联角色。这是必需的，以便亚马逊 FSx 可以管理Amazon资源代表用户。
- `logs`— 允许委托人创建日志组、日志流并将事件写入日志流。这是必需的，以便用户可以通过将审计访问日志发送到来监控 FSx 的 Windows 文件服务器文件系统访问 CloudWatch 日志。
- `firehose`— 允许委托人向 Amazon Kinesis Data Firehose 写入记录。这是必需的，以便用户可以通过向 Kinesis Data 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。
- `ec2`— 允许委托人在指定条件下创建标签。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ds:DescribeDirectories",
                "fsx:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": [
                        "fsx.amazonaws.com"
                    ]
                }
            }
```

```
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": [
                        "s3.data-source.lustre.fsx.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:/aws/fsx/*:log-group:*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "firehose:PutRecord"
            ],
            "Resource": [
                "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/AmazonFSx": "ManagedByAmazonFSx"
                },
                "ForAnyValue:StringEquals": {
                    "aws:CalledVia": ["fsx.amazonaws.com"]
                }
            }
        }
    ]
}
```

Amazon托管策略：AmazonFSxConsoleFullAccess

您可以将 `AmazonFSxConsoleFullAccess` 策略附加得到 IAM 身份。

此策略授予管理权限，允许完全访问 Amazon FSx 并访问相关权限。Amazon通过Amazon Web Services Management Console.

权限详细信息

此策略包含以下权限。

- fsx允许委托人在 Amazon FSx 管理控制台中执行所有操作。
- cloudwatch— 允许委托人查看 CloudWatch Amazon FSx 管理控制台中的警报。
- ds— 允许委托人列出有关Amazon Directory Service目录。
- 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、子网以及与 Amazon FSx 文件系统关联的 VPC。
- kms— 允许委托人列出别名Amazon Key Management Service钥匙。
- s3允许委托人列出 Amazon S3 存储桶中的部分或全部对象（最多 1000 个）。
- iam— 授予权限以创建服务关联角色，该角色允许 Amazon FSx 代表用户执行操作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:DescribeAlarms",
                "ds:DescribeDirectories",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "firehose:ListDeliveryStreams",
                "fsx:*",
                "kms:ListAliases",
                "logs:DescribeLogGroups",
                "s3:ListBucket"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": [
                        "fsx.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": [
                        "s3.data-source.lustre.fsx.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
```

```
                "arn:aws:ec2:*:*:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/AmazonFSx": "ManagedByAmazonFSx"
                },
                "ForAnyValue:StringEquals": {
                    "aws:CalledVia": ["fsx.amazonaws.com"]
                }
            }
        }
    ]
}
```

Amazon托管策略：AmazonFSxConsoleReadOnlyAccess

您可以将 `AmazonFSxConsoleReadOnlyAccess` 策略附加得到 IAM 身份。

此策略授予 Amazon FSx 及相关策略的只读权限Amazon服务，以便用户可以在Amazon Web Services Management Console.

权限详细信息

此策略包含以下权限。

- `fsx`— 允许委托人在 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`— 允许委托人查看 CloudWatch Amazon FSx 管理控制台中的警报。
- `ds`— 允许委托人查看有关Amazon Directory Service亚马逊 FSx 管理控制台中的目录。
- `ec2`— 允许委托人在 Amazon FSx 管理控制台中查看与 Amazon FSx 文件系统关联的网络接口、安全组、子网和 VPC。
- `kms`— 允许委托人查看其中的别名Amazon Key Management ServiceAmazon FSx 管理控制台中的密钥。
- `log`— 允许校长描述亚马逊 CloudWatch 记录与发出请求的账户关联的日志组。委托人可以查看 FSx for Windows File Server 文件系统的现有文件访问审核配置所必需的。
- `firehose`— 允许委托人描述与发出请求的账户关联的 Amazon Kinesis Data Firehose 交付流。委托人可以查看 FSx for Windows File Server 文件系统的现有文件访问审核配置所必需的。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:DescribeAlarms",
                "ds:DescribeDirectories",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "firehose:ListDeliveryStreams",
                "fsx:Describe*",
                "fsx:ListTagsForResource",
                "kms:DescribeKey",
                "logs:DescribeLogGroups"
```

```
            ],
            "Resource": "*"
        }
    ]
}
```

Amazon托管策略：AmazonFSxReadOnlyAccess

您可以将 AmazonFSxReadOnlyAccess 策略附加得到 IAM 身份。

此策略授予管理权限，允许对 Amazon FSx 进行只读访问。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:Describe*",
                "fsx:ListTagsForResource"
            ],
            "Resource": "*"
        }
    ]
}
```

Amazon FSx 更新Amazon托管策略

查看有关更新的详细信息AmazonAmazon FSx（自从其开始跟踪更改以来）的托管式策略。要获得有关此页面更改的自动提示，请订阅 Amazon FSx 上的 RSS 源文档历史记录 (p. 211)页.

更改	说明	日期
AmazonFSxReadOnlyAccess (p. 180)— 已开启跟踪策略	此策略授予对所有 Amazon FSx 资源以及与其关联的任何标签的只读访问权限。	2022 年 2 月 4 日
AmazonfXX 删除服务链接角色访问权限 (p. 175)— 已开启跟踪策略	此策略授予管理权限，允许 Amazon FSx 删除其适用于 Amazon S3 访问的服务关联角色。	2022 年 1 月 7 日
AmazonFSxServiceRolePolicy (p. 177)— 对现有策略的更新	亚马逊 FSx 添加了新的权限，允许亚马逊 FSx 管理亚马逊 FSx 的网络配置 NetApp ONTAP 文件系统。	2021 年 9 月 2 日
AmazonFSxFullAccess (p. 176)— 对现有策略的更新	Amazon FSx 添加了新的权限，允许 Amazon FSx 在 EC2 路由表上创建标签以进行范围下调用。	2021 年 9 月 2 日
AmazonFSxConsoleFullAccess (p. 173)— 对现有策略的更新	亚马逊 FSx 添加了新的权限，允许亚马逊 FSx 为 NetApp ONTAP 多可用区文件系统。	2021 年 9 月 2 日
AmazonFSxConsoleFullAccess (p. 173)— 对现有策略的更新	Amazon FSx 添加了新的权限，允许 Amazon FSx 在 EC2 路由表上创建标签以进行范围下调用。	2021 年 9 月 2 日

更改	说明	日期
AmazonFSxServiceRolePolicy (p. 172)—对现有策略的更新	亚马逊 FSx 添加了新的权限，以允许亚马逊 FSx 描述和写信 CloudWatch 记录日志流。 这是必需的，以便用户可以使用 CloudWatch 日志。	2021 年 6 月 8 日
AmazonFSxServiceRolePolicy (p. 172)—对现有策略的更新	亚马逊 FSx 添加了新的权限，允许亚马逊 FSx 描述并写信给 Amazon Kinesis Data Firehose 交付流。 这是必需的，以便用户可以使用 Amazon Kinesis 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
AmazonFSxFullAccess (p. 176)—对现有策略的更新	Amazon FSx 添加了新的权限，以允许委托人描述和创建 CloudWatch 记录日志组、日志流并将事件写入日志流。 这是必需的，以便委托人可以使用 CloudWatch 日志。	2021 年 6 月 8 日
AmazonFSxFullAccess (p. 176)—对现有策略的更新	亚马逊 FSx 添加了新的权限，允许委托人描述记录并将记录写入 Amazon Kinesis Data Firehose。 这是必需的，以便用户可以使用 Amazon Kinesis 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
AmazonFSxConsoleFullAccess (p. 177)—对现有策略的更新	Amazon FSx 添加了新的权限，以允许委托人描述 Amazon CloudWatch 记录与发出请求的账户关联的日志组。 这是必需的，以便委托人可以选择现有的 CloudWatch 对 FSx for Windows File Server 文件系统的文件访问审核时，记录日志组。	2021 年 6 月 8 日
AmazonFSxConsoleFullAccess (p. 177)—对现有策略的更新	亚马逊 FSx 添加了新的权限，允许委托人描述与发出请求的账户关联的 Amazon Kinesis Data Firehose 交付流。 这是必需的，以便在为适用于 Windows 文件服务器文件系统的 FSx 配置文件访问审核时，委托人可以选择现有的 Kinesis Data Firehose 传输流。	2021 年 6 月 8 日

更改	说明	日期
AmazonFSxConsoleReadOnlyAccess (p. 179) 对现有策略的更新	Amazon FSx 添加了新的权限，以允许委托人描述 Amazon CloudWatch 记录与发出请求的账户关联的日志组。 委托人可以查看 FSx for Windows File Server 文件系统的现有文件访问审核配置所必需的。	2021 年 6 月 8 日
AmazonFSxConsoleReadOnlyAccess (p. 179) 对现有策略的更新	亚马逊 FSx 添加了新的权限，允许委托人描述与发出请求的账户关联的 Amazon Kinesis Data Firehose 交付流。 委托人可以查看 FSx for Windows File Server 文件系统的现有文件访问审核配置所必需的。	2021 年 6 月 8 日
Amazon FSx 开始跟踪更改	Amazon FSx 开始跟踪其的更改 Amazon托管策略。	2021 年 6 月 8 日

Amazon FSx for Windows File Server

作为多个项目的一部分，第三方审计员将评估 Amazon FSx for Windows File Server 的安全性和合规性。Amazon合规性计划。其中包括 SOC、PCI、ISO、HIPAA 等。

有关特定合规性计划范围内的 Amazon 服务列表，请参阅合规性计划范围内的 Amazon 服务。有关常规信息，请参阅Amazon合规性计划。

您可以使用 Amazon Artifact 下载第三方审计报告。有关更多信息，请参阅下载 Amazon Artifact 中的报告。

您在使用 Amazon FSx 时的合规性责任由您的数据的敏感性、您公司的合规性目标以及适用的法律法规决定。Amazon您可以提供以下资源来帮助实现合规性：

- 安全性与合规性 Quick Start 指南安全性与合规性 Quick Start 指南 - 这些部署指南讨论了架构注意事项，并提供了在 Amazon 上部署基于安全性和合规性的基准环境的步骤。
- 《设计符合 HIPAA 安全性和合规性要求的架构》白皮书 – 此白皮书介绍公司如何使用Amazon创建符合 HIPAA 标准的应用程序。
- Amazon合规性资源 – 此业务手册和指南集合可能适用于您的行业和位置。
- Amazon Config 开发人员指南中的使用规则评估资源 – 此 Amazon Config 服务评估您的资源配置对内部实践、行业指南和法规的遵循情况。
- Amazon Security Hub – 此 Amazon 服务提供了 Amazon 中安全状态的全面视图，可帮助您检查是否符合安全行业标准和最佳实践。

Amazon FSx for Windows File Server 和接口 VPC 终端节点

您可以将 Amazon FSx 配置为使用接口 VPC 终端节点以改善 VPC 的安全状况。由以下 VPC 司提供提供提供支持Amazon PrivateLink，该技术支持您私下访问 Amazon FSx API，而无需互联网网关、NAT 设

备、VPN 连接或Amazon Direct Connect连接。VPC 中的实例即使没有公有 IP 地址也可与 Amazon FSx API 进行通信。VPC 和 Amazon FSx 之间的流量不会脱离Amazon网络。

每个接口 VPC 终端节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 Amazon FSx API 流量的入口点。

Amazon FSx 接口 VPC 终端节点的注意事项

在为 Amazon FSx 设置接口 VPC 终端节点之前，请务必查看接口 VPC 终端节点属性和限制中的Amazon VPC User Guide.

您可以从 VPC 调用任何 Amazon FSx API 操作。例如，FSx for Windows File Server 过调用 CreateFileSystem VPC 内的 API。有关 Amazon FSx API 的完整列表，请参阅操作在 Amazon FSx API 参考中。

VPC 对等连接注意事项

您可以使用 VPC 对等连接通过接口 VPC 终端节点将其他 VPC 连接到 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，或者在自己的 VPC 与其他 VPC 之间建立此连接。Amazon Web Services 账户. VPC 也可以分为两个不同的Amazon Web Services 区域.

对等 VPC 之间的流量保留在Amazon网络上，不会穿越公有互联网。建立对等 VPC 终端节点等连接后，两个 VPC 中的资源（如 Amazon Elastic Compute Cloud (Amazon EC2) 实例等）可以通过在其中一个 VPC 终端节点中创建的接口访问 Amazon FSx API。

为 Amazon FSx API 创建接口 VPC 终端节点

您可以使用 Amazon VPC 控制台或为 Amazon FSx API 创建 VPC 终端节点Amazon Command Line Interface(Amazon CLI)。有关更多信息，请参阅 。创建接口 VPC 终端节点中的Amazon VPC User Guide.

要为 Amazon FSx 创建接口 VPC 终端节点，请使用以下选项之一：

- **com.amazonaws.*region*.fsx**— 为 Amazon FSx API 操作创建终端节点。
- **com.amazonaws.*region*.fsx-fips**— 为 Amazon FSx API 创建符合的终端节点美国联邦信息处理标准 (FIPS) 140-2.

要使用私有 DNS 选项，您必须将`enableDnsHostnames`和`enableDnsSupport`您的 VPC 的属性。有关更多信息，请参阅 。查看和更新针对 VPC 的 DNS 支持中的Amazon VPC User Guide.

ExcuteAmazon Web Services 区域在中国，如果您为终端节点启用私有 DNS，则可以将其默认 DNS 名称用于Amazon Web Services 区域，例如`fsx.us-east-1.amazonaws.com`. 对于中国（北京）和中国（宁夏）Amazon Web Services 区域，您可以使用以下方法通过 VPC 终端节点发出 API 请求`fsx-api.cn-north-1.amazonaws.com.cn`和`fsx-api.cn-northwest-1.amazonaws.com.cn`，。

有关更多信息，请参阅 。通过接口 VPC 终端节点访问服务中的Amazon VPC User Guide.

为 Amazon FSx 创建 VPC 终端节点策略

要进一步控制对 Amazon FSx API 的访问权限，您可以选择附加Amazon Identity and Access ManagementVPC 终端节点的 (IAM) 策略。此策略指定以下内容：

- 可执行操作的委托人。
- 可执行的操作。
- 可对其执行操作的资源。

有关更多信息，请参阅《Amazon VPC 用户指南》中的使用 VPC 终端节点控制对服务的访问权限。

配额

您可以在下文中找到在 Windows File Server 中使用 Amazon FSx 时的配额。

主题

你可以增加的配额

以下是每个 Amazon FSx for Windows File Server 的配额。Amazon Web Services 账户，每Amazon Web Services 区域，你可以增加。

资源	默认值	描述
Windows 文件系统	100	您可以在此账户中创建的适用于 Windows Server 文件系统的最大 Amazon FSx 数。
Windows 吞吐量容量	10240	此账户中所有适用于 Windows 文件系统的 Amazon FSx 允许的总吞吐量（以 MBps 为单位）。
Windows HDD 存储容量	524288	此账户中允许的所有 Amazon FSx 适用于 Windows 文件服务器文件系统的最大硬盘存储容量（以 GiB 为单位）。
Windows SSD 存储容量	524288	此账户中允许的所有 Amazon FSx 适用于 Windows 文件服务器文件系统的最大 SSD 存储容量（以 GiB 为单位）。
Windows 备份	500	您可以在此账户中拥有的所有 Amazon FSx for Windows File Server 件系统的用户启动的最大备份数。

请求提高配额

1. 打开Amazon支持中心页面，登录（如有必要），然后选择创建案例.
2. 适用于创建案例，选择账户和账单支持.
3. 在案例细节面板输入以下条目：
   - 适用于类型选择账户.
   - 适用于类别选择其他账户问题.
   - 适用于Subject输入**`FSx for Windows File Server service limit increase request`**.

- 提供详细信息说明你的请求，包括：
  - 如果已知，你想要增加的 FSx 配额，以及你想要增加的价值。
  - 你寻求增加配额的原因。
  - 请求增加的每个文件系统的文件系统 ID 和区域。

4. 提供首选项联系选项然后选择提交.

每个文件系统的资源配额

以下是 Amazon FSx 中每个文件系统的 Windows File Server 资源的配额，Amazon Web Services 区域.

资源	每个文件系统的限制
最大标签数	50
自动备份的最长保留期限	90 天
每个账户正在进行到同一目标区域的最大备份复制请求数。	5
最低存储容量，SSD 文件系统	32 GiB
最低存储容量，HDD 文件系统	2000 GiB
最大存储容量、SSD 和 HDD	64 TiB
最小吞吐量容量	8 Mbps
最大吞吐量容量	2,048 Mbps
最大文件共享数	100000

其它注意事项

此外，请注意以下情况：

- 你可以使用每个Amazon Key Management Service(Amazon KMS) 密钥最多 125 个 Amazon FSx 文件系统。
- 有关列表Amazon Web Services 区域您可以创建文件系统的位置，请参阅Amazon FSx 终端节点和配额中的Amazon一般参考.
- 您可以使用虚拟私有云 (VPC) 中的 Amazon EC2 实例的域名服务 (DNS) 名称映射文件共享。

特定于微软 Windows 的配额

有关更多信息，请参阅 。NTFS微软 Windows 开发人员中心的限制。

Amazon FSx 故障排除

利用以下部分帮助排您使用 Amazon FSx 时遇到的问题。

如果您在使用 Amazon FSx 时遇到以下未列出的问题，请尝试在Amazon FSx 论坛.

主题

你无法访问你的文件系统

导致无法访问文件系统的潜在原因有很多，每种原因都有自己的分辨率，如下所示。

主题

文件系统elastic network interface 被修改或删除

您不得修改或删除文件系统的elastic network interface。修改或删除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。创建新的文件系统，不要修改或删除 Amazon FSx elastic network interface。有关更多信息，请参阅 使用 Amazon VPC 进行文件系统访问控制 (p. 163)。

已删除附加到文件系统elastic network interface 的弹性 IP 地址

Amazon FSx 不支持从公共互联网访问文件系统。Amazon FSx 会自动分离附加到文件系统elastic network interface 的任何弹性 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 Amazon FSx for Windows File Server 的支持的客户、访问方法和环境 (p. 14)。

文件系统安全组缺少所需的入站或出站规则。

查看中指定的入站规则Amazon VPC 安全组 (p. 163)，并确保与您的文件系统关联的安全组具有相应的入站规则。

计算实例的安全组缺少所需的出站规则

查看中指定的出站规则Amazon VPC 安全组 (p. 163)，并确保与计算实例关联的安全组具有相应的出站规则。

计算实例未加入活动目录

您的计算实例可能无法正确加入以下两种类型的 Active Directory 之一：

- 这些区域有：Amazon Managed Microsoft AD文件系统所加入的目录。
- 一个 Microsoft Active Directory 目录，它与Amazon Managed Microsoft AD目录中。。

确保您的计算实例已加入两种目录中的一种。一种类型是Amazon Managed Microsoft AD文件系统所加入的目录。另一种类型是 Microsoft AD 目录，它与Amazon Managed Microsoft AD目录中。。有关更多信息，请参阅 使用 Amazon FSxAmazon Directory Service for Microsoft Active Directory (p. 22)。

文件共享不存在

你尝试访问的微软 Windows 文件共享不存在。

如果您正在使用现有的文件共享，请确保正确指定了文件系统 DNS 名称和共享名称。要管理您的文件共享，请参阅文件共享 (p. 87).

Active Directory 用户

您正在访问文件共享的 Active Directory 用户缺少必要的访问权限。

确保文件共享的访问权限和共享文件夹的 Windows 访问控制列表 (ACL) 允许需要访问该文件夹的 Active Directory 用户进行访问。

允许删除完全控制 NTFS ACL 权限

如果你移除允许完全控制SYSTEM 用户对您共享的文件夹的 NTFS ACL 权限可能无法访问该共享，并且从那时起进行的任何文件系统备份都可能无法使用。

您需要重新创建受影响的文件共享。有关更多信息，请参阅 文件共享 (p. 87)。重新创建文件夹或共享后，您可以映射和使用计算实例中的 Windows 文件共享。

无法使用本地客户端访问文件系统

您正在使用本地 Amazon FSx 文件系统Amazon Direct Connect或 VPN，并且您正在为本地客户端使用非私有 IP 地址范围。

Amazon FSx 仅支持在 2020 年 12 月 17 日之后创建的文件系统上使用非私有 IP 地址的本地客户端进行访问。

如果您需要访问 2020 年 12 月 17 日之前使用非私有 IP 地址范围创建的 FSx for Windows File Server 文件系统，则可以通过还原文件系统的备份来创建新的文件系统。有关更多信息，请参阅 使用备份 (p. 71)。

未在 DNS 中注册新文件系统

对于加入自我管理的 Active Directory 的文件系统，Amazon FSx 在创建文件系统 DNS 时没有注册它，因为客户网络不使用 Microsoft DNS。

如果您的网络使用第三方 DNS 服务而不是 Microsoft DNS，亚马逊 FSX 不会在 DNS 中注册文件系统。您必须为 Amazon FSx 文件系统手动设置 DNS A 条目。对于单可用区 1 文件系统，您需要添加一个 DNS A 条目；对于单可用区 2 和多可用区文件系统，您需要添加两个 DNS A 条目。使用以下过程获取手动添加 DNS A 条目时要使用的文件系统 IP 地址。

1. 在https://console.aws.amazon.com/fsx/中，选择要获取 IP 地址的文件系统，以显示文件系统详细信息页面。
2. 在网络系统选项卡执行以下操作之一：
   - 对于单可用区 1 文件系统：
     - 在子网面板elastic network interface 选择网络接口以打开的网络接口Amazon EC2
     - 要使用的单可用区 1 文件系统的 IP 地址显示在主要私有 IPv4 IP IPcolumn.
   - 对于单可用区 2 或多可用区文件系统：
     - 在首选子网面板中，选择如下所示的elastic network interface网络接口以打开的网络接口Amazon EC2
     - 要使用的首选子网的 IP 地址显示在辅助私有 IPv4 IPcolumn.
     - 在Amazon FSx 中备用子网面板中，选择如下所示的elastic network interface网络接口以打开的网络接口Amazon EC2 控制台中的页面。
     - 要使用的备用子网的 IP 地址显示在辅助私有 IPv4 IPcolumn.

无法使用 DNS 别名访问文件系统

如果您无法使用 DNS 别名访问文件系统，请使用以下过程解决该问题。

1. 通过执行以下任一步骤来验证别名是否与文件系统相关联：
   a. 使用亚马逊 FSx 控制台— 选择您尝试访问的文件系统。在存储库的文件系统页面上，的DNS 别名显示在网络系统选项卡。。
   b. 使用 CLI 或 API— 使用`describe-file-system-aliases`CLI 命令或DescribeFileSystemAliasesAPI 操作，用于检索当前与文件系统关联的别名。
2. 如果未列出 DNS 别名，则必须将其与文件系统关联。有关更多信息，请参阅 管理现有文件系统上的 DNS 别名 (p. 85)。
3. 如果 DNS 别名与文件系统关联，请确认您还配置了以下必需项：
   - 创建了与 Amazon FSx 文件系统的 Active Directory 计算机对象上的 DNS 别名相对应的服务主体名称 (SPN)。

有关更多信息，请参阅 第 2 步：为 Kerberos 配置服务主体名称 (SPN) (p. 153)。

- 为解析为 Amazon FSx 文件系统的默认 DNS 名称的 DNS 别名记录创建了 DNS 别名记录。

  有关更多信息，请参阅 第 3 步：更新或创建文件系统的 DNS CNAME 记录 (p. 156)。

4. 如果您创建了有效的 SPN 和 DNS CNAME 记录，请验证客户端的 DNS 是否具有解析到正确文件系统的 DNS CNAME 记录。

   a. 运行`nslookup`以确认该记录存在并解析为文件系统的缺省 DNS 名称。

   b. 如果 DNS CNAME 解析到另一个文件系统，请等待客户端的 DNS 缓存刷新，然后再次检查 CNAME 记录。您可以使用以下命令刷新客户端的 DNS 缓存，从而加快该过程。

   ```
   ipconfig /flushdns
   ```

5. 如果 DNS 别名记录解析为 Amazon FSx 文件系统的默认 DNS，并且客户端仍无法访问该文件系统，请参阅你无法访问你的文件系统 (p. 187)以了解其他故障步骤。

尝试创建 Amazon Fsx 文件系统失败

文件系统创建请求失败，有许多潜在的原因，如以下部分所述。

主题

- 对加入的文件系统进行故障排除AmazonMicrosoft Ac (p. 190)
- 文件系统加入自管理活动目录的疑难解答 (p. 190)

对加入的文件系统进行故障排除AmazonMicrosoft Ac

使用以下部分帮助排查尝试创建 FSx for Windows File Server 系统加入自管理的 Active Directory Directory。

VPC 安全组和网络 ACL 未使用推荐的安全组配置

确保使用推荐的安全组配置配置 VPC 安全组和网络 ACL。有关更多信息，请参阅 。创建 FSx 安全组，步骤 6 (p. 163).

文件系统加入自管理活动目录的疑难解答

主题

- 亚马逊 FSx 无法访问自我管理的 AD DNS 服务器或域控制器。文件系统创建失败。 (p. 191)
- 由于服务帐户凭据无效，无法连接到 Microsoft AD 域控制器 (p. 191)
- 由于服务账户权限不足，亚马逊 FSx 无法连接到 Microsoft AD 域控制器 (p. 192)
- Amazon FSx 无法连接到 Microsoft AD 域控制器，因为提供的服务帐户无法再将任何计算机加入该域 (p. 192)
- Amazon FSx 无法连接到 Microsoft AD 域控制器，因为指定的组织单位不存在或无法访问 (p. 193)
- Amazon FSx 无法应用 Microsoft AD 配置，因为文件系统管理员组不存在或服务帐户无法访问 (p. 193)
- 亚马逊 FSx 无法应用你的微软活动目录配置。 (p. 194)
- 文件系统创建失败。提供的服务帐户无权将文件系统加入到具有指定组织单位 (OU) 的域 (p. 194)
- 亚马逊 FSx 无法在指定的 Microsoft Active Directory 中创建文件系统。 (p. 195)

亚马逊 FSx 无法访问自我管理的 AD DNS 服务器或域控制器。文件系统创建失败。

创建加入自管理 Active Directory 的文件系统失败，并显示以下错误消息：

```
Amazon FSx can't reach the DNS servers provided or the domain controllers for
your self-managed directory in Microsoft Active Directory. File system creation failed.
 Amazon FSx is
unable to communicate with your Microsoft Active Directory domain controllers.
This is because Amazon FSx can't reach the DNS servers provided or domain controllers
for your domain. To fix this problem, delete your file system and create a new
one with valid DNS servers and networking configuration that allows traffic from
the file system to the domain controller.
```

使用以下步骤对问题进行故障和解决问题。

1. 验证您是否符合在要创建 Amazon FSx 文件系统的子网与自我管理的 Active Directory 之间建立网络连接和路由的先决条件。有关更多信息，请参阅 使用自行管理的 Microsoft AD 的先决条件 (p. 31)。

   使用亚马逊 FSx 活动目录验证工具 (p. 36)来测试和验证这些网络设置。

   Note

   如果您已定义 Amazon FSx 文件系统，并且 VPC 内定义了子网，并且 VPC 内定义了子网，并且 VPC 内定义了子网，并且 VPC 内定义了子网，并且 VPC 中的子网与您其他站点中的子网之间不存在 IP 冲突。您可以使用 Active Directory 站点和服务 MMC 管理单元查看和更改这些设置。
2. 确认您已将与 Amazon FSx 文件系统关联的 VPC 安全组以及任何 VPC 网络 ACL 配置为允许所有端口上的出站网络流量。

   Note

   如果要实现最低权限，则可以只允许出站流量流向与 Active Directory 域控制器通信所需的特定端口。有关更多信息，请参阅 。Microsoft Ac.
3. 确认 Microsoft Windows 文件服务器或网络管理属性的值不包含非拉丁字符。例如，如果您使用`Domänen-Admins`作为文件系统管理员组的名称。
4. 验证您的 Active Directory 域的 DNS 服务器和域控制器是否处于活动状态，并且能够响应针对所提供域的请求。
5. 确保你的 Active Directory 域的功能级别为 Windows Server 2008 R2 或更高版本。
6. 请确保 Active Directory 域的域控制器上的防火墙规则允许来自您的 Amazon FSx 文件系统的流量。有关更多信息，请参阅 。Microsoft Ac.

由于服务帐户凭据无效，无法连接到 Microsoft AD 域控制器

创建加入自管理 Active Directory 的文件系统失败，并显示以下错误消息：

```
Amazon FSx is unable to establish a connection with your Microsoft
Active Directory domain controllers because the service account credentials provided are
invalid. To fix this problem, delete your file system and create a new one using a valid
 service
account.
```

使用以下步骤对问题进行故障和解决问题。

1. 确认您只输入了用户名作为服务账户用户名之外的压缩算法（例如`ServiceAcct`，在自行管理的 Active Directory 配置中

Important

请勿包含域名前缀 (`corp.com\ServiceAcct`) 或域后缀 (`ServiceAcct@corp.com`) 输入服务帐号用户名时。
输入服务帐户用户名时请勿使用唯一判别名 (DN) (CN=ServiceAcct，OU=xample,

2. 验证您提供的服务帐户是否存在于 Active Directory 域中。
3. 确保已将所需权限委派给您提供的服务帐号。服务帐户必须能够在您要加入文件系统的域中的 OU 中创建和删除计算机对象。服务帐号至少还需要具有执行以下操作的权限：

   - 重置密码
   - 限制账户读取和写入数据
   - 验证了写入 DNS 主机名的能力
   - 已验证写入服务主体名称的能力

   有关创建具有正确权限的服务帐号的更多信息，请参阅 将权限委派给您的 Amazon FSx 服务账户 (p. 35).

由于服务账户权限不足，亚马逊 FSx 无法连接到 Microsoft AD 域控制器

创建加入自管理 Active Directory 的文件系统失败，并显示以下错误消息：

```
Amazon FSx is unable to establish a connection with your
Microsoft Active Directory domain controllers. This is because the service account provided
 does not
have permission to join the file system to the domain with the specified organizational
 unit.
To fix this problem, delete your file system and create a new one using a service account
 with
permission to join the file system to the domain with the specified organizational unit.
```

使用以下过程排查并解决该问题。

- 确保已将所需权限委派给您提供的服务帐号。服务帐户必须能够在您要加入文件系统的域中的 OU 中创建和删除计算机对象。服务帐号至少还需要具有执行以下操作的权限：

  - 重置密码
  - 限制账户读取和写入数据
  - 验证了写入 DNS 主机名的能力
  - 已验证写入服务主体名称的能力

  有关创建具有正确权限的服务帐号的更多信息，请参阅 将权限委派给您的 Amazon FSx 服务账户 (p. 35).

Amazon FSx 无法连接到 Microsoft AD 域控制器，因为提供的服务帐户无法再将任何计算机加入该域

创建加入自管理 Active Directory 的文件系统失败，并显示以下错误消息：

```
Amazon FSx can't establish a connection with your Microsoft Active Directory
```

```
domain controllers. This is because the service account provided has reached the
maximum number of computers that it can join to the domain. To fix this problem,
delete your file system and create a new one, supplying a service account that
is able to join new computers to the domain.
```

要解决此问题，请验证您提供的服务帐户是否已达到它可以加入域的最大计算机数。如果已达到最大限制，请创建一个具有正确权限的新服务帐号。使用新的服务帐户并创建新的文件系统。有关更多信息，请参阅 将权限委派给您的 Amazon FSx 服务账户 (p. 35)。

Amazon FSx 无法连接到 Microsoft AD 域控制器，因为指定的组织单位不存在或无法访问

创建加入自管理 Active Directory 的文件系统失败，并显示以下错误消息：

```
Amazon FSx can't establish a connection with your Microsoft Active Directory domain
 controller(s).
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, delete your file system and create a
 new one specifying an
organizational unit to which the service account can join the file system.
```

使用以下步骤对问题进行故障和解决问题。

1. 验证您提供的 OU 是否在活动目录域中。
2. 确保您已将所需的权限委派给您提供的服务帐号。服务帐户必须能够在您要加入文件系统的域中的 OU 中创建和删除计算机对象。服务帐号还需要至少具有执行以下操作的权限：

   - 重置密码
   - 限制账户读取和写入数据
   - 验证了写入 DNS 主机名的能力
   - 已验证写入服务主体名称的能力
   - 被委派控制权以创建和删除计算机对象
   - 经过验证的读写能力账户限制

   有关创建具有正确权限的服务帐号的更多信息，请参阅 将权限委派给您的 Amazon FSx 服务账户 (p. 35).

Amazon FSx 无法应用 Microsoft AD 配置，因为文件系统管理员组不存在或服务帐户无法访问

创建加入自管理 Active Directory 的文件系统失败，并显示以下错误消息：

```
Amazon FSx is unable to apply your Microsoft Active Directory configuration. This is
 because the file system
administrators group you provided either doesn't exist or isn't accessible to the service
 account you
provided. To fix this problem, delete your file system and create a new one specifying a
 file
system administrators group in the domain that is accessible to the service account
provided.
```

使用以下步骤对问题进行故障和解决问题。

1. 确保您仅提供组的名称作为管理员组参数的字符串。

   Important

   请勿包含域名前缀 (`corp.com\FSxAdmins`) 或域后缀 (`FSxAdmins@corp.com`) 提供组名参数时。
   请不要使用组的可分辨名称 (DN)。唯一判别名的一个例子是 CN=FSxAdmins，OU=xample,
2. 确保提供的管理员组与要加入文件系统的管理员组位于同一 Active Directory 域中。
3. 如果您没有提供管理员组参数，Amazon FSx 会尝试使用`Builtin Domain Admins`在您的Active Directory 域中 如果此组的名称已更改，或者您正在使用其他组进行域管理，则需要为该组提供该名称。

亚马逊 FSx 无法应用你的微软活动目录配置。

创建加入自管理 Active Directory 的文件系统失败，并显示以下错误消息：

```
Amazon FSx is unable to apply your Microsoft Active
Directory configuration. To fix this problem, delete your file system and create a new one
meeting the pre-requisites described in the Amazon FSx user guide.
```

在创建文件系统时，Amazon FSx 能够访问您的 Active Directory 域的 DNS 服务器和域控制器，并将文件系统成功加入到您的 Active Directory 域。但是，在完成文件系统创建过程中，Amazon FSx 失去了与您的域的连接或成员资格。使用以下步骤对问题进行故障和解决问题。

1. 确保您的 Amazon FSx 文件系统和 Active Directory 之间继续保持网络连接。并且，通过使用路由规则、VPC 安全组规则、VPC 网络 ACL 和域控制器防火墙规则，确保它们之间继续允许网络流量。
2. 确保 Amazon FSx 为您在 Active Directory 域中的文件系统创建的计算机对象仍处于活动状态，并且未被删除或以其他方式被操纵。

文件系统创建失败。提供的服务帐户无权将文件系统加入到具有指定组织单位 (OU) 的域

创建加入自管理 Active Directory 的文件系统失败，并显示以下错误消息：

```
File system creation failed. Amazon FSx is unable to establish a connection with your
 Microsoft Active Directory domain controller(s).
This is because the service account provided does not have permission to join the file
 system to the domain with the specified
organizational unit (OU). To fix this problem, delete your file system and create a new one
 using a service account with permission
to create computer objects and reset passwords within the specified organizational unit.
```

确保您已将所需的权限委派给您提供的服务帐号。使用以下步骤对问题进行故障和解决问题。

服务帐号至少需要具有以下权限：

- 被委派控制权以在要加入文件系统的 OU 中创建和删除计算机对象
- 在要加入文件系统的 OU 中具有以下权限：
  - 能够重置密码
  - 能够限制账户读取和写入数据
  - 验证了写入 DNS 主机名的能力
  - 已验证写入服务主体名称的能力

有关创建具有正确权限的服务帐号的更多信息，请参阅 将权限委派给您的 Amazon FSx 服务账户 (p. 35).

亚马逊 FSx 无法在指定的 Microsoft Active Directory 中创建文件系统。

创建加入自管理 Active Directory 的文件系统失败，并显示以下错误消息：

```
File system creation failed. Amazon FSx is unable to create a file system within the
 specified
Microsoft Active Directory. To fix this problem, please delete your file system and create
 a new one
meeting the pre-requisites described in the Amazon FSx user guide.
```

亚马逊 FSx 不支持 Unicode 字符。确认所有创建参数都不包含 Unicode 字符，例如重音符号。这包括在自动填充默认值的情况下可以留空的参数。确保活动目录中相应的默认值也不包含 Unicode 字符。

如果您在使用 Amazon FSx 时遇到未在此处列出的问题，请在Amazon FSx 论坛或联系Amazon Web Services SeSupport.

文件系统处于错误配置状态

一个FSx for Windows File Server 文件系统可以进入配置错误状态是由于 Active Directory 环境的更改而导致的。在这种状态下，您的文件系统要么当前不可用，要么有失去可用性的风险，备份可能无法成功。

这些区域有：配置错误状态包含错误消息和建议的纠正措施，您可以使用 Amazon FSx 控制台、API 或 Amazon CLI. 采取纠正措施后，请验证文件系统的状态最终是否更改为`Available`— 请注意，此更改可能需要几分钟的时间才能完成。

你的文件系统可以进入配置错误state 有几个原因，例如：

- DNS 服务器 IP 地址不再有效。
- 服务帐号凭证不再有效，或者缺少所需的权限。
- 由于网络连接问题，例如 VPC 安全组、VPC 网络 ACL 或路由表配置或域控制器防火墙设置无效，Active Directory 域控制器无法访问。

（有关完整的 Active Directory 要求列表，请参阅使用自行管理的 Microsoft AD 的先决条件 (p. 31). 您还可以验证您的 Active Directory 环境是否已正确配置以满足这些要求，方法是使用亚马逊 FSx 活动目录验证工具 (p. 36).）

要解决其中一些问题，需要直接更新文件系统中的一个或多个参数Active Di，例如更改 DNS 服务器 IP 地址或更改服务帐户用户名或密码。在这些情况下，您的纠正措施必然涉及使用 Amazon FSx 控制台、API 或 Amazon CLI以更新必需的配置参数。

其他问题可能不需要更改任何 Active Directory 配置参数，例如更改域控制器防火墙设置或 VPC 安全组。但是，在这些情况下，您需要采取进一步的操作才能使文件系统变为`Available`. 在确保 Active Directory 环境配置正确后，只需使用 Amazon FSx 控制台、API 或Amazon CLI.

主题

- 文件系统配置错误：Amazon FSx 无法访问您域的 DNS 服务器或域控制器。 (p. 196)
- 文件系统配置错误：服务帐号凭证无效 (p. 196)
- 文件系统配置错误：提供的服务帐号无权将文件系统加入域 (p. 196)
- 文件系统配置错误：服务帐户无法将任何其他计算机加入域 (p. 197)
- 文件系统配置错误：服务帐号无权访问 OU (p. 197)

文件系统配置错误：Amazon FSx 无法访问您域的 DNS 服务器或域控制器。

文件系统将进入`Misconfigured`说明 Amazon FSx 何时无法与你的微软 Active Directory 域控制器进行通信。

要解决此情况，请执行以下操作：

1. 确保您的网络配置允许从文件系统到域控制器的流量。
2. 使用亚马逊 FSx 活动目录验证工具 (p. 36)测试和验证自管理的 Active Directory Directory 的网络设置 有关更多信息，请参阅 将 Amazon FSx 与自主管理的 Microsoft Active Directory 结合使用 (p. 30)。
3. 在 Amazon FSx 控制台中查看文件系统的自管理活动目录配置。
4. 要更新文件系统的自我管理活动目录配置，您可以使用 Amazon FSx 控制台。

   a. 在导航窗格中，选择文件系统，然后选择要更新的文件系统；文件系统此时将显示页面。

   b. 在 上文件系统页面上，选择选择更新在网络和安全性选项卡。。

   您还可以使用 Amazon Fs CX CL`update-file-system`命令或 API 操作UpdateFileSystem.

文件系统配置错误：服务帐号凭证无效

亚马逊 FSx 无法与你的 Microsoft Active Directory 域控制器建立连接。这是因为提供的服务帐号凭证无效。有关更多信息，请参阅 将 Amazon FSx 与自主管理的 Microsoft Active Directory 结合使用 (p. 30)。

要解决配置错误，请执行以下操作：

1. 确认您使用正确的服务帐号，并且 Actory 的凭证正确。
2. 然后使用 Amazon FSx 控制台使用正确的服务账户或账户凭证更新文件系统的配置。

   a. 在导航窗格中，选择文件系统，然后选择要更新的错误配置的文件系统。

   b. 在存储库的文件系统页面上，选择选择更新中的网络和安全性选项卡。。

   您还可以使用 Amazon FSx API 操作`update-file-system`. 要了解更多信息，请参阅UpdateFileSystem中的Amazon FSx API 参考.

文件系统配置错误：提供的服务帐号无权将文件系统加入域

Amazon FSx 无法建立与微软 Active Directory 域控制器的连接。这是因为提供的服务帐号无权将文件系统加入到具有指定 OU 的域。

要解决配置错误，请执行以下操作：

1. 向 Amazon FSx 服务账户添加所需的权限，或者创建具有所需权限的新服务账户。有关此操作的更多信息，请参阅 将权限委派给您的 Amazon FSx 服务账户 (p. 35).
2. 然后，使用新的服务帐户凭据更新文件系统的自我管理的 Active Directory 配置。要更新配置，您可以使用 Amazon FSx 控制台。

   a. 在导航窗格中，选择文件系统，然后选择要更新的文件系统；文件系统此时将显示页面。

b. 在 上文件系统页面上，选择选择更新在网络和安全性选项卡。。

您还可以使用 Amazon FSx API 操作`update-file-system`. 要了解更多信息，请参阅UpdateFileSystem中的Amazon FSx API 参考.

文件系统配置错误：服务帐户无法将任何其他计算机加入域

Amazon FSx 无法建立与微软 Active Directory 域控制器的连接。在这种情况下，这是因为提供的服务帐户已达到它可以加入域的最大计算机数。

要解决配置错误，请执行以下操作：

1. 确定另一个服务帐户或创建一个可以将新计算机加入域的新服务帐户。
2. 然后使用 Amazon FSx 控制台使用新的服务账户凭证更新文件系统的自我管理的 Active Directory 配置。

   a. 在导航窗格中，选择文件系统，然后选择要更新的文件系统；文件系统此时将显示页面。
   b. 在 上文件系统页面上，选择选择更新在网络和安全性选项卡。。

   您还可以使用 Amazon FSx API 操作`update-file-system`. 要了解更多信息，请参阅UpdateFileSystem中的Amazon FSx API 参考.

文件系统配置错误：服务帐号无权访问 OU

Amazon FSx 无法与你的 Microsoft Active Directory 域控制器建立连接，因为提供的服务帐户无法访问指定的 OU。

要解决配置错误，请执行以下操作：

1. 确定另一个服务帐号或创建一个有权访问 OU 的新服务帐号。
2. 然后，使用新的服务帐户凭据更新文件系统的自我管理的 Active Directory 配置。

   a. 在导航窗格中，选择文件系统，然后选择要更新的文件系统；文件系统此时将显示页面。
   b. 在 上文件系统页面上，选择选择更新在网络和安全性选项卡。。

   您还可以使用 Amazon FSx API 操作`update-file-system`. 要了解更多信息，请参阅UpdateFileSystem中的Amazon FSx API 参考.

在 FSx for Windows File Server 上使用远程电源外壳进行故障排除

您可以使用自定义远程管理系统管理 FSx for Windows File Server 文件系统 PowerShell 命令。

主题

新-FSxSmbShare 命令因单向信任而失败

亚马逊 FSx 不支持执行`New-FSxSmbShare` PowerShell 命令，如果您具有单向信任且用户所在的域未配置为信任与 Amazon FSx 文件系统关联的域。

您可以使用以下解决方案之一来解决这种情况：

- 用户正在执行`New-FSxSmbShare`命令必须与 FSx 文件系统位于同一个域中。
- 您可以使用 fsmgmt.msc GUI 在文件系统上创建共享。有关更多信息，请参阅 使用 GUI 管理文件共享 (p. 87)。

您无法使用 Remote 访问文件系统 PowerShell

无法使用 Remote 连接到文件系统的潜在原因有很多 PowerShell，每个都有自己的分辨率，如下所示。

首先要确保你可以成功连接到 Windows 远程 PowerShell 端点，你也可以运行基本的连接测试。例如，您可以运行`test-netconnection endpoint -port 5985`命令。

文件系统的安全组缺少允许远程访问所需的入站规则 PowerShell 连接

文件系统的安全组必须具有允许端口 5985 上的流量的入站规则，才能建立 Remote PowerShell 会话。有关更多信息，请参阅 Amazon VPC 安全组 (p. 163)。

您在之间配置了外部信任Amazon托管 Microsoft Active Direcor

为了使用亚马逊 FSx 遥控器 PowerShell 使用 Kerberos 身份验证，您需要在客户端上为林搜索顺序配置本地组策略。有关更多信息，请参阅 Microsoft 文档配置 Kerberos 林搜索顺序 (KFSO).

尝试启动远程数据库时发生语言本地化错误 PowerShell 会话

您需要添加以下内容`-SessionOption`按照你的命令：`-SessionOption (New-PSSessionOption -uiCulture "en-US")`

下面是两个示例`-SessionOption`启动遥控器时 PowerShell 您的文件系统上的会话。

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName Windows Remote PowerShell Endpoint
 -ConfigurationName FSxRemoteAdmin -scriptblock {fsx-command} -SessionOption (New-
PSSessionOption -uiCulture "en-US")
```

```
PS C:\Users\delegateadmin> Enter-Pssession -ComputerName Windows Remote PowerShell Endpoint
 -ConfigurationName FsxRemoteAdmin -SessionOption (New-PSSessionOption -uiCulture "en-US")
```

您无法在多可用区或单可用区 2 文件系统上配置 DFS-R

多可用区和单可用区 2 文件系统不支持 Microsoft 分布式文件系统复制 (DFS-R)。

多可用区文件系统在本地配置了跨多个访问区域的冗余。使用多可用区部署类型实现跨多个可用区的高可用性。有关更多信息，请参阅 可用性与持久性：单可用区和多可用区文件系统 (p. 18)。

存储或吞吐量容量更新失败

文件系统存储和吞吐量容量更新请求失败的潜在原因有很多，每个都有自己的解决方法。

存储容量增加失败，因为 Amazon FSx 无法访问文件系统的 KMS 加密密钥

存储容量增加请求失败，因为 Amazon FSx 无法访问文件系统的Amazon Key Management Service(Amazon KMS)：加密密钥。

您需要确保 Amazon FSx 有权访问Amazon KMS键以运行管理操作。使用以下信息解决密钥访问问题。

- 如果 KMS 密钥已被删除，则必须使用新 KMS 密钥从备份中创建新的文件系统。有关更多信息，请参阅 演练 2：从备份创建文件系统 (p. 148)。在新文件系统可用后，您可以重试该请求。
- 如果 KMS 密钥已禁用，请重新启用它，然后重试存储容量增加请求。有关更多信息，请参阅 。启用和禁用密钥中的Amazon Key Management Service开发人员指南.
- 如果密钥因其待删除而无效，则必须使用新的 KMS 密钥从备份中创建新的文件系统。在新文件系统可用后，您可以重试该请求。有关更多信息，请参阅 演练 2：从备份创建文件系统 (p. 148)。
- 如果密钥因其待导入而无效，则必须等到导入完成，然后重试存储增加请求。
- 如果已超过密钥的授予限制，则必须请求增加密钥的授权次数。有关更多信息，请参阅 。资源配额中的Amazon Key Management Service开发人员指南. 批准增加配额后，请重试存储增加请求。

存储或吞吐量容量更新失败，因为自我管理的 Active Directory 配置错误

存储容量或吞吐量容量更新请求失败，因为文件系统的自我管理的 Active Directory 处于配置错误的状态。

要解决特定的错误配置状态，请参阅文件系统处于错误配置状态 (p. 195).

由于吞吐容量不足，存储容量增加失败

存储容量增加请求失败，因为文件系统的吞吐容量设置为 8 MB/s。

将文件系统的吞吐容量增加到最低 16 MB/s，然后重试请求。有关更多信息，请参阅 管理吞吐量容量 (p. 122)。

吞吐量容量更新到 8 MB/s 失败

将文件系统的吞吐容量修改为 8 MB/s 的请求失败。

当存储容量增加请求处于待处理状态或正在进行中时，可能会发生这种情况。增加存储容量要求的最低吞吐量为 16 MB/s。等待存储容量增加请求完成，然后重试吞吐量容量修改请求。

恢复备份时将存储类型切换到 HDD 失败

从备份创建文件系统失败，并显示如下错误消息：

```
Switching storage type to HDD while creating a file system from backup
backup_id is not supported because a storage scaling activity was still under
way on the source file system to increase storage capacity from less than 2000
GiB when the backup backup_id was taken, and the minimum storage capacity for
HDD storage is 2000 GiB.
```

还原备份并且已将存储类型从 SSD 更改为 HDD 时，会出现此问题。从备份还原失败，因为您正在恢复的备份是在原始文件系统上仍在增加存储容量时进行的。在请求增加之前，文件系统的 SSD 存储容量低于 2000 GiB，这是创建 HDD 文件系统所需的最小存储容量。

请使用以下过程解决此问题。

1. 等待存储容量增加请求完成，文件系统至少有 2000 GiB 的 SSD 存储容量。有关更多信息，请参阅 监控存储容量的增加 (p. 115)。
2. 对文件系统进行用户启动的备份。有关更多信息，请参阅 使用用户启动的备份 (p. 72)。
3. 使用 HDD 存储将用户启动的备份还原到新的文件系统。有关更多信息，请参阅 还原备份 (p. 75)。

卷影副本故障排除

卷影副本丢失或无法访问有多种潜在原因，如下一节所述。

主题

缺少最早的卷影副本

在以下任一情况下，会删除最旧的卷影副本：

- 如果您有 500 个卷影副本，则下一个卷影副本将替换最旧的卷影副本，而不考虑为卷影副本分配的剩余存储卷空间。
- 如果达到配置的最大卷影副本存储量，下一个卷影副本将替换一个或多个最旧的卷影副本，即使您的卷影副本少于 500 个。

这两个结果都是预期行为。如果分配给卷影副本的存储空间不足，请考虑增加已分配的存储空间。

我所有的卷影副本都丢失了

如果文件系统上的 I/O 性能容量不足（例如，因为您使用的是 HDD 存储、HDD 存储已用完突增容量或吞吐容量不足）可能会导致 Windows Server 删除所有卷影副本，因为它无法维护具有可用 I/O 性能容量的卷影副本。请考虑以下建议来帮助防止出现此问题：

- 如果您使用的是 HDD 存储，请切换到使用 SSD 存储。为此，您可以对文件系统进行备份，然后将存储类型切换为 SSD 进行还原。
- 将文件系统的吞吐容量增加到预期工作负载的三倍。
- 除了配置的最大卷影副本存储量外，请确保您的文件系统至少有 320 MB 的可用空间。
- 在您预计文件系统处于空闲状态时安排卷影复制。

有关更多信息，请参阅 卷影副本的文件系统建议 (p. 77)。

无法在最近还原或更新的文件系统上创建 Amazon FSx 备份或访问卷影副本

这是预期行为。Amazon FSx 在最近还原的文件系统上重建卷影副本状态，并且在重建卷影副本状态时不允许访问卷影副本或备份。

重复数据删除故障排除

重复数据消除问题的潜在原因有很多，如下一节所述。

主题

重复数据删除不起作用

使用我们的重复数据删除文档 (p. 104)，运行`Get-FSxDedupStatus`命令查看最新重复数据消除作业的完成状态。如果一个或多个作业失败，则文件系统的可用存储容量可能不会增加。

重复数据消除作业失败的最常见原因是内存不足。

- 微软推荐最好是每 1 TB 逻辑数据有 1 GB 的内存（或者每 1 TB 的逻辑数据至少有 300 MB + 50 MB）。使用Amazon Fsx 绩效表 (p. 143)以确定与文件系统的吞吐容量相关的内存，并确保内存资源足以满足数据大小。
- 重复数据消除作业配置为 Windows 建议的默认内存分配 25%，这意味着对于具有 32 GB 内存的文件系统，8 GB 可用于重复数据消除。内存分配是可配置的（使用`Set-FSxDedupSchedule`带参数`-Memory`），但消耗额外的内存可能会影响文件系统性能。
- 您可以修改重复数据消除作业的配置，以进一步降低内存需求。例如，您可以将优化限制为在特定的文件类型或文件夹上运行，或者设置最小文件大小和优化期限。我们还建议将重复数据消除作业配置为在文件系统负载最小的空闲期间运行。

如果重复数据消除作业没有足够的时间来完成，您也可能会看到错误。您可能需要更改作业的最长持续时间，如中所述修改重复数据消除计划 (p. 105).

如果重复数据消除作业长期失败，并且在此期间文件系统上的数据发生了变化，则后续重复数据消除作业可能需要更多资源才能首次成功完成。

重复数据消除值意外地设置为 0

的值`SavedSpace`和`OptimizedFilesSavingsRate`对于已配置重复数据消除的文件系统，意外地为 0。

在存储优化过程中，当您增加文件系统的存储容量时，可能会发生这种情况。当您增加文件系统的存储容量时，Amazon FSx 会在存储优化过程中取消现有的重复数据消除任务，该过程会将数据从旧磁盘迁移到较大的新磁盘。存储优化任务完成后，Amazon FSx 将恢复文件系统上的重复数据消除。有关增加存储容量和存储优化的更多信息，请参阅管理存储容量 (p. 112).

删除文件后未释放文件系统上的空间

重复数据消除的预期行为是，如果删除的数据是重复数据消除节省了空间的内容，那么在垃圾回收作业运行之前，文件系统上的空间实际上不会被释放。

您可能会发现有用的做法是，在删除大量文件后立即设置运行垃圾回收作业的计划。垃圾回收作业完成后，您可以将垃圾回收计划设置回其原始设置。这样可以确保您可以立即快速看到删除的空间。

使用以下过程将垃圾回收作业设置为在 5 分钟后运行。

1. 要验证是否已启用重复数据消除，请使用`Get-FSxDedupStatus`命令。有关命令及其预期输出的更多信息，请参阅查看节省的空间量 (p. 105).
2. 使用以下命令设置从现在起 5 分钟后运行垃圾回收作业的计划。

```
$date=get-date
$DayOfWeek = $date.DayOfWeek
$Hour = $date.Hour
$Minute = $date.Minute + 5
$Time = "${Hour}:${Minute}"
Invoke-Command -ComputerName ${RPS_ENDPOINT} -ConfigurationName FSxRemoteAdmin -
ScriptBlock {
    Set-FSxDedupSchedule -Name "WeeklyGarbageCollection" -Days $Using:DayOfWeek -Start
 $Using:Time -DurationHours 9
}
```

3. 在垃圾回收作业运行并释放空间后，将计划设置回其原始设置。

其他信息

本节提供了受支持但已弃用的 Amazon FSx 功能的参考。

主题

设置自定义备份计划

我们建议使用Amazon Backup以便为文件系统设置自定义备份计划。如果您需要比使用时更频繁地安排备份，则此处提供的信息仅供参考。Amazon Backup.

启用后，Amazon FSx for Windows File Server 会在每日备份窗口内每天自动备份您的文件系统一次。Amazon FSx 强制执行您为这些自动备份指定的保留期。它还支持用户启动的备份，因此您可以随时进行备份。

接下来，您可以找到部署自定义备份计划的资源和配置。自定义备份计划按照您定义的自定义计划在 Amazon FSx 文件系统上执行用户启动的备份。例子可能是每六小时一次，每周一次，依此类推。此脚本还配置删除早于指定保留期的备份。

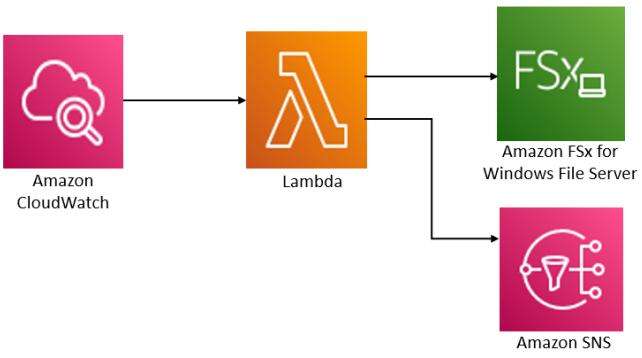
该解决方案会自动部署所有需要的组件，并采用以下参数：

- 文件系统
- 用于执行备份的 CRON 计划模式
- 备份保留期（以天为单位）
- 备份名称标签

有关 CRON 计划模式的更多信息，请参阅规则的计划表达式在 Amazon CloudWatch 用户指南。

架构概述

部署此解决方案将在Amazon Web Services 云.



此解决方案将执行以下操作：

1. 这些区域有：Amazon CloudFormation模板部署 CloudWatch 事件、Lambda 函数、Amazon SNS 队列和 IAM 角色。IAM 角色授予 Lambda 函数调用 Amazon FSx API 操作的权限。
2. 这些区域有： CloudWatch 在初始部署期间，事件按照您定义为 CRON 模式的计划运行。此事件调用解决方案的备份管理器 Lambda 函数，该函数调用 Amazon FSx`CreateBackup`用于启动备份的 API 操作。
3. 备份管理器使用以下方法检索指定文件系统的现有用户启动备份列表。`DescribeBackups`. 然后，它会删除早于您在初始部署期间指定的保留期限的备份。
4. 如果您选择在初始部署期间收到通知的选项，备份管理器会在成功备份时向 Amazon SNS 队列发送通知消息。如果发生故障，始终会发送通知。

Amazon CloudFormation 模板

此解决方案使用Amazon CloudFormation以自动部署 Amazon FSx 自定义备份计划解决方案。要使用此解决方案，请下载fsx 计划备份。模板 Amazon CloudFormation。

自动部署

以下过程配置和部署此自定义备份计划解决方案。部署需要约 5 分钟的时间。开始使用前，您必须在您的 Amazon Virtual Private Cloud (Amazon VPC) 中运行的 Amazon FSx 文件系统的 ID。Amazonaccount. 有关创建这些资源的更多信息，请参阅开始使用 Amazon FSx (p. 7).

Note

实施此解决方案需要对相关的Amazon服务。有关更多信息，请参阅这些服务的定价详情页面。

启动自定义备份解决方案堆栈

1. 下载fsx 计划备份。模板 Amazon CloudFormation。有关创建Amazon CloudFormation堆栈，请参阅在创建堆栈Amazon CloudFormation控制台中的Amazon CloudFormation用户指南.

   Note

   默认情况下，此模板将在美国东部（弗吉尼亚北部）启动Amazon区域。Amazon FSx 目前仅在特定情况下可用Amazon Web Services 区域. 你必须在Amazon亚马逊 FSx 可用的地区。有关更多信息，请参阅Amazon Web Services 区域和终端节点中的Amazon一般参考。
2. 适用于参数中，查看模板的参数，并根据文件系统的需要对其进行修改。此解决方案使用以下默认值。

参数	默认值	描述
Amazon FSx 文件系统 ID	没有默认值	要备份的文件系统的文件系统 ID。
CRON 计划备份模式。	0 0/4 * ? *	运行 CloudWatch 事件，触发新备份并在保留期之外删除旧备份。
Backup 保留期限（天）	7	保留用户启动的备份的天数。Lambda 函数删除用户启动的早于此天数的备份。
备份名称	用户计划的备份	这些备份的名称，出现在备份名称亚马逊 FSx 管理控制台的列。

参数	默认值	描述
Backup 通知	是	选择是否在成功启动备份时收到通知。如果有错误，总是会发送通知。
电子邮件地址	没有默认值	订阅 SNS 通知的电子邮件地址。

3. 选择 Next（下一步）。
4. 适用于选项，选择下一步.
5. 适用于审核中，审核并确认设置。您必须选中确认模板创建 IAM 资源的复选框。
6. 选择 Create (创建) 以部署堆栈。

您可以在 Amazon CloudFormation 控制台的 Status (状态) 列中查看堆栈的状态。您应看到状态创建 _ 完成在大约五分钟内。

其他选项

您可以使用此解决方案创建的 Lambda 函数对多个 Amazon FSx 文件系统执行定时备份。文件系统 ID 将传递给的输入 JSON 中的 Amazon FSx 函数 CloudWatch event. 传递给 Lambda 函数的默认 JSON 如下所示，其中`FileSystemId`和`SuccessNotification`从启动时指定的参数传递Amazon CloudFormation堆栈。

```
{
 "start-backup": "true",
 "purge-backups": "true",
 "filesystem-id": "${FileSystemId}",
 "notify_on_success": "${SuccessNotification}"
}
```

要为其他 Amazon FSx 文件系统安排备份，请创建另一个 CloudWatch 事件规则。您可以使用计划事件源来执行此操作，并将此解决方案创建的 Lambda 函数作为目标。选择常量（JSON 文本）下配置输入. 对于 JSON 输入，只需将 Amazon FSx 文件系统的文件系统 ID 替换为`${FileSystemId}`. 另外，也可以替换`Yes`要么`No`代替`${SuccessNotification}`在以上 JSON 中。

任何额外 CloudWatch 手动创建的事件规则不是 Amazon FSx 自定义定时备份解决方案的一部分Amazon CloudFormation堆栈。因此，如果删除堆栈，它们不会被删除。

使用 Microsoft 分布式文件系统复制

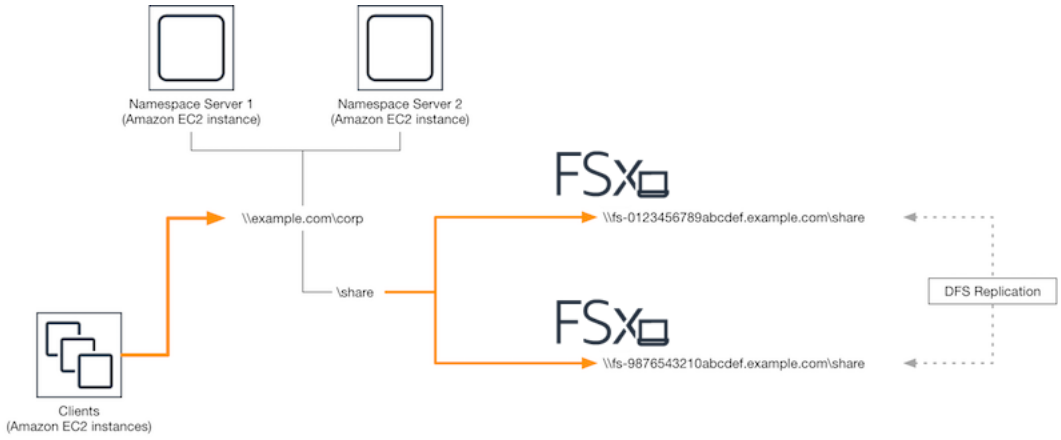
> **Note**
>
> 为了实现 FSx for Windows File Server 的高可用性，我们建议使用 Amazon FSx 多可用区。有关 Amazon FSx 多可用区的更多信息，请参阅可用性与持久性：单可用区和多可用区文件系统 (p. 18)

Amazon FSx 支持使用 Microsoft 分布式文件系统 (DFS) 跨多个可用区 (AZ) 进行文件系统部署，以获得多可用区可用性和持久性。使用 DFS 复制，您可以在两个文件系统之间自动复制数据。使用 DFS 命名空间，您可以将一个文件系统配置为主文件系统，另一个作为备用系统，如果主文件系统无响应，则可以自动故障切换到备用系统。

在使用 DFS 复制前，请执行以下步骤：

- 按照中所述设置您的安全组。Step 8 (p. 8)Amazon FSx 入门。
- 在不同的可用区中创建两个 Amazon FSx 文件系统Amazon区域。有关创建文件系统的更多信息，请参阅第 3 步：将数据写入文件共享 (p. 11).
- 确保两个文件系统都在同一个Amazon Directory Service for Microsoft Active Directory.
- 创建文件系统后，记下它们的文件系统 ID 以供以后使用。

在以下主题中，您可以找到有关如何在 Amazon FSx 中设置和使用 DFS 复制和 DFS 命名空间故障转移的说明。



设置 DFS 复制

您可以使用 DFS 复制在两个 Amazon FSx 文件系统之间自动复制数据。此复制是双向的，这意味着您可以写入任一文件系统，然后将更改复制到另一个文件系统。

> Important
>
> 你不能使用微软 Windows 管理工具 (dfsmgmt.msc) 中的 DFS 管理界面在你的 FSx 适用于 Windows 文件服务器文件系统上配置 DFS 复制。

要设置 DFS 复制（脚本化）

1. 启动实例并将其连接到加入 Amazon FSx 文件系统的 Microsoft Active Directory，开始管理 DFS 的过程。为此，请从中选择以下步骤之一：Amazon Directory Service管理指南：
   - 无缝加入 Windows EC2 实例
   - 手动加入 Windows 实例
2. 作为文件系统管理员组成员的 Active Directory 用户 Connect 到您的实例。InAmazon托管 AD，这个组被称为Amazon委托 FSx 管理员。在自我管理的 Microsoft AD 中，此组称为域管理员或您在创建过程中提供的管理员组的自定义名称。

   此用户还必须是向其授予 DFS 管理权限的组的成员。InAmazon托管 AD，这个组被称为Amazon分布式文件系统委托管理员。在自我管理的 AD 中，此用户必须是域管理员或您向其委派 DFS 管理权限的其他组的成员。

   有关更多信息，请参阅适用于 Windows 实例的 Amazon EC2 用户指南中的连接您的 Windows 实例。
3. 下载FSX-dfsr-setup.ps1 PowerShell 脚本.
4. 打开启动然后输入菜单PowerShell. 从列表中选择Windows PowerShell.
5. 运行 PowerShell 脚本具有以下指定参数，用于在两个文件系统之间建立 DFS 复制：

- DFS 复制组和文件夹的名称
- 要在文件系统上复制的文件夹的本地路径（例如，`D:\share`对于您的 Amazon FSx 文件系统附带的默认份额）
- 您在先决条件步骤中创建的主要和备用 Amazon FSx 文件系统的 DNS 名称

Example

```
FSx-DFSr-Setup.ps1 -group Group -folder Folder -path ContentPath -
primary FSxFileSystem1-DNS-Name -standby FSxFileSystem2-DNS-Name
```

要设置 DFS 复制（逐步）

1. 启动实例并将其连接到加入 Amazon FSx 文件系统的 Microsoft Active Directory，开始管理 DFS 的过程。为此，请从中选择以下步骤之一：Amazon Directory Service管理指南：
   - 无缝加入 Windows EC2 实例
   - 手动加入 Windows 实例
2. 作为文件系统管理员组成员的 Active Directory 用户 Connect 到您的实例。InAmazon托管 AD，这个组被称为Amazon委托 FSx 管理员。在自我管理的 Microsoft AD 中，此组称为域管理员或您在创建过程中提供的管理员组的自定义名称。

   此用户还必须是向其授予 DFS 管理权限的组的成员。InAmazon托管 AD，这个组被称为Amazon分布式文件系统委托管理员。在自我管理的 AD 中，此用户必须是域管理员或您向其委派 DFS 管理权限的其他组的成员。

   有关更多信息，请参阅适用于 Windows 实例的 Amazon EC2 用户指南中的连接您的 Windows 实例。
3. 打开启动然后输入菜单PowerShell. 从列表中选择Windows PowerShell.
4. 如果尚未安装 DFS 管理工具，请使用以下命令在实例上安装它们。

   ```
   Install-WindowsFeature RSAT-DFS-Mgmt-Con
   ```
5. 从 PowerShell 提示符下，使用以下命令创建 DFS 复制组和文件夹。

   ```
   $Group = "Name of the DFS Replication group"
   $Folder = "Name of the DFS Replication folder"

   New-DfsReplicationGroup -GroupName $Group
   New-DfsReplicatedFolder -GroupName $Group -FolderName $Folder
   ```
6. 使用以下命令确定与每个文件系统关联的 Active Directory 计算机名称。

   ```
   $Primary = "DNS name of the primary FSx file system"
   $Standby = "DNS name of the standby FSx file system"

   $C1 = (Get-ADObject -Filter "objectClass -eq 'Computer' -and ServicePrincipalName -eq
    'HOST/$Primary'").Name
   $C2 = (Get-ADObject -Filter "objectClass -eq 'Computer' -and ServicePrincipalName -eq
    'HOST/$Standby'").Name
   ```
7. 将文件系统添加为使用以下命令创建的 DFS 复制组的成员。

   ```
   Add-DfsrMember -GroupName $Group -ComputerName $C1
   Add-DfsrMember -GroupName $Group -ComputerName $C2
   ```

8. 使用以下命令添加本地路径（例如，D:\share) 对于每个文件系统到 DFS 复制组。在此过程中，*file system 1*充当主要成员，这意味着其内容最初同步到另一个文件系统。

```
$ContentPath1 = "Local path to the folder you want to replicate on file system 1"
$ContentPath2 = "Local path to the folder you want to replicate on file system 2"

Set-DfsrMembership -GroupName $Group -FolderName $Folder -ContentPath $ContentPath1 -
ComputerName $C1 -PrimaryMember $True
Set-DfsrMembership -GroupName $Group -FolderName $Folder -ContentPath $ContentPath2 -
ComputerName $C2 -PrimaryMember $False
```

9. 使用以下命令在文件系统之间添加连接。

```
Add-DfsrConnection -GroupName $Group -SourceComputerName $C1 -DestinationComputerName
 $C2
```

在几分钟内，两个文件系统都应开始同步ContentPath之前指定。

为故障转移设置 DFS 命名空间

您可以使用 DFS 命名空间将一个文件系统视为主文件系统，另一个将其视为备用文件系统。通过执行此操作，您可以在主节点无响应时配置自动故障转移到备用设备。DFS 命名空间使您能够将不同服务器上的共享文件夹分组到单个命名空间中，单个文件夹路径可以导致存储在多个服务器上的文件。DFS 命名空间由 DFS 命名空间服务器管理，该服务器将 DFS 命名空间文件夹映射到相应的文件服务器的计算实例。

为故障转移设置 DFS 命名空间 (UI)

1. 如果您尚未运行 DFS 命名空间服务器，请使用设置-dfsn-Server。模板 Amazon CloudFormation。有关创建Amazon CloudFormation堆栈，请参阅在创建堆栈Amazon CloudFormation 控制台中的Amazon CloudFormation用户指南.
2. 以用户身份 Connect 到在上一步中启动的 DFS 命名空间服务器之一Amazon委托管理员组。有关更多信息，请参阅适用于 Windows 实例的 Amazon EC2 用户指南中的连接您的 Windows 实例。
3. 打开 DFS 管理控制台。打开启动然后运行菜单dfsmgmt.msc. 此操作将打开 DFS 管理 GUI 工具。
4. 适用于操作，选择新命名空间，然后输入您为其启动的第一个 DFS 命名空间服务器的计算机名称服务器然后选择下一步.
5. 适用于名称中，输入您正在创建的命名空间（例如，**corp**)。
6. 选择编辑设置并根据您的要求设置适当的权限。选择 Next（下一步）。
7. 保留默认值基于域的命名空间选择选项，请保留启用 Windows Server 2008 模式选项已选中，然后选择下一步.

   Note

   Windows Server 2008 模式是命名空间的最新可用选项。
8. 查看命名空间设置并选择Create.
9. 在下面选择了新创建的命名空间命名空间在导航栏中，选择操作，那么添加命名空间 Server.
10. 适用于命名空间 Server中，输入您启动的第二个 DFS 命名空间服务器的计算机名称。
11. 选择编辑设置，根据您的要求设置适当的权限，然后选择确定.
12. 选择Add中，输入主 Amazon FSx 文件系统上文件共享的 UNC 名称（例如*fs-0123456789abcdef0*.example.com*##*) 对于文件夹的路径目标，然后选择确定.
13. 选择Add中，输入备用 Amazon FSx 文件系统上文件共享的 UNC 名称（例如，*fs-fedbca9876543210f*.example.com*##*) 对于文件夹的路径目标，然后选择确定。
14. 从新文件夹窗口中，选择确定. 新文件夹将使用命名空间下的两个文件夹目标创建。

15. 对要添加到命名空间的每个文件共享重复最后三个步骤。

为故障转移设置 DFS 命名空间 (PowerShell)

1. 如果您尚未运行 DFS 命名空间服务器，请使用设置-dfsn-Server。模板 Amazon CloudFormation。有关创建Amazon CloudFormation堆栈，请参阅在创建堆栈Amazon CloudFormation 控制台中的Amazon CloudFormation用户指南.
2. 以用户身份 Connect 到在上一步中启动的 DFS 命名空间服务器之一Amazon委托管理员组中)。有关更多信息，请参阅适用于 Windows 实例的 Amazon EC2 用户指南中的连接您的 Windows 实例。
3. 打开启动然后输入菜单PowerShell. Windows PowerShell将出现在匹配列表中。
4. 打开的上下文（右键单击）菜单Windows PowerShell然后选择作为管理员运行.
5. 如果尚未安装 DFS 管理工具，请使用以下命令将其安装在实例上。

```
Install-WindowsFeature RSAT-DFS-Mgmt-Con
```

6. 如果还没有现有 DFS 命名空间，可以使用以下命名空间创建一个 PowerShell 命令。

```
$NSS1 = computer name of the 1st DFS Namespace server
$NSS2 = computer name of the 2nd DFS Namespace server

$DNSRoot = fully qualified Active Directory domain name (e.g. mydomain.com)
$Namespace = Namespace name you want to use
$Folder = Folder path you want to use within the Namespace
$FS1FolderTarget = Share path to Folder Target on File System 1
$FS2FolderTarget = Share path to Folder Target on File System 2

$NSS1,$NSS2 | ForEach-Object { Invoke-Command -ComputerName $_ -ScriptBlock { mkdir “C:
\DFS\${using:Namespace}”;
New-SmbShare -Name ${using:Namespace} -Path “C:\DFS\${using:Namespace}” } }

New-DfsnRoot -Path "\\${DNSRoot}\${Namespace}" -TargetPath "\\${NSS1}.${DNSRoot}\
${Namespace}" -Type DomainV2
New-DfsnRootTarget -Path "\\${DNSRoot}\${Namespace}" -TargetPath "\\${NSS2}.${DNSRoot}\
${Namespace}"
```

7. 要在 DFS 命名空间中创建文件夹，可以使用以下 PowerShell 命令。这样做会创建一个文件夹，默认情况下将访问该文件夹的计算实例引导到您的主 Amazon FSx 文件系统。

```
$FS1 = DNS name of primary FSx file system
New-DfsnFolder -Path “\\${DNSRoot}\${Namespace}\${Folder}" -TargetPath “\\${FS1}\
${FS1FolderTarget}” -EnableTargetFailback $True -ReferralPriorityClass GlobalHigh
```

8. 将备用 Amazon FSx 文件系统添加到同一个 DFS 命名空间文件夹中。如果访问该文件夹的计算实例无法连接到主 Amazon FSx 文件系统，则返回到此文件系统。

```
$FS2 = DNS name of secondary FSx file system
New-DfsnFolderTarget -Path “\\${DNSRoot}\${Namespace}\${Folder}" -TargetPath “\\${FS2}\
${FS2FolderTarget}”
```

现在，您可以使用之前指定的 DFS 命名空间文件夹的远程路径从计算实例访问数据。执行此操作会将计算实例定向到主 Amazon FSx 文件系统（如果主实例无响应，则指向备用文件系统）。

例如，打开启动然后输入菜单PowerShell. 从列表中选择Windows PowerShell然后运行以下命令。

```
net use Z: \\${DNSRoot}\${Namespace}\${Folder} /persistent:yes
```

使用维护时段和 FSx 多可用区

为了帮助确保多可用区文件系统部署的高可用性，我们建议您为多可用区部署中的两个 Amazon FSx 文件系统选择不重叠的维护窗口。这样做有助于确保您的文件数据在系统维护时段内继续供应用程序和用户使用。

Note

要允许 DFS 复制流量进出文件系统，请确保添加 VPC 安全组入站和出站规则，如中所述Amazon VPC 安全组 (p. 163).

文档历史记录

- API 版本：2018-03-01
- 最近文档更新时间：2022 年 4 月 5 日

下表介绍了对亚马逊 FSx Windows 用户指南. 如需有关文档更新的通知，您可以订阅 RSS 源。

update-history-change	update-history-description	update-history-date
添加了对的 SupportAmazon PrivateLink接口 VPC 终端节点。 (p. 211)	您现在可以使用接口 VPC 终端节点从 VPC 访问 Amazon FSx API，而无需通过 Internet 发送流量。有关更多信息，请参阅 。Amazon FSx 和接口 VPC 终端节点.	2022 年 4 月 5 日
添加了对 Amazon Kendra 的 Support (p. 211)	现在，您可以将 FSx for Windows File Server 文件系统用作 Amazon Kendra 的数据源，允许您索引和搜索文件系统中存储的文档中包含的信息。有关更多信息，请参阅 。将 FSx for Windows File Server 与 Amazon Kendra 结合使用.	2022年 3 月 26 日
添加了对文件访问审计的 Support (p. 211)	现在，您可以启用对文件、文件夹和文件共享的最终用户访问权限的审计。您可以选择将审计事件日志发送到 Amazon CloudWatch 日志或 Amazon Kinesis Data Firehose 服务。有关更多信息，请参阅 。文件访问审计.	2021 年 6 月 8 日
添加了对复制备份的 Support (p. 211)	现在，您可以使用 Amazon FSx 在同一范围内复制备份Amazon另一个账户Amazon区域（跨区域副本）或同一个Amazon区域（区域内副本）。有关更多信息，请参阅 。复制备份.	2021 年 4 月 12 日
自动增加文件系统的存储容量 (p. 211)	使用Amazon开发的可自定义 Amazon CloudFormation模板，当文件系统的容量达到指定阈值时，自动增加文件系统的存储容量。有关更多信息，请参阅 。动态增加存储容量.	2021 年 2 月 17 日
添加了 Support 使用非私有 IP 地址的客户端访问的支 (p. 211)	您可以通过使用非私有 IP 地址的本地客户端访问适用于 Windows 文件服务器文件系统的 FSx。有关更多信息，请参阅 。支持的环境. 你可以将 FSx for Windows File Server 件系统加入到具有使用非私有 IP 地址的 DNS 服务器	2020 年 12 月 17 日

	和 AD 域控制器的自我管理的微软 Active Directory。有关更多信息，请参阅 。将亚马逊 FSx 与自我管理的微软活动目录一起使用.	
添加了对使用 DNS 别名的 Support (p. 211)	现在，您可以将 DNS 别名与可用于访问文件系统上的数据的 FSx for Windows 文件服务器文件系统关联起来。有关更多信息，请参阅 。管理 DNS 别名和演练 5：使用 DNS 别名访问文件系统.	2020 年 11 月 9 日
增 Support 了对 Amazon Elastic Container Service 的 (p. 211)	您现在可以将 FSx for Windows File Server 与 Amazon ECS 结合使用。有关更多信息，请参阅 。支持的客户.	2020 年 11 月 9 日
Amazon FSx 现已与集成Amazon Backup (p. 211)	现在，您可以使用Amazon Backup除了使用本机 Amazon FSx 备份之外，还可以备份和还原 FSx 文件系统。有关更多信息，请参阅 。使用Amazon Backup使用 Amazon FSx.	2020 年 11 月 9 日
增加了吞吐量容量扩展的 Support (p. 211)	现在，随着吞吐量要求的发展，您可以修改 Windows 文件服务器文件系统的现有 FSx 的吞吐量。有关更多信息，请参阅 。管理吞吐容量.	2020 年 6 月 1 日
增加了对存储容量扩展的 Support (p. 211)	随着存储需求的发展，现在可以增加 Windows 文件服务器文件系统的现有 FSx 的存储容量。有关更多信息，请参阅 。管理存储容量.	2020 年 6 月 1 日
增加了对硬盘驱动器 (HDD) 存储的 Support (p. 211)	使用 FSx for Windows File Server 时，HDD 存储可为您提供价格和性能灵活性。有关更多信息，请参阅 。使用亚马逊 FSx 优化成本.	20202020 年 3 月 26 日
添加了对文件传输的 SupportAmazon DataSync (p. 211)	现在，您可以使用Amazon DataSync将文件传输到 FSx for Windows File Server。有关更多信息，请参阅 。使用将文件迁移到 Amazon FSx for Windows File ServerAmazonDataSync.	2020 年 2 月 4 日
FSx for Windows File Server 发布了对其他 Windows 文件系统管理任务的支持 (p. 211)	现在，您可以使用 Amazon FSx CLI 在 PowerShell 上进行远程管理，管理文件共享、重复数据消除、存储配额和传输中的文件共享、存储配额和加密。有关更多信息，请参阅 。管理文件系统.	2019 年 11 月 20 日

FSx for Windows File Server 发布原生的多可用区支持 (p. 211)	您可以使用 FSx for Windows File Server 的多可用区部署，以便更轻松地创建跨多个可用区 (AZ) 的高可用性文件系统。有关更多信息，请参阅 。可用性与持久性：单可用区和多可用区文件系统.	2019 年 11 月 20 日
FSx for Windows File Server 发布了对管理用户会话和打开文件的支持 (p. 211)	现在，你可以使用 Microsoft Windows 原生的共享文件夹工具来管理用户会话并在你的 FSx for Windows 文件服务器文件系统上打开文件。有关更多信息，请参阅 。管理用户会话和打开文件.	2019 年 10 月 17 日
Amazon FSx for Microsoft Windows 卷影副本发布支持 (p. 211)	您现在可以在 FSx for Windows File Server 文件系统中配置 Windows 卷影副本。卷影副本使用户可以通过将文件恢复到以前的版本轻松撤消文件更改并比较文件版本。有关更多信息，请参阅 。使用卷影副本.	2019 年 7 月 31 日
亚马逊 FSx 发布共享的微软活动目录支持 (p. 211)	您现在可以加入 FSx for Windows File Server 文件系统，Amazon Managed Microsoft AD位于不同 VPC 或不同 VPC 中的目录 Amazon Web Services 账户比文件系统。有关更多信息，请参阅 。Active Directory Support.	2019 年 6 月 25 日
亚马逊 FSx 发布增强的微软活动目录支持 (p. 211)	您现在可以将适用于 Windows 文件服务器文件系统的 FSx 加入自我管理的 Microsoft Active Directory 域，无论是在本地还是云中。有关更多信息，请参阅 。Active Directory Support.	2019 年 6 月 24 日
亚马逊 FSx 符合 SOC 认证 (p. 211)	亚马逊 FSx 已经进行了评估，以符合 SOC 认证。有关更多信息，请参阅 。安全与数据保护.	2019 年 5 月 16 日
添加了关于Amazon Direct Connect、VPN 和区域间 VPC 对等连接支持 (p. 211)	可以使用以下方式访问 2019 年 2 月 22 日之后创建的 Amazon FSx 文件系Amazon Direct Connect、VPN 和区域间 VPC 对等连接。有关更多信息，请参阅 。支持的访问方法.	2019 年 2 月 25 日
Amazon Direct Connect增加了 VPN 和区域间 VPC 对等连接支持 (p. 211)	您现在可以从本地资源和其他 Amazon VPC 中的资源访问适用于 Windows 文件服务器的 Amazon FSx 文件服务器文件系统，或Amazon Web Services 账户. 有关更多信息，请参阅 。支持的访问方法.	2019 年 2 月 22 日

Amazon FSx 现已正式发布 (p. 211)	Amazon FSx for Windows File Server 提供完全托管的 Microsoft Windows 文件服务器，由完全原生的 Windows 文件系统提供支持。Amazon FSx for Windows File Server 提供功能、性能和兼容性，可轻松将企业应用程序直接迁移到。Amazon.	2018 年 11 月 28 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。