亚马逊云科技

Windows 用户指南

FSx 适用于 Windows 文件服务器的亚马逊

FSx 适用于 Windows 文件服务器的亚马逊: 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 (PDF)。

Table of Contents

什么 FSx 适用于 Windows 文件服务器？

亚马逊 FSx 版 Windows 文件服务器提供完全托管的微软 Windows 文件服务器，由完全原生 Windows 文件系统提供支持。 FSx 适用于 Windows File Server 的功能、性能和兼容性可以轻松地将企业应用程序提升和转移到 Amazon Web Services 云。

亚马逊 FSx 支持各种企业 Windows 工作负载，其完全托管的文件存储建立在微软 Windows 服务器上。Amaz FSx on 原生支持 Windows 文件系统功能和通过网络访问文件存储的行业标准服务器消息块 (SMB) 协议。 FSx Amazon 针对中的企业应用程序进行了优化 Amazon Web Services 云，具有原生 Windows 兼容性、企业性能和功能以及稳定的亚毫秒级延迟。

借助 Amazon FSx 上的文件存储，Windows 开发人员和管理员当今使用的代码、应用程序和工具可以继续保持不变。适用于 Amazon 的 Windows 应用程序和工作负载 FSx 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。

作为一项完全托管的服务， FSx 适用于 Windows File Server 可消除设置和配置文件服务器和存储卷的管理开销。此外，Amazon还会 FSx 使Windows软件保持最新状态，检测和解决硬件故障，并执行备份。它还提供了与其他 Amazon 服务（如 Amazon IAM、Amazon Directory Service for Microsoft Active Directory、A mazon WorkSpaces 和）的丰富集成Amazon CloudTrail。Amazon Key Management Service

FSx 适用于 Windows 文件服务器资源：文件系统、备份和文件共享

Amazon 的主要资源 FSx 是文件系统和备份。文件系统用于存储和访问文件和文件夹。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，需要指定存储容量（以 GiB 为单位）、SSD IOPS 和吞吐容量（英寸）。 MBps创建文件系统后，您可以根据需要修改这些属性。有关更多信息，请参阅管理存储容量、管理 SSD IOPS和管理吞吐能力。

FSx 对于 Windows 文件服务器 file-system-consistent，备份是高度持久的增量备份。为了确保文件系统的一致性，亚马逊在微软 Windows 中 FSx 使用卷影复制服务 (VSS)。创建文件系统时，系统会默认开启每日自动备份，您也可以随时进行额外的手动备份。有关更多信息，请参阅 使用备份保护您的数据。。

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），您可以授权计算实例通过 SMB 访问该文件夹。文件系统已随附名为 `\share` 的默认 Windows 文件共享。您可以使用 Shared Folders 图形用户界面（GUI）工具，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 使用文件共享访问数据。

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。

访问文件共享

使用 SMB 协议（支持 2.0 到 3.1.1 版本）的计算实例可以访问亚马逊 FSx 。您可以使用 Windows Server 2008 和 Windows 7 之后的所有 Windows 版本访问共享，也可以通过当前版本的 Linux 访问共享。您可以在亚马逊弹性计算云 (Amazon EC2) 实例、实例、亚马逊 AppStream 2.0 实例和 C VMware loud on 上 WorkSpaces 映射您的亚马逊 FSx 文件共享 Amazon VMs。

您可以使用 Amazon Direct Connect 或 Amazon VPN从本地计算实例访问文件共享。除了访问同一 VPC、 Amazon 账户和 Amazon Web Services 区域 文件系统中的文件共享外，您还可以从位于不同 Amazon VPC、账户或中的计算实例访问您的共享 Amazon Web Services 区域。这可以通过 VPC 对等连接或传输网关实现。有关更多信息，请参阅 从 Amazon Web Services 云 内部访问数据。

安全与数据保护

Amazon FSx 提供多个级别的安全和合规性，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 Amazon Key Management Service （文件系统和备份Amazon KMS）。还会使用 SMB Kerberos 会话密钥自动加密传输中数据。Amazon FSx 已通过评测，符合 ISO、PCI-DSS 和 SOC 认证，并且符合 HIPAA 要求。

亚马逊 FSx 通过 Windows 访问控制列表 (ACLs) 提供文件和文件夹级别的访问控制。在文件系统级别，它使用 Amazon Virtual Private Cloud（Amazon VPC）安全组来控制访问权限。另外，在 API 级别，它使用 Amazon Identity and Access Management （IAM）访问策略提供访问控制。访问文件系统的用户需要使用 Microsoft Active Directory 进行身份验证。Amazon 与 FSx 集成 Amazon CloudTrail 以监控和记录您的 API 调用，让您查看用户对您的亚马逊 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，并允许您随时进行其他备份。有关更多信息，请参阅 Amazon 的安全 FSx。

可用性与持久性

FSx 适用于 Windows File Server 的文件系统为文件系统提供了两个级别的可用性和持久性。单可用区文件通过自动检测和解决组件故障来确保单个可用区（AZ）内的高可用性。此外，多可用区文件系统通过在一个区域内的单独可用区中配置和维护备用文件服务器，跨多个可用区提供高可用性和故障转移支持。 Amazon 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，请参阅可用性与持久性：单可用区和多可用区文件系统。

> **Note**
>
> 多可用区文件系统在中国（北京）区域不可用。

管理文件系统

您可以使用自定义远程管理 PowerShell 命令管理 FSx 适用于 Windows 文件服务器的文件系统，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 FSx 为 Windows 文件系统进行管理。

灵活的价格与性能

FSx 适用于 Windows File Server 的固态硬盘 (SSD) 和硬盘驱动器 (HDD) 存储类型可为您提供价格和性能上的灵活性。HDD 存储专为各种工作负载而设计，包括主目录、用户和部门共享以及内容管理系统。SSD 存储专为性能最高、对延迟最敏感的工作负载而设计，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 Windows File Server，您可以独立配置文件系统存储、固态硬盘 IOPS 和吞吐量，以实现成本和性能的适当组合。您可以修改文件系统的存储、固态硬盘 IOPS 和吞吐能力，以满足不断变化的工作负载需求，并且您只需要为必要内容付费。

亚马逊的定价 FSx

使用Amazon FSx，无需支付前期硬件或软件成本。您只需为使用的资源付费，没有最低承付款、设置费用或额外费用。有关该服务的定价和费用的信息，请参阅亚马逊 Window FSx s 文件服务器定价。

假设

要使用 Amazon FSx，您需要一个在支持类型的 Amazon 环境中具有在 VMware 云端运行的 Amazon EC2 实例、实例、 WorkSpaces 应用程序实例或虚拟机的 Amazon 账户。 WorkSpaces

在本指南中，我们做出了以下假设：

- 如果您使用的是亚马逊 EC2，我们假设您熟悉亚马逊 EC2。有关如何使用亚马逊的更多信息 EC2，请参阅亚马逊弹性计算云文档。

- 如果您正在使用 WorkSpaces，我们假设您已经熟悉了 WorkSpaces。有关如何使用的更多信息 WorkSpaces，请参阅 Amazon WorkSpaces 用户指南。
- 如果您在 VMware Cloud on 上使用 Amazon，我们假设您已经熟悉了。有关更多信息，请参阅 VMware Cloud on Amazon。
- 我们假设您熟知 Microsoft Active Directory 的概念。

先决条件

要创建 Amazon FSx 文件系统，您需要满足以下条件：

- 具有创建亚马逊 FSx 文件系统和亚马逊 EC2 实例所需权限的 Amazon 账户。有关更多信息，请参阅 设置你的 Amazon Web Services 账户。
- 基于您要与亚马逊 FSx 文件系统关联的亚马逊 VPC 服务，在虚拟私有云 (VPC) 中运行微软 Windows Server 的亚马逊 EC2 实例。有关如何创建实例的信息，请参阅亚马逊 EC2 用户指南中的亚马逊 EC2 Windows 实例入门。
- 亚马逊 FSx 与微软 Active Directory 合作执行用户身份验证和访问控制。在创建亚马逊 FSx 文件系统时，您可以将其加入微软活动目录。有关更多信息，请参阅 使用 Microsoft Active Directory。
- 本指南假设您没有根据 Amazon VPC 服务更改 VPC 的默认安全组规则。如果有，则需要确保添加必要的规则，以允许从您的亚马逊 EC2 实例到您的亚马逊 FSx 文件系统的网络流量。有关更多详细信息，请参阅 Amazon 的安全 FSx。
- 安装并配置 Amazon Command Line Interface (Amazon CLI)。支持 1.9.12 和更高版本。有关更多信息，请参阅《Amazon Command Line Interface 用户指南》中的安装、更新和卸载 Amazon CLI。

> **Note**
>
> 你可以用`aws --version`命令检查 Amazon CLI 你正在使用的版本。

亚马逊 Window FSx s 版文件服务器论坛

如果您在使用 Amazon 时遇到问题 FSx，请使用论坛。

您是首次使用 Amazon FSx 吗？

如果您是首次使用 Amazon FSx，我们建议您按顺序阅读以下章节：

1. 如果您已准备好创建自己的第一个 Amazon FSx 文件系统，请尝试开始使用 FSx 适用于 Windows 文件服务器的亚马逊。
2. 有关性能的信息，请参阅 FSx for Windows File Server 性能。
3. 有关 Amazon FSx 安全详情，请参阅Amazon 的安全 FSx。
4. 有关亚马逊 FSx API 的信息，请参阅亚马逊 FSx API 参考。

适用于 FSx Windows 文件服务器的最佳实践

我们建议您在使用亚马逊 FSx Windows 文件服务器时遵循这些最佳实践。

主题

一般最佳实践

创建监控计划

您可以使用文件系统指标来监控存储使用情况和性能，了解您的使用模式，并在使用量接近文件系统的存储或性能限制时触发通知。通过监控您 FSx 的 Amazon 文件系统以及应用程序环境的其余部分，您可以快速调试任何可能影响性能的问题。

确保您的文件系统有足够的资源

资源不足会导致延迟增加和 I/O 请求排队，这可能显示为文件系统完全或部分不可用。有关监控性能以及访问性能警告和建议的更多信息，请参阅性能警告和建议。

安全最佳实践

在管理文件系统安全性和访问控制方面，我们建议您遵循以下最佳实践。有关配置 Amazon FSx 以满足您的安全与合规目标的更多详细信息，请参阅Amazon 的安全 FSx。

网络安全

请勿修改或删除与您的文件系统关联的 ENI

您的 Amazon FSx 文件系统可通过弹性网络接口 (ENI) 进行访问，该接口位于与您的文件系统关联的虚拟私有云 (VPC) 中。修改或删除该网络接口可能会导致永久丢失您的 VPC 和文件系统之间的连接。

使用安全组和网络 ACLs

您可以使用安全组和网络访问控制列表 (ACLs) 来限制对文件系统的访问。对于 VPC 安全组，默认安全组已添加到控制台中的文件系统。确保您创建文件系统的子网的安全组和网络 ACLs 允许端口上的流量。

Active Directory

创建亚马逊 FSx 文件系统时，您可以将其加入您的 Microsoft Active Directory 域，以提供用户身份验证以及共享、文件和文件夹级别的访问控制授权。您的用户可以使用其现有的 Active Directory 账户连接到文件共享并访问其中的文件和文件夹。此外，您 FSx 无需进行任何修改即可将现有安全 ACL 配置迁移到 Amazon。亚马逊为您 FSx提供了两个活动目录选项：Amazon 托管的微软活动目录或自我管理的微软活动目录。

如果您使用的是 Amazon 托管的 Microsoft Active Directory，我们建议您保留 Active Directory 安全组的默认设置。如果要修改这些设置，请确保使用满足网络要求的网络配置。有关更多信息，请参阅 联网先决条件。

如果您使用的是自行管理的 Microsoft Active Directory，则还可以通过其他选项配置文件系统。在将亚马逊 FSx 与自行管理的 Microsoft Active Directory 配合使用时，我们建议采用以下最佳做法进行初始配置：

- 将子网分配给单个 Active Directory 站点：如果您的 Active Directory 环境有大量域控制器，请使用 A ctive Directory 网站和服务将您的亚马逊 FSx 文件系统使用的子网分配给可用性和可靠性最高的单个 Active Directory 站点。确保 VPC 安全组、VPC 网络 ACL、您 DCs的 Windows 防火墙规则以及您的 Active Directory 基础设施中的任何其他网络路由控制允许亚马逊 FSx 通过所需端口进行通信。这允许 Windows 在无法使用分配的 Active Directory 站点时恢复到其他 DCs 站点。有关更多信息，请参阅 使用 Amazon VPC 进行文件系统访问控制。
- 使用单独的组织单位 (OU)：对您的 Amazon FSx 文件系统使用与您可能拥有的任何其他组织单位分开的 OU。
- 使用所需@@ 的最低权限配置您的服务账户：使用所需的最低权限配置或委托您提供给 Amazon FSx 的服务账户。有关更多信息，请参阅 使用自行管理的 Microsoft Active Directory。
- 持续验证您的 Active Directory 配置 ：在创建您的亚马逊 FSx FSx 文件系统之前，针对您的活动目录配置运行 Amazon Active Directory 验证工具 FSx，以验证您的配置是否适用于亚马逊，并发现该工具可能暴露的任何警告和错误。
- 使用 Amazon Secrets Manager以下方式存储 Active Directory 凭据：您可以使用 Amazon Secrets Manager 安全地存储和管理您的 Microsoft 活动目录域加入服务帐户凭据。此方法无需在应用程序代

码或配置文件中以明文形式存储敏感凭证，从而增强您的安全状况。有关更多信息，请参阅 使用存储活动目录凭证 Amazon Secrets Manager。

避免因 Active Directory 配置错误而失去可用性

将亚马逊 FSx 与自行管理的 Microsoft Active Directory 配合使用时，重要的是不仅要在创建文件系统时拥有有效的活动目录配置，还要确保持续的操作和可用性。在故障恢复事件、例行维护事件和吞吐量容量更新操作期间，Amazon 会将文件服务器资源 FSx重新加入您的 Active Directory。如果 Active Directory 配置在事件期间无效，则您的文件系统状态将更改为错误配置，且存在不可用的风险。以下是一些可避免失去可用性的方法：

- 使用 Amazon 更新您的 Active Directory 配置 FSx：如果您进行更改，例如重置服务账户的密码，请务必使用此服务账户更新所有文件系统的配置。
- 监控 Active Directory 配置错误：为自己设置“错误配置”状态通知，以便在必要时重置文件系统的 Active Directory 配置。有关使用基于 Lambda 的解决方案实现这一目标的示例，请参阅使用 Amazon 监控亚马逊 FSx 文件系统的运行状况和。 EventBridge Amazon Lambda
- 定期验证您的 Active Directory 配置：如果您想主动检测 Active Directory 配置错误，我们建议您针对您的 Active Directory 配置持续运行 Active Directory 验证工具。如果您在运行验证工具时收到警告或错误，则表示您的文件系统存在错误配置的风险。
- 请勿移动或修改由 FSx以下用户创建的计算机对象：Amazon 使用您提供的服务账户和权限在您的 Active Directory 中 FSx 创建和管理计算机对象。移动或修改这些计算机对象可能会导致文件系统错误配置。

窗户 ACLs

在 Amazon 中 FSx，您可以使用标准的 Windows 访问控制列表 (ACLs) 进行精细的共享、文件和文件夹级别的访问控制。亚马逊 FSx 文件系统会自动验证访问文件系统数据的用户的证书，以强制执行这些 Windows ACLs。

- 请勿更改系统用户的 NTFS ACL 权限：Amazon FSx 要求系统用户拥有对文件系统内所有文件夹的 NTFS ACL 完全控制权限。更改 SYSTEM 用户的 NTFS ACL 权限可能会导致您的文件系统无法访问，并且将来的文件系统备份可能无法使用。

配置文件系统并调整其大小

选择部署类型

Amazon FSx 提供两种部署选项：单可用区和多可用区。对于大多数要求共享 Windows 文件数据具有高可用性的生产工作负载，我们建议使用多可用区文件系统。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。

选择吞吐能力

为文件系统配置足够的吞吐能力，不仅要满足工作负载的预期流量，还要满足支持要在文件系统上启用的功能所需的额外性能资源。例如，如果您正在运行重复数据删除，则您选择的吞吐能力必须提供足够的内存，以便根据您拥有的存储空间运行重复数据删除。如果您使用的是影子副本，请将吞吐能力增加到至少为工作负载预期驱动值的三倍，以避免 Windows Server 删除影子副本。有关更多信息，请参阅 吞吐能力对性能的影响。

增加存储容量和吞吐能力

当文件系统的可用存储空间不足，或者您预计存储需求将超过当前存储限制时，请增加其存储容量。我们建议您的文件系统始终保持至少 20% 的可用存储容量。我们还建议在增加存储容量之前，至少将吞吐能力增加 20%，以抵消增加存储空间期间可能产生的性能影响。您可以使用该FreeStorageCapacity CloudWatch 指标来监控可用存储量并了解其趋势。有关更多信息，请参阅 管理存储容量。

如果您的工作负载受当前性能限制，则还应提高文件系统的吞吐能力。您可以使用 FSx 控制台上的 “监控和性能” 页面查看工作负载需求何时接近或超过性能限制，以确定您的文件系统是否为工作负载配置不足。

为了最大限度地缩短存储扩展的持续时间并避免写入性能降低，我们建议先提高文件系统的吞吐能力，再增加存储容量，存储容量增加完成后再降低吞吐能力。在存储扩展期间，对大多数工作负载的性能影响微乎其微。但是，使用 HDD 存储类型的文件系统，以及涉及大量终端用户、高 I/O 级别或拥有大量小文件的数据集的工作负载，可能会暂时出现性能下降的情况。有关更多信息，请参阅 增加存储容量并提升文件系统性能。

在空闲期间修改吞吐能力

更新吞吐能力会导致单可用区文件系统的可用性中断几分钟，并导致多可用区文件系统的失效转移和失效自动恢复。对于多可用区文件系统，如果在失效转移和失效自动恢复期间有持续的流量，则在此期间所做的任何数据更改都需要在文件服务器之间同步。对于写入量大和 IOPS 量大的工作负载，数据同步

进程可能需要长达数小时。尽管在此期间您的文件系统将继续可用，但我们建议您在文件系统负载最小的空闲时段安排维护时段，并更新吞吐能力，以缩短数据同步的持续时间。要了解更多信息，请参阅管理吞吐能力。

开始使用 FSx 适用于 Windows 文件服务器的亚马逊

接下来，你可以学习如何开始使用 FSx 适用于 Windows 文件服务器。此入门练习包括以下步骤。

1. 注册 Amazon Web Services 账户 并在该帐户中创建管理员用户。
2. 使用创建 Amazon 托管的 Microsoft AD 活动目录 Amazon Directory Service。您将把文件系统和计算实例加入 Active Directory。
3. 创建运行 Microsoft Windows Server 的 Amazon Elastic Compute Cloud 计算实例。您将使用此实例访问文件系统。
4. 使用亚马逊 FSx 控制台创建适用 FSx 于 Windows 的亚马逊文件服务器文件系统。
5. 将您的文件系统映射到您的 EC2 实例
6. 将数据写入文件系统。
7. 备份文件系统。
8. 清理您创建的资源。

主题

设置你的 Amazon Web Services 账户

在您首次使用 Amazon FSx 之前，请完成以下任务：

1. 注册获取 Amazon Web Services 账户

2. 保护 IAM 用户

注册获取 Amazon Web Services 账户

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

报名参加 Amazon Web Services 账户

1. 打开https://portal.aws.amazon.com/billing/注册。
2. 按照屏幕上的说明操作。

   在注册时，将接到电话或收到短信，要求使用电话键盘输入一个验证码。

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

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

保护 IAM 用户

注册后 Amazon Web Services 账户，开启多重身份验证 (MFA)，保护您的管理用户。有关说明，请参阅《IAM 用户指南》中的 为 IAM 用户启用虚拟 MFA 设备（控制台）。

要允许其他用户访问您的 Amazon Web Services 账户 资源，请创建 IAM 用户。为了保护您的 IAM 用户，请启用 MFA 并仅向 IAM 用户授予执行任务所需的权限。

有关创建和保护 IAM 用户的更多信息，请参阅《IAM 用户指南》中的以下主题：

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

步骤 1：设置 Active Directory

借助 Amazon FSx，您可以为基于 Windows 的工作负载操作完全托管的文件存储。同样， Amazon Directory Service 还提供完全托管的目录，供您在工作负载部署中使用。如果您使用 EC2实例在虚拟

私有云 (VPC) Amazon 中运行现有企业 Active Directory 域，则可以启用基于用户的身份验证和访问控制。您可以通过在 Amazon 托管 Microsoft 活动目录和公司域之间建立信任关系来实现此目的。对于 Amazon 中的 Windows 身份验证 FSx，您只需要单向林信任，即 Amazon 托管林信任公司域林。

您的公司域扮演可信域的角色，而 Amazon Directory Service 托管域则扮演信任域的角色。经过验证的身份验证请求只能在域之间单向传输，即允许企业域中的账户根据托管的域中共享的资源进行身份验证。在这种情况下，Amazon 仅与托管域进行 FSx 交互。然后，托管的域会将身份验证请求传递到您的企业域。

> **Note**
>
> 您也可以将外部信任类型与 Amazon 一起 FSx 用于可信域。

您的 Active Directory 安全组必须启用来自亚马逊 FSx 文件系统的安全组的入站访问权限。

为微软 Active Directory 创建 Amazon 目录服务

- 如果你还没有，请使用创建你的 Microsoft 活动目录 Amazon 托管。 Amazon Directory Service 有关更多信息，请参阅《AmazonAmazon Directory Service 管理指南》中的 “创建您的托管 Microsoft 活动目录”。

  > **Important**
  >
  > 请记住您为管理员用户分配的密码；您稍后在本入门练习中需要使用该密码。如果您忘记了密码，则需要使用新 Amazon Directory Service 目录和管理员用户重复本练习中的步骤。

- 如果您已有活动目录，请在您的 Amazon 托管 Microsoft 活动目录和现有活动目录之间创建信任关系。有关更多信息，请参阅《Amazon Directory Service 管理指南》中的何时创建信任关系。

第 2 步：在亚马逊 EC2 控制台中启动 Windows 实例

您可以使用启动 Windows 实例， Amazon Web Services 管理控制台 如以下过程所述。本教程旨在帮助您快速启动第一个实例，因此不会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. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。

2. 从控制台控制面板中，选择启动实例。
3. “选择亚马逊系统映像 (AMI)” 页面会显示一个名为 Amazon 系统映像 (AMIs) 的基本配置列表，这些配置可用作您的实例的模板。选择适用于 Windows Server 2016 Base 或更高版本的 AMI。请注意，这些标 AMIs 有 “符合免费套餐资格”。
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. 在核查实例启动页面上的安全组下，您将看到向导为您创建并选择了安全组。使用以下步骤，您可以使用此安全组，也可以选择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。（如果公用 DNS (IPv4) 或 (IPv6) 列处于隐藏状态，请选择页面右上角的 “显示/隐藏列”（齿轮形图标），然后选择 “公用 DNS” (IPv4) 或 ()。）IPv6

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**
>
> 请记住在您启动此实例时创建的安全组的 ID。在创建 Amazon FSx 文件系统时，您将需要它。

现在，实例已启动，您可以连接到实例了。

步骤 3：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 Administrateur，葡萄牙语则为 Administrador。有关更多信息，请参阅 Microsoft TechNet Wiki 中的 Windows 管理员帐户的本地化名称。

如果您已将实例加入到域，则可以使用您在 Amazon Directory Service中定义的域凭证来连接到您的实例。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，使用管理员的完全限定用户名和该账户的密码。例如，**`corp.example.com\Admin`**。

借助适用于 Windows Server 操作系统（OS）的许可证，可以同时进行两个远程连接以进行管理。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 Configure the Number of Simultaneous Remote Connections Allowed for a Connection。

使用 RDP 客户端连接到 Windows 实例

1. 在亚马逊 EC2 控制台中，选择实例，然后选择 Connect。
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中显示实例的默认管理员密码，会将先前显示的获取密码链接替换为实际密码。

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，可选择关闭，以关闭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 “详细信息” 选项卡，然后向下滚动到 Windows 电脑上的 “指纹” 条目或 Mac 上的 “SHA1 指纹” 条目。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，选择实例，选择操作，然后选择获取系统日志。
   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，您可以将实例加入 Amazon Directory Service 目录。

第 4 步：将您的实例加入您的 Amazon Directory Service 目录

以下过程向您展示了如何手动将现有 Amazon EC2 Windows 实例加入您的 Amazon Directory Service 目录。

将 Windows 实例加入你的 Amazon Directory Service 目录

1. 使用任何远程桌面协议客户端连接到实例。
2. 打开实例上的 TCP/ IPv4 或 IPv6 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）互联网协议版本 4 或互联网协议版本 6。
3. （可选）选择使用以下 DNS 服务器地址，将首选 DNS 服务器和备用 DNS 服务器地址更改为所 Amazon Directory Service提供的 DNS 服务器的 IPv4 或 IPv6 地址，然后选择确定。
4. 打开实例的系统属性对话框，选择计算机名称选项卡，然后选择更改。

   > **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”，输入 Amazon Directory Service 目录的完全限定名称，然后选择 “确定”。
6. 当系统提示输入域管理员的名称和密码时，输入管理员账户的用户名和密码。

> **Note**
>
> 您可以输入域的完全限定名称或 NetBios 名称，然后输入反斜杠 (\)，然后输入用户名（在本例中为 Admin）。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 Amazon Directory Service 目录管理员用户的用户名和密码登录实例。

现在，您的实例已加入该域，就可以创建您的 Amazon FSx 文件系统了。

步骤 5。创建文件系统

创建文件系统（控制台）

1. 打开 Amazon FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 在控制面板上，选择创建文件系统以启动文件系统创建向导。
3. 在 “选择文件系统类型” 页上，选择 “FSx Windows 文件服务器”，然后选择 “下一步”。显示创建文件系统页面。
4. 对于创建方法，选择标准创建。

文件系统详细信息

1. 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。命名文件系统能让您更轻松地进行查找和管理。您最多可以使用 256 个 Unicode 字母、空格和数字以及特殊字符：+ - = . _ : /
2. 对于部署类型，选择多可用区或单可用区。

> **Note**
>
> 多可用区文件系统在中国（北京）区域不可用。

- 选择多可用区部署能够容忍可用区不可用的文件系统。此选项支持 SSD 和 HDD 存储。
- 选择单可用区部署已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。

3. 您可以在存储类型中选择 SSD 或 HDD。

   FSx 适用于 Windows 文件服务器提供固态硬盘 (SSD) 和硬盘驱动器 (HDD) 存储类型。SSD 存储专为性能最高、对延迟最敏感的工作负载而设计，包括数据库、媒体处理工作负载和数据分析应用程序。HDD 存储专为各种工作负载而设计，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 关于存储类型。

4. 在预置的 SSD IOPS 中，您可以选择自动或用户预置模式。

   如果您选择自动模式， FSx Windows 文件服务器会自动扩展您的固态硬盘 IOPS，以保持每 GiB 存储容量 3 个固态硬盘 IOPS。若选择“用户预置”模式，请输入 96–400,000 范围内的任意整数。美国东部（弗吉尼亚州北部）、美国西部（俄勒冈州）、美国东部（俄亥俄州）、欧洲地区（爱尔兰）、亚太地区（东京）以及亚太地区（新加坡）的 SSD IOPS 能够扩展至 80,000 以上。有关更多信息，请参阅 管理 SSD IOPS。

5. 对于存储容量，请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 范围内的任意整数。如果您使用的是 HDD 存储，请输入 2,000 – 65,536 范围内的任意整数。创建文件系统后，您可以根据需要随时增加存储容量。有关更多信息，请参阅 管理存储容量。

6. 保持吞吐能力设置为默认设置。吞吐能力是托管文件系统的文件服务器可以持续提供数据的速度。建议的吞吐能力设置基于您选择的存储容量。如果您需要的吞吐能力超过建议吞吐能力，请选择指定吞吐能力，然后选择一个值。有关更多信息，请参阅 FSx for Windows File Server 性能。

   > **Note**
   >
   > 如果要启用文件访问审计，则必须选择 32 MBps 或更大的吞吐容量。有关更多信息，请参阅 使用文件访问审计记录最终用户的访问。

   创建文件系统后，您可以根据需要随时修改吞吐能力。有关更多信息，请参阅 管理吞吐能力。

网络与安全

1. 在网络与安全部分，选择要与文件系统关联的 Amazon VPC。在本入门练习中，请为 Amazon Directory Service 目录和亚马逊 EC2 实例选择相同的 Amazon VPC。

2.

对于 VPC 安全组，用于您的默认 Amazon VPC 的默认安全组已添加到控制台中的文件系统。如果您未使用默认安全组，请确保您选择的安全组与您的文件系统位于 Amazon Web Services 区域相同的安全组中。为确保您可以将 EC2 实例与您的文件系统连接，您需要向所选安全组添加以下规则：

a. 添加以下入站和出站规则以允许以下端口。

Rules	端口
UDP	53、88、123、389、464
TCP	53、88、135、389、445、464、636、3268、3269、5985、9389、49152-65535

添加与您要访问文件系统的客户端计算实例 IDs 关联的 IP 地址或安全组。

b. 添加出站规则，允许所有流量流向您要加入文件系统的 Active Directory。为此，请执行以下操作之一：

- 允许出站流量流向与您的 Amazon 托管 AD 目录关联的安全组 ID。
- 允许所有流量流向与您自行管理的 Microsoft Active Directory 域控制器关联的 IP 地址。

> **Note**
>
> 在某些情况下，您可能已经修改了默认设置中的 Amazon Managed Microsoft AD 安全组规则。如果是，请确保此安全组具有允许来自您的 Amazon FSx 文件系统的流量所需的入站规则。有关必需的入站规则的更多信息，请参阅《Amazon Directory Service 管理指南》中的 Amazon Managed Microsoft AD 先决条件。

有关更多信息，请参阅 使用 Amazon VPC 进行文件系统访问控制。

3. 多可用区文件系统配备主文件服务器和备用文件服务器，各服务器均位于各自的可用区和子网中。如果要创建多可用区文件系统（请参阅步骤 5），请为主文件服务器选择首选子网值，为备用文件服务器选择备用子网值。

   如果要创建单可用区文件系统，请为文件系统选择子网。

4. 对于“网络类型”，选择 IPv4（仅用于 IPv4 支持）或“双栈”（两者 IPv4兼 IPv6 而有之）。可随时更改现有文件系统的网络类型。有关更多信息，请参阅 更改网络类型。

> **Note**
>
> 如果您打算创建使用双堆栈模式 FSx 的 Windows 文件服务器文件系统，则必须先为您的 VPC 和子网分配亚马逊提供的 IPv6 CIDR 块。有关更多信息，请参阅 Amazon Virtual Private Cloud 用户指南中的添加对您的 VPC 的 IPv6 支持。

Windows 身份验证

- 对于 Windows 身份验证，您可进行如下选择：

  如果要将文件系统加入Amazon 由管理的 Microsoft Ac tive Directory 域，请选择托管 Microsoft Active Directory Amazon，然后从列表中选择您的 Amazon Directory Service 目录。有关更多信息，请参阅 使用 Microsoft Active Directory。

  如果要将文件系统加入自行管理的 Microsoft Active Directory 域，请选择自行管理的 Microsoft Active Directory，然后为 Active Directory 提供以下详细信息。有关更多信息，请参阅 使用自行管理的 Microsoft Active Directory。

  - 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 域名不得超过 47 个字符。此限制同时适用于 Amazon Directory Service 和自行管理的 Active Directory 域名。Amazon FSx 要求将内部流量直接连接到您的 DNS IP 地址。不支持通过互联网网关进行连接。请改用 Amazon Virtual Private Network VPC 对等 Amazon Direct Connect互连或 Amazon Transit Gateway 关联。

  - DNS 服务器 IP 地址 — IPv4 或您的域的 DNS 服务器 IPv6 地址。

  > **Note**
  >
  > DNS 服务器必须启用 EDNS（Extension Mechanisms for DNS）。如果禁用 EDNS，文件系统可能无法创建。

- Amazon 用于将文件系统加入您的域的 A FSx ctive Directory 服务账户的证书。可通过以下任一方式提供这些凭证：
  - 选项 1： Amazon Secrets Manager 秘密 ARN-包含您的 Active Directory 域上服务帐户的用户名和密码的密钥。有关更多信息，请参阅 使用存储活动目录凭证 Amazon Secrets Manager。
  - 选项 2：纯文本凭证
    - 服务账户用户名：现有 Microsoft Active Directory 中服务账户的用户名。请勿包含域前缀或后缀。例如，对于 `EXAMPLE\ADMIN`，仅使用 `ADMIN`。
    - 服务账户密码 – 服务账户的密码。
- （可选）组织单元（OU）– 文件系统要加入的组织单元的可分辨路径名称。
- （可选）委托文件系统管理员组 – Active Directory 中可以管理您的文件系统的组的名称。默认组为“域管理员”。有关更多信息，请参阅 亚马逊 FSx 服务账户。

加密、审计和访问（DNS 别名）

1. 对于加密，选择用于 Amazon KMS key 加密文件系统中静态数据的加密密钥。您可以通过指定密钥的 ARN 来选择由管理的默认 aws/fsx（默认） Amazon KMS、现有密钥或客户托管的密钥。有关更多信息，请参阅 静态数据加密。
2. 对于审计 – 可选，默认为禁用文件访问审计。有关启用和配置文件访问审计的信息，请参阅使用文件访问审计记录最终用户的访问。
3. 在访问 – 可选中输入您要与文件系统关联的所有 DNS 别名。每个别名的格式必须为完全限定域名（FQDN）。有关更多信息，请参阅 管理 DNS 别名。

备份和维护

有关每日自动备份和本节中设置的更多信息，请参阅 使用备份保护您的数据。。

1. 每日自动备份默认启用。如果您不希望 Amazon FSx 每天自动备份您的文件系统，则可以禁用此设置。
2. 如果启用了自动备份，则将在称为备份窗口的时间段内进行自动备份。您可以使用默认窗口，也可以选择最适合工作流程的自动备份窗口开始时间。
3. 对于自动备份保留期，您可以使用 30 天的默认设置，也可以设置一个介于 1 到 90 天之间的值，Amazon FSx 将保留文件系统的每日自动备份。此设置不适用于用户启动的备份或由 Amazon Backup执行的备份。

4. 对于标签 – 可选，您可以输入键和值来将标签添加到文件系统。标签是区分大小写的键值对，能够帮助您管理、筛选和搜索文件系统。有关更多信息，请参阅 为 Amazon FSx 资源贴标签。

   选择下一步。

检查您的配置，然后创建

1. 检查创建文件系统页面上显示的文件系统配置。您可以看到创建文件系统后可以修改以及无法修改的文件系统设置（供您参考）。选择创建文件系统。
2. Amazon FSx 创建文件系统后，从 “文件系统” 控制面板的列表中选择文件系统 ID 以查看详细信息。选择附加，然后在网络和安全选项卡上记下文件系统的 DNS 名称。在以下过程中，您将需要它来将共享映射到 EC2 实例。

步骤 6. 将您的文件共享映射到运行 Windows 服务器的 EC2 实例

现在，你可以将你的亚马逊 FSx 文件系统挂载到你的目录中基于微软 Windows 的 EC2亚马逊实例。Amazon Directory Service 文件共享的名称与文件系统的名称不同。

使用 GUI 映射亚马逊 EC2 Windows 实例上的文件共享

1. 在 Windows 实例上挂载文件共享之前，必须启动该 EC2实例并将其加入您的文件系统已加入的实例。 Amazon Directory Service for Microsoft Active Directory 要执行此操作，请从《 Amazon Directory Service 管理指南》中选择以下过程之一：

   - 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，请参阅亚马逊 EC2 用户指南中的连接到您的 Windows 实例。
3. 连接后，打开“文件资源管理器”。
4. 在导航窗格中，打开网络的上下文（右键单击）菜单，然后选择映射网络驱动器。
5. 为驱动器选择一个驱动器盘符。
6. 您可以使用 Amazon FSx 分配的默认 DNS 名称或您选择的 DNS 别名来映射文件系统。此过程介绍的是使用默认 DNS 名称映射文件共享。如果要使用 DNS 别名映射文件共享，请参阅使用 DNS 别名访问数据。

在文件夹中输入文件系统的 DNS 名称和共享名称。默认的 Amazon FSx 共享名为\share。你可以在亚马逊 FSx 控制台https://console.aws.amazon.com/fsx/、Windows 文件服务器 > 网络和安全部分或者在 DescribeFileSystems API 命令的CreateFileSystem响应中找到 DNS 名称。

- 对于加入 Amazon 托管 Microsoft Active Directory 的单可用区文件系统，DNS 名称如下所示。

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

- 对于加入自行管理的 Active Directory 的单可用区文件系统，以及所有多可用区文件系统，DNS 名称如下所示。

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

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

7. 选择文件共享是否应该在登录时重新连接，然后选择完成。

第 7 步。将数据写入文件共享

现在，您已将文件共享映射到您的实例，您可以像使用 Windows 环境中的任何其他目录一样使用您的文件共享。

将数据写入文件共享

1. 打开“记事本”文本编辑器。
2. 在文本编辑器中随意写入内容。例如：*Hello, World!*
3. 将文件保存到文件共享的驱动器盘符。
4. 使用“文件资源管理器”，导航到您的文件共享并找到刚刚保存的文本文件。

步骤 8：备份文件系统

现在，您已经有机会使用您的 Amazon FSx 文件系统及其文件共享了，您可以对其进行备份。默认情况下会在文件系统的 30 分钟备份时段中自动创建每日备份。但您可以随时创建用户启动的备份。备份具有与之相关的额外成本。有关备份定价的更多信息，请参阅定价。

通过控制台创建文件系统备份

1. 打开 Amazon FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 从控制台控制面板中，选择您要为此练习创建的文件系统的名称。
3. 在文件系统的概述选项卡中，选择创建备份。
4. 在打开的创建备份对话框中，为备份提供一个名称。此名称最多可以包含 256 个 Unicode 字母，包括空格、数字和以下特殊字符：+ - = . _ : /
5. 选择创建备份。
6. 要查看列表中的所有备份，以便恢复文件系统或删除备份，请选择备份。

在创建新备份的过程中，创建中的备份将设置为正在创建。这可能需要几分钟的时间。当备份可供使用时，其状态将更改为可用。

第 9 步。清理 资源

完成本练习后，您应按照以下步骤清理资源并保护您的 Amazon 帐户。

清理资源

1. 在 Amazon EC2 控制台上，终止您的实例。有关更多信息，请参阅 Amazon EC2 用户指南中的终止您的实例。
2. 在 Amazon FSx 控制台上，删除您的文件系统。所有自动备份都会自动删除。但是，您仍需删除所有手动创建的备份。以下为该进程具体步骤的概括。

    a. 打开 Amazon FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
    b. 从控制台控制面板中，选择您要为此练习创建的文件系统的名称。
    c. 对于操作，选择删除文件系统。
    d. 在打开的删除文件系统对话框中，选定是否要创建最终备份。若要创建，请提供最终备份的名称。所有自动创建的备份也会被删除。

    > **Important**
    >
    > 可以从备份中创建新的文件系统。作为最佳实践，我们建议您创建最终备份。如果您在一段时间后发现不需要它，则可以删除此备份和其他手动创建的备份。

    e. 在文件系统 ID 框中输入要删除的文件系统的 ID。

f. 选择删除文件系统。

g. 当 Amazon FSx 删除文件系统时，其在控制面板中的状态会更改为正在删除。控制面板中将不再显示已删除的文件系统。

h. 现在，您可以删除为文件系统手动创建的任何备份。从左侧导航窗格中，选择备份。

i. 在控制面板中，选择与您删除的文件系统具有相同文件系统 ID 的所有备份，然后选择删除备份。

j. 系统将打开删除备份对话框。保持选中所选备份的 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已删除。

3. 要删除您为本练习创建的 Amazon Directory Service 目录，请参阅《 Amazon Directory Service 管理指南》中的 “删除您的目录”。

访问您的数据

无论是从 Amazon Web Services 云，还是从本地环境中，您都可以使用多种受支持的客户端和方法来访问您的 Amazon FSx 文件系统。

主题

支持的客户端

FSx for Windows File Server 支持服务器消息块（SMB）协议版本 2.0 - 3.1.1，这使您可以灵活地使用各种计算实例和操作系统来连接文件系统。

支持将以下 Amazon 计算实例与 Amazon FSx 配合使用：

- Amazon Elastic Compute Cloud（Amazon EC2）实例，包括 Microsoft Windows、Mac、Amazon Linux 和 Amazon Linux 2 实例。有关更多信息，请参阅 映射文件共享。
- Amazon Elastic Container Service（Amazon ECS）容器 有关更多信息，请参阅《Amazon Elastic Container Service 开发人员指南》中的 FSx for Windows File Server 卷。
- WorkSpaces 实例 – 要了解更多信息，请参阅 Amazon 博客文章 Using FSx for Windows File Server with Amazon WorkSpaces。
- Amazon AppStream 2.0 实例 – 要了解更多信息，请参阅 Amazon 博客文章 Using Amazon FSx with Amazon AppStream 2.0。
- Amazon 环境下运行在 VMware Cloud 中的 VM – 要了解更多信息，请参阅 Amazon 博客文章 Storing and Sharing Files with FSx for Windows File Server in a VMware Cloud on Amazon Environment。

Amazon FSx 支持以下操作系统：

- Windows Server 2008、Windows Server 2008 R2、Windows Server 2012、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019 和 Windows Server 2022。
- Windows Vista、Windows 7、Windows 8、Windows 8.1、Windows 10（包括 WorkSpaces 的 Windows 7 和 Windows 10 桌面体验）和 Windows 11。
- 使用 `cifs-utils` 工具的 Linux。
- macOS

从 Amazon Web Services 云 内部访问数据

每个 Amazon FSx 文件系统都与虚拟私有云（VPC）相关联。无论可用区在哪里，您都可以从文件系统 VPC 中的任何位置访问 FSx for Windows File Server 文件系统。您也可以从与文件系统处于不同 Amazon Web Services 账户 或 Amazon Web Services 区域 的 VPC 中访问文件系统。除了以下各节中描述的访问 FSx for Windows File Server 资源的要求外，您还需要确保配置文件系统的 VPC 安全组，以便数据和管理流量可以在文件系统和客户端之间流动。有关为使用所需端口配置安全组的更多信息，请参阅 使用 Amazon VPC 进行文件系统访问控制。

您可以从与文件系统位于同一 VPC 中的受支持客户端访问 FSx for Windows File Server 文件系统。

下表说明了 Amazon FSx 支持从每个受支持环境中的客户端进行访问的环境，具体取决于文件系统的创建时间。

客户位于…	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
创建文件系统的子网	✓	✓	✓
创建文件系统的 VPC 的主要 CIDR 数据块	✓	✓	✓
创建文件系统的 VPC 的辅助 CIDR		IP 地址在 RFC 1918 私有 IP 地	IP 地址在以下 CIDR 数据块范围之外的客

客户位于...	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
其他 CIDR 或对等网络		址范围内的客户端： • 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	户端：198.19 .0.0/16

> **Note**
>
> 在某些情况下，您可能需要使用非私有 IP 地址范围从本地访问在 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创建一个新的文件系统。有关更多信息，请参阅使用备份保护您的数据。。

从其他 VPC、Amazon Web Services 账户 或 Amazon Web Services 区域访问数据

您可以使用 VPC 对等或传输网关，从与文件系统关联不同的 VPC、Amazon Web Services 账户 或 Amazon Web Services 区域 中的支持客户端访问 FSx for Windows File Server 文件系统。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 Amazon Web Services 账户，或位于不同的 Amazon Web Services 区域，也可以进行此类访问。

VPC 对等连接是两个 VPC 之间的网络连接，通过此连接，您可以使用私有 IPv4 或 IP 版本 6（IPv6）地址在这两个 VPC 之间路由流量。您可以使用 VPC 对等连接来连接位于同一 Amazon 区域或两个 Amazon 区域中的 VPC。有关 VPC 对等连接的更多信息，请参阅《Amazon VPC 对等连接指南》中的什么是 VPC 对等连接？。

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《Amazon VPC 中转网关》中的开始使用中转网关。

设置 VPC 对等连接或传输网关连接后，您可以使用文件系统的 DNS 名称访问文件系统。您可以像在关联的 VPC 内的计算实例中一样执行此操作。

从本地访问数据

FSx for Windows File Server 支持使用 Amazon Direct Connect 或 Amazon VPN 从本地计算实例访问您的文件系统。有了对 Amazon Direct Connect 的支持，FSx for Windows File Server 使您可以通过专用网络连接从本地环境访问文件系统。有了对 Amazon VPN 的支持，FSx for Windows File Server 使您可以通过安全的专用隧道从本地环境访问文件系统。

将本地环境连接到与 Amazon FSx 文件系统关联的 VPC 后，您可以使用文件系统的 DNS 名称或 DNS 别名访问文件系统。您可以像在 VPC 内的计算实例中一样执行此操作。有关 Amazon Direct Connect 的更多信息，请参阅《Amazon Direct Connect 用户指南》。有关设置 Amazon VPN 连接的更多信息，请参阅《Amazon VPC 用户指南》中的 VPN 连接。

> **Note**
>
> 在某些情况下，您可能需要使用非私有 IP 地址范围从本地访问在 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创建一个新的文件系统。有关更多信息，请参阅 使用备份保护您的数据。。

FSx for Windows File Server 还支持使用 Amazon FSx 文件网关，从本地计算实例提供低延迟、无缝访问云中 FSx for Windows File Server 文件共享的权限。有关更多信息，请参阅《Amazon FSx 文件网关用户指南》。

> **Note**
>
> 不再向新客户提供 Amazon FSx 文件网关。FSx 文件网关的现有客户可以继续正常使用该服务。有关与 FSx 文件网关类似的功能，请访问此博客文章。

使用默认 DNS 名称访问数据

FSx for Windows File Server 为每个文件系统提供了一个域名系统（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，从而访问 FSx for Windows File Server 文件系统。要了解更多信息，请参阅 使用文件共享访问数据。

> **Important**
>
> 只有当您使用 Microsoft DNS 作为默认 DNS 时，Amazon FSx 才会注册文件系统的 DNS 记录。如果您使用的是第三方 DNS，则须手动设置 Amazon FSx 文件系统的 DNS 条目。有关为文件系统选择正确 IP 地址的信息，请参阅获取用于手动 DNS 条目的正确文件系统 IP 地址。

查找 DNS 名称：

- 在 Amazon FSx 控制台中，选择文件系统，然后选择详细信息。在网络与安全部分查看 DNS 名称。
- 或者，在 CreateFileSystem 或 DescribeFileSystems API 命令的响应中查看。

加入 Amazon 托管的 Microsoft Active Directory 的所有单可用区文件系统的 DNS 名称具有以下格式：`fs-0123456789abcdef0.`*`ad-dns-domain-name`*

对于加入自行管理的 Active Directory 的所有单可用区文件系统，以及所有多可用区文件系统，DNS 名称具有以下格式：`amznfsxaa11bb22.`*`ad-domain`*`.com`

Kerberos 身份验证使用 DNS 名称

我们建议对 Amazon FSx 使用基于 Kerberos 的身份验证和传输中加密。Kerberos 能够为访问文件系统的客户端提供最安全的身份验证。要为您的 SMB 会话启用基于 Kerberos 的身份验证和传输中数据加密，请使用 Amazon FSx 提供的文件系统的 DNS 名称来访问您的文件系统。

如果您在 Amazon 托管的 Microsoft Active Directory 和本地 Active Directory 之间配置了外部信任，那么如果要使用带有 Kerberos 身份验证的 Amazon FSx Remote PowerShell，则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 Microsoft 文档中的 Configure Kerberos Forest Search Order（KFSO）。

支持分布式文件系统（DFS）命名空间

FSx for Windows File Server 支持使用 Microsoft DFS 命名空间。使用 DFS 命名空间将位于多个文件系统的文件共享组织到一个用于访问整个文件数据集的公共文件夹结构（命名空间）。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 命名空间为多个 FSx for Windows File Server 文件系统分组。

使用 DNS 别名访问数据

FSx for Windows File Server 为每个文件系统提供了一个 DNS 名称，可以用于访问文件共享。您还可以通过为 FSx for Windows File Server 文件系统注册别名的方法，使用默认 DNS 名称之外的其他 DNS 名称访问文件共享。

使用 DNS 别名，您可以将 Windows 文件共享数据移至 FSx for Windows File Server，然后继续使用现有的 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，从而更轻松地管理连接到 Amazon FSx 文件系统的工具和应用程序。每次最多可以将 50 个 DNS 别名与一个文件系统关联。有关将 DNS 别名与 FSx for Windows File Server 文件系统关联和取消关联的更多信息，请参阅 管理 DNS 别名。

要使用 DNS 别名配置对 FSx for Windows File Server 文件系统的访问权限，必须执行以下步骤：

1. 将 DNS 别名关联到文件系统.
2. 为文件系统以及与其相关 DNS 别名创建 DNS CNAME 记录。

有关 FSx for Windows File Server 文件系统使用 DNS 别名的更多信息，请参阅 管理 DNS 别名。

Kerberos 身份验证和加密使用 DNS 别名

我们建议对 Amazon FSx 使用基于 Kerberos 的身份验证和传输中加密。Kerberos 能够为访问文件系统的客户端提供最安全的身份验证。要对使用 DNS 别名访问 Amazon FSx 的客户端启用 Kerberos 身份验证，必须在 Amazon FSx 文件系统的 Active Directory 计算机对象上添加与 DNS 别名对应的服务主体名称（SPN）。

要在使用 DNS 别名访问文件系统时设置 Kerberos 身份验证和加密，请参阅 为 Kerberos 配置服务主体名称（SPN）。

您可以选择通过在 Active Directory 中设置以下组策略对象（GPO），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：向远程服务器传出 NTLM 流量 – 使用此策略设置拒绝或审计从计算机到运行 Windows 操作系统的任何远程服务器的传出 NTLM 流量。
- 限制 NTLM：为 NTLM 身份验证添加远程服务器例外：如果配置了“网络安全：限制 NTLM：向远程服务器传出 NTLM 流量”策略设置，则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例外列表。

要在使用 DNS 别名访问文件系统时强制执行 Kerberos 身份验证和加密，请参阅 使用组策略对象（GPO）强制执行 Kerberos 身份验证。

有关配置文件系统以使用 DNS 别名的更多信息，请参阅以下过程：

- 将 DNS 别名关联到文件系统
- 为 Kerberos 配置服务主体名称（SPN）
- 更新或创建 DNS CNAME 记录
- 使用组策略对象（GPO）强制执行 Kerberos 身份验证

将 DNS 别名关联到文件系统

在使用 Amazon FSx 控制台、CLI 和 API 创建新文件系统以及从备份创建新文件系统时，可以将 DNS 别名与现有 FSx for Windows File Server 相关联。如果您要使用其他域名创建别名，请输入包括父域名在内的全名以关联别名。

此过程将介绍如何在使用 Amazon FSx 控制台创建新文件系统时关联 DNS 别名。有关将 DNS 别名关联到现有文件系统的信息，以及有关使用 CLI 和 API 的详细信息，请参阅 管理 DNS 别名。

在创建新的文件系统时关联 DNS 别名

1. 通过以下网址打开 Amazon FSx 控制台：https://console.aws.amazon.com/fsx/。
2. 按照“入门”部分中 步骤 5。创建文件系统 所述的步骤创建新文件系统。
3. 在创建文件系统向导的访问 – 可选部分，输入要与文件系统关联的 DNS 别名。

   指定 DNS 别名时，请遵循以下准则：

   - 必须采用完全限定域名（FQDN）格式 *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. 在维护首选项中根据需要进行任何更改。
5. 在标签 – 可选部分中，添加所需的标签，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。

为 Kerberos 配置服务主体名称（SPN）

我们建议对 Amazon FSx 使用基于 Kerberos 的身份验证和传输中加密。Kerberos 能够为访问文件系统的客户端提供最安全的身份验证。

要对使用 DNS 别名访问 Amazon FSx 的客户端启用 Kerberos 身份验证，必须在 Amazon FSx 文件系统的 Active Directory 计算机对象上添加与 DNS 别名对应的服务主体名称（SPN）。一个 SPN 一次只能与一个 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 名称已具有现有 SPN，则必须首先将其删除。

Kerberos 身份验证需要以下两个 SPN：

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

如果别名是 `finance.domain.com`，则必须具有以下两个 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主机 SPN 之前，您需要删除所有与 Active Directory 计算机对象上的 DNS 别名对应的现有主机 SPN。如果 AD 中存在 DNS 别名的 SPN，则为 Amazon FSx 文件系统设置 SPN 的尝试将会失败。

以下过程将介绍如何进行操作：

- 查找原始文件系统 Active Directory 计算机对象上的所有现有 DNS 别名 SPN。
- 若查找到现有 SPN，则将其删除。
- 为 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 Directory 模块

1. 登录已加入您的 Amazon FSx 文件系统所加入的 Active Directory 的 Windows 实例。

2. 以管理员身份打开 PowerShell。
3. 使用以下命令安装 PowerShell Active Directory 模块。

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

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

如果您为已分配给 Active Directory 中某个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，然后再将 SPN 添加到文件系统的计算机对象。

1. 使用以下命令查找所有现有 SPN。将 *alias_fqdn* 替换为在步骤 1 中与文件系统关联的 DNS 别名。

```
## 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。
   - 将 *alias_fqdn* 替换为在步骤 1 中与文件系统关联的完整 DNS 别名。
   - 将 *file_system_DNS_name* 替换为原始文件系统的 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. 对在步骤 1 中与文件系统关联的每个 DNS 别名重复上述步骤。

为 Amazon FSx 文件系统的 Active Directory 计算机对象设置 SPN

1. 运行以下命令，为 Amazon FSx 文件系统设置新的 SPN。

- 将 *file_system_DNS_name* 替换为 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，然后选择文件系统详细页面上的网络与安全窗格。

  您也可以在 API 操作 DescribeFileSystems 的响应中找到 DNS 名称。

- 将 *alias_fqdn* 替换为在步骤 1 中与文件系统关联的完整 DNS 别名。

```
## 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)

##Use the following command to set both the full FQDN and Alias SPNs
Set-AdComputer -Identity $FSxAdComputer -Add @{"msDS-AdditionalDnsHostname" =
 @($Alias, $Alias.Split(".")[0])}
```

> **Note**
>
> 如果原始文件系统的 AD 计算机对象中存在 DNS 别名的 SPN，则为 Amazon FSx 文件系统设置 SPN 将失败。有关查找并删除现有 SPN 的信息，请参阅查找并删除原始文件系统 Active Directory 计算机对象上的现有 DNS 别名 SPN。

2. 使用以下示例脚本验证是否为 DNS 别名配置了新 SPN。确保响应中包括两个主机 SPN HOST/*alias* 和 HOST/*alias_fqdn*，如本过程前面所述。

   将 *file_system_DNS_name* 替换为 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，然后选择文件系统详细页面上的网络与安全窗格。

   您也可以在 API 操作 DescribeFileSystems 的响应中找到 DNS 名称。

```
## 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. 对在步骤 1 中与文件系统关联的每个 DNS 别名重复上述步骤。

更新或创建 DNS CNAME 记录

为文件系统正确配置 SPN 后，可以通过以下方式割接到 Amazon FSx：将解析为原始文件系统的每个 DNS 记录替换为解析为 Amazon FSx 文件系统默认 DNS 名称的 DNS 记录。

要运行本节中介绍的命令，则必须配备 `dnsserver` 和 `activedirectory` Windows 模块。

安装所需的 PowerShell 模块

1. 以具有 DNS 管理权限的组（对于 Amazon Managed Microsoft AD，为 Amazon 委派的域名系统管理员；对于自行管理的 Active Directory，为域管理员或您已委派 DNS 管理权限的其他组）的成员用户身份登录到已加入您的 Amazon FSx 文件系统所加入的相同 Active Directory 的 Windows 实例。

   有关详细信息，请参阅《Amazon EC2 用户指南》中的 Connecting to Your Windows Instance。
2. 以管理员身份打开 PowerShell。
3. 按照此过程中的说明操作需要 PowerShell DNS 服务器模块。使用以下命令安装该模块。

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

要为 Amazon FSx 文件系统更新或创建自定义 DNS 名称

1. 以具有 DNS 管理权限的组（对于 Amazon 托管的 Active Directory，为 Amazon 委派的域名系统管理员；对于自行管理的 Active Directory，为域管理员或您已委派 DNS 管理权限的其他组）的成员用户身份连接到您的 Amazon EC2 实例。

   有关详细信息，请参阅《Amazon EC2 用户指南》中的 Connecting to Your Windows Instance。
2. 在命令提示符下，运行以下脚本。此脚本会将所有现有的 DNS CNAME 记录迁移到您的 Amazon FSx 文件系统。如果未找到任何记录，将为 DNS 别名 *`alias_fqdn`* 创建一个新的 DNS CNAME 记录，该记录将解析为 Amazon FSx 文件系统的默认 DNS 名称。

   要运行脚本，请执行以下操作：

   - 将 *`alias_fqdn`* 替换为与文件系统关联的 DNS 别名。

- 将 *file_system_DNS_name* 替换为 Amazon FSx 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) | Select -First 1
Add-DnsServerResourceRecordCName -Name $AliasHost -ComputerName
 $DnsServerComputerName -HostNameAlias $FSxDnsName -ZoneName $ZoneName
```

3. 对在步骤 1 中与文件系统关联的每个 DNS 别名重复上一步操作。

现已使用 DNS 别名为您的 Amazon FSx 文件系统添加了 DNS CNAME 值。现在，您可以使用 DNS 别名来访问数据。

> **Note**
>
> 在通过更新 DNS CNAME 记录来指向先前指向另一个文件系统的 Amazon FSx 文件系统时，客户端可能会在短时间内无法连接到该文件系统。刷新客户端 DNS 缓存后，则应能够使用 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。

使用组策略对象（GPO）强制执行 Kerberos 身份验证

通过在 Active Directory 中设置以下组策略对象（GPO），您可以强制要求在访问文件系统时使用 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计从计算机到运行 Windows 操作系统的任何远程服务器的传出 NTLM 流量。
- 限制 NTLM：为 NTLM 身份验证添加远程服务器例外：如果配置了“网络安全：限制 NTLM：向远程服务器传出 NTLM 流量”策略设置，则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例外列表。

1. 以管理员身份登录已加入您的 Amazon FSx 文件系统所加入的 Active Directory 的 Windows 实例。如果您正在配置自行管理的 Active Directory，请将这些步骤直接应用于 Active Directory。
2. 依次选择开始、管理工具、组策略管理。

3. 选择组策略对象。
4. 若不存在组策略对象，请执行创建操作。
5. 找到现有的网络安全：限制 NTLM：向远程服务器传出 NTLM 流量策略。（若不存在现有策略，请创建新策略。）在本地安全设置选项卡中，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. 选择应用即可应用设置。
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。

   在本地安全设置选项卡中，打开上下文（右键单击）菜单，然后选择属性。
9. 输入所有要添加到例外列表的服务器的名称。
10. 选择应用即可应用设置。

使用文件共享访问数据

Microsoft Windows 文件共享是文件系统中的特定文件夹或目录。它包括可能存在的任何子文件夹。客户端使用服务器消息块（SMB）协议来访问文件系统上的文件共享。FSx for Windows File Server 文件系统随附名为 `share` 的默认 Windows 文件共享。您可以使用 Windows 共享文件夹图形用户界面（GUI）工具，根据需要创建和管理任意数量的其他文件共享。

Microsoft Windows 持续可用（CA）共享的主要优势在于，即使集群中的服务器节点出现故障，仍能确保对共享文件的不间断访问。使用 CA 文件共享可在文件系统维护时段内最大限度地减少对服务器应用程序的干扰，这些应用程序将数据文件存储在这些文件共享上。

有关在 FSx for Windows File Server 文件系统上创建和管理文件共享的更多信息，包括 CA 共享，请参阅 创建、更新、删除文件共享。

映射文件共享

要访问文件共享，请使用 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，这一过程在 Linux 中称为挂载文件共享。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，您的应用程序和用户可以像访问本地文件和文件夹一样访问文件共享中的文件和文件夹。

有关映射和挂载文件共享以访问文件系统数据的更多信息，请参阅以下过程：

- 在 Amazon EC2 Windows 实例上映射文件共享.

- 在 Amazon EC2 Mac 实例上挂载文件共享
- 在 Amazon EC2 Linux 实例上挂载文件共享

在 Amazon EC2 Windows 实例上映射文件共享

您可以使用 Windows File Explorer 或命令提示符在 EC2 Windows 实例上映射文件共享，以访问 FSx for Windows File Server 文件系统。

在 Amazon EC2 Windows 实例上映射文件共享（文件资源管理器）

1. 启动 EC2 Windows 实例，并将其连接到 Amazon FSx 文件系统加入的 Microsoft Active Directory。为此，请从《Amazon Directory Service 管理指南》中选择以下过程：
   - 无缝加入 Windows EC2 实例
   - 手动加入 Windows 实例
2. 连接到您的 EC2 Windows 实例。有关详细信息，请参阅《Amazon EC2 用户指南》中的连接到 Windows 实例。
3. 连接后，请打开 File Explorer。
4. 在导航窗格中，打开网络的上下文（右键单击）菜单，然后选择映射网络驱动器。
5. 在驱动器中，选择一个驱动器盘符。
6. 在文件夹中，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。

   > **Important**
   >
   > 使用 IP 地址（而不是 DNS 名称），这可能在多可用区文件系统的失效转移过程中导致不可用的错误。此外，在多可用区和单可用区文件系统中，基于 Kerberos 的身份验证需要 DNS 名称或关联的 DNS 别名。

   您可以通过选择 Windows File Server、网络与安全，在 Amazon FSx 控制台上找到文件系统的 DNS 名称和任何关联的 DNS 别名。或者，您也可以在 CreateFileSystem 或 DescribeFileSystems API 操作的响应中找到它们。有关使用 DNS 别名的更多信息，请参阅管理 DNS 别名。

   - 对于加入 Amazon 托管的 Microsoft Active Directory 的单可用区文件系统，DNS 名称如下所示。

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

- 对于加入自行管理的 Active Directory 的单可用区文件系统，以及所有多可用区文件系统，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，请在文件夹中输入以下内容。

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

要使用多可用区文件系统的 DNS 名称，请在文件夹中输入以下内容。

```
\\amznfsxaa11bb22.ad-domain.com\share
```

要使用与文件系统关联的 DNS 别名，请在文件夹中输入以下内容。

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

7. 为登录时重新连接选择一个选项，指示文件共享是否应在登录时重新连接，然后选择完成。

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 Amazon FSx 文件系统加入的 Microsoft Active Directory。为此，请从《Amazon Directory Service 管理指南》中选择以下过程：
   - 无缝加入 Windows EC2 实例
   - 手动加入 Windows 实例
2. 以 Amazon Managed Microsoft AD 目录中的用户身份连接 EC2 Windows 实例。有关详细信息，请参阅《Amazon EC2 用户指南》中的连接到 Windows 实例。
3. 连接后，请打开命令提示符窗口。
4. 使用所选的驱动器盘符、文件系统的 DNS 名称和共享名称挂载文件共享。您可以在 Amazon FSx 控制台上选择 Windows File Server、网络与安全，从而找到 DNS 名称。或者，您可以在 `CreateFileSystem` 或 `DescribeFileSystems` API 操作的响应中找到它们。

- 对于加入 Amazon 托管的 Microsoft Active Directory 的单可用区文件系统，DNS 名称如下所示。

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

- 对于加入自行管理的 Active Directory 的单可用区文件系统，以及所有多可用区文件系统，DNS 名称如下所示。

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

下面是用于挂载文件共享的命令示例。

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

除 `net use` 命令之外，您还可以使用任何支持的 PowerShell 命令来挂载文件共享。

在 Amazon EC2 Mac 实例上挂载文件共享

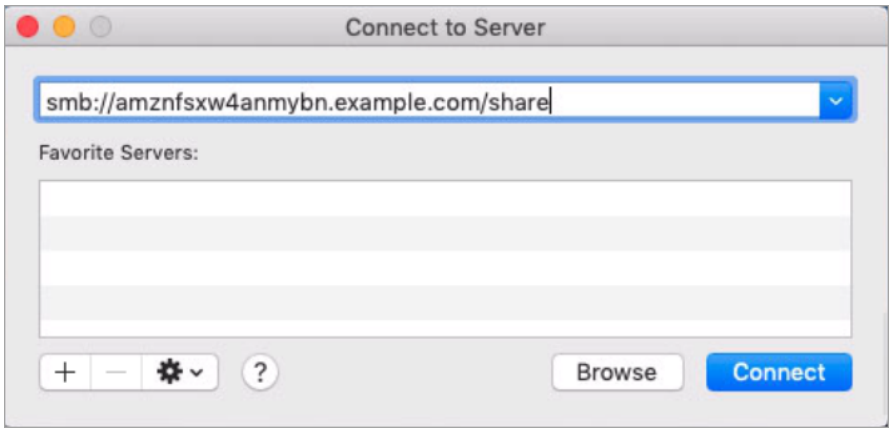
不管 Amazon EC2 Linux 实例是否加入 Active Directory 来访问 FSx for Windows File Server 文件系统，您都可以在该实例上挂载文件共享。如果实例未加入您的 Active Directory，请务必为实例所在的 Amazon Virtual Private Cloud（Amazon VPC）更新 DHCP 选项设置，以包含您的 Active Directory 域的 DNS 名称服务器。然后，重新启动实例。

在 Amazon EC2 Mac 实例上挂载文件共享（GUI）

1. 启动 EC2 Mac 实例。为此，请从《Amazon EC2 用户指南》中选择以下过程之一：
   - 使用控制台启动 Mac 实例
   - 使用 Amazon CLI 启动 Mac 实例
2. 使用 Virtual Network Computing（VNC）连接到 EC2 Mac 实例。有关更多信息，请参阅《Amazon EC2 用户指南》中的使用 VNC 连接到实例。
3. 在 EC2 Mac 实例上，连接到 Amazon FSx 文件共享，如下所示：
   a. 打开查找器，选择前往，然后选择连接到服务器。

b. 在连接到服务器对话框中，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。然后选择连接。

   您可以通过选择 Windows File Server、网络与安全，在 Amazon FSx 控制台上找到文件系统的 DNS 名称和任何关联的 DNS 别名。或者，您也可以在 CreateFileSystem 或 DescribeFileSystems API 操作的响应中找到它们。有关使用 DNS 别名的更多信息，请参阅管理 DNS 别名。



c. 在下一个屏幕上，选择连接以继续。

d. 输入 Amazon FSx 服务账户的 Microsoft Active Directory（AD）凭证，如以下示例所示。然后选择连接。

e. 如果连接成功，您会在 Finder 窗口的位置下方看到 Amazon FSx 共享。

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《Amazon EC2 用户指南》中选择以下过程之一：

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

2. 使用 Virtual Network Computing（VNC）连接到 EC2 Mac 实例。有关更多信息，请参阅《Amazon EC2 用户指南》中的使用 VNC 连接到实例。
3. 使用以下命令挂载文件共享。

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

您可以在 Amazon FSx 控制台上选择 Windows File Server、网络与安全，从而找到 DNS 名称。或者，您可以在 `CreateFileSystem` 或 `DescribeFileSystems` API 操作的响应中找到它们。

- 对于加入 Amazon 托管的 Microsoft Active Directory 的单可用区文件系统，DNS 名称如下所示。

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

- 对于加入自行管理的 Active Directory 的单可用区文件系统，以及所有多可用区文件系统，DNS 名称如下所示。

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

此过程中使用的挂载命令会在指定点执行以下操作：

- *//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* – 要挂载文件系统的 EC2 实例上的目录。

在 Amazon EC2 Linux 实例上挂载文件共享

不管 Amazon EC2 Linux 实例是否加入 Active Directory 来访问 FSx for Windows File Server 文件系统，您都可以在该实例上挂载 FSx for Windows File Server 文件共享。

> **Note**
>
> - 以下命令中指定的参数（SMB 协议、缓存，以及读取和写入缓冲区的大小）仅作为示例。Linux `cifs` 命令的参数选择以及所用 Linux 内核版本，可能会影响客户端与 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` 文档，了解您使用的 Linux 环境。
> - Linux 客户端不支持基于 DNS 的自动失效转移。有关更多信息，请参阅 Linux 客户端的失效转移经验。

在已加入 Active Directory 的 Amazon EC2 Linux 实例上挂载文件共享

1. 如果您还没有正在运行的 EC2 Linux 实例已加入 Microsoft Active Directory，请参阅《Amazon Directory Service 管理指南》中的手动加入 Linux 实例。
2. 连接到 EC2 Linux 实例。有关更多信息，请参阅《Amazon EC2 用户指南》中的连接到 Linux 实例。
3. 要安装 `cifs-utils` 包，请运行以下命令。此包用于在 Linux 上挂载 Amazon FSx 等网络文件系统。

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

4. 创建挂载点目录 **`/mnt/fsx`**。您将在此处挂载 Amazon FSx 文件系统。

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

5. 使用以下命令通过 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=no
   file-server-Ip
   ```

   您可以在 Amazon FSx 控制台上选择 Windows File Server、网络与安全，从而找到 DNS 名称。或者，您可以在 `CreateFileSystem` 或 `DescribeFileSystems` API 操作的响应中找到它们。

- 对于加入 Amazon 托管的 Microsoft Active Directory 的单可用区文件系统，DNS 名称如下所示。

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

- 对于加入自行管理的 Active Directory 的单可用区文件系统，以及所有多可用区文件系统，DNS 名称如下所示。

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

将 *CIFSMaxBufSize* 替换为内核允许的最大值。运行以下命令，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. 运行以下命令，验证文件系统是否已挂载，该命令仅返回通用 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,ui
```

此过程中使用的挂载命令会在指定点执行以下操作：

- *//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* – 要挂载文件系统的 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 File Server 的 Amazon FSx 支持 SMB 版本 2.0 至 3.1.1。
- `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。此 CIFS 缓存选项可能会影响性能，您应该测试哪些设置更适合您的内核和工作负载（并查看 Linux 文档）。建议使用选项 `strict` 和 `none`，因为 `loose` 可能会因协议语义较宽松而导致数据不一致。
- `cruid=`*ad_user* – 将凭证缓存所有者的 UID 设置为 AD 目录管理员。

- */mnt/fsx* – 在 EC2 实例上指定 Amazon FSx 文件共享的挂载点。
- 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。将 *CIFSMaxBufSize* 替换为内核允许的最大值。通过运行以下命令来确定 CIFSMaxBufSize。

```
$ 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 Amazon FSx 控制台，在文件系统详细信息页面的网络与安全选项卡上。
  - 在 describe-file-systems CLI 命令或等效 DescribeFileSystems API 命令的响应中。

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

以下过程将 Amazon FSx 文件共享挂载到未加入 Active Directory（AD）的 Amazon EC2 Linux 实例。对于未加入 AD 的 EC2 Linux 实例，您只能使用其私有 IP 地址挂载 FSx for Windows File Server 文件共享。您可以访问 Amazon FSx 控制台，在网络与安全选项卡上的首选文件服务器 IP 地址中获取文件系统的私有 IP 地址。

此示例使用 NTLM 身份验证。为此，您需要以用户身份（即，FSx for Windows File Server 文件系统所加入的 Microsoft Active Directory 域的成员）挂载文件系统。EC2 实例 creds.txt 上所创建的文本文件中会提供用户账户的凭证。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 控制台启动 Amazon Linux EC2 实例。有关更多信息，请参阅《Amazon EC2 用户指南》中的启动实例。
2. 连接到 Amazon Linux EC2 实例。有关更多信息，请参阅《Amazon EC2 用户指南》中的连接到 Linux 实例。

3. 要安装 cifs-utils 包，请运行以下命令。此包用于在 Linux 上挂载 Amazon FSx 等网络文件系统。

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

4. 创建您计划挂载 Amazon FSx 文件系统的挂载点 **/mnt/fsxx**。

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

5. 使用之前显示的格式在 /home/ec2-user 目录中创建 creds.txt 凭证文件。
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来读取和写入文件。

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

挂载文件系统

1. 您可以使用私有 IP 地址挂载未加入 Active Directory 的文件共享。您可以访问 Amazon FSx 控制台，在网络与安全选项卡上的首选文件服务器 IP 地址中获取文件系统的私有 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
```

将 *CIFSMaxBufSize* 替换为内核允许的最大值。运行以下命令，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. 运行以下命令，验证是否挂载了文件系统，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.EXA
```

此过程中使用的挂载命令会在指定点执行以下操作：

- *//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 File Server 的 Amazon FSx 支持 SMB 版本 2.0 至 3.1.1。
- `sec=ntlmsspi` – 指定使用 NT LAN Manager Security Support Provider Interface（NTLMSSPI）进行身份验证。
- `cache=`*cache_mode*：设置缓存模式。此 CIFS 缓存选项可能会影响性能，您应该测试哪些设置更适合您的内核和工作负载（并查看 Linux 文档）。建议使用选项 `strict` 和 `none`，因为 `loose` 可能会因协议语义较宽松而导致数据不一致。
- `cred=/home/ec2-user/creds.txt`：指定从何处获取用户凭证。
- */mnt/fsx* – 在 EC2 实例上指定 Amazon FSx 文件共享的挂载点。
- `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。将 *CIFSMaxBufSize* 替换为内核允许的最大值。通过运行以下命令来确定 `CIFSMaxBufSize`。

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

在 Amazon EC2 Linux 实例上自动挂载文件共享

每当挂载 FSx for Windows File Server 文件共享的 Amazon EC2 Linux 实例重启时，您可以自动挂载该文件共享以访问 FSx for Windows File Server 文件系统。为此，请在 EC2 实例上的 `/etc/fstab` 文件中添加一个条目。`/etc/fstab` 文件包含有关文件系统的信息。命令 mount -a 会在实例启动期间运行，用于挂载 `/etc/fstab` 文件中列出的文件系统。

对于未加入 Active Directory 的 Amazon EC2 Linux 实例，您只能使用其私有 IP 地址挂载 FSx for Windows File Server 文件共享。您可以访问 Amazon FSx 控制台，在网络与安全选项卡上的首选文件服务器 IP 地址中获取文件系统的私有 IP 地址。

以下过程使用 Microsoft NTLM 身份验证。您需要以用户身份（即，FSx for Windows File Server 文件系统所加入的 Microsoft Active Directory 域的成员）挂载文件系统。您可以使用下面的命令从 `creds.txt` 文件检索用户账户凭证。

```
$ 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 控制台启动 Amazon Linux EC2 实例。有关更多信息，请参阅《Amazon EC2 用户指南》中的启动实例。
2. 连接到您的实例。有关更多信息，请参阅《Amazon EC2 用户指南》中的连接到 Linux 实例。
3. 要安装 `cifs-utils` 包，请运行以下命令。此包用于在 Linux 上挂载 Amazon FSx 等网络文件系统。

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

4. 创建 `/mnt/fsx` 目录。您将在此处挂载 Amazon FSx 文件系统。

   ```
   $ sudo mkdir /mnt/fsx
   ```

5. 在 `/home/ec2-user` 目录中创建 `creds.txt` 凭证文件。
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来读取文件。

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

自动挂载文件系统

1. 您可以使用私有 IP 地址自动挂载未加入 Active Directory 的文件共享。您可以访问 Amazon FSx 控制台，在网络与安全选项卡上的首选文件服务器 IP 地址中获取文件系统的私有 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，请在 `/etc/fstab` 文件中添加以下行。

   ```
   //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 0 0
   ```

   将 *CIFSMaxBufSize* 替换为内核允许的最大值。运行以下命令，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. 将带“fake”选项的 mount 命令与“all”和“verbose”选项结合使用，从而测试 fstab 条目。

```
$ sudo mount -fav
home/ec2-user/fsx      : successfully mounted
```

4. 要挂载文件共享，请重启 Amazon EC2 实例。
5. 当实例再次可用时，运行以下命令以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.EXA
```

在此过程中为 /etc/fstab 文件添加的行在指定点执行以下操作：

- *//file-system-IP-address/file_share* – 指定要挂载的 Amazon FSx 文件系统的 IP 地址和共享。
- /mnt/fsx – 在 EC2 实例上指定 Amazon FSx 文件系统的挂载点。
- 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 File Server 的 Amazon FSx 支持 SMB 版本 2.0 至 3.1.1。
- sec=ntlmsspi – 指定使用 NT LAN Manager Security Support Provider Interface 来加速质询-响应身份验证。
- cache=*cache_mode*：设置缓存模式。此 CIFS 缓存选项可能会影响性能，您应该测试哪些设置更适合您的内核和工作负载（并查看 Linux 文档）。建议使用选项 strict 和 none，因为 loose 可能会因协议语义较宽松而导致数据不一致。
- cred=/home/ec2-user/creds.txt：指定从何处获取用户凭证。
- _netdev – 向操作系统指示文件系统位于需要网络访问的设备上。该选项会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 – 指示文件系统应该由 dump 备份，如果它是非零值。对于 Amazon FSx，该值应该是 0。
- 0：指定 fsck 在启动时检查文件系统的顺序。对于 Amazon FSx 文件系统，该值应为 0，表示 fsck 不应在启动时运行。

创建、更新、删除文件共享

本主题介绍了如何通过执行以下任务来管理文件共享。

- 创建新文件共享
- 修改现有文件共享
- 删除现有文件共享

您可以使用 Windows 本机共享文件夹 GUI 和 Amazon FSx CLI 在 PowerShell 上远程管理 FSx for Windows File Server 文件系统上的文件共享。使用共享文件夹 GUI（fsmgmt.msc）时，在首次打开位于其他文件系统上的共享上下文菜单时，可能会出现延迟。为避免延迟，请使用 PowerShell 管理位于多个文件系统上的文件共享。

Microsoft Windows 对文件和目录的命名实施规则和限制。为确保能够成功创建和访问数据，应根据这些 Windows 指南命名文件和目录。有关更多信息，请参阅命名惯例。

> **Warning**
>
> Amazon FSx 要求系统用户对创建 SMB 文件共享的每个文件夹都拥有完全控制 NTFS ACL 权限。请勿更改此用户在您文件夹上的 NTFS ACL 权限，否则会导致您的文件共享无法访问。

使用共享文件夹 GUI 管理文件共享

要管理 Amazon FSx 文件系统上的文件共享，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央位置。以下过程介绍了如何管理文件共享。

将共享文件夹连接到 FSx for Windows File Server 文件系统

1. 启动 Amazon EC2 实例，并将其连接到 Amazon FSx 文件系统加入的 Microsoft Active Directory。为此，请从《Amazon Directory Service 管理指南》中选择以下过程：
   - 无缝加入 Windows EC2 实例
   - 手动加入 Windows 实例
2. 以文件系统管理员组成员的用户身份连接到实例。在 Amazon 托管的 Microsoft Active Directory 中，该组被称为 Amazon 委派的 FSx 管理员。在您自行管理的 Microsoft Active Directory 中，该组被称为“域管理员”，或者使用您在创建时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 Elastic Compute Cloud 用户指南》中的连接 Windows 实例。

3. 打开开始菜单，然后使用以管理员身份运行来运行 fsmgmt.msc。此操作将打开共享文件夹 GUI 工具。
4. 在操作中，选择连接到另一台计算机。
5. 在另一台计算机中，输入您的 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，接着选择您的文件系统，然后查看文件系统详情页面的网络与安全部分。您也可以在 API 操作 DescribeFileSystems 的响应中找到 DNS 名称。
6. 选择确定。随后，共享文件夹工具的列表中将显示 Amazon FSx 文件系统的条目。

现在，共享文件夹已连接到您的 Amazon FSx 文件系统，您可以管理文件系统上的 Windows 文件共享。默认共享名为 `\share`。可通过执行以下步骤来做到这一点：

- 创建新文件共享 – 在共享文件夹工具中，选择左侧窗格中的共享，查看 Amazon FSx 文件系统的活动共享。选择新建共享，然后完成“创建共享文件夹”向导。

  在创建新文件共享之前，必须先创建本地文件夹。您可以按如下步骤执行操作：

  - 使用共享文件夹工具：指定本地文件夹路径时单击“浏览”，然后单击“创建新文件夹”，来创建本地文件夹。
  - 使用命令行：

    ```
    New-Item -Type Directory -Path \\amznfsxabcd0123.corp.example.com\D$\share
    \MyNewShare
    ```
- 修改文件共享 – 在共享文件夹工具的右侧窗格中，打开要修改的文件共享的上下文（右键单击）菜单，然后选择属性。修改属性并选择确定。
- 删除文件共享 – 在共享文件夹工具的右侧窗格中，打开要删除的文件共享的上下文（右键单击）菜单，然后选择停止共享。

> **Note**
>
> 对于单可用区 2 和多可用区文件系统，只有使用 Amazon FSx 文件系统的 DNS 名称连接到 fsmgmt.msc，才能使用共享文件夹 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）。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 工具将不支持这些操作。

> **Note**
>
> 如果您使用 fsmgmt.msc 共享文件夹 GUI 工具访问位于多个 FSx for Windows File Server 文件系统上的共享，则在首次打开位于不同文件系统的共享的文件共享上下文菜单时，可能会出现延迟。为避免延迟，您可以使用 PowerShell 管理文件共享，如下所述。

使用 PowerShell 管理文件共享

您可以使用适用于 PowerShell 的自定义 FSx for Windows File Server 远程管理命令来管理文件共享。这些命令有助于自动管理文件共享任务，例如：

- 将文件共享从现有文件服务器迁移到 Amazon FSx
- 在 Amazon Web Services 区域 中同步文件共享以便进行灾难恢复
- 对持续文件共享工作流程进行编程管理，如团队文件共享预置

要了解如何在 PowerShell 上使用 Amazon FSx CLI 进行远程管理，请参阅将 Amazon FSx CLI 用于 PowerShell。

下表列出了可用于管理 FSx for Windows File Server 文件系统上的文件共享的 Amazon FSx CLI 远程管理 PowerShell 命令。

共享管理命令	描述
New-FSxSmbShare	创建新文件共享。
Remove-FSxSmbShare	删除文件共享。
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）。
Grant-FSxSmbShareAccess	在共享的安全描述符中添加受信任者的允许访问控制条目（ACE）。

共享管理命令	描述
Revoke-FSxSmbShareAccess	从共享的安全描述符中删除受信任者的所有允许 ACE。
Block-FSxSmbShareAccess	在共享的安全描述符中添加受信任者的拒绝 ACE。
Unblock-FSxSmbShareAccess	从共享的安全描述符中删除受信任者的所有拒绝 ACE。

每个命令的联机帮助中都提供所有命令选项的参考信息。要访问此帮助，请运行包含 `-?` 的命令，例如 `New-FSxSmbShare -?`。

将凭证传递给 New-FSxSmbShare

您可以将凭证传递给 New-FSxSmbShare，这样就可以循环运行它来创建成百上千个共享了，而不必每次都重新输入凭证。

使用以下方法之一，准备在 FSx for Windows File Server 文件服务器上创建文件共享所需的凭证对象。

- 要以交互方式生成凭证对象，请使用以下命令。

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

- 要使用 Amazon Secrets Manager 资源生成凭证对象，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)))
```

创建持续可用（CA）的共享

您可以在 PowerShell 上使用 Amazon FSx CLI 以远程管理的方式来创建持续可用的（CA）共享。在 FSx for Windows File Server 多可用区文件系统上创建的 CA 共享具有出色的持久性和耐用性。Amazon FSx 单可用区文件系统构建于单节点集群之上。因此，在单可用区文件系统上创建的 CA 共享具有出色的持久性，但可用性不高。使用 `New-FSxSmbShare` 命令并将 `-ContinuouslyAvailable` 选项设置为 `$True` 来指定该共享是持续可用的共享。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
```

您可以使用 Set-FSxSmbShare 命令修改现有文件共享上的 -ContinuouslyAvailable 选项。

确定现有文件共享是否持续可用

使用以下命令查看现有文件共享的“持续可用”属性的值。

```
Invoke-Command -ComputerName powershell_endpoint -ConfigurationName FSxRemoteAdmin -
scriptblock { get-fsxsmbshare -name share_name }
```

如果启用 CA，则输出将包含以下行：

```
[...]
ContinuouslyAvailable : True
[...]
```

如果未启用 CA，则输出将包含以下行：

```
[...]
ContinuouslyAvailable : False
[...]
```

要在现有文件共享上启用“持续可用”，应使用以下命令：

```
Invoke-Command -ComputerName powershell_endpoint -ConfigurationName FSxRemoteAdmin -
scriptblock { set-fsxsmbshare -name share_name -ContinuouslyAvailable $True}
```

New-FSxSmbShare 命令因单向信任失败

如果您具有单向信任，并且用户所在的域未配置为信任与 Amazon FSx 文件系统关联的域，则 Amazon FSx 不支持执行 New-FSxSmbShare PowerShell 命令。

您可以使用以下解决方案之一来解决这种情况：

- 执行 New-FSxSmbShare 命令的用户必须与 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 使用共享文件夹 GUI 管理文件共享。

可用性与持久性：单可用区和多可用区文件系统

适用于 Windows File Server 的 Amazon FSx 提供两种文件系统部署类型：单可用区和多可用区。以下各节提供了帮助为工作负载选择正确部署类型的信息。有关该服务的可用性 SLA（服务等级协议）的信息，请参阅 Amazon FSx 服务等级协议。

> **Note**
>
> 多可用区文件系统在中国（北京）区域不可用。

单可用区文件系统由单个 Windows 文件服务器实例和单个可用区（AZ）内的一组存储卷组成。对于单可用区文件系统，在大多数情况下，数据会自动复制，以保护其免受单个组件故障的影响。Amazon FSx 会持续监控硬件故障，并通过更换发生故障的基础设施组件自动从故障事件中恢复。在故障恢复事件期间，以及在为文件系统配置的计划内维护时段，单可用区文件系统通常会经历约 30 分钟的停机时间。对于单可用区文件系统，在极少数情况下，文件系统故障可能无法恢复，例如由于多个组件故障，或者由于单个文件服务器的非正常故障导致文件系统处于不一致状态，在这种情况下，您可以从最新的备份中恢复文件系统。

多可用区文件系统由分布在两个可用区（首选可用区和备用可用区）的 Windows 文件服务器高可用性集群组成，利用 Windows Server 失效转移群集（WSFC）技术和两个可用区上的一组存储卷。数据在各可用区内和两个可用区之间同步复制。相对于单可用区部署，多可用区部署通过进一步跨可用区复制数据来提高持久性，并通过自动失效转移到备用可用区来提高计划内系统维护和计划外服务中断期间的可用性。这样您可以继续访问数据，并有助于保护您的数据免受实例故障和可用区中断的影响。

选择单可用区或多可用区文件系统部署类型

鉴于多可用区文件系统提供的高可用性和持久性模型，我们建议将多可用区文件系统用于大多数生产工作负载。单可用区部署是为测试和开发工作负载、某些在应用程序层内置复制功能且不需要额外存储级冗余的生产工作负载，以及可用性和恢复点目标（RPO）需求较为宽松的生产工作负载设计的一种经济高效的解决方案。在计划内文件系统维护或计划外服务中断的情况下，可用性和 RPO 需求较为宽松的工作负载最长可以承受可用性暂时丧失 20 分钟，在极少数情况下，可承受自最近一次备份以来的数据更新丢失。

此外还建议您查看文件系统的可用性模型，并确保在文件系统维护、吞吐能力更改和计划外服务中断等事件期间，您的工作负载能够适应所选部署类型的预期恢复行为。

按部署类型划分的功能支持

下表汇总了 FSx for Windows File Server 文件系统部署类型支持的功能：

部署类型	SSD 和存储	HDD 存储	DFS 命名空间	DFS 复制	自定义 DNS 名称	CA 共享
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 文件系统上创建持续可用的（CA）共享，但在 SQL Server HA 部署中，您应该在多可用区文件系统上使用 CA 共享。

故障转移过程

出现以下情况时，多可用区文件系统会自动从首选文件服务器失效转移到备用文件服务器：

- 可用区发生中断。
- 首选文件服务器不可用。
- 首选文件服务器进行计划内维护。

从一台文件服务器失效转移到另一台文件服务器时，新的活动文件服务器会自动开始处理所有文件系统的读取和写入请求。当首选子网中的资源可用时，Amazon FSx 会将失效自动恢复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将备用文件服务器提升为活动状态，失效转移通常会在 30 秒内完成。原始多可用区配置的失效自动恢复也会在不到 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。

在您的文件系统进行失效转移和失效自动恢复的短时间内，I/O 可能会暂停，Amazon CloudWatch 指标可能暂时不可用。对于多可用区文件系统，在失效转移和失效自动恢复期间发生的任何文件读写活动，都需在主文件服务器和辅助文件服务器之间进行同步。对于采用 HDD 存储的文件系统，以及写入

密集型和 IOPS 密集型的工作负载，此过程可能需要长达数小时。我们建议在文件系统负载较小时测试失效转移对应用程序的影响。

Windows 客户端上的失效转移经验

从一台文件服务器失效转移到另一台文件服务器时，新的活动文件服务器会自动开始处理所有文件系统的读取和写入请求。首选子网中的资源可用后，Amazon FSx 会将失效自动恢复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，因此失效转移对 Windows 应用程序是透明的，这些应用程序无需手动干预即可恢复文件系统的操作。从在活动文件服务器上检测到故障到将备用文件服务器提升为活动状态，失效转移通常会在 30 秒内完成。原始多可用区配置的失效自动恢复也会在不到 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。

Linux 客户端的失效转移经验

Linux 客户端不支持基于 DNS 的自动失效转移。因此，在失效转移期间，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失效自动恢复到首选子网中的文件服务器之后，它们将自动恢复文件系统的操作。

在文件系统上测试失效转移

您可以通过修改多可用区文件系统的吞吐能力来测试其失效转移。当您修改文件系统的吞吐能力时，Amazon FSx 会关闭文件系统的文件服务器。当 Amazon FSx 首先替换首选文件服务器时，多可用区文件系统会自动失效转移到辅助服务器。然后文件系统会失效自动恢复到新的主服务器，Amazon FSx 将替换辅助文件服务器。

您可以在 Amazon FSx 控制台、CLI 和 API 中监控吞吐能力更新请求的进度。成功完成更新后，您的文件系统已失效转移到辅助服务器，并将失效自动恢复到主服务器。有关修改文件系统的吞吐能力和监控请求进度的更多信息，请参阅 管理吞吐能力。

单可用区和多可用区文件系统资源

单可用区和多可用区文件系统对子网和弹性网络接口的使用方式有所不同，如以下各节所述。

子网

创建虚拟私有云（VPC）时，其可跨越 Amazon Web Services 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。每个可用区中默认 VPC 有一个子网。子网是您的 VPC 内的 IP 地址范围。子网必须位于单个可用区中。

FSx for Windows File Server 单可用区文件系统需要一个子网，该子网需在创建时指定。您选择的子网将定义所创建文件系统中的可用区。

多可用区文件系统需要两个子网，分别用于首选文件服务器和备用文件服务器。您选择的两个子网必须位于同一 Amazon 区域的不同可用区中。

对于 Amazon 中的应用程序，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

弹性网络接口是 VPC 中表示虚拟网卡的逻辑网络组件。当您创建 Amazon FSx 文件系统时，Amazon FSx 会在您与文件系统关联的 VPC 中预置一个或多个弹性网络接口。弹性网络接口使客户端能够与文件系统通信并挂载该文件系统。该弹性网络接口虽然是您账户 VPC 的一部分，但仍视作在 Amazon FSx 的服务范围内。多可用区文件系统有两个弹性网络接口，每个文件服务器一个。单可用区文件系统只有一个弹性网络接口。

> **Warning**
>
> 请勿修改或删除与文件系统关联的弹性网络接口。修改或删除该网络接口可能会导致永久丢失您的 VPC 和文件系统之间的连接。

下表汇总 FSx for Windows File Server 单可用区文件系统和多可用区文件系统的资源利用率：

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向公共互联网公开。如果弹性 IP 地址（可从互联网访问的公有 IP 地址）附加到文件系统弹性网络接口，Amazon FSx 会将其自动分离。

使用 Microsoft Active Directory

创建 FSx for Windows File Server 文件系统时，您可以将其加入您的 Active Directory 域，以提供用户身份验证以及文件和文件夹级别的访问控制。Amazon FSx 使用 Microsoft Active Directory 与您的现有的 Microsoft Windows 环境集成。Amazon FSx 提供了 将 Amazon FSx 与 Amazon Directory Service for Microsoft Active Directory 结合使用 和 使用自行管理的 Microsoft Active Directory 两个选项，使您可以通过 Active Directory 使用 FSx for Windows File Server 文件系统。

Active Directory 是 Microsoft 目录服务，用于存储有关网络上对象的信息，使管理员和用户能够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账户。

然后，您的用户可以使用其在 Active Directory 中的现有用户身份自行进行身份验证并访问 FSx for Windows File Server 文件系统。用户还可以使用其现有身份来控制对单个文件和文件夹的访问。此外，还可以将现有文件和文件夹及其安全访问控制列表（ACL）配置迁移到 Amazon FSx，而无需进行任何修改。

> **Note**
>
> Amazon FSx 支持 Microsoft Azure Active Directory 域服务，您可以将此服务加入 Microsoft Azure Active Directory。

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

- 服务用户凭证
- DNS 服务器的 IP 地址

对于创建文件系统后加入的 Microsoft AD，您无法更改以下属性：

- DomainName
- OrganizationalUnitDistinguishedName
- FileSystemAdministratorsGroup

但是，您可以通过备份来创建新的文件系统，并在新文件系统的 Microsoft Active Directory 集成配置中更改上述属性。有关更多信息，请参阅 将备份还原至新文件系统。

> **Note**
>
> Amazon FSx 不支持 Active Directory Connector 和 Simple Active Directory。

如果由于 Active Directory 的配置发生更改而导致其与文件系统的连接中断，则 FSx for Windows File Server 可能会出现配置错误。要将您的文件系统恢复到可用状态，请在 Amazon FSx 控制台中选择尝试恢复按钮，或者在 Amazon FSx API 或控制台中使用 `StartMisconfiguredStateRecovery` 命令。有关更多信息，请参阅文件系统处于配置错误状态。

主题

将 Amazon FSx 与 Amazon Directory Service for Microsoft Active Directory 结合使用

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 目录。您可以在工作负载部署中使用这些 Active Directory 目录。

如果您的组织使用 Amazon Managed Microsoft AD 管理身份和设备，我们建议您将 Amazon FSx 文件系统与 Amazon Managed Microsoft AD 集成。此操作将为您提供一个使用 Amazon FSx 和 Amazon Managed Microsoft AD 的一站式解决方案。Amazon 会处理这两项服务的部署、操作、高可用性、可靠性、安全性和无缝集成，使您能够专注于高效操作自己的工作负载。

您可以使用 Amazon FSx 控制台来将 Amazon FSx 与 Amazon Managed Microsoft AD 设置结合使用。在控制台中创建新的 FSx for Windows File Server 文件系统时，请选择 Windows 身份验证部分下的 Amazon 托管 Active Directory。您还可以选择要使用的特定目录。有关更多信息，请参阅 步骤 5。创建文件系统。

您的组织可能会在自行管理的 Active Directory 域（本地或云端）上管理身份和设备。如果是，您可以将您的 Amazon FSx 文件系统直接加入到现有的自行管理的 Active Directory 域中。有关更多信息，请参阅 使用自行管理的 Microsoft Active Directory。

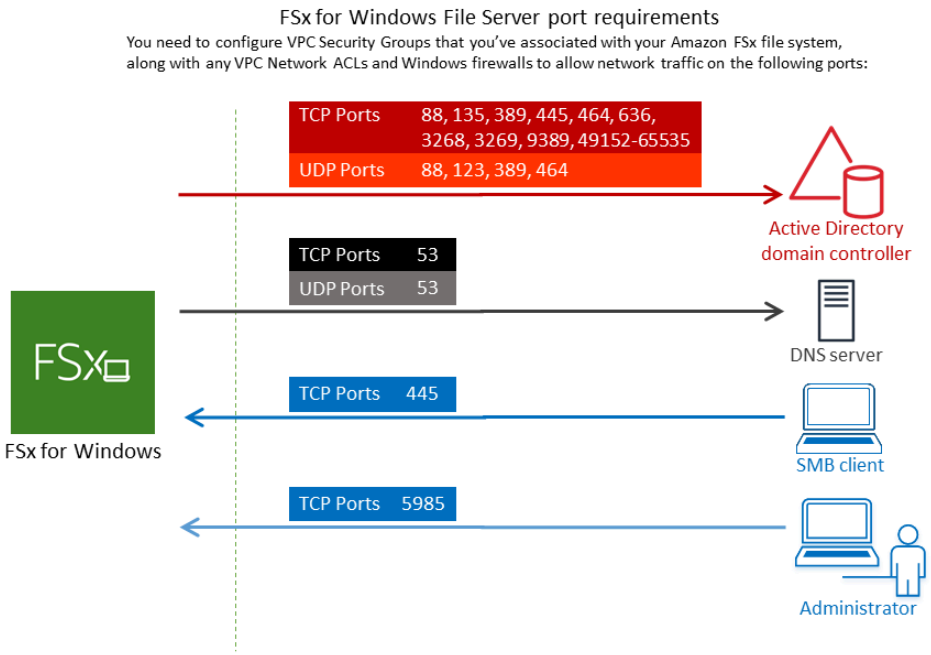
此外，您还可以将系统设置为从资源林隔离模型获益。在此模型中，您可以将资源（包括 Amazon FSx 文件系统）隔离到与用户所在的 Active Directory 林相互独立的 AD 林中。

> **Important**
>
> 对于单可用区 2 和所有多可用区文件系统，Active Directory 完全限定域名（FQDN）不得超过 47 个字符。

联网先决条件

在创建已加入 Amazon Microsoft 托管 Active Directory 域的 FSx for Windows File Server 文件系统之前，请确保您已经创建并设置了以下网络配置：

- 对于 VPC 安全组，用于您的默认 Amazon VPC 的默认安全组已添加到控制台中的文件系统。请确保要在其中创建 FSx 文件系统的子网的安全组和 VPC 网络 ACL 在端口上允许有下图所示方向的流量。



下表确定了每个端口的作用。

协议	端口	角色
TCP/UDP	53	域名系统（DNS
TCP/UDP	88	Kerbe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

协议	端口	角色
UDP	123	网络时间协议（NTP）
TCP	135	分布式计算环境/端点映射器（DCEPMA
TCP	445	目录服务 SMB 文件共享

协议	端口	角色
TCP	636	基于 TLS/SSL 的轻型目录访问协议（LDA
TCP	3268	Micros 全局目录
TCP	3269	基于 SSL 的 Micros 全局目录

协议	端口	角色
TCP	5985	WinRI 2.0（M soft Windo 远程管理）
TCP	9389	Micros AD DS Web 服务、P hell
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，则还必须允许动态端口（49152-65535）上的出站流量。

- 若要将 Amazon FSx 文件系统连接到位于其他 VPC 或账户中的 Amazon 托管 Microsoft Active Directory，则请确保此 VPC 与您要在其中创建文件系统的 Amazon VPC 之间已建立连接。有关更多信息，请参阅 在不同的 VPC 或账户中将 Amazon FSx 与 Amazon Managed Microsoft AD 结合使用。

> **Important**
>
> 虽然 Amazon VPC 安全组要求仅在发起网络流量的方向打开端口，但大多数 VPC 网络 ACL 要求双向打开端口。

使用 Amazon FSx 网络验证工具验证与 Active Directory 域控制器之间的连接。

使用资源林隔离模型

将文件系统加入到 Amazon Managed Microsoft AD 设置。即可在您创建的 Amazon Managed Microsoft AD 域和现有的自行管理的 Active Directory 域之间建立单向林信任关系。对于 Amazon FSx 中的 Windows 身份验证，您只需要单向林信任，即 Amazon 托管的林信任企业域林。

您的企业域为受信任域，而 Amazon Directory Service 托管的域为信任域。经过验证的身份验证请求只能在域之间单向传输，即允许企业域中的账户根据托管的域中共享的资源进行身份验证。在这种情况下，Amazon FSx 仅与 Amazon 托管的域进行交互。在 Kerberos 身份验证场景中，来自公司客户端的身份验证请求由公司域进行验证，然后公司域将其转交给 Amazon Managed Microsoft AD，最后客户端向 FSx for Windows File Server 文件系统提交服务票证。有关信任的更多信息，请参阅 Amazon 安全博客中的 Everything you wanted to know about trusts with Amazon Managed Microsoft AD。

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 域控制器之间的连接。有关更多信息，请参阅 验证与 Active Directory 域控制器的连接。

下列相关资源能够帮助您将 Amazon Directory Service for Microsoft Active Directory 与 FSx for Windows File Server 结合使用：

- 《Amazon Directory Service 管理指南》中的什么是 Amazon Directory Service
- 《Amazon Directory Service 管理指南》中的创建 Amazon 托管 Active Directory
- 《Amazon Directory Service 管理指南》中的何时创建信任关系。

在不同的 VPC 或账户中将 Amazon FSx 与 Amazon Managed Microsoft AD 结合使用

您可以使用 VPC 对等连接将 FSx for Windows File Serverr 文件系统加入到同一账户内不同 VPC 中的 Amazon Managed Microsoft AD 目录中。您还可以使用目录共享将您的文件系统加入到不同 Amazon 账户下的 Amazon Managed Microsoft AD 目录中。

> **Note**
>
> 只能选择与文件系统处于相同 Amazon Web Services 区域 中的 Amazon Managed Microsoft AD。如果要使用跨区域 VPC 对等设置，则应使用自行管理的 Microsoft Active Directory。有关更多信息，请参阅 使用自行管理的 Microsoft Active Directory。

将文件系统加入其他 VPC 中的 Amazon Managed Microsoft AD 的工作流程包括以下步骤：

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

有关更多信息，请参阅《Amazon Directory Service 管理指南》中的共享目录。

您可以使用 Amazon Transit Gateway 或 Amazon VPC 并创建 VPC 对等连接来设置您的网络环境。此外，请确保两个 VPC 之间允许网络流量。

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《Amazon VPC 中转网关指南》中的开始使用中转网关。

VPC 对等连接是两个 VPC 之间的网络连接。使用连接，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。可以使用 VPC 对等，在同一 Amazon Web Services 区域中或在 Amazon Web Services 区域之间连接 VPC。有关 VPC 对等连接的更多信息，请参阅《Amazon VPC 对等连接指南》中的什么是 VPC 对等连接？。

要将文件系统加入到与该文件系统使用不同账户的 Amazon Managed Microsoft AD 目录时，还需要满足另一个先决条件。您还需要与另一个账户共享您的 Microsoft Active Directory 目录。要执行此操作，您可以使用 Amazon 托管 Microsoft Active Directory 的目录共享功能。要了解更多信息，请参阅《Amazon Directory Service 管理指南》中的共享目录。

验证与 Active Directory 域控制器的连接

在创建已加入 Active Directory 的 FSx for Windows File Server 文件系统之前，请使用 Amazon FSx Active Directory 验证工具来验证与 Active Directory 域之间的连接。无论您与 FSx for Windows File Server 结合使用的是 Amazon 托管 Microsoft Active Directory，还是自行管理的 Active Directory 配置，都可以使用此测试。域控制器网络连接测试（test-fsxadControllerConnection）不会对域中的每个域控制器运行整套网络连接检查。相反，应使用此测试针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. 在同一个子网中，启动一个具有相同 Amazon VPC 安全组且您要将其用于 FSx for Windows File Server 文件系统的 Amazon EC2 Windows 实例。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 Active Directory 有关更多信息，请参阅《Amazon Directory Service 管理指南》中的手动加入 Windows 实例。
3. 连接到您的 EC2 实例。有关详细信息，请参阅《Amazon EC2 用户指南》中的 Connecting to Your Windows Instance。
4. 在 EC2 实例上打开 Windows PowerShell 窗口（使用以管理员身份运行）。

   请使用以下测试命令测试是否已安装 Windows PowerShell 所需的 Active Directory 模块。

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

   如果上一操作返回错误，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. 使用以下命令下载 zip 文件。

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

7. 将 AmazonFSxADValidation 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. 以下示例所示为检索包含结果为连接测试成功的测试输出。

```
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
```

以下示例所示为运行测试以及获得失败的结果。

```
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

> **Note**
>
> 作为上述过程的替代方法，您可以使用 AWSSupport-ValidateFSxWindowsADConfig 运行手册，验证自行管理的 Active Directory 配置。有关更多信息，请参阅《Amazon Systems Manager Automation 运行手册参考》中的 AWSSupport-ValidateFSxWindowsADConfig。

使用自行管理的 Microsoft Active Directory

如果您的组织在本地或云端使用自行管理的 Active Directory 管理身份和设备，则可以在创建时将 FSx 适用于 Windows 文件服务器的文件系统加入到您的 Active Directory 域中。

当您将文件系统加入自我管理的 Active Directory 时， FSx 适用于 Windows 的文件服务器的文件系统与您的用户和现有资源（包括现有文件服务器）位于同一 Active Directory 林（包含域、用户和计算机的 Active Directory 配置中的顶级逻辑容器）和同一 Active Directory 域中。

> **Note**
>
> 您可以将您的资源（包括您的 Amazon FSx 文件系统）隔离到与用户所在林分开的 Active Directory 林中。为此，请将您的文件系统加入 Amazon 托管的 Microsoft Active Directory，并在您创建的 Amazon 托管的 Microsoft Active Directory 和现有的自行管理的 Active Directory 之间建立单向林信任关系。

- 您的 Active Directory 域上的服务账户的用户名和密码，供亚马逊用于 FSx将文件系统加入到您的 Active Directory 域中。您可以将这些凭证以纯文本形式提供，也可以将其存储在其中 Amazon Secrets Manager 并提供密钥 ARN（推荐）。
- （可选）您希望将文件系统加入其中的域中的组织单元（OU）。
- （可选）您要委派授权，使其对文件系统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访问控制列表 (ACLs)、获取文件和文件夹的所有权等。如果您未指定此组，则默认情况下，亚马逊 FSx 会将此权限委托给您的 Active Directory 域中的域管理员组。

  > **Note**
  >
  > 您提供的域组名称在 Active Directory 中必须是唯一的。 FSx Windows 文件服务器在以下情况下不会创建域组：
  >
  > - 如果已经存在一个名称由您指定过的群组
  > - 如果未指定名称，Active Directory 中已经存在一个名为“域管理员”的群组。

有关更多信息，请参阅 将亚马逊 FSx 文件系统加入自我管理的 Microsoft Active Directory 域。

主题

先决条件

在将 FSx 适用于 Windows 的文件服务器文件系统加入自我管理的 Microsoft Active Directory 域之前，请查看以下先决条件，以帮助确保您可以成功地将亚马逊 FSx 文件系统加入到自我管理的 Active Directory 中。

本地配置

这些是你要加入亚马逊 FSx 文件系统的自行管理的 Microsoft Active Directory（本地或云端）的先决条件。

- Active Directory 域控制器：
  - 必须具有 Windows Server 2008 R2 或更高版本的域功能级别。
  - 必须可写入。
  - 至少有一个可访问的域控制器必须是林的全局目录。
- DNS 服务器必须能够解析如下所示的名称：
  - 在要加入文件系统的域中
  - 在林的根域中
- DNS 服务器和 Active Directory 域控制器 IP 地址必须满足以下要求，这些要求因创建亚马逊 FSx 文件系统的时间而异：

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
IP 地址必须在 RFC 1918 私有 IP 地址范围内： • 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	IP 地址可以位于任何范围内，但以下情况除外： • 与文件系统所在的 Amazon Web Services 拥有的 IP 地址冲突的 IP 地址。 Amazon Web Services 区域 有关按地区划分的 Amazon 拥有的 IP 地址列表，请参阅 Amazon IP 地址范围。 • IP 地址在以下 CIDR 数据块范围内：198.19.0.0/16

如果您需要使用非私有 IP 地址范围访问 2020 年 12 月 17 日之前创建的 Windows 文件服务器文件系统，则可以通过恢复文件系统的备份来创建新的文件系统。 FSx 有关更多信息，请参阅 将备份还原至新文件系统。

- 自行管理的 Active Directory 的域名必须满足以下要求：
  - 该域名未采用单标签域（SLD）格式。Amazon 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，域名不得超过 47 个字符。
- 您定义的任何 Active Directory 站点必须满足以下先决条件：
  - VPC 中与文件系统关联的子网必须在 Active Directory 站点中进行定义。
  - VPC 子网与任何 Active Directory 站点子网之间没有产生冲突。

Amazon FSx 需要连接到您在活动目录环境中定义的域控制器或 Active Directory 站点。亚马逊 FSx 将忽略所有在端口 389 上屏蔽了 TCP 和 UDP 的域控制器。对于您的 Active Directory 中的其余域控制器，请确保它们满足 Amazon FSx 连接要求。此外，确认对服务账户所做的任何更改均已传播到所有这些域控制器。

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

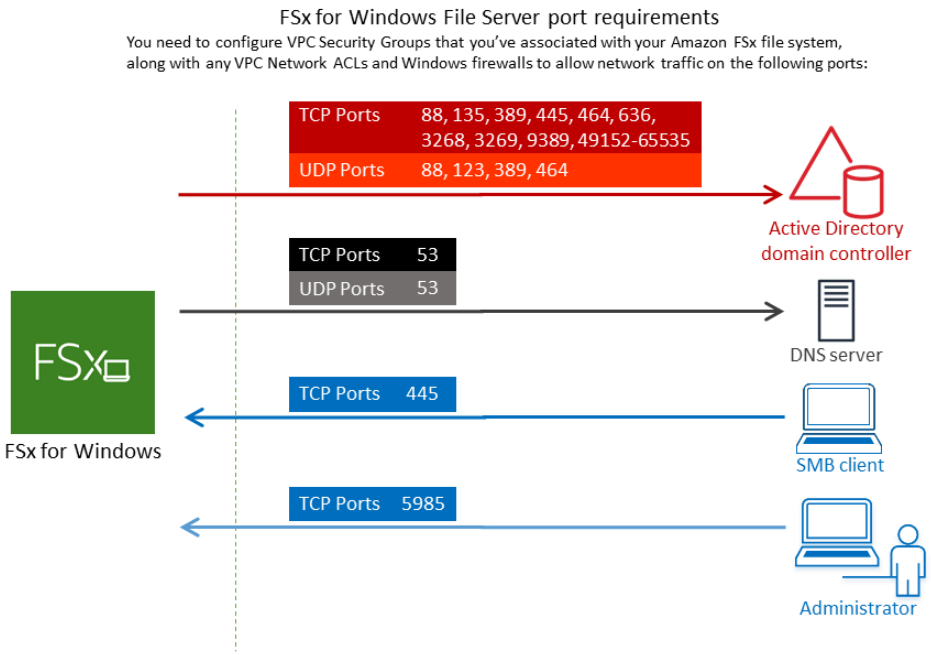
您可以使用 Amazon Active Directory 验证工具验证您的 Act FSx ive Directory 配置，包括测试多个域控制器的连接。要限制需要连接的域控制器的数量，您还可以在本地域控制器和 Amazon Managed Microsoft AD之间建立信任关系。有关更多信息，请参阅 使用资源林隔离模型。

> **Important**
>
> FSx 只有当你使用微软 DNS 作为默认 DNS 服务时，亚马逊才会注册文件系统的 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手动设置文件系统的 DNS 记录条目。

网络配置

本节介绍了将文件系统加入自行管理的 Active Directory 的网络配置要求。我们强烈建议您在尝试将文件系统加入自行管理的 A ct FSx ive Directory 之前，使用 Amazon Active Directory 验证工具测试您的网络设置。

- 确保您的防火墙规则允许您的 Active Directory 域控制器与 Amazon FSx 之间的 ICMP 流量。
- 必须在您要在其中创建文件系统的 Amazon VPC 与自行管理的 Active Directory 之间配置连接。您可以使用 Amazon Direct Connect、Amazon Virtual Private Network、VPC 对等连接或 Amazon Transit Gateway 来设置此连接。
- 必须使用亚马逊 FSx 控制台将默认 Amazon VPC 的默认 VPC 安全组添加到您的文件系统中。确保您创建文件系统的子网的安全组和 VPC 网络 ACLs 允许下图所示的端口和方向的流量。



下表明确了协议、端口及其角色。

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 Environment/End 点映射器 (DCE/EPMAP)
TCP	445	目录服务 SMB 文件共享
TCP	636	轻量级目录访问协议 TLS/SSL (LDAPS)
TCP	3268	Microsoft 全局目录

协议	端口	角色
TCP	3269	基于 SSL 的 Microsoft 全局目录
TCP	5985	WinRM 2.0（Microsoft Windows 远程管理）
TCP	9389	微软活动目录 DS Web 服务， PowerShell **Important** 单可用区 2 和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。
TCP	49152 - 65535	RPC 的临时端口

这些流量规则还需要镜像到适用于每个 Active Directory 域控制器、DNS 服务器、 FSx 客户端和管理员的防火墙上。 FSx

Note

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

Important

虽然 Amazon VPC 安全组要求仅在网络流量启动的方向上打开端口，但大多数 Windows 防火墙和 VPC 网络都 ACLs 要求双向打开端口。

服务账户权限

您需要在自行管理的 Microsoft Active Directory 中有一个服务账户，该账户具有将计算机对象加入该自行管理的 Microsoft Active Directory 域的委派权限。服务账户是自行管理的 Active Directory 中的一个用户账户，该账户已被委派某些任务。

以下是必须向要加入文件系统的 OU 中的 Amazon FSx 服务账户委派的最低权限集。

- 如果使用 Active Directory 用户和计算机 MMC 中的委派控制：
  - 重置密码
  - 读取和写入账户限制
  - 已验证写入 DNS 主机名
  - 已验证写入服务主体名称
- 如果使用 Active Directory 用户和计算机 MMC 中的高级功能：
  - 修改权限
  - 创建计算机对象
  - 删除计算机对象

有关更多信息，请参阅主题为错误：当已委派控制的非管理员用户尝试将计算机加入域控制器时，访问被拒绝的 Microsoft Windows Server 文档。

有关设置所需权限的更多信息，请参阅 向 Amazon FSx 服务账户或群组委派权限。

使用自行管理 Active Directory 时的最佳实践

主题

- 使用存储活动目录凭证 Amazon Secrets Manager

我们建议您在将亚马逊 FSx 版 Windows 文件服务器文件系统加入自行管理的 Microsoft Active Directory 时，遵循这些最佳实践。这些最佳实践有助于您保持文件系统的持续、不间断的可用性。

为亚马逊使用单独的服务账户 FSx

使用单独的服务账户授予所需的权限，让 Amazon FSx 完全管理加入您自行管理的 Active Directory 的文件系统。我们不建议为此使用域管理员。

使用 Active Directory 组

使用 Active Directory 组管理与亚马逊 FSx 服务账户关联的活动目录权限和配置。

隔离组织单元（OU）

为了便于查找和管理您的 Amazon FSx 计算机对象，我们建议您将用于 Windows File Server 文件系统的组织单位 (OU) 与其他域控制器问题区分开来。 FSx

保留活动目录配置 up-to-date

必须保留文件系统的 Active Directory 配置 up-to-date而不作任何更改。例如，如果自行管理的 Active Directory 使用基于时间的密码重置策略，则在密码重置后，应立即更新文件系统上的服务账户密码。有关更多信息，请参阅 更新自行管理的 Active Directory 配置。

更改 Amazon FSx 服务账户

如果您使用新服务账户更新文件系统，则此账户必须拥有加入 Active Directory 的所需权限和特权，并对与文件系统关联的现有计算机对象拥有完全控制权限。有关更多信息，请参阅 更改 Amazon FSx 服务账户。

将子网分配给单个 Microsoft Active Directory 站点

如果您的 Active Directory 环境中有大量域控制器，请使用 A ctive Directory 网站和服务将您的亚马逊 FSx 文件系统使用的子网分配给可用性和可靠性最高的单个 Active Directory 站点。确保 VPC 安全组、VPC 网络 ACL、您 DCs的 Windows 防火墙规则以及您的 Active Directory 基础设施中的任何其他网络路由控制允许亚马逊 FSx 通过所需端口进行通信。这允许 Windows 在无法使用分配的 Active Directory 站点时还原至其他域控制器。有关更多信息，请参阅 使用 Amazon VPC 进行文件系统访问控制。

使用安全组规则限制流量

使用安全组规则在虚拟私有云（VPC）中实现最低权限原则。可以使用 VPC 安全组规则限制文件允许的入站和出站网络流量的类型。例如，我们建议仅允许出站流量流向自行管理的 Active Directory 域控制器或所用子网或安全组内部。有关更多信息，请参阅 使用 Amazon VPC 进行文件系统访问控制。

请勿移动 Amazon 创建的计算机对象 FSx

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

验证 Active Directory 配置

在尝试将 FSx 适用于 Windows 的文件服务器文件系统加入您的活动目录之前，我们强烈建议您使用亚马逊 Active Directory 验证工具验证您的 FSx 活动目录配置。

使用存储活动目录凭证 Amazon Secrets Manager

你可以使用 Amazon Secrets Manager 安全地存储和管理你的 Microsoft Active Directory 域加入服务帐户凭据。此方法无需在应用程序代码或配置文件中以明文形式存储敏感凭证，从而增强您的安全状况。

您还可以配置 IAM 策略，以管理对密钥的访问权限，并为密码设置自动轮换策略。

将活动目录凭据存储在 Amazon Secrets Manager （控制台）

步骤 1：创建 KMS 密钥

创建 KMS 密钥，以在 Secrets Manager 中对 Active Directory 凭证进行加密和解密。

创建密钥

> **Note**
>
> 对于加密密钥，请创建新密钥，不要使用 Amazon 默认 KMS 密钥。请务必 Amazon KMS key 在包含要加入 Active Directory 的文件系统的同一个区域中创建。

1. 在 https://console.aws.amazon.com /km Amazon KMS s 处打开控制台
2. 选择创建密钥。
3. 对于密钥类型，选择对称。
4. 对于密钥用法，选择加密和解密。
5. 对于高级选项，执行以下操作：
   a. 对于密钥材料源，选择 KMS。
   b. 对于区域性，选择单区域密钥，然后选择下一步。
6. 选择下一步。
7. 对于别名，提供 KMS 密钥的名称。
8. （可选）对于描述，提供 KMS 密钥的描述。
9. （可选）对于标签，提供 KMS 密钥的标签，然后选择下一步。
10. （可选）对于密钥管理员，提供获授权管理此密钥的 IAM 用户和角色。
11. 对于密钥删除，确保选中允许密钥管理员删除此密钥复选框，然后选择下一步。
12. （可选）对于密钥用户，提供获授权在加密操作中使用此密钥的 IAM 用户和角色。选择下一步。

13. 对于密钥策略，选择编辑并在政策声明中包含以下内容以允许 Amazon FSx 使用 KMS 密钥，然后选择下一步。请务必将替换*us-west-2*为文件系统的部署 Amazon Web Services 区域 位置和您*123456789012*的 Amazon Web Services 账户 ID。

```
{
    "Sid": "Allow FSx to use the KMS key",
    "Version": "2012-10-17",
    "Effect": "Allow",
    "Principal": {
        "Service": "fsx.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:DescribeKey"
    ],
    "Resource": "arn:aws:kms:us-west-2:123456789012:key:*",
    "Condition": {
        "StringEquals": {
            "kms:EncryptionContext:SecretARN": "arn:aws:secretsmanager:us-
west-2:123456789012:secret:*",
            "kms:ViaService": "secretsmanager.us-west-2.amazonaws.com",
            "aws:SourceAccount": "123456789012"
        },
        "ArnLike": {
            "aws:SourceArn": "arn:aws:fsx:us-west-2:123456789012:file-system/*"
        }
    }
}
```

14. 选择结束。

> **Note**
>
> 通过修改 Resource 和 aws:SourceArn 字段，您可以设置更精细的访问控制，以针对特定的密钥和文件系统。

第 2 步：创建 Amazon Secrets Manager 密钥

创建密钥

1. 打开 Secrets Manager 控制台，网址为https://console.aws.amazon.com/secretsmanager/。
2. 选择存储新密钥。
3. 对于密钥类型，请选择其他密钥类型。
4. 对于键/值对，请执行以下操作以添加您的两个密钥：
   a. 对于第一个密钥，请输入 CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME。
   b. 对于第一个密钥的值，请仅输入 AD 用户的用户名（不带域前缀）。
   c. 对于第二个密钥，请输入 CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD。
   d. 对于第二个密钥的值，请输入您在域中为 AD 用户创建的密码。
5. 对于加密密钥，输入上一步所创建 KMS 密钥的 ARN，然后选择下一步。
6. 在密钥名称中，输入一个描述性名称，以便您稍后查找自己的密钥。
7. （可选）对于描述，输入密钥名称的描述。
8. 对于资源权限，选择编辑。

   在权限策略中添加以下策略以允许 Amazon FSx 使用该密钥，然后选择 Next。请务必将替换*us-west-2*为文件系统的部署 Amazon Web Services 区域 位置和您*123456789012*的 Amazon Web Services 账户 ID。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "fsx.amazonaws.com"
            },
            "Action": [
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret"
            ],
            "Resource": "arn:aws:secretsmanager:us-west-2:123456789012:secret:*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012"
                },
```

```
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:fsx:us-west-2:123456789012:file-
system/*"
                }
            }
        }
    ]
}
```

> **Note**
>
> 通过修改 Resource 和 aws:SourceArn 字段，您可以设置更精细的访问控制，以针对特定的密钥和文件系统。

9. （可选）您可以将 Secrets Manager 配置为自动轮换凭证。选择下一步。
10. 选择结束。

将活动目录凭据存储在 Amazon Secrets Manager (CLI)

步骤 1：创建 KMS 密钥

创建 KMS 密钥，以在 Secrets Manager 中对 Active Directory 凭证进行加密和解密。

要创建 KMS 密钥，请使用 Amazon CLI 命令创建密钥。

在此命令中，设置 --policy 参数，以指定定义 KMS 密钥权限的密钥策略。该策略必须包含以下内容：

- Amazon 的服务主体 FSx，即fsx.amazonaws.com。
- 所需的 KMS 操作：kms:Decrypt 和 kms:DescribeKey。
- 您的 Amazon Web Services 区域 和账户的资源 ARN 模式。
- 限制密钥使用的条件键：
  - kms:ViaService，以确保请求通过 Secrets Manager 发出。
  - aws:SourceAccount，以限制您的账户。
  - aws:SourceArn仅限于特定的 Amazon FSx 文件系统。

以下示例创建了一个对称加密 KMS 密钥，其策略允许 Amazon FSx 使用该密钥进行解密和密钥描述操作。该命令会自动检索您的 Amazon Web Services 账户 ID 和区域，然后使用这些值配置密钥策略，

以确保亚马逊 FSx、Secrets Manager 和 KMS 密钥之间进行适当的访问控制。确保您的 Amazon CLI 环境与将加入 Active Directory 的文件系统位于同一区域。

```
# Set region and get Account ID
REGION=${AWS_REGION:-$(aws configure get region)}
ACCOUNT_ID=$(aws sts get-caller-identity --query 'Account' --output text)

# Create Key
KMS_KEY_ARN=$(aws kms create-key --policy "{
  \"Version\": \"2012-10-17\",
  \"Statement\": [
    {
      \"Sid\": \"Enable IAM User Permissions\",
      \"Effect\": \"Allow\",
      \"Principal\": {
        \"AWS\": \"arn:aws:iam::$ACCOUNT_ID:root\"
      },
      \"Action\": \"kms:*\",
      \"Resource\": \"*\"
    },
    {
      \"Sid\": \"Allow FSx to use the KMS key\",
      \"Effect\": \"Allow\",
      \"Principal\": {
        \"Service\": \"fsx.amazonaws.com\"
      },
      \"Action\": [
        \"kms:Decrypt\",
        \"kms:DescribeKey\"
      ],
      \"Resource\": \"*\",
      \"Condition\": {
        \"StringEquals\": {
          \"kms:ViaService\": \"secretsmanager.$REGION.amazonaws.com\",
          \"aws:SourceAccount\": \"$ACCOUNT_ID\"
        },
        \"ArnLike\": {
          \"aws:SourceArn\": \"arn:aws:fsx:$REGION:$ACCOUNT_ID:file-system/*\"
        }
      }
    }
  ]
}" --query 'KeyMetadata.Arn' --output text)
```

```
echo "KMS Key ARN: $KMS_KEY_ARN"
```

> **Note**
>
> 通过修改 Resource 和 aws:SourceArn 字段，您可以设置更精细的访问控制，以针对特定的密钥和文件系统。

第 2 步：创建 Amazon Secrets Manager 密钥

要为亚马逊 FSx 创建用于访问您的活动目录的密钥，请使用 c reate-secre Amazon CLI t 命令并设置以下参数：

- `--name`：密钥的标识符。
- `--description`：密钥用途的描述。
- `--kms-key-id`：您在步骤 1 中创建的 KMS 密钥 ARN，用于加密静态密钥。
- `--secret-string`：包含 AD 凭证的 JSON 字符串，格式如下：
  - `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME`：不带域前缀的 AD 服务账户用户名，例如 `svc-fsx`。请勿提供域前缀，例如 `CORP\svc-fsx`。
  - `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD`：AD 服务账户密码。
- `--region`：您的 Amazon FSx 文件系统将在 Amazon Web Services 区域 哪里创建。如果 `AWS_REGION` 未设置，则默认为您配置的区域。

创建密钥后，使用put-resource-policy命令附加资源策略，并设置以下参数：

- `--secret-id`：要附加策略的密钥的名称或 ARN。以下示例使用 **`FSxSecret`** 作为 `--secret-id`。
- `--region`: 和你的秘密 Amazon Web Services 区域 一样。
- `--resource-policy`：授予亚马逊访问密钥 FSx 权限的 JSON 政策文档。该策略必须包含以下内容：
  - Amazon 的服务主体 FSx，即**`fsx.amazonaws.com`**。
  - 所需的 Secrets Manager 操作：`secretsmanager:GetSecretValue` 和 `secretsmanager:DescribeSecret`。
  - 您的 Amazon Web Services 区域 和账户的资源 ARN 模式。

- 以下限制访问的条件键：
  - `aws:SourceAccount`，以限制您的账户。
  - `aws:SourceArn`仅限于特定的 Amazon FSx 文件系统。

以下示例创建了一个具有所需格式的密钥，并附加了允许 Amazon FSx 使用该密钥的资源策略。此示例会自动检索您的 Amazon Web Services 账户 ID 和区域，然后使用这些值配置资源策略，以确保在 Amazon FSx 和密钥之间进行适当的访问控制。

确保使用您在步骤 1 中所创建密钥的 ARN 替换 `KMS_KEY_ARN`，并使用 Active Directory 服务账户凭证替换 `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME` 和 `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD`。此外，请验证您的 Amazon CLI 环境配置是否与将要加入 Active Directory 的文件系统的区域相同。

```
# Set region and get account ID
REGION=${AWS_REGION:-$(aws configure get region)}
ACCOUNT_ID=$(aws sts get-caller-identity --query 'Account' --output text)

# Replace with your KMS key ARN from Step 1
KMS_KEY_ARN="arn:aws:kms:us-east-2:123456789012:key/1234542f-d114-555b-9ade-
fec3c9200d8e"

# Replace with your Active Directory credentials
AD_USERNAME="Your_Username"
AD_PASSWORD="Your_Password"

# Create the secret
SECRET_ARN=$(aws secretsmanager create-secret \
  --name "FSxSecret" \
  --description "Secret for FSx access" \
  --kms-key-id "$KMS_KEY_ARN" \
  --secret-string "{\"CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME\":\"$AD_USERNAME\",
\"CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD\":\"$AD_PASSWORD\"}" \
  --region "$REGION" \
  --query 'ARN' \
  --output text)

echo "Secret created with ARN: $SECRET_ARN"

# Attach the resource policy with proper formatting
aws secretsmanager put-resource-policy \
  --secret-id "FSxSecret" \
```

```
  --region "$REGION" \
  --resource-policy "{
    \"Version\": \"2012-10-17\",
    \"Statement\": [
      {
        \"Effect\": \"Allow\",
        \"Principal\": {
          \"Service\": \"fsx.amazonaws.com\"
        },
        \"Action\": [
          \"secretsmanager:GetSecretValue\",
          \"secretsmanager:DescribeSecret\"
        ],
        \"Resource\": \"$SECRET_ARN\",
        \"Condition\": {
          \"StringEquals\": {
            \"aws:SourceAccount\": \"$ACCOUNT_ID\"
          },
          \"ArnLike\": {
            \"aws:SourceArn\": \"arn:aws:fsx:$REGION:$ACCOUNT_ID:file-system/*\"
          }
        }
      }
    ]
  }"

echo "Resource policy attached successfully"
```

> **Note**
>
> 通过修改 `Resource` 和 `aws:SourceArn` 字段，您可以设置更精细的访问控制，以针对特定的密钥和文件系统。

亚马逊 FSx 服务账户

加入自我管理的 Active Directory 的 Amazon FSx 文件系统在整个生命周期中都需要有效的服务账户。Amazon FSx 使用该服务账户来全面管理您的文件系统并执行管理任务，这些任务需要将计算机对象退出并重新加入到您的 Active Directory 域中。这些任务包括更换出现故障的文件服务器并给 Microsoft Windows Server 软件打补丁。 FSx 要让亚马逊执行这些任务，亚马逊 FSx 服务账户必须至少拥有服务账户权限委托给它的一组权限，如中所述。

尽管域管理员组的成员拥有足够的权限来执行这些任务，但我们强烈建议您使用单独的服务账户将所需的权限委托给 Amazon FSx。

有关如何使用 Active Directory 用户和计算机 MMC 管理单元中的委派控制或高级功能功能来委派权限的更多信息，请参阅 向 Amazon FSx 服务账户或群组委派权限。

如果您使用新服务账户更新文件系统，新服务账户必须拥有加入 Active Directory 的所需权限和特权，并对与文件系统关联的现有计算机对象拥有完全控制权限。有关更多信息，请参阅 更改 Amazon FSx 服务账户。

我们建议将您的 Active Directory 服务账户凭证存储在 Amazon Secrets Manager 中，以增强安全性。这样就无需以明文形式存储敏感凭证，且符合安全最佳实践。有关更多信息，请参阅 使用自行管理的 Microsoft Active Directory。

向 Amazon FSx 服务账户或群组委派权限

亚马逊 FSx 服务账户或管理员组必须具有必要的权限，才能将 Windows 文件服务器文件系统加入 FSx 您的自我管理的 Active Directory 域。要委派这些权限，可以使用 Active Directory User and Computers MMC 管理单元中的委派控制或高级功能，如以下过程所述。

使用委派控制分配权限

使用委派控制为服务账号或群组分配权限

1. 以 Active Directory 域的域管理员身份登录系统。
2. 打开 Active Directory User and Computers MMC 管理单元。
3. 在任务窗格中，展开域节点。
4. 找到并打开您要修改的 OU 的上下文（右键单击）菜单，然后选择委派控制。
5. 在控制委派向导页面上，选择下一步。
6. 选择 “添加” 以添加您的亚马逊 FSx 服务账户或群组的名称，然后选择 “下一步”。
7. 在要委派的任务页面上，选择创建要委派的自定义任务，然后选择下一步。
8. 选择仅文件夹中的以下对象，然后选择计算机对象。
9. 选择在此文件夹中创建选定对象和删除此文件夹中的选定对象。然后选择下一步。
10. 在权限中，请选择以下选项：

    - 重置密码
    - 读取和写入账户限制

- 已验证写入 DNS 主机名
- 已验证写入服务主体名称

11. 选择下一步，然后选择完成。
12. 关闭 Active Directory User and Computers MMC 管理单元。

使用高级功能分配权限

1. 以 Active Directory 域的域管理员身份登录系统。
2. 打开 Active Directory User and Computers MMC 管理单元。
3. 从菜单栏中选择查看，并确保已启用高级功能（如果启用了该功能，则旁边会显示一个对勾标记）。
4. 在任务窗格中，展开域节点。
5. 找到并打开您要修改的 OU 的上下文菜单（右键单击），然后选择属性。
6. 在 OU 属性窗格中，选择安全选项卡。
7. 在安全选项卡上，选择高级。然后选择添加。
8. 在 “权限输入” 页面上，选择 “选择委托人”，然后输入您的亚马逊 FSx 服务账户或群组的名称。在适用于:中，选择此对象和所有后代计算机。请确保选择了以下权限：

   - 修改权限
   - 创建计算机对象
   - 删除计算机对象

9. 选择应用，然后选择确定。
10. 关闭 Active Directory User and Computers MMC 管理单元。

验证 Active Directory 配置

在创建加入活动目录 FSx 的 Windows 文件服务器文件系统之前，我们建议您使用亚马逊 Active Directory 验证工具验证您的 FSx 活动目录配置。请注意，成功验证 Active Directory 配置需要出站互联网连接。

验证 Active Directory 配置

1. 在您用 EC2 于 Windows 文件服务器文件系统的相同子网和相同的 Amazon VPC 安全组中启动一个 Ama FSx zon Windows 实例。确保您的 EC2 实例具有所需的 `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《IAM 用户指南》中的使用 IAM 策略模拟器测试 IAM 策略。

2. 将你的 EC2 Windows 实例加入你的活动目录。有关更多信息，请参阅《Amazon Directory Service 管理指南》中的手动加入 Windows 实例。
3. Connect 连接到您的 EC2 实例。有关更多信息，请参阅亚马逊 EC2 用户指南中的连接到您的 Windows 实例。
4. 在 EC2 实例上打开 Windows PowerShell 窗口（使用以管理员身份运行）。

   要测试是否安装了 Windows 所需 PowerShell 的 Active Directory 模块，请使用以下测试命令。

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

   如果上一操作返回错误，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. 使用以下命令下载 zip 文件。

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

7. 将 AmazonFSxADValidation 模块添加到当前会话。

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

8. 通过替换为以下命令来设置必需的参数：

   - 活动目录域名 (*DOMAINNAME.COM*)
   - 使用以下选项之一为服务账户密码准备 $Credential 对象。
     - 要以交互方式生成凭证对象，请使用以下命令。

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

- 要使用 Amazon Secrets Manager 资源生成凭证对象，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*)
- 您计划在其中创建 Amazon FSx 文件系统的子网的子网 ID（例如 *SUBNET_1SUBNET_2*，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）在运行验证工具之前 DomainControllersMaxCount，按照随附README.md文件中的说明设置组织单位、委派管理员组并启用服务帐户权限验证。

> **Note**
>
> 如果操作系统非英语，则 Domain Admins 组的名称会有所不同。例如，该组在法语 OS 版本中被命名为 Administrateurs du domaine。如果未指定值，则将使用默认 Domain Admins 组名，且文件系统创建失败。

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
```

以下是测试结果有误的示例。

```
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
```

如果您在运行验证工具时收到警告或错误，请参阅验证工具包（TROUBLESHOOTING.md）和 对亚马逊进行故障排除 FSx 中包含的《问题排查指南》。

将亚马逊 FSx 文件系统加入自我管理的 Microsoft Active Directory 域

当你 FSx 为 Windows 文件服务器创建新的文件系统时，你可以配置 Microsoft Active Directory 集成，使其加入你自行管理的 Microsoft Active Directory 域。为此，请为您的 Microsoft Active Directory 提供以下信息：

- 本地 Microsoft Active Directory 目录的完全限定域名（FQDN）。

> **Note**
>
> Amazon FSx 目前不支持单一标签域名 (SLD) 域名。

- 域的 DNS 服务器的 IP 地址。

- Amazon 用于将文件系统加入您的域的 A FSx ctive Directory 服务账户的证书。可通过以下任一方式提供这些凭证：
  - 选项 1： Amazon Secrets Manager 秘密 ARN-包含您的 Active Directory 域上服务帐户的用户名和密码的密钥。有关更多信息，请参阅 使用存储活动目录凭证 Amazon Secrets Manager。
  - 选项 2：纯文本凭证
    - 服务账户用户名：现有 Microsoft Active Directory 中服务账户的用户名。请勿包含域前缀或后缀。例如，对于 `EXAMPLE\ADMIN`，仅使用 `ADMIN`。
    - 服务账户密码 – 服务账户的密码。

或者，您也可以指定以下内容：

- 您希望 Amazon FSx 文件系统加入的域内的特定组织单位 (OU)。
- 域组的名称，其成员被授予 Amazon FSx 文件系统的管理权限。您提供的域组名称在 Active Directory 中必须是唯一的。

在您指定此信息后，Amazon 会使用您提供的服务账户将您的新文件系统 FSx 加入到您自行管理的 Active Directory 域中。

> **Important**
>
> FSx 只有当你加入的活动目录域使用微软 DNS 作为默认 DNS 时，亚马逊才会注册文件系统的 DNS 记录。如果您使用的是第三方 DNS，则需要在创建 FSx 文件系统后手动设置 Amazon 文件系统的 DNS 条目。有关为文件系统选择正确 IP 地址的更多信息，请参阅获取用于手动 DNS 条目的正确文件系统 IP 地址。

开始前的准备工作

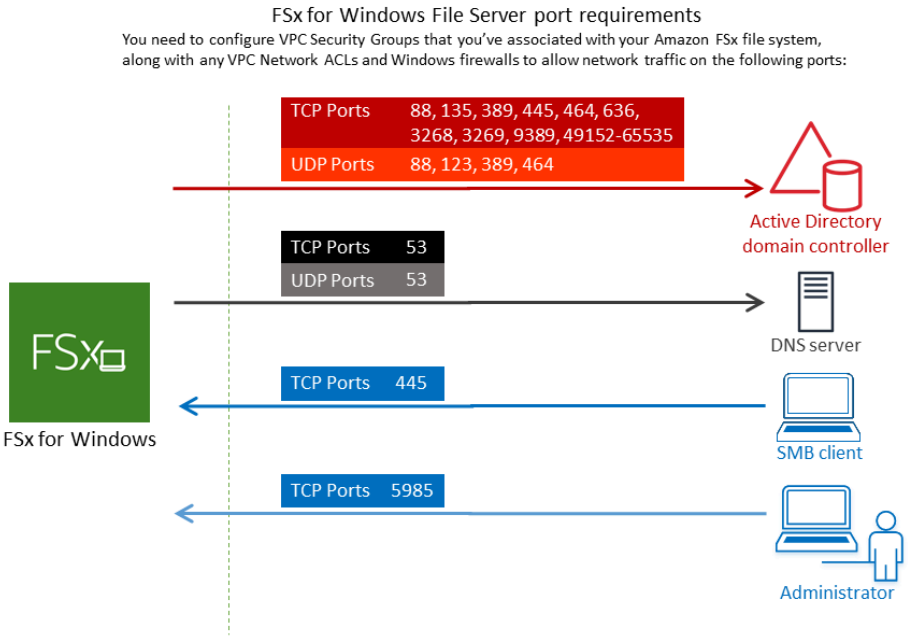
确保您已完成 使用自行管理的 Microsoft Active Directory 中详述的 先决条件。

创建加入自我管理 FSx 的 Active Directory 的 Windows 文件服务器文件系统（控制台）

1. 打开 Amazon FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 在控制面板上，选择创建文件系统以启动文件系统创建向导。
3. 选择 “Window FSx s 文件服务器”，然后选择 “下一步”。显示创建文件系统页面。

4. 为您的文件提供名称。您最多可以使用 256 个 Unicode 字母、空格和数字以及特殊字符：+ - = . _ : /
5. 对于存储容量，请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 范围内的任意整数。如果您使用的是 HDD 存储，请输入 2,000 – 65,536 范围内的任意整数。创建文件系统后，您可以根据需要随时增加存储容量。有关更多信息，请参阅 管理存储容量。
6. 保持吞吐能力设置为默认设置。吞吐能力是托管文件系统的文件服务器可以持续提供数据的速度。建议的吞吐能力设置基于您选择的存储容量。如果您需要的吞吐能力超过建议吞吐能力，请选择指定吞吐能力，然后选择一个值。有关更多信息，请参阅 FSx for Windows File Server 性能。

   创建文件系统后，您可以根据需要随时修改吞吐能力。有关更多信息，请参阅 管理吞吐能力。
7. 选择要与文件系统关联的 VPC。在本入门练习中，请选择与您的 Amazon Directory Service 目录和 Amazon EC2 实例相同的 VPC。
8. 为可用区和子网选择任意值。
9. 对于 VPC 安全组，用于您的默认 Amazon VPC 的默认安全组已添加到控制台中的文件系统。请确保您创建 FSx 文件系统的子网的安全组和 VPC 网络 ACLs 允许以下图所示的端口和方向上的流量。



下表确定了每个端口的作用。

协议	端口	角色
TCP/UDP	53	域名系统（DNS
TCP/UDP	88	Kerbe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

协议	端口	角色
UDP	123	网络时间协议（NTP）
TCP	135	分布式计算环境/端点映射器（DCEPMA
TCP	445	目录服务 SMB 文件共享

协议	端口	角色
TCP	636	轻量级目录访问协议 TLS/SSL (LDAP
TCP	3268	Micros 全局目录
TCP	3269	基于 SSL 的 Micros 全局目录

协议	端口	角色
TCP	5985	WinRI 2.0（M soft Windo 远程管理）
TCP	9389	微软活动目录 DS Web 服务，Powe l
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 ACLs，则还必须允许来自文件系统的动态端口 (49152-65535) 上的出站流量。 FSx

- 允许所有流量流向与您自行管理的 Microsoft Active Directory 域的 DNS 服务器和域控制器关联的 IP 地址的出站规则。有关更多信息，请参阅 Microsoft 关于为 Active Directory 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 Active Directory 域控制器、DNS 服务器、 FSx 客户端和管理员的防火墙上。 FSx

> **Note**
>
> 如果您定义了 Active Directory 站点，则必须确保与 Amazon FSx 文件系统关联的 VPC 中的子网在 Active Directory 站点中定义，并且您的 VPC 中的子网与其他站点中的子网之间不存在冲突。您可以使用 Active Directory Sites and Services MMC 管理单元查看和更改这些设置。

> **Important**
>
> 虽然 Amazon VPC 安全组要求仅在网络流量启动的方向上打开端口，但大多数 Windows 防火墙和 VPC 网络都 ACLs 要求双向打开端口。

10. 对于 Windows 身份验证，选择自行管理的 Microsoft Active Directory。
11. 输入自行管理的 Microsoft Active Directory 目录的完全限定域名值。

> **Note**
>
> 域名不能采用单标签域（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 域名不得超过 47 个字符。

12. 输入自行管理的 Microsoft Active Directory 目录的组织单元值。

> **Note**
>
> 确保您提供的服务账号已将权限委托给您在此处指定的 OU，或者如果您未指定，则委托给默认 OU。

13. 在自行管理的 Microsoft Active Directory 目录的 DNS 服务器 IP 地址中至少输入一个值（不超过两个）。
14. 服务账户凭证：选择如何提供服务账户凭证：

    - 选项 1： Amazon Secrets Manager 秘密 ARN-包含您的 Active Directory 域上服务帐户的用户名和密码的密钥。有关更多信息，请参阅 使用存储活动目录凭证 Amazon Secrets Manager。
    - 选项 2：纯文本凭证
      - 服务账户用户名：现有 Microsoft Active Directory 中服务账户的用户名。请勿包含域前缀或后缀。例如，对于 `EXAMPLE\ADMIN`，仅使用 `ADMIN`。
      - 服务账户密码 – 服务账户的密码。
      - 确认密码 – 服务账户的密码。

    > **Important**
    >
    > 输入服务账户用户名时，请勿包含域前缀（`corp.com\ServiceAcct`）或域后缀（`ServiceAcct@corp.com`）。
    > 输入服务账户用户名（`CN=ServiceAcct,OU=example,DC=corp,DC=com`）时，请勿使用可分辨名称（DN）。

15. 对于委派的文件系统管理员组，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您的文件系统上执行管理任务的委托授权。如果您不提供值，Amazon 会 FSx 使用内置`Domain Admins`组。请注意，Amazon FSx 不支持`Delegated file system administrators group`将（您指定的`Domain Admins`群组或自定义群组）置于内置容器中。

> **Important**
>
> 如果您未提供委派文件系统管理员组，则默认情况下，Amazon 会 FSx 尝试在您的 Active Directory 域中使用该内置Domain Admins组。如果此内置组的名称已更改，或者您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**
>
> 在提供群组名称参数时，请勿包含域名前缀 (corp.com\ FSx Admins) 或域后缀 (FSxAdmins@corp.com)。
> 请勿使用该组的可分辨名称（DN）。可分辨名称的一个例子是 CN= FSx Admins、ou=Example、dc=Corp、dc=com。

要创建加入自我管理 FSx 的 Active Directory 的 Windows 文件服务器文件系统 ()Amazon CLI

以下示例创建了一个 FSx 适用于 Windows 文件服务器的文件系统，该文件系统SelfManagedActiveDirectoryConfiguration位于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",FileSystemAdmini
 \
UserName="FSxService",Password="password", \
   DnsIps=["10.0.1.18"]}',ThroughputCapacity=8
```

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

获取用于手动 DNS 条目的正确文件系统 IP 地址

FSx 只有当你使用微软 DNS 作为默认 DNS 服务时，亚马逊才会注册文件系统的 DNS 记录。如果您使用的是第三方 DNS，则需要为您的 Amazon FSx 文件系统手动设置 DNS 条目。本节介绍在必须手动将文件系统添加到 DNS 时，如何获取要使用的正确的文件系统 IP 地址。请注意，创建文件系统后，在删除文件系统之前，其 IP 地址不会更改。

如何获取用于 DNS A 条目的文件系统 IP 地址

1. 在中 https://console.aws.amazon.com/fsx/，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. 在网络与安全选项卡中，执行以下任一操作：

   - 对于单可用区 1 文件系统：
     - 在 “子网” 面板中，选择 “网络接口” 下显示的 elastic 网络接口，在 Amazon EC2 控制台中打开 “网络接口” 页面。
     - 要使用的单可用区 1 文件系统的 IP 地址显示在主私 IPv4 有 IP 列中。
   - 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 “网络接口” 下显示的 elastic n etwork 接口，在 Amazon EC2 控制台中打开 “网络接口” 页面。
     - 要使用的首选子网的 IP 地址显示在 “辅助私 IPv4 有 IP” 列中。
     - 在 Amazon FSx 待机子网面板中，选择网络接口下显示的弹性网络接口，在亚马逊 EC2 控制台中打开网络接口页面。
     - 备用子网要使用的 IP 地址显示在 “辅助私 IPv4 有 IP” 列中。

> **Note**
>
> 如果您需要为单可用区 2 或多可用区文件系统的 Windows 远程 PowerShell 终端节点设置 DNS 条目，则应使用首选子网的弹性网络接口的主私有 IPv4 地址。有关更多信息，请参阅 将 Amazon FSx CLI 用于 PowerShell。

更新自行管理的 Active Directory 配置

为了帮助确保您的 Amazon FSx 文件系统持续、不间断地可用，当以下任何 Active Directory 属性发生变化时，您必须更新文件系统的 Active Directory 配置：

- DNS 服务器的 IP 地址
- 自行管理的 Active Directory 的服务账户凭证

当您更新 Amazon FSx 文件系统的自我管理的 Active Directory 配置时，在应用更新时，您的文件系统的状态将从 “可用” 切换为 “正在更新”。验证状态是否在应用更新后切换回可用 – 请注意，更新可能需要几分钟时间才能完成。有关更多信息，请参阅 监控自行管理的 Active Directory 更新。

如果自行管理的 Active Directory 配置在更新后出现问题，则文件系统状态会切换为错误配置。在此状态下，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更正措施。采取建议的更正措施后，请验证文件系统的状态是否最终变为可用。

> **Important**
>
> 如果您使用新服务账户更新文件系统，请确保新服务账户对与文件系统关联的现有计算机对象具有完全控制权限。

若要了解如何排查与自行管理的 Active Directory 配置相关的可能问题，请参阅 文件系统处于配置错误状态。

您可以使用 Amazon Web Services 管理控制台、Amazon FSx API 或 Amazon CLI 更新文件系统自我管理的 Active Directory 配置的服务账户凭证和 DNS 服务器 IP 地址。您可以随时使用 Amazon Web Services 管理控制台、CLI 和 API 跟踪自我管理的 Active Directory 配置更新的进度。有关更多信息，请参阅 监控自行管理的 Active Directory 更新。

更新自行管理的 Active Directory 配置（控制台）

1. 打开 Amazon FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 导航到文件系统，然后选择要更新自行管理的 Active Directory 配置的 Windows 文件系统。
3. 然后在网络与安全选项卡中，根据要更新的 Active Directory 属性，为 DNS 服务器 IP 地址或服务账户用户名选择更新。
4. 在出现的对话框中，输入新的 DNS 服务器 IP 地址或新的服务账户凭证（用户名和密码）或密钥 ARN。您可以使用 Amazon Secrets Manager 来存储您的凭据。有关更多信息，请参阅 使用存储活动目录凭证 Amazon Secrets Manager。
5. 选择更新以启动 Active Directory 配置更新。

   您可以使用 Amazon Web Services 管理控制台 或监控更新进度 Amazon CLI。

更新自行管理的 Active Directory 配置（CLI）

- 要更新 FSx 适用于 Windows 文件服务器的文件系统的自行管理的 Active Directory 配置，请使用 Amazon CLI 命令update-file-system。设置以下参数：
  - `--file-system-id` 设置为要更新的文件系统的 ID。
  - `UserName` 自行管理的 Active Directory 服务账户的新用户名。
  - `Password` 自行管理的 Active Directory 服务账户的新密码。
  - `DomainJoinServiceAccountSecret`包含您的 Active Directory 域上服务帐户的用户名和密码的 Amazon Secrets Manager 密钥

    > **Note**
    >
    > 您不能同时提供两者 username/password 以及域名加入服务帐户密钥来连接您的 Active Directory。仅提供一组凭证。

  - `DnsIps` 自行管理的 Active Directory 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=[192.0.2.0,192.0.2.24]}'
```

如果此更新操作成功，则该服务将返回 HTTP 200 响应。响应中的 `AdminstrativeActions` 对象描述了请求及其状态。

更改 Amazon FSx 服务账户

如果您使用新服务账户更新文件系统，新服务账户必须拥有加入 Active Directory 的所需权限和特权，并对与文件系统关联的现有计算机对象拥有完全控制权限。此外，确保新的服务账户属于启用了组策略设置域控制器：允许在域加入期间重复使用计算机账户的受信任账户的一部分。

我们强烈建议使用 Active Directory 组管理与服务账户关联的 Active Directory 权限和配置。

更改 Amazon 的服务账户时 FSx，请确保服务账户具有以下设置：

- 新的服务账户（或其所属的 Active Directory 组）对与文件系统关联的现有计算机对象拥有完全控制权限。

- 新服务账户和以前的服务账户（或其所属的 Active Directory 组）是受信任账户（或受信任的 Active Directory 组）的一部分，并在 Active Directory 中的所有域控制器上启用了域控制器：允许在域加入期间重复使用计算机账户的组策略设置。

如果服务账户不满足这些要求，可能会出现以下情况：

- 对于单可用区文件系统，文件系统可能会变为 MISCONFIGURED_UNAVAILABLE。
- 对于多可用区文件系统，文件系统可能会配置错误，并且 RemotePowerShell 端点名称可能会更改。

配置域控制器的组策略

以下 Microsoft 推荐过程描述了如何使用域控制器组策略来配置允许列表策略。

配置域控制器的允许列表策略

1. 在自行管理的 Microsoft Active Directory 中的所有成员计算机和域控制器上安装 2023 年 9 月 12 日或之后版本的 Microsoft Windows 更新。
2. 在适用于自行管理的 Active Directory 中所有域控制器的新组策略或现有组策略中，配置以下设置。
   a. 导航到计算机配置 > 策略 > Windows 设置 > 安全设置 > 本地策略 > 安全选项。
   b. 双击域控制器：允许在域加入期间重复使用计算机账户。
   c. 选择定义此策略设置和 <编辑安全 ...>。
   d. 使用对象选择器将用户或受信任的计算机账户创建者和拥有者组添加至允许权限。（作为最佳实践，我们强烈建议使用群组获取权限。）请勿添加执行域加入的用户账户。

   > **Warning**
   > 将策略的成员资格限制为受信任用户和服务账户。请勿将经过身份验证的用户、所有人或其他大型群组添加至此策略。相反，应将特定的受信任用户和服务账户添加至群组，然后将这些群组添加至策略。

3. 在组策略刷新间隔内等待或在所有域控制器上运行 gpupdate /force。
4. 验证 HKLM\ System\ CCS\ Control\ SAM — “ComputerAccountReuseAllowList” 注册表项是否填充了所需的 SDDL。请勿手动编辑注册表。

5. 尝试加入一台安装了 2023 年 9 月 12 日或更高版本更新的计算机。确保策略中列出的其中一个账户拥有该计算机账户。还要确保其注册表未启用该NetJoinLegacyAccountReuse密钥（设置为 1）。如果域加入失败，请查看 **`c:\windows\debug\netsetup.log`**。

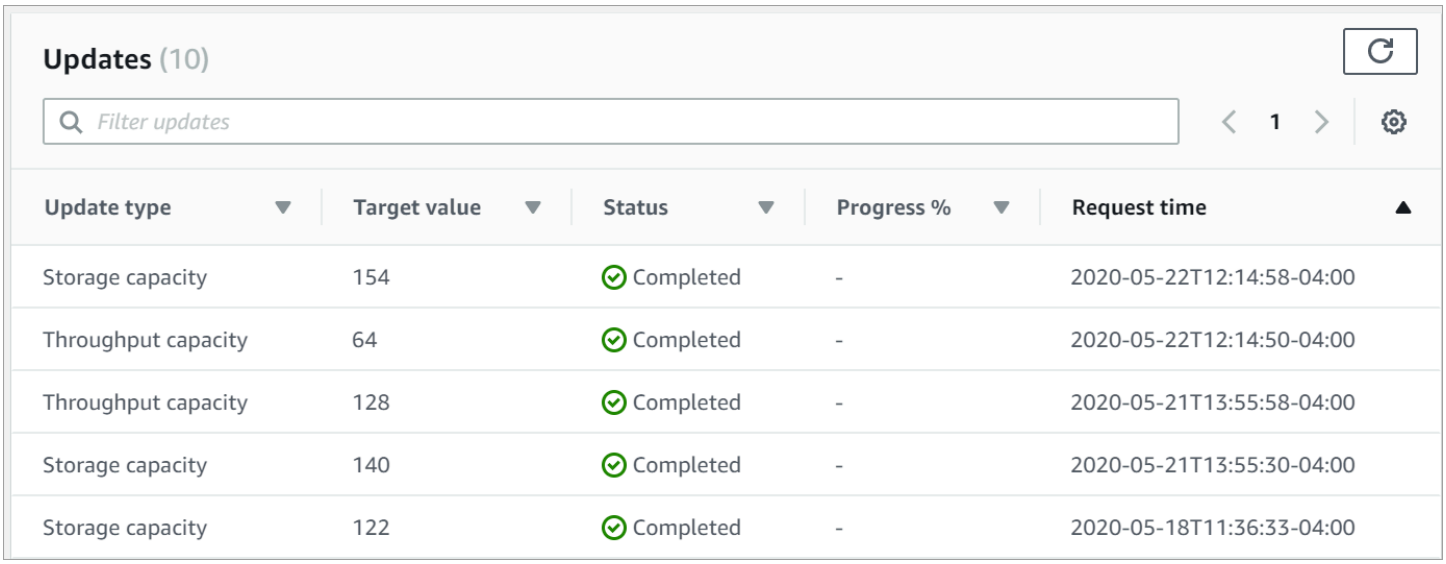
监控自行管理的 Active Directory 更新

您可以使用 Amazon Web Services 管理控制台、API 或监控自行管理的 Active Directory 配置更新的进度 Amazon CLI，如以下过程所述。

更新文件系统的自行管理的 Active Directory 配置时，在应用更新时，文件系统的状态会从可用切换为正在更新。更新完成后，状态将切换回可用。Active Directory 配置更新可能需要几分钟才能完成。

在控制台中监控更新

在文件系统详细信息窗口的更新选项卡中，您可以查看每种更新类型的 10 个最近更新。



对于自行管理的 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
- 服务账户凭证

目标值

要将文件系统属性更新到的所需值。对于服务账户凭证更新，仅显示用户名，此字段中从不包含服务账户密码。

状态

当前更新状态。对于自行管理的 Active Directory 更新，可能的值如下所示：

- 待处理 — Amazon FSx 已收到更新请求，但尚未开始处理。
- 处理@@ 中 — Amazon FSx 正在处理更新请求。
- 已完成 – 文件系统更新成功完成。
- 失败 – 文件系统更新失败。选择问号（？）可查看失败的详细信息。

进度百分比

以完成百分比的形式显示文件系统更新的进度。

请求时间

Amazon FSx 收到更新操作请求的时间。

使用 Amazon CLI 和 API 监控更新

您可以使用describe-file-systems Amazon CLI 命令和 DescribeFileSystemsAPI 操作查看和监控正在进行的文件系统更新请求。`AdministrativeActions` 数组列出每种管理操作类型的 10 个最近更新操作。

以下示例显示了 CLI 命令 describe-file-systems 的响应摘录。输出显示了两个自我管理的 Active Directory 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."
                }
            }
        ],
    .
    .
    .
```

FSx for Windows File Server 性能

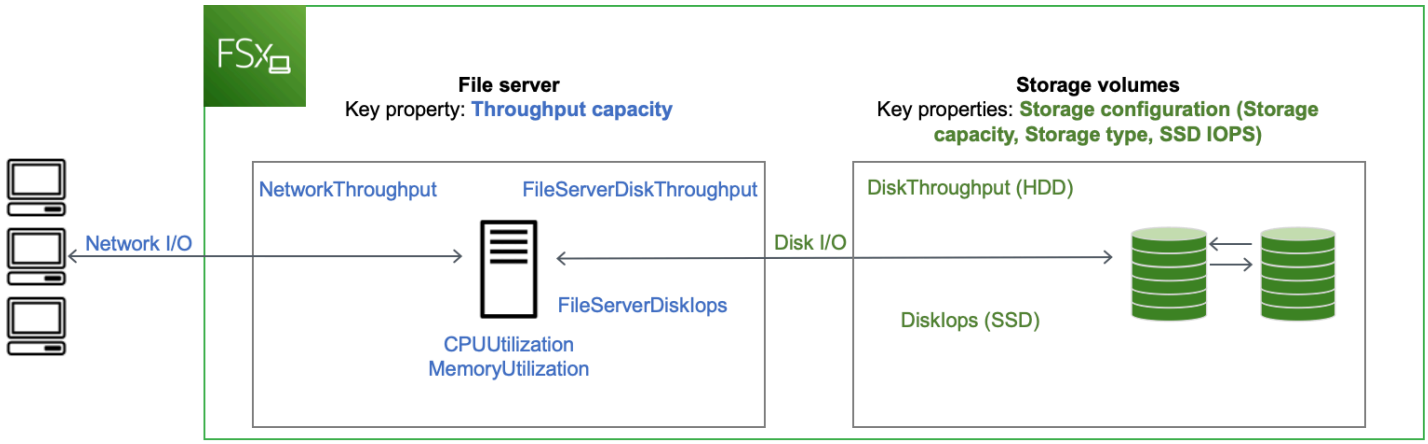
FSx for Windows File Server 提供文件系统配置选项以满足各种性能需求。以下是关于 Amazon FSx 文件系统性能的概述，以及关于可用性能配置选项和有用的性能提示的讨论。

主题

文件系统性能

每个 FSx for Windows File Server 文件系统都由与客户机通信的 Windows 文件服务器和一组附加到文件服务器的存储卷或磁盘组成。每台文件服务器都使用快速内存缓存来增强最常访问数据的性能。

下图说明了如何从 FSx for Windows File Server 文件系统访问数据。



当客户端访问存储在内存缓存中的数据时，这些数据将作为网络 I/O 直接提供给发出请求的客户端。文件服务器无需从磁盘读取或写入磁盘。这种数据访问的性能取决于网络 I/O 限制和内存缓存的大小。

当客户端访问不在缓存中的数据时，文件服务器会将其作为磁盘 I/O 从磁盘读取或写入磁盘。然后，数据作为网络 I/O 从文件服务器提供给客户端。这种数据访问的性能由网络 I/O 限制和磁盘 I/O 限制决定。

网络 I/O 性能和文件服务器内存缓存由文件系统的吞吐能力决定。磁盘 I/O 性能由吞吐能力和存储配置组合决定。您的文件系统可以达到的最大磁盘 I/O 性能（包括磁盘吞吐量和磁盘 IOPS 级别）是以下两者中较低的一方：

- 文件服务器提供的磁盘 I/O 性能级别，基于您为文件系统选择的吞吐能力。
- 您的存储配置提供的磁盘 I/O 性能级别（存储容量、存储类型和您为文件系统选择的 SSD IOPS 级别）。

其他性能注意事项

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

延迟

FSx for Windows File Server 文件服务器采用快速的内存缓存，为经常访问的数据实现稳定的亚毫秒级延迟。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 来处理的文件操作，Amazon FSx 的固态硬盘（SSD）存储提供亚毫秒级的文件操作延迟，硬盘驱动器（HDD）存储提供个位数毫秒延迟。

吞吐量和 IOPS

Amazon FSx 文件系统在所有 Amazon FSx 可用的 Amazon Web Services 区域 中提供最高 2Gbps 吞吐量和 80000IOPS，在美国东部（弗吉尼亚州北部）、美国西部（俄勒冈州）、美国东部（俄亥俄州）、欧洲地区（爱尔兰）、亚太地区（东京）和亚太地区（新加坡）提供 12Gbps 吞吐量和 400000IOPS。您的工作负载可以在文件系统上驱动的具体吞吐量和 IOPS 数取决于文件系统的吞吐能力、存储容量和存储类型，以及工作负载的性质，包括活动工作集的大小。

单客户端性能

借助 Amazon FSx，您可以通过单个客户端访问文件系统，从而获得完整的吞吐量和 IOPS 级别。Amazon FSx 支持 SMB 多通道。此功能使 Amazon FSx 能够为访问文件系统的单个客户端提供多 GBps 吞吐量和数十万 IOPS。SMB 多通道会在客户端和服务器之间同时使用多个网络连接，以此来聚合网络带宽，从而最大化利用率。尽管 Windows 支持的 SMB 连接次数存在理论限制，但该限制是百万级的，实际上您可以拥有无限的 SMB 连接次数。

突增性能

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

吞吐能力对性能的影响

吞吐能力决定以下几类文件系统的性能：

- 网络 I/O – 文件服务器向访问文件的客户端提供文件数据的速度。
- 文件服务器 CPU 和内存 – 可用于提供文件数据和执行重复数据删除和影子副本等后台活动的资源。
- 磁盘 I/O – 文件服务器支持文件服务器和存储卷之间的 I/O 的速度。

下表详细介绍了每个预置吞吐能力配置可以驱动的最大级别网络 I/O（吞吐量和 IOPS）和磁盘 I/O（吞吐量和 IOPS），以及可用于缓存和支持重复数据删除和影子副本等后台活动的内存量。虽然在使用 Amazon FSx API 或 CLI 时，您可以选择低于每秒 32 兆比特（MBps）的吞吐能力级别，但请记住，这种级别适用于测试和开发工作负载，而非生产工作负载。

> **Note**
>
> 请注意，仅以下区域支持 4,608 MBps 及以上级别吞吐能力：美国东部（弗吉尼亚州北部）、美国西部（俄勒冈州）、美国东部（俄亥俄州）、欧洲地区（爱尔兰）、亚太地区（东京）和亚太地区（新加坡）。

网络 I/O 和内存

FSx 吞吐能力（MBps）	网络吞吐量（MBp）		网络 IOPS	内存（GB）
	基准	突增（每天几分钟）		
32	32	600	千	4

FSx 吞吐能力（MBps）	网络吞吐量（MBp）		网络 IOPS	内存（GB）
64	64	600	数万	8
128	150	1,250		8
256	300	1,250	数十万	16
512	600	1,250		32
1024	1,500	–		72
2048	3,125	–		144
4608	9,375	–	数百万	192
6144	12,500	–		256
9216	18,750	–		384
12288	21,250	–		512

磁盘 I/O

FSx 吞吐能力（MBps）	磁盘吞吐量（MBps）		磁盘 IOPS	
	基准	突增（每天 30 分钟）	基准	突增（每天 30 分钟）
32	32	260	2K	12K
64	64	350	4K	16K
128	128	600	6K	20K
256	256	600	10K	20K
512	512	–	20K	–

FSx 吞吐能力（MBps）	磁盘吞吐量（MBps）		磁盘 IOPS	
1024	1,024	–	40K	–
2048	2,048	–	80K	–
4608	4,608	–	150K	–
6144	6,144	–	200K	–
9216	9,216[1]	–	300K[1]	–
12288	12,288[1]	–	400K[1]	–

> **Note**
>
> [1]如果您的多可用区文件系统吞吐能力为 9,216 或 12,288 MBps，则仅写入流量的性能将限制在 9,000 MBps 和 262,500 IOPS 以内。否则，对于所有多可用区文件系统的读取流量、所有单可用区文件系统的读取和写入流量以及所有其他吞吐能力级别，您的文件系统将支持表中所示的性能限制。

选择正确的吞吐能力级别

当您使用 Amazon Web Services Management Console 创建文件系统时，Amazon FSx 会根据您配置的存储容量自动为您的文件系统选择推荐的吞吐能力级别。虽然推荐的吞吐能力应该足以满足大多数工作负载，但您可以选择覆盖建议，并配置特定的吞吐能力，以满足工作负载的需求。例如，如果您的工作负载需要将 1GBps 的流量驱动至文件系统，则应选择至少 1024MBps 的吞吐能力。下表基于预配置的存储容量，提供文件系统的最低推荐吞吐能力级别。

SSD 存储容量（GiB）	HDD 存储容量（GiB）	最低推荐吞吐能力（Mbps）
最多 640	最多 3200	32
641 至 1280	3201 至 6400	64
1281 至 2560	6401 至 12800	128

SSD 存储容量（GiB）	HDD 存储容量（GiB）	最低推荐吞吐能力（Mbps）
2561 至 5120	12801 至 25600	256
5121 至 10240	25601 至 51200	512
10241 至 20480	>51200	1024
>20480	NA	2048

在决定要配置的吞吐量级别时，还应考虑计划在文件系统上启用的功能。例如，启用影子副本可能需要将吞吐能力提高至预期工作负载的三倍，以确保文件服务器能够在可用的 I/O 性能容量下维护影子副本。如果您启用了重复数据删除，则应确定与文件系统的吞吐能力关联的内存量，并确保该内存量足以容纳您的数据大小。

创建吞吐能力后，您可以随时上调或下调其数量。有关更多信息，请参阅 管理吞吐能力。

您可以通过查看 Amazon FSx 控制台的监控和性能 > 性能选项卡，监控工作负载对文件服务器性能资源的利用率，并获得有关选择哪种吞吐能力的建议。我们建议在预生产环境中进行测试，以确保您选择的配置符合工作负载的性能要求。对于多可用区文件系统，我们还建议您测试在文件系统维护、吞吐能力更改和计划外服务中断期间发生的失效转移进程对工作负载的影响，并确保您已预置足够的吞吐能力以防止在这些事件期间对性能造成影响。有关更多信息，请参阅 访问文件系统指标。

存储配置对性能的影响

文件系统的存储容量、存储类型和 SSD IOPS 级别都会影响文件系统的磁盘 I/O 性能。您可以配置这些资源，以便为您的工作负载提供所需的性能级别。

您可以随时增加存储容量和扩展 SSD IOPS。有关更多信息，请参阅 管理存储容量 和 管理 SSD IOPS。您也可以将文件系统从 HDD 存储类型升级到 SSD 存储类型。有关更多信息，请参阅 管理文件系统存储类型。

您的文件系统提供以下默认级别的磁盘吞吐量和 IOPS：

存储类型	磁盘吞吐量 [每 TiB 存储速率（MBps）]	磁盘 IOPS（存储的每 TiB）
SSD	750	3000[1]

存储类型	磁盘吞吐量 [每 TiB 存储速率（MBps）]	磁盘 IOPS（存储的每 TiB）
HDD	基准 12；突增 80（每个文件系统最多 1Gbps）	基准 12；突增 80

> **Note**
>
> [1]对于采用 SSD 存储类型的文件系统，您可以预置额外的 IOPS，最大比例 500 IOPS/GiB 存储，400,000 IOPS/文件系统。

HDD 突增性能

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

HDD 存储卷的可用吞吐量由以下公式表示：

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

对于 1TiB HDD 卷，突增吞吐量限制为 80MiBps，存储桶以 12MiBps 的速度填充，最多可容纳 1TiB 积分。

根据工作负载，HDD 存储卷可能会出现显著的性能差异。IOPS 或吞吐量突然激增可能导致磁盘性能下降。`DiskThroughputBalance` 指标提供有关磁盘吞吐量和磁盘 IOPS 利用率的突增积分余额的信息。例如，如果工作负载超过了基准 HDD IOPS 限制（每 TiB 存储 12 次 IOPS），则磁盘 IOPS 利用率（HDD）将高于 100%，这会导致突增积分余额耗尽，如 `DiskThroughputBalance` 指标所示。为了让工作负载继续推动高水平的 I/O，您可能需要执行以下操作之一：

- 减小工作负载的 I/O 需求，以便补充突增积分余额。
- 增加文件系统的存储容量，提供更高基准水平的磁盘 IOPS。
- 升级文件系统以使用 SSD 存储，提供更高基准水平的磁盘 IOPS，以便更好地匹配工作负载的要求。

示例：存储容量和吞吐能力

以下示例说明了存储容量和吞吐能力对文件系统性能的影响。

配置有 2 TiB HDD 存储容量和 32 MBps 吞吐能力的文件系统具有以下吞吐量级别：

- 网络吞吐量 – 基准 32 MBps 和突增 600 MBps（参阅吞吐能力表）
- 磁盘吞吐量 – 基准 24 MBps 和突增 160 MBps，这是以下两者中较低的一个：
  - 基于文件系统的吞吐能力，文件服务器支持的磁盘吞吐量级别为 32 Mbps 基准和 260 Mbps 突增
  - 根据存储类型和容量，存储卷支持的磁盘吞吐量水平为 24 Mbps（12 MBps/TB * 2 TiB）基准和 160 Mbps 突增（80 MBps/TiB * 2 TiB）

因此，访问文件系统的工作负载将能够提供高达 32 MBps 的基准吞吐量和 600 MBps 的突增吞吐量，用于对缓存在文件服务器内存缓存中经常访问的数据执行文件操作，以及高达 24 MBps 的基准吞吐量和 160 MBps 的突增吞吐量，用于由于缓存未命中而需要对整个磁盘执行的文件操作。

使用 CloudWatch 指标衡量性能

您可以使用 Amazon CloudWatch 来衡量和监控文件系统的吞吐量以及 IOPS。有关更多信息，请参阅使用 Amazon CloudWatch 监控。

文件系统性能问题排查

FSx for Windows File Server 文件系统的性能取决于多个因素，包括推送到文件系统的流量、文件系统的配置方式以及由启用的功能消耗的资源，例如重复数据删除或影子副本。有关了解文件系统性能的更多信息，请参阅 FSx for Windows File Server 性能。

主题

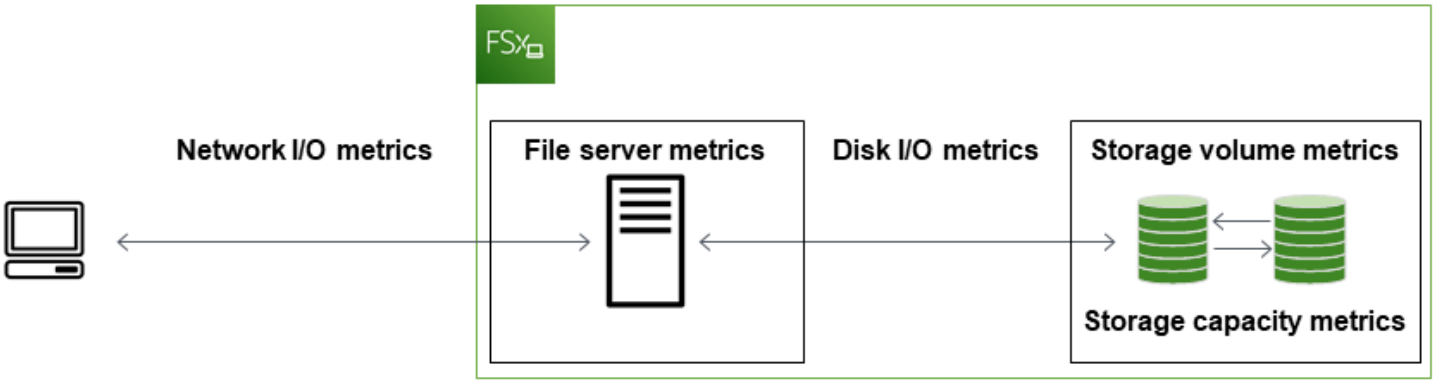
- 如何确定我的文件系统的吞吐量和 IOPS 限制？
- 网络 I/O 和磁盘 I/O 有什么区别？ 为什么我的网络 I/O 与磁盘 I/O 不同？
- 为什么即使我的网络 I/O 很低，CPU 或内存利用率仍然很高？
- 什么是突增？ 我的文件系统使用了多少突增？ 突增点数用完时会发生什么？
- 我在监控和性能页面上看到一条警告，我需要更改文件系统的配置吗？
- 我的指标暂时丢失，我应该担心吗？

如何确定我的文件系统的吞吐量和 IOPS 限制？

要查看文件系统的吞吐量和 IOPS 限制，请根据预置吞吐能力参阅性能水平表。

网络 I/O 和磁盘 I/O 有什么区别？为什么我的网络 I/O 与磁盘 I/O 不同？

Amazon FSx 文件系统包括一个或多个文件服务器，这些服务器通过网络向访问文件系统的客户端提供数据。这是网络 I/O。文件服务器使用快速内存缓存来增强最常访问数据的性能。文件服务器还会将流量推送到托管文件系统数据的存储卷。这是磁盘 I/O。下图阐明了 Amazon FSx 文件系统的网络和磁盘 I/O。



有关更多信息，请参阅 使用 Amazon CloudWatch 监控。

为什么即使我的网络 I/O 很低，CPU 或内存利用率仍然很高？

文件服务器 CPU 和内存利用率不仅取决于您推送的网络流量，还取决于您在文件系统上启用的功能。如何配置和计划这些功能可能会影响 CPU 和内存利用率。

正在进行的重复数据删除作业可能会消耗内存。您可以修改重复数据删除作业的配置，以降低内存需求。例如，您可以将优化限制为针对特定文件类型或文件夹运行，或者设置优化的最小文件大小和期限。我们还建议将重复数据删除作业配置为在文件系统负载最小的空闲期间运行。有关更多信息，请参阅 通过重复数据删除来降低存储成本。

如果您启用了基于访问权限的枚举，则可能会在最终用户查看或列出文件共享时，或者在存储扩展作业的优化阶段，看到 CPU 利用率很高。有关更多信息，请参阅《Microsoft 存储文档》中的对命名空间启用基于访问的枚举。

什么是突增？我的文件系统使用了多少突增？突增点数用完时会发生什么？

基于文件的工作负载通常处于尖峰状态，其特点是短暂而密集的高 I/O 周期，且两次突增之间有空闲时间。为了支持这些工作负载类型，除了文件系统可以维持的基准速度外，Amazon FSx 还提供在一段时间内突增至更高速度的功能，用于网络 I/O 和磁盘 I/O 操作。

Amazon FSx 会使用 I/O 点数机制，根据平均利用率分配吞吐量和 IOPS，即当文件系统的吞吐量和 IOPS 用量低于其基准限制时，文件系统会累积点数，然后可以在必要时对超过基准限制的突增（最高至突增限制）时使用这些点数。有关文件系统的突增限制和持续时间的更多信息，请参阅 FSx for Windows File Server 性能。

我在监控和性能页面上看到一条警告，我需要更改文件系统的配置吗？

监控和性能页面出现警告，指明最近的工作负载需求何时接近或超过资源限制，具体取决于您的文件系统配置方式。这并不一定意味着您需要更改配置，但如果不采取建议的措施，您的文件系统可能无法满足您的工作负载需求。

如果导致警告的工作负载并不典型，并且您预计它不会持续，那么不采取任何措施但同时密切监控未来的利用率可能是安全的。但是，如果导致警告的工作负载是典型工作负载，并且您预计它会持续甚至加剧，我们建议您按照建议的操作来提高文件服务器性能（通过增加吞吐能力）或提高存储卷性能（通过增加存储容量或从 HDD 切换到 SSD 存储）。

> **Note**
>
> 某些文件系统事件可能会消耗磁盘 I/O 性能资源，并可能触发性能警告。例如：
>
> - 存储容量扩展的优化阶段会增加磁盘吞吐量，如 增加存储容量并提升文件系统性能 中所述
> - 对于多可用区文件系统，吞吐能力扩展、硬件更换或可用区中断等事件会导致自动失效转移和失效自动恢复事件。在此期间发生的任何数据更改都需要在主文件服务器和辅助文件服务器之间进行同步，Windows Server 运行的数据同步作业可能会消耗磁盘 I/O 资源。有关更多信息，请参阅 管理吞吐能力。

我的指标暂时丢失，我应该担心吗？

在文件系统维护、基础设施组件更换以及可用区不可用时，单可用区文件系统会出现不可用情况。在这段时间内，指标将不可用。

在多可用区部署中，Amazon FSx 会自动在不同可用区中配置和维护一个备用文件服务器。如果文件系统维护或计划外服务中断，Amazon FSx 通常会自动失效转移到备用文件服务器，让您无需人工干预即可继续访问数据。在您的文件系统进行失效转移和失效自动恢复的短时间内，指标可能暂时不可用。

FSx 为 Windows 文件系统进行管理

Amazon FSx 提供多种管理功能，可帮助您轻松管理和扩展 Amazon FSx for Windows 文件服务器文件系统，以满足不断变化的工作负载和用户要求以及组织的监管和合规需求。以下是您可以使用 Amazon CLI 和 API Amazon Web Services 管理控制台、用于远程管理的 Amazon FSx CLI 和原生 Microsoft Windows Server 图形界面 PowerShell管理的一些文件系统配置的列表。

- 存储容量
- 存储类型
- SSD IOPS
- 吞吐能力
- DNS 别名
- 重复数据删除
- 影子副本
- 存储配额
- 文件访问审计
- 文件共享

以下部分介绍了您可用的文件系统管理功能和设置。我们提供了指南来帮助确定最适合您情况的具体选项，并提供了适用的最佳实践。

主题

- 管理 FSx for Windows File Server 上的存储
- 使用 DFS 命名空间
- 管理吞吐能力
- 管理网络类型
- 为 Amazon FSx 资源贴标签
- 使用 Amazon CLI 更新文件系统

Amazon FSx 文件系统状态

您可以使用亚马逊 FSx 控制台、 Amazon CLI 命令describe-file-systems或 API 操作查看亚马逊 FSx 文件系统的状态DescribeFileSystems。

文件系统状态	说明
AVAILABLE	文件系统处于正常状态，可以访问并可供使用。
CREATING	亚马逊 FSx 正在创建一个新的文件系统。
DELETING	亚马逊 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。
MISCONFIGURED	由于您的 Active Directory 环境发生了变化，文件系统处于受损状态。当前您的文件系统不可用，或者有失去可用性的风险，并且有可能会备份失败。有关恢复可用性的更多信息，请参阅文件系统处于配置错误状态。
MISCONFIGURED_UNAVAILABLE	由于您的 Active Directory 环境发生了变化，文件系统当前不可用。有关恢复可用性的更多信息，请参阅文件系统处于配置错误状态。
FAILED	• 在创建新文件系统时 FSx ，Amazon 无法创建新的文件系统。 • 文件系统不可用。 • 文件系统出现故障，Amazon FSx 无法恢复。

文件系统状态	说明
	• FSx Amazon 无法创建备份。

将 Amazon FSx CLI 用于 PowerShell

本章介绍如何访问 Amazon FSx CLI 进行远程管理 PowerShell ，从而为 FSx Windows 文件系统执行文件系统管理任务。您也可以使用 Microsoft Windows 原生图形用户界面（ GUI ）来执行部分管理任务。

上用于远程管理的 Amazon FSx CLI PowerShell 允许文件系统管理员组中的用户管理文件系统。要在 Windows File Server 文件系统上启动远程 PowerShell 会话，首先需要满足以下先决条件： FSx

- 能够连接到与您的 for Windows 文件服务器文件系统具有网络连接 FSx 的 Windows 计算实例。
- 以文件系统管理员组成员的身份登录 Windows 计算实例。如果您使用 Amazon Managed Microsoft AD的是 “Amazon 委派 FSx管理员” 组。如果您使用的是自行管理的 Microsoft Active Directory，这是域管理员组或您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 使用自行管理 Active Directory 时的最佳实践。
- 文件系统的 VPC 安全组入站规则允许端口 5985 上的流量。

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

- 使用 Kerberos 身份验证对用户凭证进行身份验证。
- 使用 Kerberos 对连接的客户端和文件系统之间的管理会话通信进行加密。

您可以通过两种方式在 Amazon FSx 文件系统上运行远程管理 CLI 命令：

- 您可以建立长时间运行的远程 PowerShell 会话并在会话中运行命令。
- 您可以使用`Invoke-Command`来运行单个命令或单个命令块，而无需建立长时间运行的远程 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，您只能在文件系统使用其首选文件服务器时使用 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。

您需要使用文件系统的 Windows 远程 PowerShell 端点才能访问远程服务器 PowerShell。例如，远程管理端点采用 `amznfsxctlyaa1k.`*`ActiveDirectory-DNS-name`* 格式，比如 `amznfsxctlyaa1k.corp.example.com`。您可以使用网络和安全选项卡上文件系统详细信息页面 Amazon Web Services 管理控制台 中的来查找端点名称。使用 Amazon CLI `describe-file-systems`命令查看响应中返回的`RemoteAdministrationEndpoint`属性。

您可以使用 `Get-Command` cmdlet 检索有关中可用的 cmdlet、函数和别名的信息。 PowerShell有关更多信息，请参阅 Microsoft Get-Command 文档。

您也可以使用 FSx c `Invoke-Command` mdlet 对文件系统上的 PowerShell 命令运行 Amazon CLI 进行远程管理 CLI，使用以下语法：

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName
 amznfsxctlyaa1k.corp.example.com -ConfigurationName FSxRemoteAdmin -scriptblock { fsx-
command}
```

有关如何在 for Windows 文件服务器文件系统上启动长寿命远程 PowerShell 会话 FSx 的说明，请参阅 启动 Amazon FSx 远程 PowerShell 会话

启动 Amazon FSx 远程 PowerShell 会话

本主题提供有关在 Windows 文件服务器文件服务器上启动长期远程 PowerShell 会话 FSx 的说明。

在您的文件系统上启动远程 PowerShell 会话

1. 作为您在创建文件系统时选择的委派 FSx 管理员组成员的用户，连接到与您的文件系统具有网络连接的计算实例。
2. 在计算实例上 PowerShell 打开 Windows 窗口。
3. 在中 PowerShell，输入以下命令以在您的 Amazon FSx 文件系统上打开一个长期存在的远程会话。*`Remote-PowerShell-Endpoint`*替换为要管理的文件系统的 Windows 远程 PowerShell 端点。使用 `FsxRemoteAdmin` 作为会话配置名称。

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

如果您的实例不是 Amazon Act FSx ive Directory 域的一部分，则系统会在弹出窗口中提示您输入用户证书。输入作为 FSx 管理员组成员的用户的凭据。如果您的实例已加入域，则系统将不会要求您提供凭证。

> **Important**
>
> 如果您使用的是自行管理的 Active Directory 配置，并且在没有正确的 Active Directory 组策略设置的情况下更改服务帐户，Windows Remote PowerShell 端点可能会发生变化。有关更多信息，请参阅 更改 Amazon FSx 服务账户 了解更多详情。

使用 Amazon FSx CLI 进行远程管理的一次性文件系统设置任务 PowerShell

在 PowerShell命令上使用以下 Amazon FSx CLI 进行远程管理，按照我们的最佳实践快速实施文件系统管理任务。

管理存储消耗量

使用以下命令来管理文件系统的存储消耗量。

- 要按默认计划开启重复数据删除，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对文件执行重复数据删除操作，无需任何最短文件期限。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FSxDedupConfiguration -MinimumFileAgeDays 0 }
```

有关更多信息，请参阅 通过重复数据删除来降低存储成本。

- 使用以下命令开启“跟踪”模式下的用户存储限额，该模式仅用于报告目的，不用于强制执行。

```
$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 管理存储配额。

启用影子副本，使最终用户能够将文件和文件夹恢复到以前的版本

按照默认时间表（工作日上午 7 点和中午 12 点）开启影子副本，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 配置影子副本使用默认存储和计划。

在传输过程中强制加密

以下命令对连接到您的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，并强制当前连接的客户端使用加密重新连接。

```
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和用户会话和打开的文件。

对访问 Amazon FSx CLI 进行故障排除 PowerShell

导致无法使用 Remote 连接到文件系统的潜在原因有很多 PowerShell，每种原因都有自己的分辨率，如下所示。

要首先确保您可以成功连接到 Windows 远程 PowerShell 端点，还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 PowerShell 连接所需的入站规则

文件系统的安全组必须有允许端口 5985 上流量的入站规则，才能建立远程 PowerShell 会话。有关更多信息，请参阅 Amazon VPC 安全组。

你在 Amazon 托管的 Microsoft 活动目录和你的本地活动目录之间配置了外部信任

要使用 PowerShell 带有 Kerberos 身份验证的 Amazon FSx Remote，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 Configure Kerberos Forest Search Order（KFSO）。

尝试启动远程会 PowerShell 话时出现语言本地化错误

您需要在 `-SessionOption (New-PSSessionOption -uiCulture "en-US")` 命令中添加以下命令：`-SessionOption`

以下是在文件系统上启动远程会 PowerShell 话`-SessionOption`时使用的两个示例。

```
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")
```

文件系统维护时段

亚马逊 FSx 版 Windows 文件服务器对其管理的微软 Windows Server 软件执行例行软件修补。维护时段指定此维护流程开始的具体日期和时间。您可以在创建文件系统期间指定维护时段的开始时间。如果

您未指定时间，系统会默认分配 30 分钟的维护开始时段。维护时段的持续时间取决于多个因素，包括维护范围，以及在多可用区文件系统中，将主从服务器之间维护期间发生的任何文件读写活动进行同步的过程。有关更多信息，请参阅 故障转移过程。

FSx for Windows File Server 允许您调整维护时段的开始时间以适应您的工作负载和操作要求。您可以根据需要频繁更改维护时段的开始时间，但至少每 14 天安排一次维护时段开始时间。如果已发布补丁但您尚未在 14 天内安排维护窗口， FSx 则 Windows File Server 会继续维护文件系统，以确保其安全性和可靠性。有关如何调整文件系统维护时段开始时间的更多信息，请参阅 更改每周维护时段。

在修补过程中，您的单可用区文件系统将变为不可用状态，该状态通常会持续 20 分钟。多可用区文件系统会保持可用状态，并自动在首选和备用文件服务器之间进行失效转移和失效自动恢复。有关更多信息，请参阅 故障转移过程。由于多可用区文件系统的修补会引起文件服务器之间的失效转移和失效自动恢复，因此在此期间，必须在首选文件服务器和备用文件服务器之间同步发生的任何文件读写操作。为了缩短修补时间，我们建议将维护时段安排在文件系统负载最小的空闲时段。

> **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所有待处理写入操作。

更改每周维护时段

FSx for Windows File Server 允许您调整文件系统的维护时段何时开始，以适应您的工作负载和操作要求。您可以使用 Amazon Web Services 管理控制台 Amazon CLI、和 Amazon FSx API 更改每周维护时段的开始时间，如以下过程所述。

更改每周维护时段的开始时间（控制台）

1. 打开 Amazon FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 在左侧导航栏中选择文件系统。
3. 选择要更改每周维护时段的文件系统。随即显示文件系统详细信息页面。
4. 选择管理，会显示文件系统管理设置面板。
5. 选择更新，会显示更改维护时段窗口。
6. 输入您希望每周维护时段开始的新日期和时间。
7. 选择保存以保存您的更改。设置面板中将显示新的维护开始时间。

要使用 update-file-systemCLI 命令更改每周维护窗口的开始时间，请参见使用 Amazon CLI 更新文件系统。

管理 DNS 别名

除了 Amazon FSx 提供的默认域名系统 (DNS) 名称外，您还可以将自己选择的 DNS 别名与您的文件系统相关联。使用 DNS 别名，在将文件系统存储从本地迁移到亚马逊 FSx 时，您可以继续使用现有 DNS 名称访问存储在 Amazon 上的数据 FSx，而无需更新任何工具或应用程序。

您可以将 DNS 别名与 Windows 文件服务器文件系统的新别名和现有 FSx 别名关联，也可以在将备份还原到新文件系统时，使用 Amazon Web Services 管理控制台 和 Amazon CLI进行关联。每次最多可以将 50 个 DNS 别名与一个文件系统关联。

> **Note**
>
> 美国东部时间 2020 年 11 月 9 日 FSx 中午 12:00 之后创建的 Windows 文件服务器文件系统支持 DNS 别名。若要在美国东部时间 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，请执行如下操作：
>
> 1. 备份现有文件系统。有关更多信息，请参阅 使用用户启动备份。
> 2. 将备份恢复到新的文件系统。有关更多信息，请参阅 将备份还原至新文件系统。
>
> 新文件系统可用后，您将能够根据本节中提供的信息使用 DNS 别名访问该文件系统。

> **Note**
>
> 此处提供的信息假设您完全在 Active Directory 内进行工作，并且您没有使用外部 DNS 提供商。第三方 DNS 提供商可能会导致意外行为。
> FSx 只有当你加入的活动目录域使用微软 DNS 作为默认 DNS 时，亚马逊才会注册文件系统的 DNS 记录。如果您使用的是第三方 DNS，则需要在创建 FSx 文件系统后手动设置 Amazon 文件系统的 DNS 条目。有关为文件系统选择正确 IP 地址的更多信息，请参阅获取用于手动 DNS 条目的正确文件系统 IP 地址。

在创建新文件系统时，以及通过备份创建新文件系统时，可以将 DNS 别名与 Windows 文件服务器文件系统的现有 FSx 别名相关联。每次最多可以将 50 个 DNS 别名与一个文件系统关联。

除了将 DNS 别名关联到文件系统外，客户端要使用 DNS 别名连接到文件系统，您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 (SPNs)。
- 为解析为亚马逊 FSx 文件系统的默认 DNS 名称的 DNS 别名配置 DNS 别名记录。

有关更多信息，请参阅 使用 DNS 别名访问数据。

您的 Windows 文件服务器文件系统 FSx 的 DNS 别名需要满足以下要求：

- 必须采用完全限定域名（FQDN）格式。
- 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 会将字母字符 FSx 存储为小写字母 (a-z)，无论您如何指定它们：大写字母、小写字母或转义码中的相应字母。

若您尝试关联已与文件系统关联的别名，则操作无效。如果您尝试取消别名与文件系统无关的文件系统的关联，Amazon 会以错误的请求错误 FSx 做出响应。

> **Note**
>
> 当 Amazon 在文件系统上 FSx 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 non-Continuously-Available（非 CA）共享的客户端打开的所有文件都必须由客户端重新打开。

主题

DNS 别名状态

DNS 别名可以具有以下某个状态值：

- 可用-DNS 别名与 Amazon FSx 文件系统相关联。
- 创建 — Amazon FSx 正在创建 DNS 别名并将其与文件系统关联。
- 正在删除 — 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。

Kerberos 身份验证使用 DNS 别名

我们建议您在通过 Amazon 传输时使用基于 Kerberos 的身份验证和加密。 FSxKerberos 能够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，您必须配置与文件系统 Active Directory 计算机对象上的 DNS 别名相对应的服务主体名称 (SPNs)。

如果您已在 A SPNs ctive Directory 中的计算机对象上配置了分配给另一个文件系统的 DNS 别名，则必须先将其删除， SPNs 然后才能将其 SPNs 添加到文件系统的计算机对象中。有关更多信息，请参阅 为 Kerberos 配置服务主体名称（SPN）。

查看与文件系统和备份的 DNS 别名

您可以使用 Amazon Web Services 管理控制台、和 API 查看当前与您 FSx 的 for Windows 文件服务器文件系统关联的 DNS 别名和备份，如以下过程所述。 Amazon CLI

查看与文件系统关联的 DNS 别名

- 使用控制台 – 选择一个文件系统，查看文件系统详细信息页面。选择网络与安全选项卡，查看 DNS 别名。
- 使用 CLI 或 API-使用 `describe-file-system-aliases` CLI 命令或 DescribeFileSystemAliasesAPI 操作。

查看与备份关联的 DNS 别名

- 使用控制台 – 在导航窗格中，选择备份，然后选择您要查看的备份。在摘要窗格中，查看 DNS 别名字段。

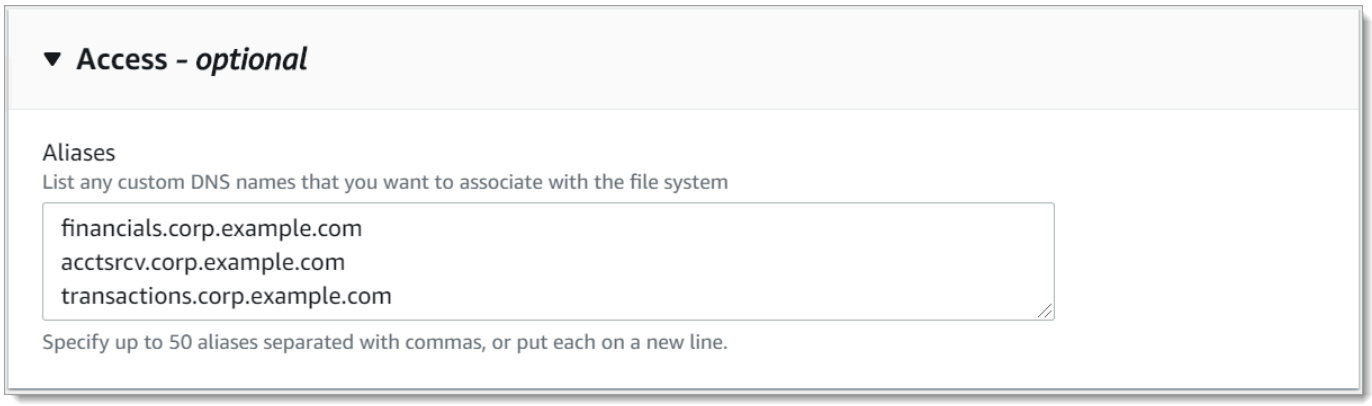
- 使用 CLI 或 API-使用 `describe-backups` CLI 命令或 DescribeBackupsAPI 操作。

将 DNS 别名与文件系统相关联

在从头开始 FSx 为 Windows 文件服务器创建新的文件系统或将备份恢复到新文件系统时，可以使用、和 API 关联 DNS 别名 Amazon Web Services 管理控制台 Amazon CLI，如以下过程所述。

在创建新的文件系统时关联 DNS 别名（控制台）

1. 打开 Amazon FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 按照“入门”部分的步骤 5。创建文件系统中所述的步骤创建新文件系统。
3. 在创建文件系统向导的访问 – 可选部分，输入要与文件系统关联的 DNS 别名。



4. 当文件系统可用时，您可以使用 DNS 别名访问该文件系统，方法是配置服务主体名称 (SPNs)，并为该别名更新或创建 DNS CNAME 记录。有关更多信息，请参阅 使用 DNS 别名访问数据。

在创建新的亚马逊 FSx 文件系统 (CLI) 时关联 DNS 别名

1. 创建新文件系统时，使用带有 CreateFileSystemAPI 操作的 Ali as 属性将 DNS 别名与新文件系统相关联。

```
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. 当文件系统可用时，您可以使用 DNS 别名访问该文件系统，方法是配置服务主体名称 (SPNs)，并为该别名更新或创建 DNS CNAME 记录。有关更多信息，请参阅 使用 DNS 别名访问数据。

在还原备份时添加或删除 DNS 别名（CLI）

1. 通过现有文件系统的备份创建新文件系统时，可以将 Aliases 属性与 CreateFileSystemFromBackupAPI 操作配合使用，如下所示：

   - 默认情况下，与备份关联的所有别名都会被关联到新的文件系统。
   - 要使用备份创建文件系统而不保留其中的任何别名，请使用带有空集的 `Aliases` 属性。

     要关联其他 DNS 别名，请使用 `Aliases` 属性，并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. 当文件系统可用时，您可以使用 DNS 别名访问该文件系统，方法是配置服务主体名称 (SPNs)，并为该别名更新或创建 DNS CNAME 记录。有关更多信息，请参阅 使用 DNS 别名访问数据。

管理现有文件系统上的 DNS 别名

您可以使用和在现有 FSx 的 Windows 文件服务器文件系统上添加 Amazon Web Services 管理控制台和删除别名 Amazon CLI，如以下过程所述。

管理文件系统的 DNS 别名（控制台）

1. 打开 Amazon FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 导航到文件系统，然后选择要管理其 DNS 别名的 Windows 文件系统。
3. 在网络与安全选项卡上，选择 DNS 别名对应的管理，即可显示管理 DNS 别名窗口。

   - 关联 DNS 别名 – 在关联新的别名框中，输入要关联的 DNS 别名。选择关联。

- 取消关联 DNS 别名 – 在当前别名列表中，选择要取消关联的别名。选择取消关联。

可以在当前别名列表中监控管理的别名的状态。刷新列表，更新状态。将别名关联到文件系统或取消关联最多需要 2.5 分钟。

4. 当别名为 “可用” 时，您可以使用 DNS 别名访问您的文件系统，方法是配置服务主体名称 (SPNs) 并为该别名更新或创建 DNS CNAME 记录。有关更多信息，请参阅 使用 DNS 别名访问数据。

将 DNS 别名与现有文件系统关联（CLI）

1. 使用 `associate-file-system-aliases` CLI 命令或 AssociateFileSystemAliasesAPI 操作将 DNS 别名与现有文件系统关联。

   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
```

   响应显示了 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（等效DescribeFileSystemAliases的 API 操作）监控您正在关联的别名的状态。
3. 当的值`Lifecycle`为 AVAILABLE（此过程最多可能需要 2.5 分钟）时，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 (SPNs) 并更新或创建别名的 DNS CNAME 记录。有关更多信息，请参阅 使用 DNS 别名访问数据。

取消 DNS 别名与文件系统的关联（CLI）

- 使用 `disassociate-file-system-aliases` CLI 命令或 DisassociateFileSystemAliasesAPI 操作解除 DNS 别名与现有文件系统的关联。

  以下命令会取消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
  ```

  响应显示了 Amazon FSx 正在取消与文件系统的关联的别名的状态。

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

  使用 `describe-file-system-aliases` CLI 命令（等同DescribeFileSystemAliases于 API 操作）监控别名的状态。删除别名最多需要 2.5 分钟。

用户会话和打开的文件

您可以使用共享文件夹工具监视连接的用户会话，并在 FSx for Windows 文件服务器文件系统上打开文件。“共享文件夹”工具会提供一个集中位置，用于监控谁连接到文件系统，以及谁打开了哪些文件。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。
- 断开用户会话的连接，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 工具和用于远程管理的 Amazon FSx CLI PowerShell 来管理用户会话并打开 FSx 适用于 Windows 文件服务器的文件系统上的文件。

使用 GUI 管理用户和会话

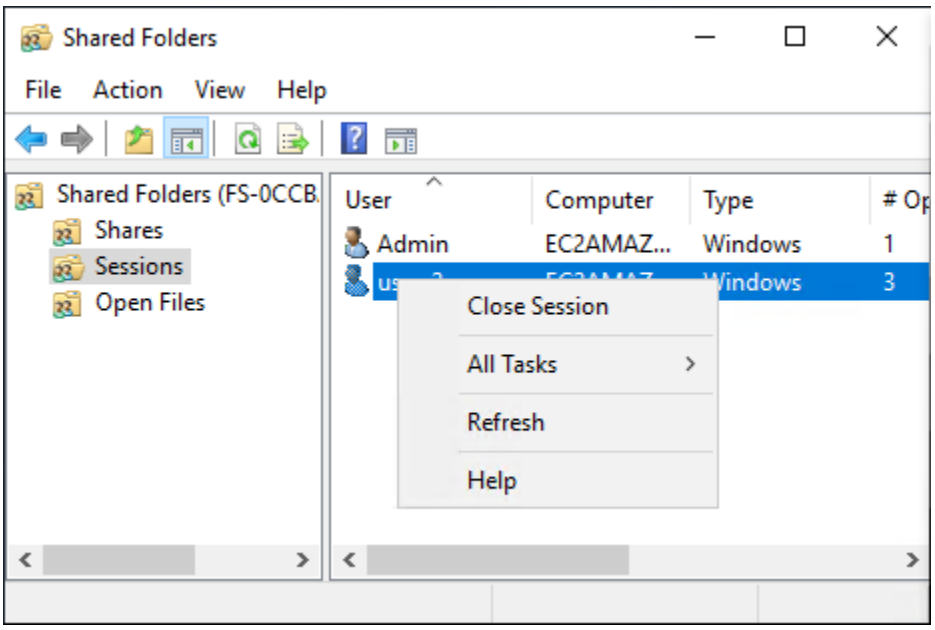
以下过程详细介绍了如何使用微软 Windows 共享文件夹工具管理用户会话和打开亚马逊 FSx 文件系统上的文件。

启动共享文件夹工具

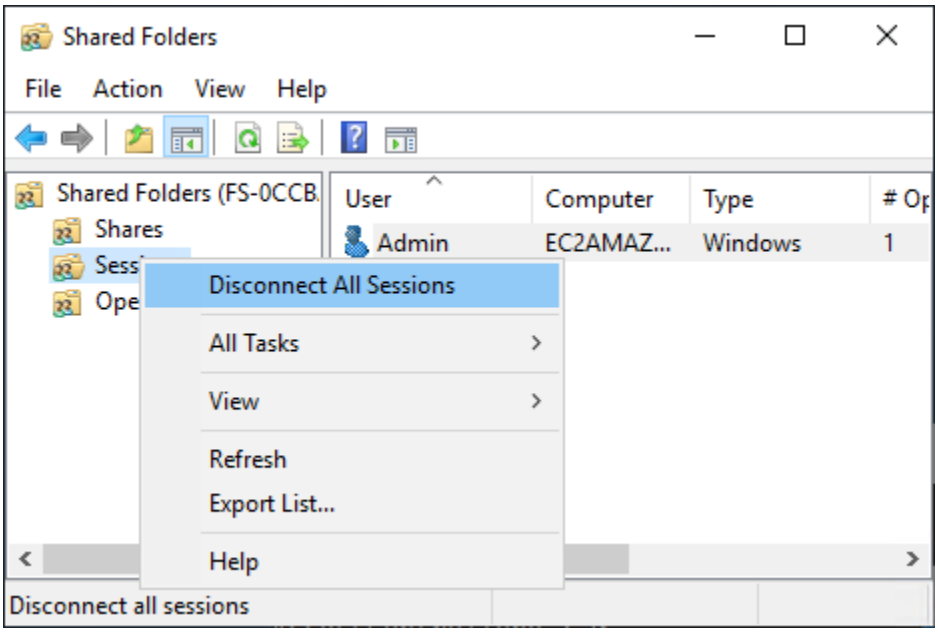
1. 启动您的亚马逊 EC2 实例，并将其连接到您的亚马逊 FSx 文件系统所加入的 Microsoft 活动目录。为此，请从《Amazon Directory Service 管理指南》中选择以下过程：
   - 无缝加入 Windows EC2 实例
   - 手动加入 Windows 实例
2. 以文件系统管理员组成员的用户身份连接到实例。在 Amazon 托管的 Microsoft 活动目录中，该组被称为 Amazon 委派 FSx管理员。在您自行管理的 Microsoft Active Directory 中，该组被称为“域管理员”，或者使用您在创建时提供的管理员组的自定义名称。有关更多信息，请参阅亚马逊 EC2 用户指南中的连接到您的 Windows 实例。
3. 打开开始菜单，然后使用 `Run As Administrator` 来运行 fsmgmt.msc。此操作将打开共享文件夹 GUI 工具。
4. 在操作中，选择连接到另一台计算机。
5. 例如，对于另一台计算机，输入您的 Amazon FSx 文件系统的 DNS 名称`fs-`*`01234567890123456`*`.`*`ad-domain`*`.com`。
6. 选择确定。然后，您的 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（GUI）

在 “共享文件夹” 工具中，选择 “会话” 以查看连接到您 FSx 的 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 文件系统上的 FSx 文件共享，则此管理单元会向您显示他们的会话。您可以打开会话的上下文（右键单击）菜单，然后选择关闭会话，即可断开会话连接。

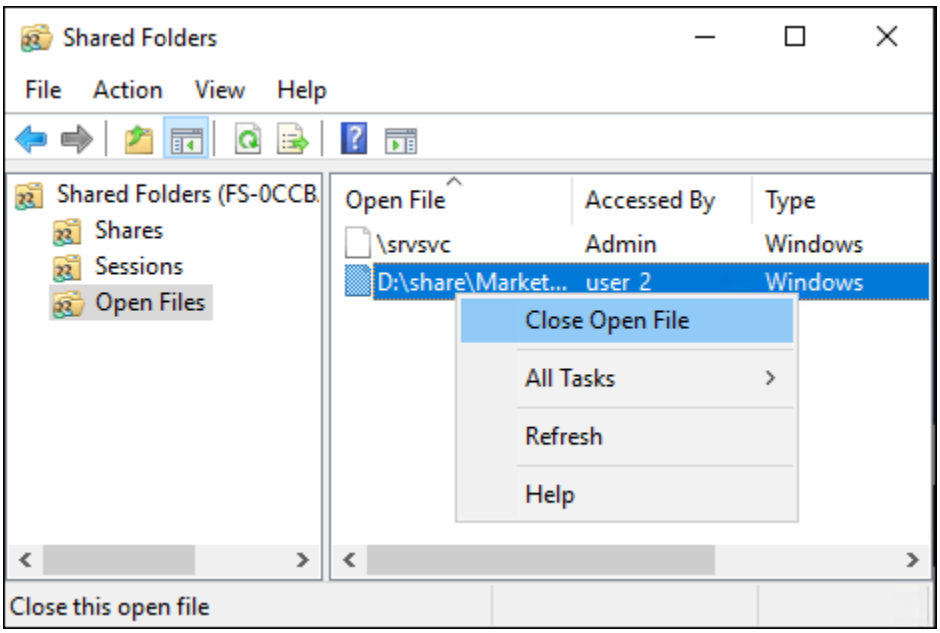


要断开所有打开的会话连接，请打开会话的上下文（右键单击）菜单，选择断开所有会话连接，然后确认操作。

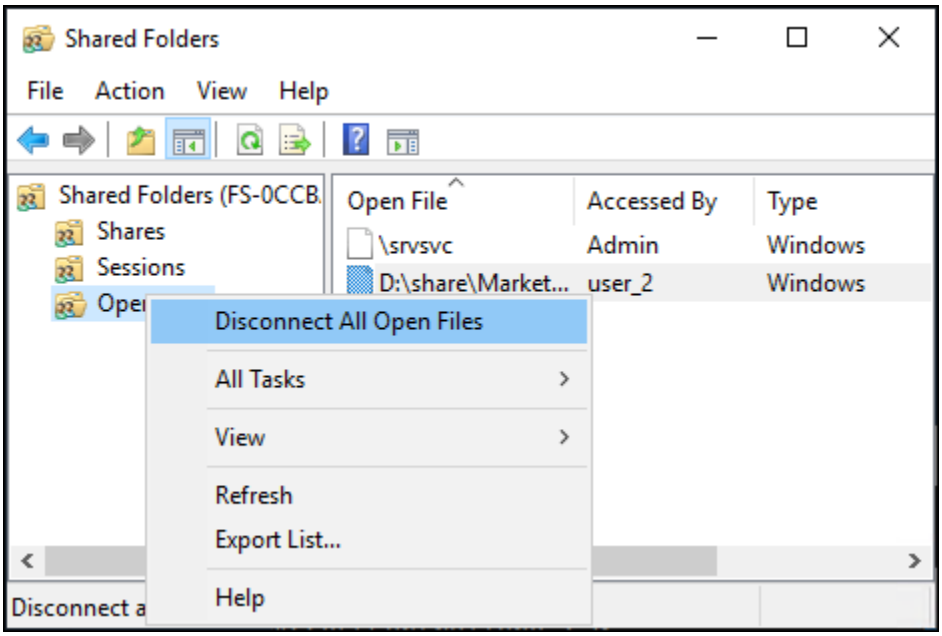


管理打开文件（GUI）

在“共享文件夹”工具中，选择打开的文件即可查看系统上当前打开的所有文件。该视图还会显示打开了文件或文件夹的用户。此信息有助于追踪其他用户无法打开某些文件的原因。只需打开列表中文件条目的上下文（右键单击）菜单，然后选择关闭打开的文件，即可关闭由任何用户打开的任何文件。



要断开文件系统上所有打开的文件的连接，请在打开的文件的上下文（右键单击）菜单中选择断开所有打开的文件的连接，然后确认操作。



PowerShell 用于管理用户会话和打开文件

您可以使用 Amazon FSx CLI 管理文件系统中的活动用户会话和打开文件，以便在上进行远程管理 PowerShell。要了解如何使用此 CLI，请参阅将 Amazon FSx CLI 用于 PowerShell。

下述为可用于管理用户会话和打开的文件的命令。

命令	说明
Get-FSxSmbSession	检索有当前建立在文件系统和已关联的客户端之间的服务器消息块（SMB）会话的相关信息。
Close-FSxSmbSession	结束 SMB 会话。
Get-FSxSmbOpenFile	检索为连接到文件系统的客户端打开的文件的相关信息。
Close-FSxSmbOpenFile	关闭一个已为 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中都提供所有命令选项的参考信息。要访问此帮助，请运行包含 -? 的命令，例如 Get-FSxSmbSession -?。

文件服务器资源管理器已开 FSx 启 Windows 文件服务器

文件服务器资源管理器 (FSRM) 是一项 Windows 服务器功能，可帮助您管理和分类存储在 Ama FSx zon for Windows 文件服务器文件系统上的数据。FSRM 提供自动策略实施和报告功能，可帮助您控制存储成本，保持对数据管理策略的合规性，并根据业务规则组织文件。

使用 FSRM，您可以设置存储限制以防止用户消耗过多的存储空间，自动识别和分类敏感数据，阻止将未经授权的文件类型保存到业务文件夹，并生成有关存储使用模式的详细报告。这些功能可帮助您维护一个井井有条、高效且合规的文件系统，而无需对每个文件或文件夹进行手动干预。

FSRM 对于有以下需求的组织特别有价值：

- 通过限制用户和部门可以存储的磁盘空间来控制存储成本
- 识别敏感数据，例如个人身份信息或财务记录
- 强制执行关于允许在特定文件夹中使用哪些文件类型的政策
- 生成有关数据保留、文件所有权或存储使用情况的合规性报告
- 保持对整个组织存储使用情况的可见性

关键功能

- 配额管理-设置文件夹的存储限制，以控制用户和应用程序可以消耗的空间。您可以配置硬配额以防止用户超出限制，也可以配置允许在发送通知时超额的软配额。配额可帮助您管理存储成本，防止用户或部门消耗不成比例的存储量。

- 文件筛选-控制用户可以将哪些类型的文件保存到特定文件夹。您可以阻止业务文件夹中未经授权的文件类型，例如可执行文件、媒体文件或个人文档。文件筛选可帮助您强制执行数据管理策略，降低安全风险，并防止非业务文件造成存储浪费。
- 文件分类-根据文件的内容或位置自动为其分配元数据属性。分类可以帮助您整理文件、识别敏感数据、应用保留策略以及根据文件特征生成报告。您可以按数据敏感度、部门、保留期或您定义的任何其他自定义属性对文件进行分类。
- 存储报告-生成有关文件系统使用情况的详细报告，包括大文件、重复文件、按所有者划分的文件、按类型划分的文件和配额使用情况。存储报告可帮助您了解存储的使用情况，识别可以存档或删除的文件，并就存储管理做出明智的决策。

主题

文件服务器资源管理器入门

您可以在创建新的 Ama FSx zon for Windows 文件服务器文件系统时启用文件服务器资源管理器 (FSRM)，也可以更新现有文件系统以启用 FSRM。

仅亚马逊支持 FSRM， FSx 适用于具有 SSD 存储且吞吐容量为 128 MB/s 或更大的 Windows 文件服务器文件系统。创建文件系统后，您可以随时将存储类型更新为 SSD 并修改吞吐容量。有关更多信息，请参阅更新 FSx for Windows 文件系统的存储类型和管理吞吐能力。

在创建文件系统时启用 FSRM（控制台）

1. 打开亚马逊 FSx 控制台，网址为 https://console.aws.amazon.com/fsx/
2. 在控制面板上，选择创建文件系统以启动文件系统创建向导。

3. 选择 FSx 适用于 Windows 文件服务器的亚马逊，然后选择下一步。
4. 选择 “标准创建” 选项
5. 提供所需信息
6. 打开 “文件服务器资源管理器” 块，选择 “启用”。
7. 对于事件日志目标，请选择以下选项之一：
   - CloudWatch 日志-选择要接收 FSRM 事件日志的日志组。 CloudWatch CloudWatch 日志日志组的名称必须以`'/aws/fsx/'`前缀开头。
   - Kinesis Data Firehos e-选择 Kinesis Data Firehose 传输流来接收 FSRM 事件日志
8. 完成其余部分并选择创建文件系统。

在创建文件系统时启用 FSRM (CLI)

要在创建 FSx 适用于 Windows 的文件服务器文件系统时启用 FSRM，请使用 CL Amazon I 命令。`create-file-system`在参数中包括以下 FSRM 配置：`--windows-configuration`

- `FsrmServiceEnabled` – 设置为 `true`
- `EventLogDestination`-指定 FSRM 事件日志目标的亚马逊资源名称 (ARN)。可以是 CloudWatch 日志日志组 ARN 或 Kinesis Data Firehose 传输流 ARN。

```
aws fsx create-file-system \
        --file-system-type WINDOWS \
        --storage-capacity 300 \
        --storage-type SSD \
        --subnet-ids subnet-0123456789abcdef0 \
        --windows-configuration
 "ThroughputCapacity=128,WindowsFsrmConfiguration={FsrmServiceEnabled=true,EventLogDestination=
east-1:123456789012:log-group:/aws/fsx/fsrm}"
```

修改现有文件系统上的 FSRM 配置（控制台）

1. 打开 Amazon FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 导航到 “文件系统”，然后选择要修改的 Windows 文件系统。
3. 选择管理选项卡。
4. 在 “文件服务器资源管理器” 部分，选择管理。
5. 进行所需的更改：

- 要更改事件日志目标，请选择其他 CloudWatch 日志组或 Kinesis Data Firehose 传输流
- 要启用 FSRM，请选择启用
- 要禁用 FSRM，请选择 “已禁用”

> **Important**
>
> 在此过程中，多可用区文件系统将经历自动故障转移和故障恢复事件，而单可用区文件系统将经历短暂的不可用期。

6. 选择保存。

您可以在文件系统详细信息页面的更新选项卡上监控更新进度。

修改现有文件系统上的 FSRM 配置 (CLI)

要在现有 FSx 的 Windows 文件服务器文件系统上启用和禁用 FSRM，请使用 CL Amazon I 命令。`update-file-system`

启用 FSRM

要启用 FSRM，请在参数中包含以下 FSRM 配置：`--windows-configuration`

- `FsrmServiceEnabled` – 设置为 `true`
- `EventLogDestination`-指定 FSRM 事件日志目标的亚马逊资源名称 (ARN)。可以是 CloudWatch 日志日志组 ARN 或 Kinesis Data Firehose 传输流 ARN。

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --windows-configuration
 FsrmConfiguration='{FsrmServiceEnabled=true,EventLogDestination=”arn:aws:logs:us-
east-1:123456789012:log-group:/aws/fsx/fsrm”}'
```

禁用 FSRM

要禁用 FSRM，请执行以下操作：

```
aws fsx update-file-system \
```

```
    --file-system-id fs-0123456789abcdef0 \
    --windows-configuration FsrmConfiguration='{FsrmServiceEnabled=false}'
```

> **Important**
>
> 在此过程中，多可用区文件系统将经历自动故障转移和故障恢复事件，而单可用区文件系统将经历短暂的不可用期。

FSx 远程 PowerShell

要配置和使用 FSRM 功能，您必须使用 Amazon CL FSx I 在上进行远程管理。 PowerShell有关信息，请参阅启动 Amazon FSx 远程 PowerShell 会话。

配额管理

您可以使用文件服务器资源管理器 (FSRM) 配额管理来控制用户在您的 Windows 文件服务器文件系统上消耗 FSx 的存储空间量。配额可以限制可存储在特定文件夹中的数据量，并在存储使用量接近或超过定义的阈值时生成通知，从而帮助您管理存储容量。

配额管理的工作原理

配额管理提供两种类型的配额，您可以将其应用于文件系统上的文件夹：

硬限额

防止用户在达到配额限制后保存文件。当用户尝试保存超出配额限制的文件时，操作将失败，并且用户会收到一条错误消息。

软限额

允许用户在记录违规行为时超过配额限制。软配额可用于监控存储使用情况，而无需强制执行严格的限制。

配额模板

配额模板提供可重复使用的配置，用于定义配额设置，包括大小限制、配额类型（硬性或软性）和阈值通知。创建配额模板后，您可以将其应用于多个文件夹，而不必每次都重新配置相同的设置。更新配额模板时，您可以选择将更改应用于根据该模板创建的所有配额。

使用配额模板有以下几个好处：

- 一致性-确保相似的文件夹具有相同的配额配置
- 效率-将配额设置快速应用于多个文件夹
- 可维护性-通过修改模板来更新多个文件夹的配额设置

自动申请配额

自动应用配额会根据指定的模板自动为子文件夹创建配额。在父文件夹上创建 auto apply 配额时，FSRM 会自动为每个现有子文件夹以及用户将来创建的任何新子文件夹生成配额。这种方法对于想要在多个用户目录或部门文件夹中应用一致的配额限制的场景非常有用。

阈值通知

阈值定义了 FSRM 采取特定操作的使用级别。您可以为每个配额配置多个阈值，将每个阈值设置为配额限制的百分比。当存储使用率达到阈值百分比时，FSRM 可以执行以下操作：

事件日志记录

将事件记录到亚马逊 CloudWatch 或亚马逊 Kinesis Data Firehose 进行监控和分析。您可以指定事件严重性级别（信息、警告或错误），并提供自定义消息正文。事件记录对于监控配额使用情况和与现有监控系统集成非常有用。

存储报告

生成存储使用情况报告，其中提供有关占用存储空间的文件和文件夹的详细信息。存储报告可帮助您确定哪些用户或应用程序消耗的存储空间最多，并就存储管理做出明智的决策。有关更多信息，请参阅 存储报告。

您可以为每个配额配置多个阈值，并对每个配额执行不同的操作。例如，您可以将配额配置为使用率为 75% 的信息事件和使用率为 90% 的警告事件。

配额管理命令

您可以访问三个系列的 FSx 远程 PowerShell 命令来管理配额：

1. 配额命令-创建、检索、修改、删除和更新特定文件夹的配额。当您需要 folder-by-folder逐一管理配额时，请使用这些命令。
2. 配额模板命令-创建、检索和修改定义可重复使用的配额配置的配额模板。使用这些命令来建立可以应用于多个文件夹的标准配额策略。

3. 自动配额命令-创建、检索、修改、移除和更新自动为子文件夹生成配额的自动应用配额。如果您需要在多个子文件夹中应用一致的配额限制，而无需手动创建单独的配额，请使用这些命令。

配额管理 FSx 远程 PowerShell 命令列表

> **Note**
>
> 本页中的所有示例都假设您已经使用文件系统的 Windows Remote PowerShell 端点定义了该 `$FSxWindowsRemotePowerShellEndpoint`变量。您可以在文件系统的详细信息页面上的 Amazon FSx 控制台中找到此终端节点，也可以使用 Amazon CLI `describe-file-systems`命令找到此终端节点。

配额命令

全新-FSx FSRMQuota

为文件夹创建新的配额。配额限制了用户可以在文件夹中存储的数据量。您可以选择将配额配置为在用户超过配额阈值时生成通知。

参数：

- `Folder (string)` – 必需。将应用配额的文件夹路径。
- `Size (string)`-不使用模板时为必填项：配额大小限制。
- `Template (string)` – 可选。要使用的现有配额模板的名称。指定模板时，只能使用描述参数；所有其他设置均继承自该模板。
- `Description (string)` – 可选。配额的描述。
- `SoftLimit (boolean)` – 可选。如果设置为 true，则会创建一个软配额，允许用户在记录违规行为时超出限制。
- `Disabled (boolean)` – 可选。如果设置为 true，则在禁用状态下创建配额。
- `ThresholdConfigurations (array)` – 可选。一系列阈值配置，用于指定在不同使用级别下要采取的操作。每种配置都具有以下属性：
  - `ThresholdPercentage (number)`：触发操作的配额限制的百分比。输入一个介于 0 和 250 之间的值。
  - `Action (array)`：达到阈值时要采取的一项或多项操作。每个操作都具有以下属性：
    - `ActionType`：要执行的操作类型。可以指定以下值：

1. Event：将事件记录到文件系统的事件日志。指定 “事件” 时，还必须指定以下属性：
   - EventType: 信息、警告或错误
   - MessageBody：要与事件一起记录的消息文本。
2. Report：生成存储使用情况报告。

示例：

1。在不使用配额模板的情况下创建 5GB 的硬配额。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMQuota -Folder "share\test" -Size 5GB
}
```

2。使用阈值通知创建软配额

```
$thresholds = [System.Collections.ArrayList]@()
$warning = @{
    ThresholdPercentage = 75
    Action = @(
        @{
            ActionType = "Event"
            EventType = "Warning"
            MessageBody = "Quota usage has reached 75%"
        }
    )
}

$thresholds.Add($warning)

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList ($thresholds) -ScriptBlock {
        param($thresholds)
        New-FSxFSRMQuota -Folder "share/test" -Size 1GB -Description "Test quota" -
SoftLimit -ThresholdConfigurations $Using:thresholds
}
```

Get-FSx FSRMQuota

从您的文件系统中检索一个或多个配额。该命令返回有关配额配置的详细信息，包括大小限制、阈值和当前使用情况。

参数：

- `Folder (string)` – 可选。从中检索配额的文件夹路径。如果您未指定文件夹路径，则该命令将返回文件系统上的所有配额。

示例：

1。获取文件系统上的所有现有配额。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMQuota
}
```

移除-FSx FSRMQuota

从文件系统上的指定文件夹中移除配额。

参数：

- `Folder (string)` – 必需。要从中删除配额的文件夹路径。
- `PassThru (boolean)` – 可选。如果设置为 true，则返回已删除的配额对象。

示例：

1。移除配额。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Remove-FSxFSRMQuota -Folder "share\test" -PassThru
}
```

Set-FSx FSRMQuota

修改现有配额的配置。

参数：

- Folder（string）– 必需。包含要修改的配额的文件夹路径。
- Description（string）– 可选。配额的新描述。
- Size（string）– 可选。配额的新大小限制。
- SoftLimit（boolean）– 可选。如果设置为 true，则将配额更改为软限制，允许用户在记录违规行为时超过限制。
- Disabled（boolean）– 可选。如果设置为 true，则禁用配额。如果设置为 false，则启用配额。
- ThresholdConfigurations（array）– 可选。一系列新的阈值配置。每个阈值配置都具有以下属性：
  - ThresholdPercentage（number）：触发操作的配额限制的百分比。输入一个介于 0 和 250 之间的值。
  - Action（array）：达到阈值时要采取的一项或多项操作。每个操作都具有以下属性：
    - ActionType：要执行的操作类型。可以指定以下值：
      1. Event：将事件记录到文件系统的事件日志。指定“事件”时，还必须指定以下属性：
         - EventType: 信息、警告或错误
         - MessageBody：要与事件一起记录的消息文本。
      2. Report：生成存储使用情况报告。
- PassThru（boolean）– 可选。如果设置为 true，则返回修改后的配额对象。

示例：

1。修改配额大小和描述。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Set-FSxFSRMQuota  -Folder "share\department"  -Size 2GB  -Description "Updated
 quota for department share"
}
```

2。禁用配额

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Set-FSxFSRMQuota -Folder "share\department" -Disabled: $true
}
```

更新-FSx FSRMQuota

通过扫描文件夹来确定实际使用的空间量，重新计算配额的当前使用情况统计信息。

参数：

- Folder（string）– 必需。包含要更新的配额的文件夹路径。
- PassThru（boolean）– 可选。如果设置为 true，则返回更新的配额对象。

示例：

1。重新计算指定配额的当前使用情况统计信息。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Update-FSxFSRMQuota -Folder "share\department" -PassThru
}
```

配额模板命令

全新-FSx FSRMQuota 模板

创建新的配额模板，该模板定义了可重复使用的配额配置。

参数：

- Name（string）– 必需。配额模板的名称。
- Size（string）– 必需。配额模板强制执行的大小限制。
- Description（string）– 可选。配额模板的描述。
- SoftLimit（boolean）– 可选。如果设置为 true，则为软配额创建一个模板，该模板会报告使用情况，但不强制执行限制。
- ThresholdConfigurations（array）– 可选。一系列阈值配置，用于指定在不同使用级别下要采取的操作。每种配置都具有以下属性：
  - ThresholdPercentage（number）：触发操作的配额限制的百分比。输入一个介于 0 和 250 之间的值。
  - Action（array）：达到阈值时要采取的一项或多项操作。每个操作都具有以下属性：
    - ActionType：要执行的操作类型。可以指定以下值：
      1. Event：将事件记录到文件系统的事件日志。指定 “事件” 时，还必须指定以下属性：

- EventType: 信息、警告或错误
- MessageBody：要与事件一起记录的消息文本。

2. Report：生成存储使用情况报告。

示例：

1。创建 1 GB 的硬限制模板。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMQuotaTemplate -Name "1GB Hard Limit" -Size 1GB -Description "Standard
 1GB hard limit template"
}
```

2。创建一个 5 GB 的软限制模板，并在使用率为 90% 时设置警告阈值

```
$threshold = @{
    ThresholdPercentage = 90
    Action = @(
        @{
            ActionType = "Event"
            EventType = "Warning"
            MessageBody = "Quota usage has reached 90% of the limit"
        }
    )
}

$thresholds = [System.Collections.ArrayList]@()
$thresholds.Add($threshold)

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $thresholds -ScriptBlock {
    param($thresholds)

    New-FSxFSRMQuotaTemplate -Name "5GB Soft Limit" -Size 5GB -Description "5GB soft
 limit with 90% warning" -SoftLimit -ThresholdConfigurations $Using:thresholds
}
```

获取-FSx FSRMQuota 模板

从您的文件系统中检索一个或多个配额模板。

参数：

- Name（string）– 可选。要检索的特定配额模板的名称。如果您未指定名称，则该命令将返回所有配额模板。

示例：

1。检索文件系统上的所有配额模板。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMQuotaTemplate
}
```

套装-FSx FSRMQuota 模板

修改配额模板的属性。

参数：

- Name（string）– 必需。要修改的配额模板的名称。
- Description（string）– 可选。模板的新描述。
- Size（string）– 可选。模板的新大小限制。
- SoftLimit（boolean）– 可选。如果设置为 true，则更改模板以创建软配额，这些配额会报告使用情况，但不强制执行限制。
- ThresholdConfigurations（array）– 可选。一系列阈值配置，用于指定在不同使用级别下要采取的操作。每种配置都具有以下属性：
  - ThresholdPercentage（number）：触发操作的配额限制的百分比。输入一个介于 0 和 250 之间的值。
  - Action（array）：达到阈值时要采取的一项或多项操作。每个操作都具有以下属性：
    - ActionType：要执行的操作类型。可以指定以下值：
      1. Event：将事件记录到文件系统的事件日志。指定 “事件” 时，还必须指定以下属性：
         - EventType: 信息、警告或错误
         - MessageBody：要与事件一起记录的消息文本。
      2. Report：生成存储使用情况报告。
- UpdateDerived（boolean）– 可选。如果设置为 true，则更新根据此模板创建的所有配额。

- UpdateDerivedMatching (boolean) – 可选。如果设置为 true，则仅更新根据此模板创建且自创建以来未修改的配额。
- PassThru (boolean) – 可选。如果设置为 true，则返回修改后的模板对象。

示例：

1。修改配额模板的大小和描述。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Set-FSxFSRMQuotaTemplate -Name "5GB Soft Limit" -Size 10GB -Description "Updated to
 10GB soft limit"
}
```

2。修改配额模板并更新根据该模板创建的所有配额。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Set-FSxFSRMQuotaTemplate -Name "1GB Hard Limit" -Size 2GB -UpdateDerived
}
```

重置-FSx FSRMQuota

重置配额以匹配指定模板的设置。

Parameters

- Folder (string) – 必需。包含要重置的配额的文件夹路径。
- Template (string) – 必需。要应用的配额模板的名称。

示例

示例：重置配额以匹配配额模板中定义的设置。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Reset-FSxFSRMQuota -Folder "share\department" -Template "1GB Hard Limit"
}
```

自动配额命令

新增-FSx FSRMAuto 配额

该New-FSxFSRMAutoQuota命令在指定文件夹上创建 auto apply 配额。auto apply 配额会根据指定的模板自动为每个现有子文件夹和在指定文件夹中创建的任何新子文件夹生成配额。

Parameters

- Folder (string) – 必需。将在其中创建 auto apply 配额的文件夹路径。
- Template (string) – 可选。用于自动应用配额的现有配额模板的名称。
- Disabled (boolean) – 可选。如果设置为 true，则在禁用状态下创建自动应用配额。

示例

1。创建 auto apply 配额，自动将指定模板应用于所有子文件夹。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMAutoQuota -Folder "share\department" -Template "250 MB Extended Limit"
}
```

获取-FSx FSRMAuto 配额

该Get-FSxFSRMAutoQuota命令会从您的文件系统中检索一个或多个 auto apply 配额。

Parameters

- Folder (string) – 可选。要从中检索 auto 应用配额的文件夹路径。您也可以在路径末尾使用...来包含所有子文件夹。

如果您未指定文件夹路径，则该命令将返回文件系统上的所有 auto apply 配额。

示例

1。检索文件系统上的所有 auto apply 配额。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
```

```
    Get-FSxFSRMAutoQuota
}
```

移除-FSx FSRMAuto 配额

该Remove-FSxFSRMAutoQuota命令从指定文件夹中删除自动申请的配额。当您删除 auto apply 配额时，该命令还会删除从关联配额模板派生的子文件夹中的所有配额。

Parameters

- Folder (string) – 必需。要从中删除 auto 应用配额的文件夹路径。
- PassThru (boolean) – 可选。如果设置为 true，则返回已删除的自动应用配额对象。

示例

1。从特定文件夹中移除 auto 应用配额。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Remove-FSxFSRMAutoQuota -Folder "share\department" -PassThru
}
```

设定-FSx FSRMAuto 配额

该Set-FSxFSRMAutoQuota命令修改 auto apply 配额的配置设置。

Parameters

- Folder (string) – 必需。包含要修改的 auto 应用配额的文件夹路径。
- Template (string) – 可选。要应用的配额模板的名称。
- Disabled (boolean) – 可选。如果设置为 true，则禁用自动应用配额。如果设置为 false，则启用自动应用配额。
- UpdateDerived (boolean) – 可选。如果设置为 true，则更新从该自动应用配额中派生的所有现有配额。
- UpdateDerivedMatching (boolean) – 可选。如果设置为 true，则仅更新自创建以来未修改的派生配额。
- PassThru (boolean) – 可选。如果设置为 true，则返回修改后的自动应用配额对象。

示例

1。更改 auto 应用配额使用的配额模板。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Set-FSxFSRMAutoQuota -Folder "share\department" -Template "100 MB Limit"
}
```

2。禁用 auto apply 配额并更新从中派生的所有配额。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Set-FSxFSRMAutoQuota -Folder "share\department" -Disabled: $true -UpdateDerived
}
```

更新-FSx FSRMAuto 配额

该Update-FSxFSRMAutoQuota命令通过扫描文件夹来确定实际使用的空间量，从而重新计算 auto apply 配额的属性以及从中派生的配额。

Parameters

- Folder (string) – 必需。包含要更新的自动应用配额的文件夹路径。
- PassThru (boolean) – 可选。如果设置为 true，则返回更新的自动应用配额对象。

示例

1。重新计算使用情况统计信息并返回更新后的 auto apply quota 对象。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Update-FSxFSRMAutoQuota -Folder "share\department" -PassThru
}
```

文件组

文件组定义了在配置文件屏幕时必须使用的文件名模式的逻辑集合，也可以在生成存储报告时选择使用这些模式。文件组包含包含模式（要匹配的文件）和排除模式（要从匹配项中排除的文件），您可以通过文件组名称来引用它们，而不是每次都指定单独的模式。

如何使用文件组

以下 FSRM 功能需要文件组：

- 文件屏幕-必须指定一个或多个文件组来定义要屏蔽或监视的文件类型。
- 文件屏幕例外-您必须指定一个或多个文件组，以定义尽管父文件夹中屏蔽了文件屏幕，但仍允许哪些文件类型。
- 文件屏幕模板-必须指定一个或多个文件组来定义模板将屏蔽或监视哪些文件类型。

对于以下 FSRM 功能，文件组是可选的：

- 存储报告-您可以选择按文件组筛选报告，以分析特定文件类型的存储使用情况。例如，您可以生成仅显示音频和视频文件的报告。

文件名模式

文件组使用通配符模式来匹配文件名。您可以指定包含模式（要匹配的文件）和排除模式（要从匹配项中排除的文件）。

FSRM 支持以下通配符：

- 星号 (*)-匹配零个或多个字符
- 问号 (？) -恰好匹配一个字符

例如，该模式`*.doc*`匹配、和之类的文件 `report.doc` `report.docxdocument.doc`，而 `~$*`排除模式不包括由 Microsoft Office 应用程序创建的临时文件。

默认文件组

在文件系统上启用 FSRM 时，会自动创建以下文件组：

音频和视频文件

匹配常见的音频和视频文件格式`*.mp3`，包括 `*.wav`、`*.avi`、`*.mp4`、`*.mpeg`、和 `*.wmv`

Backup 文件

匹配备份文件格式`*.bak`，包括`*.backup`、和 `*.old`

压缩文件

匹配存档和压缩文件格式*.zip，包括 *.rar、*.7z、*.gz、和 *.tar

通过电子邮件发送文件

匹配电子邮件和邮箱格式*.eml，包括 *.msg、和 *.pst

可执行文件

匹配可执行文件和脚本文件格式*.exe，包括 *.dll*.com、*.bat、、*.cmd、和 *.vbs

图像文件

匹配常见的图像文件格式*.jpg，包括 *.jpeg、*.png、*.gif、*.bmp、和 *.tif

办公文件

匹配微软 Office 文档格式 *.doc *.docx，包括*.xls、*.xlsx、*.ppt、、和 *.pptx

系统文件

匹配 Windows 系统文件格式*.sys，包括 *.dll、*.ocx、和 *.drv

临时文件

匹配临时文件格式*.tmp，包括*.temp、和 ~*

文本文件

匹配基于文本的文件格式*.txt，包括、*.log*.csv、和 *.xml

网页文件

匹配 Web 内容文件格式*.html，包括 *.htm*.asp、、*.aspx、*.php、和 *.js

您可以立即在文件屏幕和存储报告中使用这些默认文件组，也可以对其进行修改以满足您的特定要求。

文件组管理命令

FSRM 提供用于创建和管理文件组的 PowerShell 命令。使用这些命令来定义与贵组织的文件管理策略相匹配的自定义文件组。

> **Note**
>
> 本页中的所有示例都假设您已经使用文件系统的 Windows Remote PowerShell 端点定义了该$FSxWindowsRemotePowerShellEndpoint变量。您可以在 Amazon FSx 控制台的文件系

统的详细信息页面上找到此端点，也可以使用 Amazon CLI `describe-file-systems` 命令找到此端点。

全新-FSx FSRMFile 群组

创建用于定义文件名模式逻辑集合的文件组。这些模式可用于文件屏幕、文件屏幕异常和存储报告。

参数：

- `Name (string)` – 必需。文件组的名称。
- `Description (string)` – 可选。文件组的描述。
- `IncludePattern (array)` – 可选。指定要包含的文件的模式字符串数组。
- `ExcludePattern (array)` – 可选。指定要排除的文件的模式字符串数组。

示例：

1. 为文本文件创建文件组。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMFileGroup -Name "My Text Files" -IncludePattern "*.txt"
}
```

2. 使用包含和排除模式为源代码创建文件组。

```
$includePatterns = @("*.cpp", "*.h", "*.cs", "*.py")
$excludePatterns = @("*.tmp", "*.bak")

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList @($includePatterns, $excludePatterns) -ScriptBlock {
    param($includePatterns, $excludePatterns)
    New-FSxFSRMFileGroup -Name "Source Code" -Description "Programming source files"
 -IncludePattern $includePatterns -ExcludePattern $excludePatterns
}
```

Get-G FSx FSRMFile roup

从您的文件系统中检索一个或多个文件组。文件组定义了文件筛选和报告中使用的文件模式集合。

参数：

- Name （array）– 可选。要检索的文件组名称数组。如果未指定名称，则该命令将返回文件系统上的所有文件组。

示例：

1. 检索文件系统上的所有文件组。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMFileGroup
}
```

移除-FSx FSRMFile 群组

从您的文件系统中移除一个或多个文件组。删除后，文件组将无法在文件屏幕或文件屏幕异常中使用。

参数：

- Name （array）– 必需。要删除的文件组名称数组。
- PassThru （boolean）– 可选。如果设置为 true，则返回已删除的文件组对象。

示例：

1. 移除单个文件组。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Remove-FSxFSRMFileGroup -Name "My Text Files" -PassThru
}
```

套装-FSx FSRMFile 群组

修改现有文件组的属性。

参数：

- Name （array）– 必需。要修改的文件组名称数组。

- Description (string) – 可选。文件组的新描述。
- IncludePattern (array) – 可选。一个新的模式字符串数组，用于指定要包含的文件。
- ExcludePattern (array) – 可选。一个新的模式字符串数组，用于指定要排除的文件。
- PassThru (boolean) – 可选。如果设置为 true，则返回修改后的文件组对象。

示例：

1. 更新文件组的描述和模式。

```
$includePatterns = @("*.docx", "*.pdf", "*.rtf")
$excludePatterns = @("~$*", "*.tmp")

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList @($includePatterns, $excludePatterns) -ScriptBlock {
    param($includePatterns, $excludePatterns)
    Set-FSxFSRMFileGroup -Name "Documents" -Description "Updated document types" -
IncludePattern $includePatterns -ExcludePattern $excludePatterns -PassThru
}
```

文件筛选

文件筛选控制用户可以将哪些类型的文件保存到文件系统的文件夹中。文件筛选可帮助您强制执行存储策略，防止未经授权的文件类型，并保持对组织要求的合规性。

> **Note**
>
> 文件屏幕使用文件组来定义要屏蔽或监视哪些文件类型。有关创建和管理文件组的更多信息，请参阅文件组。

FSRM 支持两种类型的文件屏幕：

1. 活动文件屏幕-阻止用户保存与指定文件组匹配的文件，并在用户尝试保存被阻止的文件时生成通知。当您需要对特定文件夹中允许哪些文件类型实施严格政策时，请使用活动文件屏幕。
2. 被动文件屏幕-在用户保存与指定文件组匹配的文件时进行监控和记录，但不阻止保存操作。如果您想在不中断用户工作流程的情况下跟踪文件使用模式，请使用被动文件屏幕。

文件屏幕模板

文件屏幕模板提供了可重复使用的配置，用于定义文件筛选设置，包括要屏蔽或监控哪些文件组以及要生成哪些通知。创建文件屏幕模板后，可以将其应用于多个文件夹，而不必每次都重新配置相同的设置。更新文件屏幕模板时，可以选择将更改应用于根据该模板创建的所有文件屏幕。

使用文件屏幕模板有以下几个好处：

- 一致性-确保相似的文件夹具有相同的文件筛选配置
- 效率-将文件筛选设置快速应用于多个文件夹
- 可维护性-通过修改模板来更新多个文件夹中的文件筛选设置

文件屏幕异常

文件屏幕例外会覆盖原本适用于文件夹及其所有子文件夹的文件筛选规则。创建文件屏幕异常时，您可以指定允许哪些文件组，尽管父文件夹中存在任何屏蔽文件屏幕。当您需要允许在某些子文件夹中使用特定的文件类型，同时在文件夹层次结构的更高级别上保持更广泛的限制时，文件屏幕例外非常有用。

例如，您可以屏蔽整个共享中的可执行文件，但会为管理员需要在其中存储安装文件的特定子文件夹创建一个例外。

文件筛选通知

当用户尝试保存被活动文件屏幕屏蔽的文件时，FSRM 可以生成通知，提醒管理员或向用户提供信息。您可以配置以下类型的通知：

- 事件记录-将事件记录到亚马逊 CloudWatch 或亚马逊 Kinesis Data Firehose 以进行监控和分析。您可以指定事件的严重性级别（信息、警告或错误），并提供自定义消息正文。事件记录对于跟踪文件屏幕违规行为以及与现有监控系统集成非常有用。
- 存储报告-生成存储使用情况报告，提供有关文件筛选活动的详细信息。存储报告可帮助您识别文件保存尝试中的模式，并就文件筛选策略做出明智的决定。有关更多信息，请参阅 存储报告。

文件筛选管理命令

您可以访问三个系列的 FSx 远程 PowerShell 命令来管理文件屏幕：

1. 文件屏幕命令-在特定文件夹上创建、检索、修改、删除和重置单个文件屏幕。当您需要 folder-by-folder逐一管理文件屏幕时，请使用这些命令。

2. 文件屏幕模板命令-创建、检索、修改和删除定义可重复使用的文件筛选配置的文件屏幕模板。使用这些命令来建立可以应用于多个文件夹的标准文件筛选策略。
3. 文件屏幕异常命令-创建、检索、修改和删除会覆盖父文件夹中文件筛选规则的文件屏幕异常。如果您需要允许某些子文件夹中的特定文件类型，同时保持更广泛的限制，请使用这些命令。

文件筛选 FSx远程 PowerShell 命令列表

> **Note**
>
> 本页中的所有示例都假设您已经使用文件系统的 Windows Remote PowerShell 端点定义了该 `$FSxWindowsRemotePowerShellEndpoint`变量。您可以在文件系统的详细信息页面上的 Amazon FSx 控制台中找到此终端节点，也可以使用 Amazon CLI `describe-file-systems`命令找到此终端节点。

文件屏幕命令

全新-FSx FSRMFile 屏幕

创建文件屏幕，阻止用户将指定类型的文件保存到文件夹。

参数：

- `Folder (string)` – 必需。将应用文件屏幕的文件夹路径。
- `Description (string)` – 可选。文件屏幕的描述。
- `IncludeGroup (array)` – 可选。文件组名称数组，用于指定要阻止或监视哪些文件。
- `Active (boolean)` – 可选。如果设置为 true，则会创建一个屏蔽文件的活动文件屏幕。如果设置为 false，则会创建一个仅监视文件的被动文件屏幕。默认设置为 true。
- `Template (string)` – 可选。要使用的现有文件屏幕模板的名称。
- `NotificationConfigurations (array)` – 可选。一系列配置，用于在用户尝试保存被阻止的文件时发出通知。每种配置都具有以下属性：
  - `ActionType (string)`：要执行的操作类型。可以指定以下值：
    1. `Event`：将事件记录到文件系统的事件日志。指定 “事件” 时，还必须指定以下属性：
       - `EventType (string)`: 信息、警告或错误
       - `MessageBody (string)`：要与事件一起记录的消息文本。

2. Report：生成存储使用情况报告。指定 “报告” 时，还必须指定：
   - ReportType（string）：报告的类型。您可以指定以下值：DuplicateFiles、FilesByFileGroup、FilesByOwner、FilesByProperty、LargeF或QuotaUsage。

示例：

1. 创建一个屏蔽音频文件的基本活动文件屏幕。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMFileScreen -Folder "share\department" -IncludeGroup "Audio and Video
 Files"
}
```

2. 创建一个文件屏幕，用于屏蔽视频文件，并在用户尝试保存视频文件时生成事件日志条目。

```
$notifications = [System.Collections.ArrayList]@()
$eventNotification = @{
    ActionType = "Event"
    EventType = "Warning"
    MessageBody = "File screen violation detected"
}
$null = $notifications.Add($eventNotification)

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $notifications -ScriptBlock {
    param($notifications)
    New-FSxFSRMFileScreen -Folder "share\projects" -IncludeGroup "Audio and Video
 Files" -NotificationConfigurations $Using:notifications
}
```

获取-FSx FSRMFile 屏幕

从您的文件系统中检索一个或多个文件屏幕。

参数：

- Folder（string）– 可选。从中检索文件的文件夹路径。如果您未指定文件夹路径，则该命令将返回文件系统上的所有文件屏幕。

示例：

1. 检索文件系统上的所有文件屏幕。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMFileScreen
}
```

设置-FSx FSRMFile 屏幕

修改现有文件屏幕的属性。

参数：

- Folder（string）– 必需。包含要修改的文件屏幕的文件夹路径。
- Description（string）– 可选。文件屏幕的新描述。
- IncludeGroup（array）– 可选。一个新的文件组名称数组，用于定义要阻止或监视哪些文件。
- Active（boolean）– 可选。如果设置为 true，则将文件屏幕设置为活动模式（屏蔽）。如果设置为 false，则将文件屏幕设置为被动模式（仅限监控）。默认设置为 true。
- NotificationConfigurations（array）– 可选。一系列新的通知配置。
- PassThru（boolean）– 可选。如果设置为 true，则返回修改后的文件屏幕对象。

示例：

1. 修改文件屏幕的描述和文件组。

```
$includeGroups = @("Audio and Video Files")
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $includeGroups -ScriptBlock {
    param($includeGroups)
    Set-FSxFSRMFileScreen -Folder "share\projects" -Description "Updated screen" -
IncludeGroup $includeGroups
}
```

2. 将文件屏幕设置为活动模式并添加通知。

```
$notifications = [System.Collections.ArrayList]@()
```

```
$eventNotification = @{
    ActionType = "Event"
    EventType = "Warning"
    MessageBody = "File screen violation detected"
}
$null = $notifications.Add($eventNotification)

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $notifications -ScriptBlock {
    param($notifications)
    Set-FSxFSRMFileScreen -Folder "share\projects" -Active: $true -
NotificationConfigurations $Using:notifications -PassThru
}
```

移除-FSx FSRMFile 屏幕

从指定文件夹中移除文件屏幕。

参数：

- `Folder (string)` – 必需。要从中删除文件屏幕的文件夹路径。
- `PassThru (boolean)` – 可选。如果设置为 true，则返回已删除的文件屏幕对象。

示例：

1. 从特定文件夹中移除文件屏幕。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Remove-FSxFSRMFileScreen -Folder "share\projects" -PassThru
}
```

重置-FSx FSRMFile 屏幕

重置文件屏幕以匹配指定模板的设置。

参数：

- `Folder (string)` – 必需。包含要重置的文件屏幕的文件夹路径。
- `Template (string)` – 必需。要应用的现有文件屏幕模板的名称。

示例：

1. 重置文件屏幕，使其与文件屏幕模板中定义的设置相匹配。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Reset-FSxFSRMFileScreen -Folder "share\department" -Template "Block Audio Files"
}
```

文件屏幕模板命令

Get-FSx FSRMFile ScreenTemplate

该Get-FSxFSRMFileScreenTemplate命令会从您的文件系统中检索一个或多个文件屏幕模板。

Parameters

- Name （array）– 可选。要检索的文件屏幕模板的名称数组。如果您未指定名称，则该命令将返回文件系统上的所有文件屏幕模板。

示例

1. 检索所有文件屏幕模板。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMFileScreenTemplate
}
```

全新-FSx FSRMFile ScreenTemplate

该New-FSxFSRMFileScreenTemplate命令创建一个文件屏幕模板，该模板为文件屏幕定义了可重复使用的配置。该模板指定要阻止哪些文件组，以及在用户尝试保存被阻止的文件时生成哪些通知。

Parameters

- Name （string）– 必需。文件屏幕模板的名称。
- Description （string）– 可选。文件屏幕模板的描述。
- IncludeGroup （array）– 可选。文件组名称数组，用于指定要阻止或监视哪些文件。

- Active（boolean）– 可选。如果设置为 true，则创建用于屏蔽文件的活动文件屏幕模板。如果设置为 false，则创建仅监视文件的被动模板。默认设置为 true。
- NotificationConfigurations（array）– 可选。一系列配置，用于在用户尝试保存被阻止的文件时发出通知。每种配置都具有以下属性：
  - ActionType（string）：要执行的操作类型。可以指定以下值：
    1. Event：将事件记录到文件系统的事件日志。指定 “事件” 时，还必须指定以下属性：
       - EventType（string）: 信息、警告或错误
       - MessageBody（string）：要与事件一起记录的消息文本。
    2. Report：生成存储使用情况报告。指定 “报告” 时，还必须指定：
       - ReportType（string）：报告的类型。您可以指定以下值：DuplicateFiles、FilesByFileGroup、FilesByOwner、FilesByProperty、LargeF或 QuotaUsage

示例

1. 创建带有通知的文件屏幕模板。

```
$notifications = [System.Collections.ArrayList]@()
$eventNotif = @{
    ActionType = "Event"
    EventType = "Warning"
    MessageBody = "Blocked file detected"
}
$null = $notifications.Add($eventNotif)

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $notifications -ScriptBlock {
    param($notifications)
    New-FSxFSRMFileScreenTemplate -Name "Block Executables" -Description
 "Blocks executable files" -IncludeGroup "Executable Files" -Active: $true -
NotificationConfigurations $Using:notifications
}
```

移除-FSx FSRMFile ScreenTemplate

该Remove-FSxFSRMFileScreenTemplate命令将从您的文件系统中移除一个或多个文件屏幕模板。移除模板时，根据该模板创建的文件屏幕将保持不变。

Parameters

- Name（array）– 必需。要删除的文件屏幕模板的名称数组。
- PassThru（boolean）– 可选。如果设置为 true，则返回已删除的文件屏幕模板对象。

示例

1. 移除单个文件屏幕模板。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Remove-FSxFSRMFileScreenTemplate -Name "Block Executables" -PassThru
}
```

Set-FSx FSRMFile ScreenTemplate

该Set-FSxFSRMFileScreenTemplate命令修改现有文件屏幕模板的属性。（可选）更新使用修改后的模板创建的文件屏幕。

Parameters

- Name（array）– 必需。要修改的文件屏幕模板的名称数组。
- Description（string）– 可选。模板的新描述。
- IncludeGroup（array）– 可选。一个新的文件组名称数组，用于定义要阻止或监视哪些文件。
- Active（boolean）– 可选。如果设置为 true，则将模板设置为活动模式（阻止）。如果设置为 false，则将模板设置为被动模式（监控）。默认设置为 true。
- NotificationConfigurations（array）– 可选。一系列新的通知配置。
- UpdateDerived（boolean）– 可选。如果设置为 true，则更新根据此模板创建的所有现有文件屏幕，无论对这些文件屏幕进行了何种修改。
- UpdateDerivedMatching（boolean）– 可选。如果设置为 true，则仅更新自该模板创建以来未修改过的文件屏幕。
- PassThru（boolean）– 可选。如果设置为 true，则返回修改后的文件屏幕模板对象。

示例

1. 使用新的文件组更新文件屏幕模板。

```
$includeGroups = @("Audio and Video Files")
```

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $includeGroups -ScriptBlock {
    param($includeGroups)
    Set-FSxFSRMFileScreenTemplate -Name "Block Executables" -IncludeGroup
 $includeGroups
}
```

2. 将文件屏幕模板更新为活动模式并更新所有派生的文件屏幕。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Set-FSxFSRMFileScreenTemplate -Name "Block Executables" -Active: $true -
UpdateDerived
}
```

文件屏幕异常命令

全新-FSx FSRMFile ScreenException

该New-FSxFSRMFileScreenException命令会创建一个文件屏幕异常，该例外会覆盖原本适用于文件夹及其所有子文件夹的所有文件筛选规则。这允许在异常文件夹中创建特定的文件类型，即使它们被父文件夹中的文件屏幕屏蔽也是如此。

Parameters

- Folder (string) – 必需。将应用文件屏幕异常的文件夹路径。例外情况适用于此文件夹及其所有子文件夹。
- Description (string) – 可选。文件屏幕异常的描述。
- IncludeGroup (array) – 可选。一组文件组名称，用于指定允许哪些文件，尽管存在任何屏蔽文件屏幕，否则这些屏幕会从父文件夹中应用。

示例

1. 为特定文件夹和文件组创建文件屏幕例外。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMFileScreenException -Folder "share\department" -IncludeGroup "Text
 Files"
}
```

2. 创建包含多个文件组的文件屏幕异常。

```
$includeGroups = @("Audio and Video Files", "Documents")
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $includeGroups -ScriptBlock {
    param($includeGroups)
    New-FSxFSRMFileScreenException -Folder "share\projects" -Description "Allow media
 files in project folder" -IncludeGroup $includeGroups
    }
```

Get-FSx FSRMFile ScreenException

该Get-FSxFSRMFileScreenException命令会从您的文件系统中检索一个或多个文件屏幕异常。

Parameters

- `Folder (string)` – 可选。从中检索文件屏幕异常的文件夹路径。如果您未指定文件夹路径，则该命令将返回文件系统上的所有文件屏幕异常。

示例

1. 检索文件系统上的所有文件屏幕异常。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMFileScreenException
}
```

2. 检索特定文件夹的文件屏幕异常。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMFileScreenException -Folder "share\department"
}
```

移除-FSx FSRMFile ScreenException

该Remove-FSxFSRMFileScreenException命令从指定文件夹中删除文件屏幕异常。删除后，该文件夹及其子文件夹将受以前被例外覆盖的父文件夹中所有文件筛选规则的约束。

Parameters

- `Folder (string)` – 必需。要从中删除文件屏幕异常的文件夹路径。
- `PassThru (boolean)` – 可选。如果设置为 true，则返回已删除的文件屏幕异常对象。

示例

1. 从特定文件夹中移除文件屏幕异常。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Remove-FSxFSRMFileScreenException -Folder "share\projects" -PassThru
}
```

Set-FSx FSRMFile ScreenException

该`Set-FSxFSRMFileScreenException`命令修改文件屏幕异常的属性。

Parameters

- `Folder (string)` – 必需。包含要修改的文件屏幕异常的文件夹路径。
- `Description (string)` – 可选。文件屏幕异常的新描述。
- `IncludeGroup (array)` – 可选。一个新的文件组名称数组，用于定义允许哪些文件，尽管存在任何屏蔽文件屏幕，否则这些屏幕会从父文件夹中应用。
- `PassThru (boolean)` – 可选。如果设置为 true，则返回修改后的文件屏幕异常对象。

示例

1. 针对文件屏幕异常更新允许的文件组。

```
$includeGroups = @("Audio and Video Files")
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $includeGroups -ScriptBlock {
    param($includeGroups)
    Set-FSxFSRMFileScreenException -Folder "share\projects" -IncludeGroup
 $includeGroups -PassThru
}
```

文件分类

文件分类根据文件的内容、位置或其他属性自动为文件分配元数据属性。分类可以识别包含敏感信息、属于特定业务类别或需要保留期的文件，从而帮助您整理文件、强制执行数据管理策略并满足合规性要求。

文件分类的工作原理

文件分类使用三个步骤的过程：

1. 定义属性-创建分类属性定义来指定要分配给文件的元数据类型，例如"Data Sensitivity"或"ContainsPII"。
2. 创建规则-配置分类规则，根据您指定的标准（例如文件内容模式或文件夹位置）自动为文件分配属性值。例如，包含诸如社会安全号码之类的模式的文件(XXX-XX-XXXX)可以自动归类为ContainsPII=Yes。
3. 运行分类-执行分类过程以扫描文件并应用规则。您可以按需手动运行分类，也可以按计划运行分类，也可以在后台连续运行分类。

分类完成后，您可以使用分配的属性来生成存储报告文件管理任务、应用或搜索具有特定特征的文件。

分类属性定义

分类属性定义指定可以分配给文件的元数据类型。每个属性定义都有一个名称、一个属性类型和一个允许值的列表（可选）。例如，您可以创建一个名为的属性，"Data Sensitivity"其OrderedList类型和可能的值为：PublicInternal、Confidential、和Restricted。

支持以下属性类型：

- OrderedList-一个有序列表，其中值具有特定的序列（例如，低、中、高）。当值的顺序对报告或政策决策很重要时，请使用此类型。
- MultiChoice-允许从列表中选择多个值（例如，文件可能同时标有 “财务” 和 “法律” 类别）。
- SingleChoice-仅允许从列表中选择一个值。
- String-没有预定义选项的单个文本值。
- MultiString-多个文本值，没有预定义选项。
- Integer-一个数值。
- YesNo-布尔值（真或假）。

- DateTime-日期和时间值。

属性定义可在多个分类规则中重复使用。创建属性定义后，可以在任何需要为该属性分配值的分类规则中引用该定义。

分类规则

分类规则定义了自动为文件分配属性值的逻辑。每条规则都规定：

- 要设置哪个属性
- 为该属性分配什么值
- 在哪里应用规则（哪些文件夹）
- 如何识别应接收属性值的文件。您可以使用两种分类机制：

内容分类器

内容分类器会扫描文件内容中的特定文本模式或正则表达式。使用此机制根据文件所包含的内容来识别文件。内容分类器提供了三种匹配文件内容的方法：

- ContentString-搜索不区分大小写的文本字符串。如果您想查找特定的单词或短语，而不考虑大小写，请使用此选项。例如，搜索 “机密” 将匹配 “机密”、“机密” 和 “机密”。
- ContentStringCaseSensitive-搜索区分大小写的文本字符串。当大小写对您的搜索很重要时，请使用此选项。例如，搜索 “SSN” 将匹配 “SSN”，但不匹配 “ssn” 或 “Ssn”。这对于首字母缩略词、产品代码或其他大小写重要的标识符很有用。
- ContentRegularExpression-使用正则表达式搜索模式。当需要匹配复杂模式或可变格式时，请使用此选项。例如，您可以使用正则表达式来检测：
  - 格式为 123-45-6789 的社会安全号码： `\b\d{3}-\d{2}-\d{4}\b`
  - 带有可选空格或破折号的信用卡号： `\b\d{4}[\s-]?\d{4}[\s-]?\d{4}[\s-]?\d{4}\b`
  - 电子邮件地址、电话号码或其他结构化数据

您可以在单个规则中指定多个字符串或模式，如果文件内容与任何指定值相匹配，则将对其进行分类。

文件夹分类器

文件夹分类器根据文件的存储位置分配属性值。使用此机制按文件在文件夹层次结构中的位置对文件进行分类。例如：

- 为 “法律文档” 文件夹中的所有文件设置保留期属性
- 使用项目标识符标记特定项目文件夹中的所有文件

此外，您还可以使用ReevaluateProperty参数来控制在已有该属性值的文件上运行分类时会发生什么。您可以选择以下配置：

- Never-仅对没有此属性值的文件进行分类
- Overwrite-文件更改时替换现有值
- Aggregate-将新值与现有值合并（适用于多值属性）

管理属性

管理属性是应用于文件夹而不是文件的分类属性。您可以使用管理属性来组织和分类文件系统层次结构中的文件夹。与通过分类规则自动分配的文件属性不同，您可以使用 ##-FSx FSRMMgmt ##命令手动设置管理属性。

要对文件夹进行分类，请使用FolderUsage_MS属性。可以指定以下值：

- User Files
- Group Share
- Application Files
- Backup and Archival

跑步分类

您可以通过三种方式运行文件分类：

1. 手动分类-开始-FSx FSRMClassification 用于立即运行分类。这种方法对于测试新规则或执行一次性分类任务非常有用。
2. 计划分类-Set-FSx FSRMClassification 用于配置自动分类的时间表。您可以将分类安排为每周或每月在特定时间运行。计划分类适用于大多数需要定期、可预测的分类运行的生产环境。
3. 连续分类-与Continuous参数Set-FSx FSRMClassification一起使用可启用连续运行的背景分类。连续分类会在新文件和修改文件创建或更改后不久自动对其进行分类。这种方法提供的 up-to-date 分类最多，但会消耗更多的系统资源。

开始分类时，可以指定 a RunDuration 来限制该过程的运行时间。如果分类未在指定时间内完成，则分类将在下次计划运行期间或您再次手动启动时停止并恢复。

分类完成后，您可以在 Windows 文件资源管理器中右键单击文件，选择 “属性”，然后选择 “分类” 选项卡，来查看分配给文件的分类属性。此选项卡显示文件的所有分类属性及其值。

分类流程管理

您可以使用以下命令监视和控制分类过程：

- Get-FSx FSRMClassification-查看分类的当前状态（RunningQueued、NotRunning、或Unknown）
- 停下来-FSx FSRMClassification-停止正在运行或排队的分类作业
- 等等-FSx FSRMClassification-暂停脚本执行，直到分类完成或超时到期

使用这些命令将分类与其他任务协调起来。例如，您可以等待分类完成后再生成依赖于保密文件属性的存储报告。

分类最佳实践

请遵循这些最佳实践，以确保高效和有效的文件分类。

1. 性能注意事项

基于内容的分类是资源密集型的，因为 FSRM 必须读取和扫描文件内容。

- 首先在小型数据集上测试规则-在将分类规则应用于整个文件系统之前，请在具有代表性的文件样本上对其进行测试，以验证它们是否按预期工作，并估计分类需要多长时间。
- 限制内容扫描范围-基于内容的分类是资源密集型的，因为它需要读取文件内容。使用Namespace参数将规则限制在特定的文件夹，而不是扫描整个文件系统。
- 尽可能使用文件夹分类-文件夹分类器比内容分类器快得多，因为它不需要读取文件内容。当可以根据文件位置对文件进行分类时，请使用文件夹分类器而不是内容分类器。
- 在非高峰时段安排分类-在系统活动较少的时段运行计划分类，以最大限度地减少对用户性能的影响。避免在备份窗口或其他维护任务期间运行分类。
- 设置适当的 RunDuration 限制-使用RunDuration参数可防止分类运行时间过长并影响系统性能。如果分类未在时限内完成，则将在下一次计划运行期间恢复。
- 监控分类性能- Get-FSxFSRMClassification 用于检查分类状态并确定分类所需的时间是否超过预期。长期运行的分类可能表明需要优化规则或系统需要更多资源。

2. 规则设计

- 使用特定的正则表达式-使用时`ContentRegularExpression`，写出尽可能具体的模式以避免错误匹配。在生产环境中部署正则表达式之前，请对其进行全面测试。
- 有效地组合多个模式-与其为相似的模式创建单独的规则，不如将它们组合成具有多个`ContentString`或`ContentRegularExpression`值的单个规则。这减少了 FSRM 需要扫描每个文件的次数。
- 排除不必要的文件夹-`Set-FSxFSRMClassification` 使用中的`ExcludeNamespace`参数排除临时目录和其他不需要分类的位置。

3. 物业管理

- 规划您的属性架构-在创建规则之前设计您的分类属性。考虑报告、合规性和文件管理策略需要哪些属性。
- 文档属性定义-使用 “描述” 字段解释每个属性的含义以及应如何使用。这可以帮助其他管理员了解您的分类架构。

4. 持续维护

- 定期查看分类结果-生成存储报告，以验证分类是否按预期运行，以及文件接收的属性值是否正确。
- 根据需要更新规则-随着组织数据管理要求的变化，更新分类规则以反映新的政策或合规性要求。
- 清理未使用的属性-删除不再需要的属性定义和规则，以保持分类配置的可管理性。

分类管理命令

您可以访问四个系列的 FSx 远程 PowerShell 命令来管理文件分类：

1. 属性定义命令-创建和管理分类属性定义，用于指定可以分配给文件的元数据类型。
2. 分类规则命令-创建和管理根据文件内容或位置分配属性值的自动分类规则。
3. 管理属性命令-设置和检索文件夹（而不是文件）的分类属性。
4. 分类过程命令-启动、停止、监控和配置分类过程。

文件分类 FSx远程 PowerShell 命令列表

> **Note**
>
> 本页中的所有示例都假设您已经使用文件系统的 Windows Remote PowerShell 端点定义了该 `$FSxWindowsRemotePowerShellEndpoint`变量。您可以在文件系统的详细信息页面上的 Amazon FSx 控制台中找到此终端节点，也可以使用 Amazon CLI `describe-file-systems`命令找到此终端节点。

属性定义命令

新-FSx FSRMClassification PropertyDefinition

`New-FSxFSRMClassificationPropertyDefinition`：创建可用于对文件进行分类的分类属性定义。属性定义定义了可以通过分类规则分配给文件的属性。

参数：

- `Name (string)` – 必需。属性定义的名称。
- `DisplayName (string)` – 可选。属性定义的显示名称。
- `Description (string)` – 可选。对属性定义的描述。
- `Type (string)` – 必需。分类属性的类型。可以指定以下值：
  - `OrderedList`: 可能值的有序列表
  - `MultiChoice`: 从可能的值中进行多项选择
  - `SingleChoice`: 从可能的值中进行单选
  - `String`: 单个文本字符串
  - `MultiString`: 多个文本字符串
  - `Integer`: 数值
  - `YesNo`: 布尔值
  - `DateTime`: 日期和时间值
- `PossibleValueConfigurations (array)` – 可选。 OrderedList MultiChoice、或 SingleChoice 属性类型的配置数组。每种配置都具有以下属性：
  - `Name (string)`: 值的名称（必填）
  - `Description (string)`: 值的描述（可选）

- Parameters（array）– 可选。"name=value"格式为用于额外配置的字符串数组。

示例：

1。为 PII 数据创建属性列表。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMClassificationPropertyDefinition -Name "ContainsPII" -Type OrderedList -
PossibleValueConfigurations @(
            @{ Name = "Yes" },
            @{ Name = "No" })
}
```

2。为数据敏感度创建有序列表属性。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMClassificationPropertyDefinition -Name "DataSensitivity" -Type
 OrderedList -PossibleValueConfigurations @(
            @{ Name = "Public" },
            @{ Name = "Internal" },
            @{ Name = "Confidential" },
            @{ Name = "Restricted" }
        )
}
```

获取-FSx FSRMClassification PropertyDefinition

Get-FSxFSRMClassificationPropertyDefinition：从您的文件系统中检索一个或多个分类属性定义。

参数：

- Name（array）– 可选。要检索的属性定义名称数组。如果未指定名称，则该命令将返回文件系统上的所有属性定义。

示例：

1。检索文件系统上的所有分类属性定义。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMClassificationPropertyDefinition
}
```

套装-FSx FSRMClassification PropertyDefinition

修改现有分类属性定义的属性。

Parameters

- Name （array）– 必需。要修改的属性名称数组。
- DisplayName （string）– 可选。属性定义的新显示名称。
- Description （string）– 可选。属性定义的新描述。
- PossibleValueConfigurations （array）– 可选。 OrderedList、 MultiChoice或 SingleChoice 属性的新配置阵列。每种配置都具有以下属性：
  - Name （string）: 值的名称（必填）
  - Description （string）: 值的描述（可选）
- Parameters （array）– 可选。“名称=值” 格式的新字符串数组。
- PassThru （boolean）– 可选。如果设置为 true，则返回修改后的属性定义对象。

示例：

1. 使用现有属性定义的描述更新可能的值。

```
$values = [System.Collections.ArrayList]@()
$null = $values.Add(@{
    Name = "High"
    Description = "High Risk Content"
})
$null = $values.Add(@{
    Name = "Medium"
    Description = "Medium Risk Content"
})

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $values -ScriptBlock {
    param($values)
```

```
    Set-FSxFSRMClassificationPropertyDefinition -Name "RiskLevel" -
PossibleValueConfigurations $Using:values -PassThru
}
```

删除-FSx FSRMClassification PropertyDefinition

从文件系统中移除一个或多个分类属性定义。只能删除本地定义的属性定义。

Parameters

- Name (array) – 必需。要删除的属性名称数组。
- PassThru (boolean) – 可选。如果设置为 true，则返回已删除的属性定义对象。

示例：

1. 移除单个属性定义。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Remove-FSxFSRMClassificationPropertyDefinition -Name "RiskLevel" -PassThru
}
```

分类规则命令

新-FSx FSRMClassification 规则

创建自动分类规则，根据指定的标准为文件分配属性值。每条规则都为单个属性设置一个值。

Parameters

- Name (string) – 必需。分类规则的名称。
- Description (string) – 可选。分类规则的描述。
- Property (string) – 必需。要设置的分类属性的名称。必须是现有的属性定义名称。
- PropertyValue (string) – 可选。要分配给属性的值。必须对指定的分类机制有效。
- Namespace (array) – 必需。规则适用的路径或文件夹类型的数组。
- Disabled (boolean) – 可选。如果设置为 true，则创建处于禁用状态的规则。
- ReevaluateProperty (string) – 可选。指定何时重新评估文件。可以指定以下值：

  - Never: 仅评估不存在属性值的文件
  - Overwrite: 重新评估文件何时更改并覆盖现有值
  - Aggregate: 重新评估文件何时更改并与现有值合并
- Flags (array) – 可选。为规则指定特殊行为。可以指定以下值：
  - ClearAutomaticallyClassifiedProperty
  - ClearManuallyClassifiedProperty
  - Deprecated
- ContentRegularExpression (array) – 可选。用于匹配文件内容的正则表达式数组。
- ContentString (array) – 可选。要在文件内容中搜索的不区分大小写的字符串数组。
- ClassificationMechanism (string) – 必需。用于对文件进行分类的机制。可以指定以下值：
  - Content Classifier：扫描文件内容中的特定字符串或正则表达式模式。指定内容分类器时，可以使用 ContentString ContentStringCaseSensitive、或 ContentRegularExpression 参数来定义要搜索的内容。
  - Folder Classifier: 根据文件文件夹位置对文件进行分类
- Parameters (array) – 可选。用于其他配置的"name=value"字符串数组。

示例：

1. 使用正则表达式检测社会安全号码。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMClassificationRule -Name "Detect_SSN" -Property "ContainsPII" -
PropertyValue "Yes" -Namespace "share" -ClassificationMechanism "Content Classifier" -
ContentRegularExpression "\b\d{3}-\d{2}-\d{4}\b"
}
```

2. 使用正则表达式检测信用卡号。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMClassificationRule -Name "Detect_CreditCard" -Property "ContainsPII" -
PropertyValue "Yes" -Namespace "share" -ClassificationMechanism "Content Classifier" -
ContentRegularExpression "\b\d{4}[\s-]?\d{4}[\s-]?\d{4}[\s-]?\d{4}\b"
```

```
}
```

3. 对保留期为 7 年的文件夹下的每个文件进行分类属性。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMClassificationRule -Name "Contracts_Records_7Year" -Property
 "RetentionPeriod" -PropertyValue "7 years" -Namespace "share/Legal Documents" -
ClassificationMechanism "Folder Classifier"
}
```

Get-FSx FSRMClassification 规则

从您的文件系统中检索一个或多个分类规则。

Parameters

- `Name (array)` – 可选。要检索的分类规则名称数组。如果您未指定名称，则该命令将返回文件系统上的所有规则。

示例：

1. 检索文件系统上的所有分类规则。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMClassificationRule
}
```

设定-FSx FSRMClassification 规则

修改现有分类规则的属性。

Parameters

- `Name (array)` – 必需。要修改的分类规则名称数组。
- `Description (string)` – 可选。该规则的新描述。
- `Property (string)` – 可选。要设置的分类属性的名称。
- `PropertyValue (string)` – 可选。要分配给属性的新值。

- Namespace (array) – 可选。该规则适用的新路径或文件夹类型数组。
- Disabled (boolean) – 可选。如果设置为 true，则禁用该规则。如果设置为 false，则启用该规则。
- ReevaluateProperty (string) – 可选。更改重新评估文件的时间。可以指定以下值：
  - Never: 仅评估不存在属性值的文件
  - Overwrite: 重新评估文件何时更改并覆盖现有值
  - Aggregate: 重新评估文件何时更改并与现有值合并
- Flags (array) – 可选。该规则的新特殊行为。可以指定以下值：
  - ClearAutomaticallyClassifiedProperty
  - ClearManuallyClassifiedProperty
  - Deprecated
- ContentRegularExpression (array) – 可选。一个新的正则表达式数组。
- ContentString (array) – 可选。一个新的不区分大小写的搜索字符串数组。
- ContentStringCaseSensitive (array) – 可选。一个新的区分大小写的搜索字符串数组。
- ClassificationMechanism (string) – 可选。一种新的分类机制可供使用。可以指定以下值：
  - Content Classifier：扫描文件内容中的特定字符串或正则表达式模式。指定内容分类器时，可以使用 ContentString ContentStringCaseSensitive、或 ContentRegularExpression参数来定义要搜索的内容。
  - Folder Classifier: 根据文件文件夹位置对文件进行分类
- Parameters (array) – 可选。新的"name=value"配置字符串数组。
- PassThru (boolean) – 可选。如果设置为 true，则返回修改后的规则对象。

示例：

1. 更新现有分类规则的规则属性和命名空间。

```
$namespaces = @("share\finance", "share\accounting")

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $namespaces -ScriptBlock {
    param($namespaces)
    Set-FSxFSRMClassificationRule -Name "Detect_CreditCard" -Description "Updated PII
 detection" -Namespace $Using:namespaces -ReevaluateProperty "Overwrite"
```

```
}
```

移除-FSx FSRMClassification 规则

从您的文件系统中移除一条或多条分类规则。

Parameters

- Name （array）– 必需。要删除的分类规则名称数组。
- PassThru （boolean）– 可选。如果设置为 true，则返回已删除的规则对象。

示例：

1. 移除单个分类规则。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Remove-FSxFSRMClassificationRule -Name "Find Confidential Files" -PassThru
}
```

管理属性命令

获取-FSx FSRMMgmt 属性

从指定文件夹检索管理属性。管理属性是应用于文件夹而不是文件的分类属性。

Parameters

- Namespace （string）– 可选。文件夹的路径。
- Name （string）– 可选。要检索的管理属性的名称。如果您未指定名称，则该命令将检索所有管理属性。
- Recurse （boolean）– 可选。如果设置为 true，则检索命名空间内所有文件夹的管理属性。需要命名空间参数。
- Effective （boolean）– 可选。如果设置为 true，则检索最近具有指定名称的文件夹的管理属性。搜索包括指定的命名空间及其父层次结构。需要名称参数。

示例：

1. 检索文件系统上的所有管理属性。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMMgmtProperty
}
```

2. 检索特定文件夹的管理属性。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMMgmtProperty -Namespace "share\department"
}
```

移除-FSx FSRMMgmt 属性

从指定文件夹中移除管理属性。

Parameters

- Namespace (string) – 可选。文件夹的路径。
- Name (string) – 必需。要删除的管理属性的名称。
- Recurse (boolean) – 可选。如果设置为 true，则删除命名空间内所有文件夹的管理属性。需要命名空间参数。

示例：

1. 移除管理属性的所有实例。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Remove-FSxFSRMMgmtProperty -Name "FolderUsage_MS"
}
```

2. 从特定文件夹中移除管理属性。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Remove-FSxFSRMMgmtProperty -Name "FolderUsage_MS" -Namespace "share\department"
}
```

设置-FSx FSRMMgmt 属性

更改指定命名空间的管理属性的值。管理属性是适用于文件夹且未设置 Secure 标志的分类属性。

Parameters

- `Namespace (string)` – 可选。文件夹路径。
- `Name (string)` – 必需。要修改的管理属性的名称。必须是适用于文件夹的现有分类属性。
- `Value (string)` – 必需。要分配给管理属性的新值。

示例：

1. 设置文件夹使用属性。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Set-FSxFSRMMgmtProperty -Namespace "share\department" -Name "FolderUsage_MS" -Value
 "User Files"
}
```

分类过程命令

Get-FSx FSRMClassification

检索正在运行的文件分类过程的状态。状态可以是以下值之一：

- `Unknown`: 无法确定分类状态
- `NotRunning`: 当前未运行任何分类
- `Queued`: 分类已排队等候启动
- `Running`: 分类目前正在进行中

Parameters

无

示例：

1. 检索当前的分类状态。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMClassification
}
```

开始-FSx FSRMClassification

启动文件分类过程，该过程将分类规则应用于文件并生成分类报告。

Parameters

- Queue （boolean）– 可选。如果设置为 true，则将分类任务添加到队列中，以便在接下来的 5 分钟内运行。在此期间排队的所有任务都将一起运行。如果设置为 false 或未指定，则会立即开始分类。
- RunDuration （number）– 可选。指定取消分类过程之前应运行多少小时。有效值：-1 到 2147483。特殊值：
  - -1: 运行直到取消
  - 0: 运行至完成
  - 如果未指定，则运行直至完成。

示例：

1. 开始分类，没有时间限制。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Start-FSxFSRMClassification -RunDuration 0
}
```

停下来-FSx FSRMClassification

停止文件系统上任何正在运行或排队的分类作业。

Parameters

无

示例：

1. 停止正在运行的分类。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Stop-FSxFSRMClassification
}
```

等等-FSx FSRMClassification

等待文件分类过程完成。当您需要执行依赖于分类完成的操作（例如根据保密文件生成报告）时，请使用此命令。

Parameters

- Timeout（number）– 可选。指定等待分类完成的时间（以秒为单位）。如果超时在分类完成之前过期，则命令会返回，但分类将继续在后台运行。有效值：-1 到 2147483。特殊值：
  - -1: 无限期等待，直到分类完成（默认）
  - 0: 检查当前状态并立即返回，无需等待

示例：

1. 无限期等待分类完成。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Wait-FSxFSRMClassification
}
```

Set-FSx FSRMClassification

修改文件分类的配置设置。

Parameters

- ExcludeNamespace（array）– 可选。要从分类中排除的一系列其他文件夹。
- ScheduleConfigurations（hashtable）– 可选。包含具有以下属性的计划配置的哈希表：
  - Time（datetime）: 指定何时运行任务的 DateTime 对象（必需）
  - RunDuration（number）: 运行任务的小时数（可选）
  - Weekly（array）: 工作日数组（可选）
  - Monthly（array）: 一个月中的几天数组，最后一天使用 -1（可选）

- `Continuous (boolean)` – 可选。如果设置为 true，则启用连续背景分类。
- `PassThru (boolean)` – 可选。如果设置为 true，则返回修改后的分类配置对象。

示例：

1. 启用连续分类。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Set-FSxFSRMClassification -Continuous $true
}
```

2. 设置每周运行分类的时间表。

```
$schedule = @{
    Time = ("12:00am")
    Weekly = @('Monday', 'Wednesday', 'Friday')
}

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $schedule -ScriptBlock {
    param($schedule)
    Set-FSxFSRMClassification -ScheduleConfigurations $schedule
}
```

3. 设置包含自定义排除项的月度计划。

```
$schedule = @{
    Time = ("12:00am")
    Monthly = @(1, 15, -1) # 1st, 15th, and last day
    RunDuration = 4
}
$excludeNamespaces = @("share\folder /s")

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList @($schedule, $excludeNamespaces) -ScriptBlock {
    param($schedule, $excludeNamespaces)
    Set-FSxFSRMClassification -ScheduleConfigurations $schedule -ExcludeNamespace
 $excludeNamespaces
}
```

存储报告

存储报告提供对文件系统使用情况的详细分析，帮助您了解存储的使用情况，识别可以存档或删除的文件，并监控文件管理策略的遵守情况。您可以生成多种类型的报告，用于分析文件所有权、文件类型、重复文件、大文件、文件筛选和配额使用情况。

报告类型

您可以创建以下报告类型：

- `DuplicateFiles`

  根据文件大小和哈希比较来识别内容相同的文件。使用此报告可以查找消耗不必要存储空间的冗余文件。该报告将重复文件组合在一起，并显示通过删除重复文件可以恢复的总空间。

- `FilesByFileGroup`

  按文件组成员资格对文件进行分组，并显示每个文件组的存储消耗情况。使用此报告可以了解哪些类型的文件（文档、媒体、可执行文件等）占用的存储空间最多。

- `FilesByOwner`

  按所有者对文件进行分组，并显示每个用户或组占用的存储空间。使用此报告可以识别占用存储空间最多的用户，并适当地分配存储成本或配额。

- `FilesByProperty`

  按分类属性值对文件进行分组，并显示每个属性值的文件数量和存储消耗。使用此报告可以根据文件分类来分析文件，例如数据敏感度级别、部门或保留期。此报告要求使用对文件进行分类分类规则。

- `FileScreenAuditFiles`

  列出用户试图保存被活动文件屏幕屏蔽的文件的文件筛选违规行为。使用此报告可以监控文件筛选策略的遵守情况，并识别经常尝试保存未经授权的文件类型的用户。

- `FoldersByProperty`

  按管理属性值对文件夹进行分组，并显示每个属性值的存储消耗量。使用此报告可以按文件夹用途分析存储使用情况，例如用户文件、群组共享或应用程序文件。

- `LargeFiles`

  列出超过指定大小阈值的文件。使用此报告可以识别占用大量存储空间且可能成为存档、压缩或删除对象的文件。

- `LeastRecentlyAccessed`

  列出在指定天数内未被访问的文件。使用此报告可以识别可以存档或移动到成本较低的存储层的非活动文件。

- `MostRecentlyAccessed`

  列出在指定天数内访问过的文件。

- `QuotaUsage`

  显示已配置配额的文件夹的配额使用统计信息。使用此报告来监控配额合规性并识别接近配额限制的文件夹。

报告格式

您可以生成多种格式的报告，以适应不同的用例：

- DHTML-动态 HTML 格式，具有排序和过滤等交互功能。
- HTML-适合存档或发送电子邮件的静态 HTML 格式。
- XML-用于编程处理的结构化数据格式。
- CSV-用于导入电子表格应用程序的逗号分隔值格式。
- Text-纯文本格式，便于查看或处理。

您可以为单个报告指定多种格式。

交互式和预定报告

您可以创建两种类型的存储报告：

1. 交互式报告-创建后立即运行，仅执行一次。使用交互式报告进行临时分析或故障排除。交互式报告没有时间表，创建后无法修改。要运行另一个交互式报告，必须使用不同的名称创建一个新报告。
2. 计划报告-根据配置的时间表自动运行。使用计划报告进行定期监控和合规性报告。您可以将报告安排为每周或每月在特定时间运行。可以修改计划报告以更改其配置，也可以使用开始-FSx FSRMStorage 报告命令按需运行这些报告，而无需等待预定时间。

正在运行的报告

创建计划报告后，您可以通过多种方式运行该报告：

- 自动执行-计划报告按其配置的计划时间自动运行。
- 手动执行-用于按开始-FSx FSRMStorage 报告需运行计划报告，无需等待预定时间。

您可以使用来监控报告执行情况获取-FSx FSRMStorage 报告，以检查状态。

访问存储报告

FSRM 生成存储报告后，报告文件将保存到文件系统的默认位置。要访问这些报告，您需要映射文件系统的管理 D$ 共享。

访问存储报告

1. 使用以下路径格式映射管理 D$ 共享：

   ```
   \\file-system-dns-name\D$
   ```

   例如：

   ```
   \\amznfsxaa11bb22.corp.example.com\D$
   ```

2. 导航到该 StorageReports 文件夹。此文件夹包含按报告类型和执行日期组织的子文件夹。

> **Note**
>
> 访问管理 D$ 共享需要管理员凭据。

存储报告最佳实践

请遵循以下最佳做法，确保存储报告的效率和效力：

性能注意事项

存储报告的生成是资源密集型的，因为 FSRM 必须扫描大量文件。

- 限制报告范围-使用Namespace参数将报告限制在特定的文件夹，而不是扫描整个文件系统。扫描大型目录结构需要大量资源，可能需要数小时才能完成。
- 在非高峰时段安排报告-在系统活动较少的时段运行计划报告，以最大限度地减少对性能的影响。避免在备份窗口或其他维护任务期间运行报告。

- 设置合理的阈值-使用阈值参数将报告输出限制为可操作的数据。例如，设置`LargeFileMinimum`为标识值得调查的文件的值，而不是每个超过 1MB 的文件。
- 使用 RunDuration 限制-设置`RunDuration`参数以防止报告运行时间过长并影响系统性能。如果报告未在时限内完成，则将在下次计划运行期间恢复。
- 监控报告性能-用于获取-FSx FSRMStorage 报告检查报告需要多长时间才能完成。如果报告持续时间过长，可以考虑缩小报告范围或降低运行频率。

报告设计

- 使用描述性名称-为报告提供清晰的描述性名称，说明其分析内容和运行时间，例如 “每周大文件-财务共享” 或 “每月重复文件-所有共享”。
- 合并相关分析-为同一个命名空间生成多个报告类型时，请创建具有多个`ReportType`值的单个报告，而不是单独的报告。这样效率更高，因为 FSRM 只需要扫描一次目录结构。
- 按文件模式筛选-使用文件模式参数将报告的重点放在特定的文件类型上。例如，在分析大文件时，您可以为视频文件、数据库文件和存档文件创建单独的报告，以更好地了解存储消耗模式。
- 利用分类属性-使用`FilesByProperty`报告根据文件的分类分析文件。这提供了更有意义的见解。

报告管理

- 定期审查报告-安排时间审查报告结果并对调查结果采取行动。只有当您使用报告来做出存储管理决策时，报告才有价值。
- 存档旧报告-报告文件会随着时间的推移而累积并占用存储空间。为报告文件制定保留政策，删除或存档不再需要的旧报告。
- 计划之前的测试报告-创建交互式报告以测试报告配置，并在创建计划版本之前验证报告配置是否产生预期结果。

存储报告管理命令

您可以访问两个系列的 FSx 远程 PowerShell 命令来管理存储报告：

1. 报告定义命令-创建、检索、修改和删除存储报告配置，这些配置指定要分析的数据、何时运行报告以及要生成的格式。
2. 报告执行命令-启动、停止、监视和等待存储报告生成。使用这些命令按需运行报告或管理长时间运行的报告作业。

存储报告 FSx 远程 PowerShell 命令列表

> **Note**
>
> 本页中的所有示例都假设您已经使用文件系统的 Windows Remote PowerShell 端点定义了该 `$FSxWindowsRemotePowerShellEndpoint`变量。您可以在文件系统的详细信息页面上的 Amazon FSx 控制台中找到此终端节点，也可以使用 Amazon CLI `describe-file-systems`命令找到此终端节点。

报告定义命令

全新-FSx FSRMStorage 报告

新建FSxFSRMStorage报告：创建存储报告，用于分析指定目录以生成一种或多种报告类型。

参数：

- `Name (string)` – 必需。存储报告的名称。
- `Namespace (array)` – 必需。要分析的路径或文件夹类型数组。您可以指定多种格式的路径：
  - 文件夹路径
  - 文件夹分类。例如，[FolderUsage_ms= “用户文件"]
- `ReportType (array)` – 必需。要生成的报告类型数组。可以指定以下值：
  - `DuplicateFiles`：根据文件大小和内容识别重复文件
  - `FilesByFileGroup`: 按文件组成员资格对文件进行分组
  - `FilesByOwner`: 按所有者对文件进行分组
  - `FilesByProperty`: 按分类属性对文件进行分组
  - `FileScreenAuditFiles`: 列出文件筛选违规行为
  - `FoldersByProperty`: 按管理属性对文件夹进行分组
  - `LargeFiles`: 列出超过指定大小阈值的文件
  - `LeastRecentlyAccessed`: 列出最近未被访问过的文件
  - `MostRecentlyAccessed`: 列出最近访问过的文件
  - `QuotaUsage`: 显示配额使用情况统计信息
- `ReportFormat (array)` – 可选。输出格式的数组。可以指定以下值：
  - `DHTML`: 动态 HTML 格式

  - HTML: 静态 HTML 格式
  - XML: XML 格式
  - CSV: 逗号分隔值格式
  - Text: 纯文本格式
- Interactive（boolean）– 可选。如果设置为 true，则生成交互式报告。交互式报表创建后无法修改。
- ScheduleConfigurations（hashtable）-除非报告是交互式的，否则为必填项。包含具有以下属性的计划配置的哈希表：
  - Time（datetime）: 指定何时运行任务的 DateTime 对象（必需）
  - RunDuration（number）: 运行任务的小时数（可选）
  - Weekly（array）: 工作日数组（可选）
  - Monthly（array）: 一个月中的几天数组，-1用于最后一天（可选）

特定于报告的参数：

- FileScreenAuditDaysSince（number）– 可选。对于 FileScreenAuditFiles 报告，请指定包含审计事件的天数。
- FileScreenAuditUser（array）– 可选。对于 FileScreenAuditFiles 报告，指定要包含在报告中的用户帐户数组。只有这些用户违反文件筛选的行为才会包括在内。
- FileGroupIncluded（array）– 可选。对于 FilesByFileGroup 报告，指定要包括哪些文件组。
- FileOwnerFilePattern（string）– 可选。对于 FilesByOwner 报告，指定用于筛选结果的文件模式。
- PropertyName（string）– 可选。对于 FilesByProperty 报告，指定要作为分组依据的分类属性。
- FolderPropertyName（string）– 可选。对于 FoldersByProperty 报告，指定要作为分组依据的文件夹属性。
- PropertyFilePattern（string）– 可选。对于 FilesByProperty 和 FoldersByProperty，指定用于筛选结果的文件模式。
- LargeFileMinimum（number）– 可选。对于 LargeFiles 报告，指定最小文件大小（以字节为单位）。
- LargeFilePattern（string）– 可选。对于 LargeFiles 报告，指定用于筛选结果的文件模式。
- LeastAccessedMinimum（number）– 可选。对于 LeastRecentlyAccessed 报告，请指定自上次访问以来的最小天数。

- LeastAccessedFilePattern（string）– 可选。对于 LeastRecentlyAccessed 报告，指定用于筛选结果的文件模式。
- MostAccessedMaximum（number）– 可选。对于 MostRecentlyAccessed 报告，指定自上次访问以来的最大天数。
- MostAccessedFilePattern（string）– 可选。对于 MostRecentlyAccessed 报告，指定用于筛选结果的文件模式。
- QuotaMinimumUsage（number）– 可选。对于 QuotaUsage 报告，请指定要包括的最低配额使用百分比。

示例：

1. 创建每月大文件报告。

```
$schedule = @{
    Time = ("3:00 AM")
    Monthly = @(1) # Run on first day
}

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $schedule -ScriptBlock {
    param($schedule)
    New-FSxFSRMStorageReport -Name "Monthly Large Files" -Namespace "share
\data" -ReportType "LargeFiles" -LargeFileMinimum 100MB -ReportFormat "HTML" -
ScheduleConfigurations $schedule
}
```

2. 创建包含多种命名空间和格式的每周重复文件报告。

```
$schedule = @{
    Time = ("12:00 AM")
    Weekly = @('Sunday')
    RunDuration = 4
}

$namespaces = @("share\docs", "[FolderUsage_MS=User Files]")
$reportFormats = @("HTML", "CSV")
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList @($schedule, $namespaces, $reportFormats) -ScriptBlock {
    param($schedule, $namespaces, $reportFormats)
```

```
    New-FSxFSRMStorageReport -Name "Weekly Duplicates" -Namespace $namespaces -
ReportType "DuplicateFiles" -ReportFormat $reportFormats -ScheduleConfigurations
 $schedule
}
```

3. 创建可立即运行的交互式报告。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMStorageReport -Name "Find large files" -Namespace "share" -Interactive
 $true -ReportType "QuotaUsage"
}
```

获取-FSx FSRMStorage 报告

获取FSxFSRMStorage报告：从您的文件系统检索一份或多份存储报告。返回有关报告配置和状态的详细信息。

参数：

- Name （array）– 可选。要检索的报告名称数组。如果您未指定名称，则该命令将返回文件系统上的所有存储报告。

示例：

1. 检索文件系统上的所有存储报告。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMStorageReport
}
```

移除-FSx FSRMStorage 举报

删除-FSx FSRMStorage 报告：从您的文件系统中删除一个或多个存储报告。您无法删除当前正在运行的报告。

参数：

- Name （array）– 必需。要删除的报告名称数组。

- PassThru（boolean）– 可选。如果设置为 true，则返回已删除的报表对象。

示例：

1. 移除单个存储报告。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Remove-FSxFSRMStorageReport -Name "Monthly Report" -PassThru
}
```

Set-FSx FSRMStorage Report

Parameters

- Name（array）– 必需。要修改的报告名称数组。
- Namespace（array）– 可选。要分析的路径或文件夹类型数组。您可以指定多种格式的路径：
  - 文件夹路径
  - 文件夹分类。例如，[FolderUsage_ms= “用户文件"]
- ReportType（array）– 可选。要生成的报告类型数组。可以指定以下值：
  - DuplicateFiles：根据文件大小和内容识别重复文件
  - FilesByFileGroup: 按文件组成员资格对文件进行分组
  - FilesByOwner: 按所有者对文件进行分组
  - FilesByProperty: 按分类属性对文件进行分组
  - FileScreenAuditFiles: 列出文件筛选违规行为
  - FoldersByProperty: 按管理属性对文件夹进行分组
  - LargeFiles: 列出超过指定大小阈值的文件
  - LeastRecentlyAccessed: 列出最近未被访问过的文件
  - MostRecentlyAccessed: 列出最近访问过的文件
  - QuotaUsage: 显示配额使用情况统计信息
- ReportFormat（array）– 可选。输出格式的数组。可以指定以下值：
  - DHTML: 动态 HTML 格式
  - HTML: 静态 HTML 格式
  - XML: XML 格式

  - CSV: 逗号分隔值格式
  - Text: 纯文本格式
- ScheduleConfigurations（hashtable)-除非报告是交互式的，否则为必填项。包含具有以下属性的计划配置的哈希表：
  - Time（datetime): 指定何时运行任务的 DateTime 对象（必需）
  - RunDuration（number): 运行任务的小时数（可选）
  - Weekly（array): 工作日数组（可选）
  - Monthly（array): 一个月中的几天数组，-1用于最后一天（可选）
- PassThru（boolean) – 可选。如果设置为 true，则返回修改后的报表对象。

特定于报告的参数

- FileScreenAuditDaysSince（number) – 可选。对于 FileScreenAuditFiles 报告，请指定包含审计事件的天数。
- FileScreenAuditUser（array) – 可选。对于 FileScreenAuditFiles 报告，指定要包含在报告中的用户帐户数组。只有这些用户违反文件筛选的行为才会包括在内。
- FileGroupIncluded（array) – 可选。对于 FilesByFileGroup 报告，指定要包括哪些文件组。
- FileOwnerFilePattern（string) – 可选。对于 FilesByOwner 报告，指定用于筛选结果的文件模式。
- PropertyName（string) – 可选。对于 FilesByProperty 报告，指定要作为分组依据的分类属性。
- FolderPropertyName（string) – 可选。对于 FoldersByProperty 报告，指定要作为分组依据的文件夹属性。
- PropertyFilePattern（string) – 可选。对于 FilesByProperty 和 FoldersByProperty，指定用于筛选结果的文件模式。
- LargeFileMinimum（number) – 可选。对于 LargeFiles 报告，指定最小文件大小（以字节为单位）。
- LargeFilePattern（string) – 可选。对于 LargeFiles 报告，指定用于筛选结果的文件模式。
- LeastAccessedMinimum（number) – 可选。对于 LeastRecentlyAccessed 报告，请指定自上次访问以来的最小天数。
- LeastAccessedFilePattern（string) – 可选。对于 LeastRecentlyAccessed 报告，指定用于筛选结果的文件模式。

- MostAccessedMaximum（number）– 可选。对于 MostRecentlyAccessed 报告，指定自上次访问以来的最大天数。
- MostAccessedFilePattern（string）– 可选。对于 MostRecentlyAccessed 报告，指定用于筛选结果的文件模式。
- QuotaMinimumUsage（number）– 可选。对于 QuotaUsage 报告，请指定要包括的最低配额使用百分比。

示例：

1. 更新现有报告的日程安排和格式。

```
$schedule = @{
    Time = ("3:00 AM")
    Monthly = @(1)
}
$reportFormats = @("HTML", "CSV")

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList @($schedule, $reportFormats) -ScriptBlock {
    param($schedule, $reportFormats)
    Set-FSxFSRMStorageReport -Name "Monthly Report" -ScheduleConfigurations $schedule -
ReportFormat $reportFormats -PassThru
}
```

报告执行命令

开始-FSx FSRMStorage 报告

Parameters

- Name（array）– 必需。要开始的报告名称数组。
- Queue（boolean）– 可选。如果设置为 true，则将报告添加到队列中，以便在接下来的 5 分钟内运行。在此期间排队的所有报告都将一起运行。如果设置为 false 或未指定，则报告将立即启动。
- RunDuration（number）– 可选。指定报告在取消之前应运行多少小时。有效值：-1 到 2147483。特殊值：
  - 0: 运行至完成
  - -1: 运行直到取消

  如果未指定，则运行直至完成。

示例

1. 立即开始提交存储报告。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Start-FSxFSRMStorageReport -Name "Monthly Report"
}
```

2. 对具有持续时间限制的存储报告进行排队。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Start-FSxFSRMStorageReport -Name "Quarterly Report" -Queue: $true -RunDuration 4
}
```

停止-FSx FSRMStorage 举报

Parameters

- Name （array）– 必需。要停止的报告名称数组。

示例：

1. 停止单个存储报告。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Stop-FSxFSRMStorageReport -Name "Monthly Report"
}
```

等着FSxFSRMStorage举报

Parameters

- Name （array）– 必需。要等待的报告名称数组。
- Timeout （number）– 可选。指定报告完成需要等待多长时间（以秒为单位）。如果超时在报告完成之前过期，则命令会返回，但报告生成将继续在后台运行。有效值：-1 到 2147483。特殊值：
  - -1: 无限期等待，直到报告完成（默认）

- 0: 检查当前状态并立即返回，无需等待

示例：

1. 无限期地等待存储报告完成。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Wait-FSxFSRMStorageReport -Name "Monthly Report"
}
```

文件管理任务

亚马逊 FSx 版 Windows 文件服务器不支持 FSRM 文件管理任务。但是，您可以使用具有文件系统网络访问权限的客户端计算机上的本机 PowerShell 命令来实现常见用例，例如数据存档和保留策略。

例如，您可以使用客户端计算机上的 PowerShell 脚本来：

- 根据时间或上次访问时间移动或存档文件
- 删除超过保留期的保密文件
- 根据分类属性将文件复制到存档存储

您可以使用`Get-FsrmClassification`命令访问文件属性并根据值采取操作。

要从客户端 PowerShell 脚本访问 FSRM 分类属性或其他 FSRM 元数据，客户端计算机还必须安装了 FSRM。

FSRM 设置

FSRM 设置提供系统范围的配置，允许您自定义行为并简化功能管理。使用这些设置来控制 FSRM 在文件系统中的运行方式，并设置默认值以简化存储报告和文件筛选等功能的创建和配置。

设置类别

FSRM 设置分为三类：

文件屏幕审计

当用户尝试保存被活动文件屏幕屏蔽的文件时，文件屏幕审计会记录。这些信息对于监控文件筛选策略的遵守情况以及识别经常尝试保存未经授权的文件类型的用户至关重要。

- ReportFileScreenAuditEnable-此设置控制 FSRM 是否记录文件筛选违规行为。如果禁用，FSRM 不会记录文件屏幕违规行为，FileScreenAuditFiles报告也不会显示任何数据。必须启用此设置才能使用文件屏幕审核报告。
- ReportFileScreenAuditDaysSince-此设置提供文件屏幕审核报告的默认时间范围。当您在创建FileScreenAuditFiles报告时没有指定要回顾多久时，FSRM 会使用此值。设置适当的默认值（例如 30 天）可确保报告侧重于最近的违规行为，而不会包含过多的历史数据。
- ReportFileScreenAuditUser-此设置提供要包含在文件屏幕审核报告中的默认用户列表。当您在创建FileScreenAuditFiles报告时未指定要包括哪些用户时，FSRM 会使用此列表。如果为空，则默认情况下，报告将包括所有用户。您可以使用此设置将报告的重点放在特定的用户组或部门上。

默认报告过滤器

默认报告筛选器设置提供了在不指定特定参数的情况下创建存储报告时使用的值。这些默认值简化了报告的创建，并确保了相似报告之间的一致性。

每种报告类型都有相关的默认设置：

- 大文件报告-ReportLargeFileMinimum 设置默认的最小文件大小，并ReportLargeFilePattern设置默认文件模式过滤器。
- 最少访问的文件报告-ReportLeastAccessedMinimum 设置自上次访问以来的默认天数，并ReportLeastAccessedFilePattern设置默认的文件模式过滤器。
- 访问次数最多的文件报告-ReportMostAccessedMaximum 设置自上次访问以来默认的最大天数，并ReportMostAccessedFilePattern设置默认的文件模式过滤器。
- 按所有者列出的文件报告-ReportFileOwnerFilePattern 设置默认文件模式筛选器，并ReportFileOwnerUser设置要包含的默认用户列表。
- 按属性列出的文件报告-ReportPropertyName 设置要分析的默认分类属性，并ReportPropertyFilePattern设置默认的文件模式过滤器。
- 按文件组列出的文件报告-ReportFileGroupIncluded 设置要包含的文件组的默认列表。
- 配额使用情况报告-ReportQuotaMinimumUsage 设置默认的最低配额使用百分比。

创建报告时，您可以通过在报告配置中明确指定参数来覆盖这些默认值中的任何一个。仅当您未指定值时，全局默认值才适用。

报告限制

报告限制设置控制存储报告中包含的最大项目数。这些限制有两个目的：

1. 性能管理-限制报告中的项目数可防止报告花费太长时间生成或消耗过多的系统资源。分析数百万个文件的大型报告可能需要数小时才能完成，并且会影响系统性能。
2. 报告的可用性-包含数千个条目的报告很难审查和分析。报告限制可确保报告始终侧重于最相关的数据。

您可以设置对报告限制的精细控制：

- 总体限制-`ReportLimitMaxFile` 限制任何报告中的文件总数，无论其类型如何。
- Per-report-type 限制-诸如`ReportLimitMaxFileGroup` `ReportLimitMaxOwner`、之类的设置，以及`ReportLimitMaxPropertyValue`限制要包含在特定报告类型中的群组、所有者或属性值的数量。
- 每组限制-诸如`ReportLimitMaxFilesPerFileGroup` `ReportLimitMaxFilesPerOwner`、和之类的设置， `ReportLimitMaxFilesPerPropertyValue`限制报告中每个组中显示多少个文件。

当报告达到限制时，FSRM 会包括占用最多存储空间或与报告类型最相关的项目，并在报告中指出已达到限制。

FSRM 设置命令

您可以访问用于检索和修改全局设置的命令。使用这些命令配置系统范围的 FSRM 行为。

FSRM 设置 FSx 远程命令列表 PowerShell

> **Note**
>
> 本页中的所有示例都假设您已经使用文件系统的 Windows Remote PowerShell 端点定义了该 `$FSxWindowsRemotePowerShellEndpoint`变量。您可以在文件系统的详细信息页面上的 Amazon FSx 控制台中找到此终端节点，也可以使用 Amazon CLI `describe-file-systems`命令找到此终端节点。

Get-FSx FSRMSetting

Get-FSxFSRMSetting：检索文件系统上的当前文件服务器资源管理器设置。仅返回可以使用 Set-修改的设置FSxFSRMSetting。

参数：

无

示例：

1. 检索所有当前的 FSRM 设置。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
Get-FSxFSRMSetting
}
```

Set-FSx FSRMSetting

Set-FSxFSRMSetting：修改文件系统上的全局文件服务器资源管理器设置。这些设置为存储报告提供默认值并控制 FSRM 行为。

参数：

文件屏幕审核设置：

- ReportFileScreenAuditEnable（boolean）– 可选。控制文件筛选审计事件是否包含在 FSRM 报告中。
- ReportFileScreenAuditDaysSince（number）– 可选。生成 FileScreenAuditFiles 报告时查看文件筛选违规行为的默认天数。
- ReportFileScreenAuditUser（array）– 可选。要包含在 FileScreenAuditFiles 报告中的默认用户帐户列表的数组。

默认报告筛选器设置：

- ReportFileGroupIncluded（array）– 可选。默认情况下要包含在报告中的文件组名称数组。
- ReportFileOwnerFilePattern（string）– 可选。所有者报告的默认文件模式。支持通配符（*和？）。

- ReportFileOwnerUser（array）– 可选。所有者报告的文件采用 “域\ 用户” 格式的用户数组。
- ReportLargeFileMinimum（number）– 可选。大文件报告的默认最小文件大小（以字节为单位）。
- ReportLargeFilePattern（string）– 可选。大文件报告的默认文件模式。支持通配符（*和?）。
- ReportLeastAccessedFilePattern（string）– 可选。访问量最少的文件报告的默认文件模式。支持通配符（*和?）。
- ReportLeastAccessedMinimum（number）– 可选。自上次访问次数最少的文件报告以来默认的最小天数。
- ReportMostAccessedFilePattern（string）– 可选。访问量最大的文件报告的默认文件模式。支持通配符（*和?）。
- ReportMostAccessedMaximum（number）– 可选。自上次访问量最大的文件报告以来默认的最大天数。
- ReportPropertyFilePattern（string）– 可选。属性报告的默认文件模式。支持通配符（*和?）。
- ReportPropertyName（string）– 可选。属性报告的默认属性名称。
- ReportQuotaMinimumUsage（number）– 可选。配额使用情况报告的默认最低配额使用百分比。

报告限制设置：

- ReportLimitMaxDuplicateGroup（number）– 可选。重复文件报告中包含的重复文件组的最大数量。
- ReportLimitMaxFile（number）– 可选。存储报告中包含的最大文件数。
- ReportLimitMaxFileGroup（number）– 可选。要包含在报告中的文件组的最大数量。
- ReportLimitMaxFileScreenEvent（number）– 可选。文件屏幕审核报告中包含的最大文件屏幕事件数。
- ReportLimitMaxFilesPerDuplicateGroup（number）– 可选。重复文件报告中每个重复组的最大文件数。
- ReportLimitMaxFilesPerFileGroup（number）– 可选。按文件组报告列出的文件中每个文件组的最大文件数。
- ReportLimitMaxFilesPerOwner（number）– 可选。所有者报告中的文件中每个所有者的最大文件数。

- ReportLimitMaxFilesPerPropertyValue (number) – 可选。按属性报告列出的文件中每个属性值的最大文件数。
- ReportLimitMaxOwner (number) – 可选。按所有者报告在文件中包含的最大所有者数量。
- ReportLimitMaxPropertyValue (number) – 可选。属性报告中要包含在文件中的属性值的最大数量。
- ReportLimitMaxQuota (number) – 可选。要包含在配额使用情况报告中的最大配额数。

其他设置：

- PassThru (boolean) – 可选。如果设置为 true，则返回修改后的设置对象。

示例：

1. 使用 30 天历史记录配置默认文件屏幕审计。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Set-FSxFSRMSetting -ReportFileScreenAuditDaysSince 30 -PassThru
}
```

2. 配置默认的大文件报告设置。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Set-FSxFSRMSetting -ReportLargeFileMinimum 100MB -ReportLargeFilePattern "*.iso"
 -PassThru
}
```

事件日志

当您在文件系统上启用 FSRM 时， Amazon FSx Windows 文件服务器会生成文件管理活动的事件日志，并将其发送到您配置的目标（Amazon CloudWatch 日志或 Amazon Kinesis Data Firehose）。这些日志可帮助您监控 FSRM 操作、解决问题并维护文件管理活动的审计跟踪。

FSRM 记录了什么

当您在文件系统上启用 FSRM 时， Amazon FSx Windows 文件服务器会记录事件并将其发送到您配置的目的地。将记录以下事件：

- 文件筛选违规-当用户尝试保存由具有事件通知操作的文件屏幕监控的文件时
- 配额阈值通知-当配额使用量达到具有事件通知操作的配置阈值时
- FSRM 服务事件-确认通知设置、服务错误和操作故障

访问 FSRM 日志

访问 FSRM 日志的位置取决于您在启用 FSRM 时配置的目标：

CloudWatch 日志

导航到您指定的 CloudWatch 日志组，在日志控制台中查看日志。您可以使用 Logs Insights 搜索、筛选和分析 CloudWatch 日志，并设置 CloudWatch 警报以通知您特定事件。

Kinesis Data Firehose

日志将传送到您的 Kinesis Data Firehose 传输流中配置的目标，例如亚马逊 S3 Amazon 、Redshift 或服务。 Amazon OpenSearch 您可以使用与您的交付流集成的工具和服务来处理和分析日志。

常见使用案例

本主题提供了文件服务器资源管理器常见任务的 step-by-step示例。这些示例演示了如何使用和实现 FSRM 功能来解决典型的文件管理难题。

> **Note**
>
> 本页中的所有示例都假设您已经使用文件系统的 Windows Remote PowerShell 端点定义了该 `$FSxWindowsRemotePowerShellEndpoint`变量。您可以在文件系统的详细信息页面上的 Amazon FSx 控制台中找到此终端节点，也可以使用 Amazon CLI `describe-file-systems`命令找到此终端节点。

为文件夹设置硬配额

此示例说明如何创建硬配额，防止用户在 “部门” 文件夹中存储超过 10 GB 的空间。

要为文件夹设置配额，请执行以下操作：

1. 创建限制为 10 GB 的硬配额：

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMQuota -Folder "share\department" -Size 10GB -Description "10 GB hard
 limit for department folder"
}
```

2. （可选）修改配额以添加使用率为 85% 的阈值通知：

```
$thresholds = [System.Collections.ArrayList]@()
$threshold = @{
    ThresholdPercentage = 85
    Action = @(
        @{
            ActionType = "Event"
            EventType = "Warning"
            MessageBody = "Department folder has reached 85% of quota limit"
        }
    )
}

$null = $thresholds.Add($threshold)

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList ($thresholds) -ScriptBlock {
    param($thresholds)
    Set-FSxFSRMQuota -Folder "share\department" -ThresholdConfigurations
 $Using:thresholds
}
```

3. 验证配额是否已创建：

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMQuota -Folder "share\department"
}
```

使用文件组限制特定的文件类型

此示例说明如何使用默认 “Audio and Video Files” 文件组阻止用户将音频和视频文件保存到业务文档文件夹。

要使用文件组限制文件类型，请执行以下操作：

1. 创建一个屏蔽音频和视频文件的活动文件屏幕：

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
New-FSxFSRMFileScreen -Folder "share\business-documents" -IncludeGroup "Audio and
 Video Files" -Description "Block media files in business documents folder"
}
```

2. （可选）更新文件屏幕，以便在用户尝试保存被阻止的文件时添加通知：

```
$notifications = [System.Collections.ArrayList]@()

$eventNotification = @{
    ActionType = "Event"
    EventType = "Warning"
    MessageBody = "User attempted to save blocked media file"
}
$null = $notifications.Add($eventNotification)

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $notifications -ScriptBlock {
    param($notifications)
    Set-FSxFSRMFileScreen -Folder "share\business-documents" -
NotificationConfigurations $Using:notifications
}
```

3. 验证文件屏幕是否已创建：

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMFileScreen -Folder "share\business-documents"
}
```

识别和分类 PII 数据

此示例说明如何自动识别包含社会安全号码的文件并将其归类为包含个人身份信息 (PII) 的文件。

要识别和分类 PII 数据，请执行以下操作：

1. 为 PII 创建分类属性：

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMClassificationPropertyDefinition -Name "ContainsPII" -Type
 OrderedList -PossibleValueConfigurations @(
        @{ Name = "Yes" },
        @{ Name = "No" })
}
```

2. 创建分类规则以检测社会安全号码：

> **Note**
>
> 以下正则表达式将在文件中搜索带有该模式的文本 XXX-XX-XXXX。对于生产用途，可以考虑使用更复杂的模式或组合多种检测方法。

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMClassificationRule -Name "Detect_SSN" -Property "ContainsPII"
 -PropertyValue "Yes" -Namespace "share" -ClassificationMechanism "Content
 Classifier" -ContentRegularExpression "\b\d{3}-\d{2}-\d{4}\b"
}
```

3. 运行分类：

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Start-FSxFSRMClassification
}
```

4. （可选）配置连续分类以自动对新文件进行分类：

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Set-FSxFSRMClassification -Continuous $true
}
```

5. 检查状态（1 表示已完成）：

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMClassification
}
```

6. 分类完成后，您可以通过在 Windows 文件资源管理器中右键单击文件，选择属性，然后选择分类选项卡，来查看分配给文件的分类属性。此选项卡显示文件的所有分类属性及其值。

为文件创建保留策略

此示例说明如何根据文件的文件夹位置按保留期对文件进行分类，然后您可以将其与客户端 PowerShell 脚本一起用于存档或删除文件。

要为文件创建保留策略，请执行以下操作：

1. 为保留期创建分类属性：

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMClassificationPropertyDefinition -Name "RetentionPeriod" -Type
 String -Description "File retention period"
}
```

2. 为不同的保留期创建分类规则：

   - “法律文件” 文件夹下的法律文件保留 7 年：

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -
ConfigurationName FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMClassificationRule -Name "Legal_7Year" -Property
 "RetentionPeriod" -PropertyValue "7 years" -Namespace "share/Legal Documents" -
ClassificationMechanism "Folder Classifier"
}
```

   - “财务：” 文件夹下的财务记录保留 3 年

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -
ConfigurationName FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMClassificationRule -Name "Finance_3Year" -Property
 "RetentionPeriod" -PropertyValue "3 years" -Namespace "share/Finance" -
ClassificationMechanism "Folder Classifier"
```

```
}
```

您还可以按文件内容进行分类并搜索诸如 “保留期七年” 之类的字符串。为此，请使用`ClassificationMechanism "Content Classifier"`和`ContentString "Retention seven years"`。

3. 运行分类以应用保留属性：

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Start-FSxFSRMClassification
}
```

4. （可选）配置连续分类以自动对新文件进行分类：

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Set-FSxFSRMClassification -Continuous $true
}
```

5. 检查状态（1 表示已完成）：

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMClassification
}
```

6. 分类完成后，您可以通过在 Windows 文件资源管理器中右键单击文件，选择属性，然后选择分类选项卡，来查看分配给文件的分类属性。此选项卡显示文件的所有分类属性及其值。
7. 根据保留期对文件进行分类后，您可以使用客户端 PowerShell 脚本根据文件的`RetentionPeriod`属性和期限对其进行存档或删除。例如，您可以扫描文件系统并将文件的保存期限与其保留期分类进行比较。有关更多信息，请参阅 文件管理任务。

设置常用存储报告

本节介绍如何创建两个常用的存储报告：大文件报告和所有者文件报告。

大文件报告

此示例创建一个月度报告，用于识别大于 200 MB 的文件。

要创建大文件报告，请执行以下操作：

1. 创建计划的大文件报告：

```
$schedule = @{
    Time = "2:00 AM"
    Monthly = @(1) # Run on the 1st of each month
}

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $schedule -ScriptBlock {
    param($schedule)
    New-FSxFSRMStorageReport -Name "Monthly Large Files Report" -Namespace "share"
 -ReportType "LargeFiles" -LargeFileMinimum 200MB -ReportFormat "HTML","CSV" -
ScheduleConfigurations $schedule
}
```

2. （可选）立即运行报告进行测试：

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Start-FSxFSRMStorageReport -Name "Monthly Large Files Report"
}
```

按所有者列出的文件报告

此示例创建每周报告，显示用户的存储消耗情况。

要按所有者报告创建文件，请执行以下操作：

1. 按所有者报告创建预定文件：

```
$schedule = @{
    Time = "3:00 AM"
    Weekly = @('Sunday')
}

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ArgumentList $schedule -ScriptBlock {
    param($schedule)
```

```
    New-FSxFSRMStorageReport -Name "Weekly Files by Owner Report" -
Namespace "share" -ReportType "FilesByOwner" -ReportFormat "HTML","CSV" -
ScheduleConfigurations $schedule
}
```

2. （可选）立即运行报告进行测试：

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock {
    Start-FSxFSRMStorageReport -Name "Weekly Files by Owner Report"
}
```

通过映射管理 D$ 共享来访问生成的报告。有关更多信息，请访问访问存储报告。

管理 FSx for Windows File Server 上的存储

文件系统的存储配置包括预置存储容量、存储类型，以及存储类型为固态硬盘（SSD）时的 SSD IOPS 数量。可以在创建文件系统时以及创建之后，配置这些资源以及文件系统吞吐能力，以实现工作负载所需的性能。通过浏览以下主题，了解如何使用 Amazon Web Services 管理控制台、Amazon CLI 和 Amazon FSx CLI for Remote Management on Powershell 来管理文件系统的存储以及与存储相关的性能。

主题

- 优化存储成本
- 管理存储容量
- 管理文件系统存储类型
- 管理 SSD IOPS
- 通过重复数据删除来降低存储成本
- 管理存储配额
- 增加文件系统存储容量
- 监控存储容量增加
- 动态增加 FSx for Windows File Server 文件系统的存储容量
- 更新 FSx for Windows 文件系统的存储类型
- 监控存储类型更新
- 更新文件系统的 SSD IOPS

- 监控预置的 SSD IOPS 更新
- 管理重复数据删除
- 重复数据删除问题排查

优化存储成本

可以使用 FSx for Windows 提供的存储配置选项来优化存储成本。

存储类型选项 - FSx for Windows File Server 提供两个存储类型 – 硬盘驱动器（HDD）和固态硬盘（SSD），使您能够优化性价比以满足工作负载需求。HDD 存储专为各种工作负载而设计，包括主目录、用户和部门共享以及内容管理系统。SSD 存储专为性能最高、对延迟最敏感的工作负载而设计，包括数据库、媒体处理工作负载和数据分析应用程序。有关存储类型和文件系统性能的更多信息，请参阅 FSx for Windows File Server 性能。

重复数据删除 - 大型数据集中通常存在冗余数据，这会增加数据存储成本。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在各个内部版本中都保持不变的二进制文件。您可以通过为文件系统开启重复数据删除功能来降低数据存储成本。开启后，重复数据删除只存储一次数据集的重复部分，从而自动减少或消除多余的数据。有关重复数据删除以及如何为 Amazon FSx 文件系统轻松启用重复数据删除功能的更多信息，请参阅 通过重复数据删除来降低存储成本。

管理存储容量

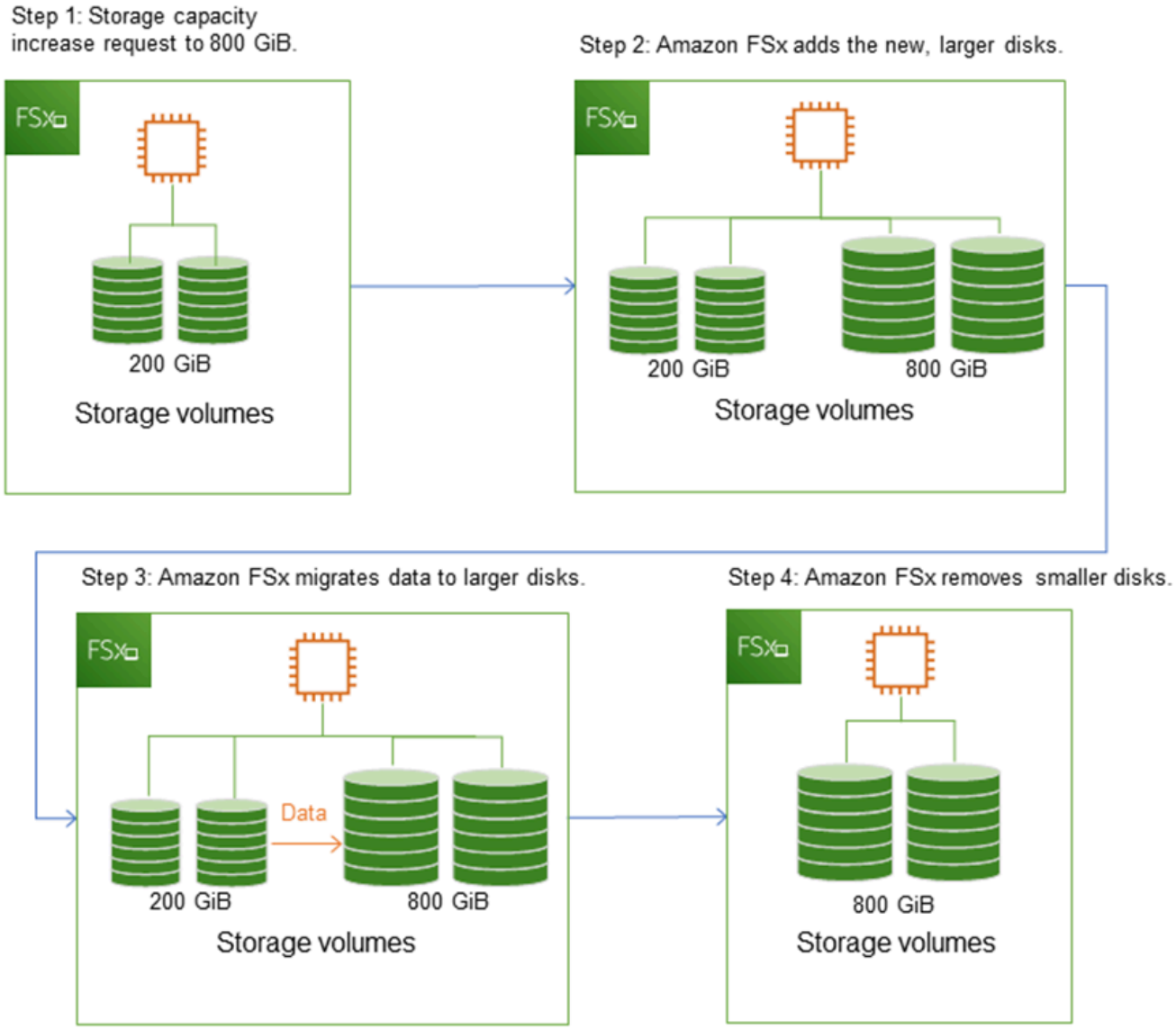
您可以随着存储要求的变化增加 FSx for Windows 文件系统的存储容量。您可以使用 Amazon FSx 控制台、Amazon RDS API 或 Amazon Command Line Interface（Amazon CLI）来实现。计划增加存储容量时需要考虑的因素包括了解何时需要增加存储容量、了解 Amazon FSx 如何处理存储容量的增加以及跟踪存储增加请求的进度。您可以仅增加文件系统的存储容量；不得减少存储容量。

> **Note**
>
> 对于 2019 年 6 月 23 日之前创建的文件系统，或者从 2019 年 6 月 23 日之前创建的文件系统的备份中恢复的文件系统，无法增加其存储容量。

增加 Amazon FSx 文件系统的存储容量时，Amazon FSx 会在后台为文件系统添加一组容量更大的新磁盘。然后，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磁盘。根据存储类型和其他因素，存储优化可能需要几小时到几天的时间，对工作负载性能的影响微乎其微。在此优化期间，备份使用率会暂时增加，因为文件系统级备份中既包含旧存储卷也包含新存储卷。包含这两

组存储卷是为了确保 Amazon FSx 即使在存储扩展活动期间也能成功获取备份以及从备份中恢复。备份历史记录中不再包含旧存储卷后，备份使用率将恢复到之前的基准水平。新存储容量可用后，您只需为新存储容量付费。

下图显示了 Amazon FSx 在增加文件系统存储容量时采用的四个主要步骤。



您可以随时使用 Amazon FSx 控制台、CLI 或 API 跟踪存储优化、SSD 存储容量增加或 SSD IOPS 更新的进度。有关更多信息，请参阅 监控存储容量增加。

有关增加文件系统存储容量的需知事项

以下是增加存储容量时需要考虑的几个重要事项：

- 仅增加：您可以仅增加文件系统的存储容量；不得减少存储容量。
- 最低增量：每次增加的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 65536GiB。
- 最低吞吐能力：要增加存储容量，文件系统的最低吞吐能力必须为 16MBps。这是因为存储优化步骤是一个吞吐量密集型过程。
- 两次增加的间隔时间：在上次增加请求后 6 小时或存储优化过程完成（以较长的时间为准）之前，无法进一步增加文件系统的存储容量。存储优化可能需要几个小时到几天的时间才能完成。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先增加文件系统的吞吐能力（在存储扩展完成之后可以缩减吞吐能力），并在文件系统上流量最低时增加存储容量。

> **Note**
>
> 某些文件系统事件可能会消耗磁盘 I/O 性能资源。例如：
> 存储容量扩展的优化阶段可能会增加磁盘吞吐量，并可能导致性能警告。有关更多信息，请参阅 性能警告和建议。

知道何时增加存储容量

当文件系统的可用存储容量不足时，请增加其存储容量。使用 `FreeStorageCapacity` CloudWatch 指标来监控文件系统上的可用存储容量。您可以根据此指标创建 Amazon CloudWatch 警报，并在指标降至特定阈值以下时收到通知。有关更多信息，请参阅 使用 Amazon CloudWatch 监控。

我们建议在文件系统上始终保持至少 20% 的可用存储容量。使用所有存储容量可能会对性能产生负面影响，并可能会导致数据不一致。

可用存储容量低于您指定的定义阈值时，您可以自动增加文件系统的存储容量。使用 Amazon 开发的自定义 Amazon CloudFormation 模板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。

增加存储容量并提升文件系统性能

新存储容量可用后，Amazon FSx 会在后台运行存储优化流程，对大多数工作负载性能的影响微乎其微。但是，使用 HDD 存储类型的文件系统，以及涉及大量终端用户、高 I/O 级别或包含大量小文件的

数据集的工作负载，可能会暂时出现性能下降的情况。对于这些情况，我们建议您先提高文件系统的吞吐能力，然后再增加存储容量。对于这些类型的工作负载，我们还建议在文件系统负载较低的空闲时段更改吞吐能力。这使您能够继续提供相同级别的吞吐量，满足应用程序的性能需求。有关更多信息，请参阅 管理吞吐能力。

管理文件系统存储类型

可以使用 Amazon Web Services 管理控制台 和 Amazon CLI 将文件系统存储类型从 HDD 更改为 SSD。将存储类型更改为 SSD 时，请注意，在上次请求更新后 6 小时或存储优化过程完成（以较长的时间为准）之前，无法再次更新文件系统配置。存储优化可能需要几小时到几天才能完成。为了最大限度地缩短这段时间，我们建议您在文件系统上的流量最小时更新存储类型。有关更多信息，请参阅 更新 FSx for Windows 文件系统的存储类型。

无法将文件系统存储类型从 SSD 更改为 HDD。如果要将文件系统的存储类型从 SSD 更改为 HDD，则需要将文件系统的备份还原到配置为使用 HDD 存储的新文件系统。有关更多信息，请参阅 将备份还原至新文件系统。

关于存储类型

您可以将 FSx for Windows File Server 文件系统配置为使用固态硬盘（SSD）或磁性硬盘驱动器（HDD）存储类型。

SSD 存储适用于大多数具有高性能要求和延迟敏感性的生产工作负载。这些工作负载的示例包括数据库、数据分析、媒体处理和业务应用程序。对于涉及大量最终用户、高 I/O 级别或包含大量小文件的数据集的使用案例，我们也建议使用 SSD。最后，如果您计划启用影子副本，我们建议您使用 SSD 存储。SSD 存储文件系统可配置和扩展 SSD IOPS，但 HDD 存储不能。

HDD 存储专为各种工作负载而设计，包括主目录、用户和部门文件共享以及内容管理系统。与 SSD 存储相比，HDD 存储的成本更低，但延迟更高，单位存储磁盘吞吐量和磁盘 IOPS 也更低。它可能适用于 I/O 要求较低的通用用户共享和主目录、不经常检索数据的大型内容管理系统（CMS）或包含少量大文件的数据集。

有关更多信息，请参阅 存储配置和性能。

管理 SSD IOPS

对于配置了 SSD 存储的文件系统，SSD IOPS 的数量决定了文件系统从磁盘读取数据以及向磁盘写入数据时的可用磁盘 I/O 数量，而不是缓存中的数据。您可以独立于存储容量选择和扩展 IOPS 数量。您可以预置的最大 SSD IOPS 取决于您为文件系统选择的存储容量和吞吐能力。如果您尝试将 SSD

IOPS 提高到超出吞吐能力支持的上限，则可能需要增加吞吐能力才能获得这一级别的 SSD IOPS。有关更多信息，请参阅 FSx for Windows File Server 性能 和 管理吞吐能力。

以下是更新文件系统的预置 SSD IOPS 时需要了解的几个重要事项：

- 选择 IOPS 模式 - 有以下两种 IOPS 模式可供选择：
  - 自动 – 选择此模式时，Amazon FSx 会自动扩展 SSD IOPS，保持每 GiB 存储容量 3 SSD IOPS，每个文件系统最多保持 40 万 SSD IOPS。
  - 用户预置 – 选择此模式可以指定 SSD IOPS 的数量，范围在 96 - 40 万之间。为所有推出 Amazon FSx 的 Amazon Web Services 区域 指定每 GiB 存储容量 3–50 IOPS，或者在美国东部（弗吉尼亚州北部）、美国西部（俄勒冈州）、美国东部（俄亥俄州）、欧洲地区（爱尔兰）、亚太地区（东京）和亚太地区（新加坡）指定每 GiB 存储容量 3–500 IOPS。当选择用户预置的模式，且指定的 SSD IOPS 数量未达到每 GiB 至少 3 IOPS 的要求，请求将失败。对于更高级别的预置 SSD IOPS，如果每个文件系统每 GiB 的平均 IOPS 超过 3，则需付费。
- 存储容量更新 - 如果增加了文件系统的存储容量，而在默认情况下，所需的 SSD IOPS 数量大于当前用户预置的 SSD IOPS 级别，则 Amazon FSx 会自动将文件系统切换到“自动”模式，此时文件系统可满足每 GiB 存储容量 3 SSD IOPS 的最低要求。
- 吞吐能力更新 – 如果您提高了吞吐能力，且新吞吐能力支持的最大 SSD IOPS 高于用户预置的 SSD IOPS 级别，则 Amazon FSx 会自动将您的文件系统切换到自动模式。
- 增加 SSD IOPS 频率 – 在上次增加请求后 6 小时，或存储优化过程完成（以较长的时间为准）之前，无法进一步提高文件系统的 SSD IOPS、增加文件系统的吞吐能力或更新文件系统的存储类型。存储优化可能需要几个小时到几天的时间才能完成。为了最大限度地缩短完成存储优化所需的时间，我们建议在文件系统流量最小的时候扩展 SSD IOPS。

> **Note**
>
> 请注意，仅以下 Amazon Web Services 区域 支持 4608 MBps 及以上级别吞吐能力：美国东部（弗吉尼亚州北部）、美国西部（俄勒冈州）、美国东部（俄亥俄州）、欧洲地区（爱尔兰）、亚太地区（东京）和亚太地区（新加坡）。

有关如何更新 FSx for Windows File Server 文件系统的预置 SSD IOPS 数量的更多信息，请参阅 更新文件系统的 SSD IOPS。

通过重复数据删除来降低存储成本

重复数据删除（通常简称为数据删重）有助于存储管理员降低与重复数据相关的成本。您可以使用 FSx for Windows File Server 来识别和消除冗余数据。大型数据集中通常存在冗余数据，这会增加数据存储成本。例如：

- 用户文件共享可能有多个相同或相似的文件副本。
- 软件开发共享可以有多个在各个内部版本中都保持不变的二进制文件。

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。重复数据删除只存储一次数据集的重复部分，从而减少或消除多余的数据。启用重复数据删除时默认启用数据压缩，从而在删除重复数据后进行数据压缩，以进一步节省空间。重复数据删除可优化冗余，而不会影响数据的保真度或完整性。重复数据删除会作为后台进程运行，能够持续、自动地扫描和优化您的文件系统，并且这对您的用户和连接的客户端是透明的。

能够通过重复数据删除节省的存储容量取决于数据集的性质，包括文件之间存在的重复数据量。通用文件共享通常可节省 50-60% 的成本。在共享中，节省范围为用户文档的 30–50% 到软件开发数据集的 70–80%。您可以使用 `Measure-FSxDedupFileMetadata` 远程 PowerShell 命令来衡量重复数据删除可能实现的节省量。

您还可以自定义重复数据删除以满足您的特定存储需求。例如，您可以将其配置为仅在特定文件类型上运行重复数据删除，也可以创建自定义作业计划。由于重复数据删除作业会消耗文件服务器资源，因此我们建议使用 `Get-FSxDedupStatus` 来监控重复数据删除作业的状态。

有关在文件系统上配置重复数据删除的信息，请参阅 管理重复数据删除。

有关解决重复数据删除相关问题的信息，请参阅

使用以下信息帮助排查配置和使用重复数据删除时产生的一些常见问题。

主题

- 重复数据删除不起作用
- 重复数据删除值意外设置为 0
- 删除文件后，文件系统上的空间未被释放

重复数据删除不起作用

要查看重复数据删除的当前状态，请运行 `Get-FSxDedupStatus` PowerShell 命令查看最新重复数据删除作业的完成状态。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。

重复数据删除作业失败的最常见原因是内存不足。

- Microsoft 建议最好每 1 TB 的逻辑数据有 1 GB 的内存（或者每 1 TB 的逻辑数据至少有 350 MB 的内存）。使用 Amazon FSx 性能表来确定与文件系统的吞吐能力关联的内存，并确保内存资源足以容纳您的数据大小。如果不够，则需要提高文件系统的吞吐能力，使其满足每 1 TB 逻辑数据提供 1 GB 内存的要求。
- 重复数据删除作业使用 Windows 推荐的默认 25% 内存分配配置，这意味着对于具有 32 GB 内存的文件系统，8 GB 可用于重复数据删除。内存分配是可配置的（使用带 `-Memory` 参数的 `Set-FSxDedupSchedule` 命令）。请注意，为重复数据删除使用较高的内存分配可能会影响文件系统的性能。
- 您可以修改重复数据删除作业的配置，以降低内存需求量。例如，您可以将优化限制为针对特定文件类型或文件夹运行，或者设置优化的最小文件大小和期限。我们还建议将重复数据删除作业配置为在文件系统负载最小的空闲期间运行。

如果重复数据删除作业没有足够的时间完成，也可能会出错。您可能需要更改作业的最长持续时间，如修改重复数据删除计划 中所述。

如果重复数据删除作业已经失败了很长时间，并且在此期间文件系统上的数据发生了变化，那么后续的重复数据删除作业可能需要更多资源才能首次成功完成。

重复数据删除值意外设置为 0

对于已配置重复数据删除的文件系统，`SavedSpace` 和 `OptimizedFilesSavingsRate` 的值意外设为 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当前的重复数据删除作业，该过程会将数据从旧磁盘迁移到更大的新磁盘。存储优化作业完成后，Amazon FSx 将恢复文件系统的重复数据删除。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。

删除文件后，文件系统上的空间未被释放

重复数据删除的预期行为是，如果删除的数据是重复数据删除节省空间的内容，那么文件系统上的空间实际上要在垃圾回收作业运行后才会释放。

您可能会发现，将计划设置为在删除大量文件后立即运行垃圾回收作业很有用。垃圾回收作业完成后，您可以将垃圾回收计划恢复回其原始设置。这便可以确保您能立即快速查看删除内容释放的空间。

按照以下步骤将垃圾回收作业设置为 5 分钟后运行。

1. 要验证是否启用了重复数据删除，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。

2. 按照以下步骤将计划设置为垃圾回收作业在从现在起 5 分钟后运行。

```
$FiveMinutesFromNowUTC = ((get-date).AddMinutes(5)).ToUniversalTime()
$DayOfWeek = $FiveMinutesFromNowUTC.DayOfWeek
$Time = $FiveMinutesFromNowUTC.ToString("HH:mm")

Invoke-Command -ComputerName ${RPS_ENDPOINT} -ConfigurationName FSxRemoteAdmin -
ScriptBlock {
    Set-FSxDedupSchedule -Name "WeeklyGarbageCollection" -Days $Using:DayOfWeek -
Start $Using:Time -DurationHours 9
}
```

3. 在运行垃圾回收作业并释放空间后，将计划恢复回其原始设置。

。

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。

> **Warning**
>
> 我们不建议您运行某些带有重复数据删除功能的 Robocopy 命令，因为这些命令可能会影响 Chunk Store 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。

使用重复数据删除的最佳实践

以下是使用重复数据删除的一些最佳实践：

- 将重复数据删除作业安排在文件系统空闲时运行：默认计划包括每周六 2:45 UTC 进行 `GarbageCollection` 作业。如果您的文件系统中有大量数据流失，则可能需要几个小时才能完成。如果此时间不适合您的工作负载，请将此作业安排在您预计文件系统流量较低的时候运行。

- 为完成重复数据删除配置足够的吞吐能力：更高的吞吐能力可提供更高级别的内存。Microsoft 建议每 1 TB 逻辑数据有 1 GB 的内存来运行重复数据删除。使用 Amazon FSx 性能表来确定与文件系统的吞吐能力关联的内存，并确保内存资源足以容纳您的数据大小。
- 自定义重复数据删除设置以满足您的特定存储需求并降低性能要求：您可以将优化限制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期限以进行优化。要了解更多信息，请参阅 通过重复数据删除来降低存储成本。

管理存储配额

您可以在文件系统上配置用户存储配额，以限制用户可以消耗的数据存储量。设置配额后，您可以通过跟踪配额状态来监控使用情况，并查看用户在何时超过其配额。

您还可以通过阻止达到配额的用户向存储空间执行写入操作来强制实施限额。当您强制实施限额时，超过其配额的用户就会收到“磁盘空间不足”的错误消息。

您可以为配额设置设定以下阈值：

- 警告 – 用于跟踪用户或组是否即将达到其配额限制，仅与跟踪有关。
- 限制 – 对用户或组的存储配额限制。

您可以为访问文件系统的新用户配置默认配额，也可以配置适用于特定用户或组的配额。您还可以通过查看报告来了解每个用户或组正在消耗的存储空间以及他们是否即将超出配额。

根据文件所有权跟踪用户级别的存储量消耗情况。在计算存储量消耗时使用的是逻辑文件的大小，而不是文件占用的实际物理存储空间。系统会在数据被写入文件时跟踪用户存储配额。

若要为多个用户更新配额，则需要为每个用户运行一次更新命令，也可以将用户组织成一个组然后更新该组的配额。

您可以使用 Amazon FSx CLI for Remote Management on PowerShell 管理文件系统上的用户存储配额。要了解如何使用此 CLI，请参阅将 Amazon FSx CLI 用于 PowerShell。

以下是可用于管理用户存储配额的命令。

用户存储配额命令	描述
Enable-FSxUserQuotas	开始跟踪和/或强制执行用户存储配额。

用户存储配额命令	描述
Disable-FSxUserQuotas	停止跟踪和强制执行用户存储配额。
Get-FSxUserQuotaSettings	检索文件系统的当前用户存储配额设置。
Get-FSxUserQuotaEntries	检索文件系统上的单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。配额值以字节为单位指定。

每个命令的联机帮助中都提供所有命令选项的参考信息。要访问此帮助，请运行包含 -? 的命令，例如 Enable-FSxUserQuotas -?。

增加文件系统存储容量

您可以随着存储要求的变化增加 FSx for Windows File Server 文件系统的存储容量。使用 Amazon FSx 控制台、Amazon CLI 或 Amazon FSx API 增加文件系统的存储容量，如以下过程所述。有关更多信息，请参阅 管理存储容量。

增加文件系统的存储容量（控制台）

1. 通过以下网址打开 Amazon FSx 控制台：https://console.aws.amazon.com/fsx/。
2. 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. 在操作中，选择更新存储。或者，在摘要面板中，选择文件系统存储容量旁边的更新。

   将出现更新存储容量窗口。
4. 在输入类型中，选择百分比，输入新的存储容量（相比于当前值的百分比变化），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%，最大不得超过 65536 GiB。

6. 选择更新，启动存储容量更新。
7. 可以在文件系统详细信息页面的更新选项卡上监控更新进度。

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 update-file-system。设置以下参数：

- `--file-system-id` 设置为要更新的文件系统的 ID。
- `--storage-capacity` 设置为比当前值至少大 10% 的值。

您可以使用 Amazon CLI 命令 describe-file-systems 来监控更新进度。在输出中，查找 `administrative-actions`。

有关更多信息，请参阅 AdministrativeAction。

监控存储容量增加

增加文件系统的存储容量后，可以使用 Amazon FSx 控制台、API 或 Amazon CLI 监控存储容量增加的进度，如以下过程所述。

在控制台中监控增加

在文件系统详细信息窗口的更新选项卡中，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，可以查看以下信息。

更新类型

可能的值是存储容量。

目标值

要将文件系统存储容量更新到的所需值。

状态

当前更新状态。对于存储容量更新，可能的值如下：

- 待处理 – Amazon FSx 已收到更新请求，但尚未开始处理。
- 正在进行中 – Amazon FSx 正在处理更新请求。
- 已更新；正在优化 – Amazon FSx 已增加文件系统的存储容量。现在，存储优化过程正在将文件系统数据迁移到容量更大的新磁盘。
- 已完成 – 存储容量增加成功完成。

- 失败 – 存储容量增加失败。选择问号（？）可查看关于存储容量更新失败原因的详细信息。

进度百分比

以完成百分比的形式显示存储优化流程的进度。

请求时间

Amazon FSx 收到更新操作请求的时间。

使用 Amazon CLI 和 API 监控增量

您可以使用 describe-file-systems Amazon CLI 命令和 DescribeFileSystems API 操作查看和监控文件系统存储容量增加请求。AdministrativeActions 数组列出每种管理操作类型的 10 个最近更新操作。增加文件系统的存储容量时，会生成两个 AdministrativeActions：FILE_SYSTEM_UPDATE 和 STORAGE_OPTIMIZATION 操作。

以下示例显示了 CLI 命令 describe-file-systems 的响应摘录。文件系统的存储容量为 300 GB，有一个待处理的管理操作要将存储容量增加到 1000 GB。

```
{
    "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 首先处理 FILE_SYSTEM_UPDATE 操作，为文件系统添加容量更大的新存储磁盘。当新的存储空间可供文件系统使用时，FILE_SYSTEM_UPDATE 状态将更改为 UPDATED_OPTIMIZING。存储容量显示新的更大值，随后 Amazon FSx 开始处理 STORAGE_OPTIMIZATION 管理操作。如以下 CLI 命令 describe-file-systems 的响应摘录中所示。

ProgressPercent 属性显示存储优化流程的进度。存储优化流程成功完成后，FILE_SYSTEM_UPDATE 操作的状态将更改为 COMPLETED，并且 STORAGE_OPTIMIZATION 操作不再显示。

```
{
    "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,
                }
            ]
```

如果增加存储容量失败，则 FILE_SYSTEM_UPDATE 操作的状态将更改为 FAILED。FailureDetails 属性提供失败相关信息，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
                }
            ]
```

有关对失败操作进行问题排查的信息，请参阅存储或吞吐能力更新失败。

动态增加 FSx for Windows File Server 文件系统的存储容量

除了在存储的数据量增加时对 FSx for Windows File Server 文件系统的存储容量进行手动增加之外，您还可以使用 Amazon CloudFormation 模板自动增加存储。当可用存储容量低于您指定的定义阈值时，本节提供的解决方案可动态增加文件系统的存储容量。

此 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、基于该阈值的 Amazon CloudWatch 警报以及增加文件系统存储容量的 Amazon Lambda 函数。

该解决方案方法采用以下参数：

- 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（%）
- 订阅 SNS 的电子邮件地址
- 调整警报阈值（是/否）

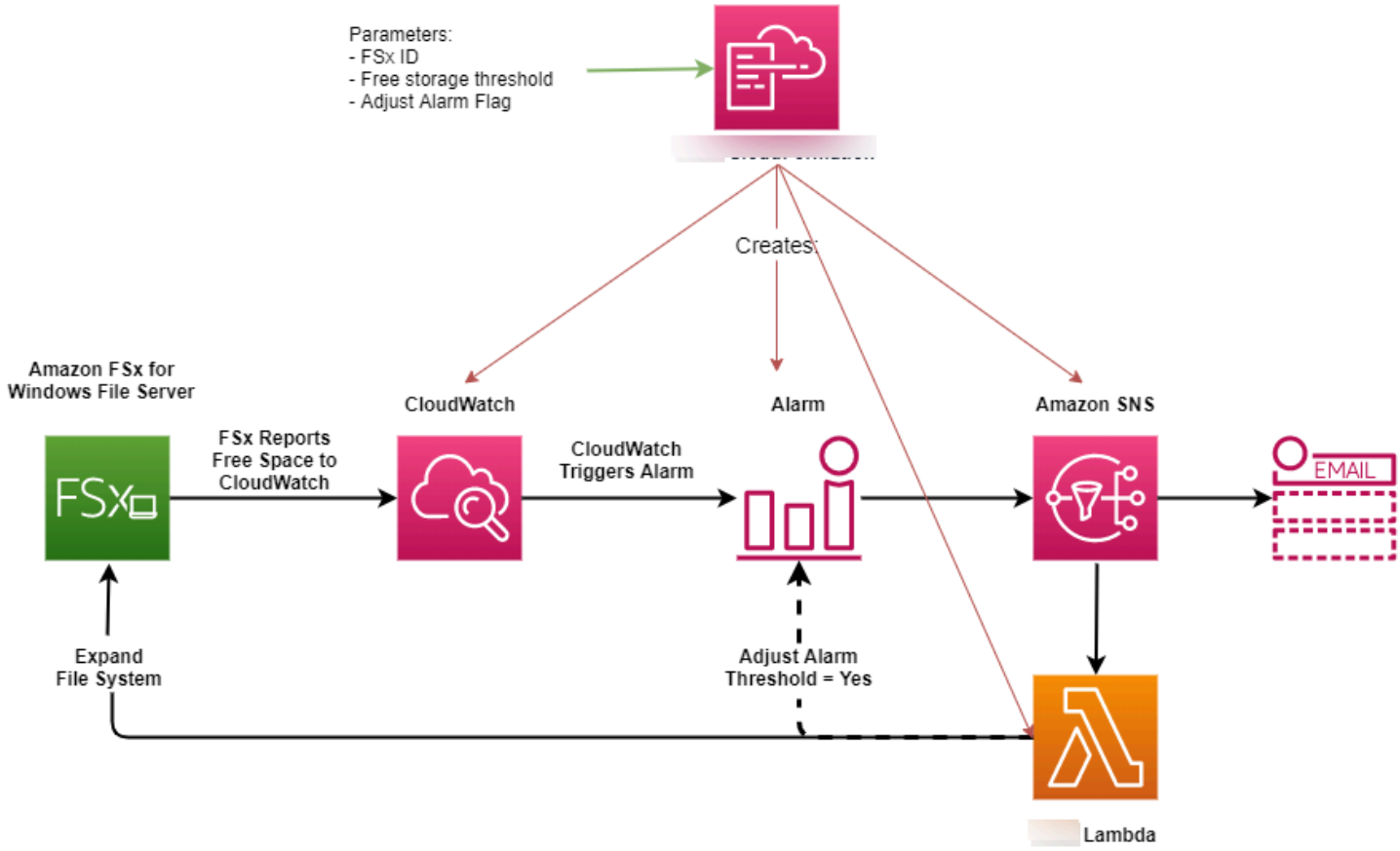
主题

- 架构概述

- Amazon CloudFormation 模板
- 使用 Amazon CloudFormation 自动部署

架构概述

部署此解决方案将在 Amazon 云中生成以下资源。



下图说明了以下步骤：

1. 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. 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 队列发送一条消息。
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. 原始 CloudWatch 警报状态和 Lambda 函数操作结果将发送到 Amazon SNS 队列。

要接收关于 CloudWatch 警报的响应操作的通知，您必须使用订阅确认电子邮件中提供的链接来确认 Amazon SNS 主题订阅。

Amazon CloudFormation 模板

此解决方案使用 Amazon CloudFormation 自动部署自动增加 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 IncreaseFSxSize Amazon CloudFormation 模板。

该模板使用如下所述的参数。查看模板参数及其默认值，并根据文件系统的需求对它们进行修改。

FileSystemId

无默认值。您想要自动增加存储容量的文件系统的 ID。

LowFreeDataStorageCapacityThreshold

无默认值。以 GiB 单位或文件系统的当前存储容量的百分比（%）指定初始可用存储容量阈值。达到该阈值时，触发警报并自动增加文件系统的存储容量。当以百分比表示时，为了与 CloudWatch 警报设置相符，CloudFormation 模板会重新计算为 GiB。

LowFreeDataStorageCapacityThresholdUnit

默认为 %。以 GiB 为单位或以当前存储容量的百分比指定 `LowFreeDataStorageCapacityThreshold` 单位。

AlarmModificationNotification

默认值为是。如果设置为“是”，则初始 `LowFreeDataStorageCapacityThreshold` 值将按比例增加到后续警报阈值 `PercentIncrease` 的值。

例如，如果将 `PercentIncrease` 设置为 20，并将 AlarmModificationNotification 设置为 “是”，则以 GiB 为单位指定的可用空间阈值（`LowFreeDataStorageCapacityThreshold`）将在后续存储容量增加事件中增加 20%。

EmailAddress

无默认值。指定 SNS 订阅使用的电子邮件地址，并接收存储容量阈值警报。

PercentIncrease

无默认值。以当前存储容量的百分比指定存储容量的增量。

使用 Amazon CloudFormation 自动部署

以下过程会配置和部署 Amazon CloudFormation 堆栈，以自动增加 FSx for Windows File Server 文件系统的存储容量。部署可能需要五分钟才能完成。

> **Note**
>
> 实施此解决方案会产生相关 Amazon 服务的账单。有关更多信息，请参阅有关这些服务的定价详细信息页面。

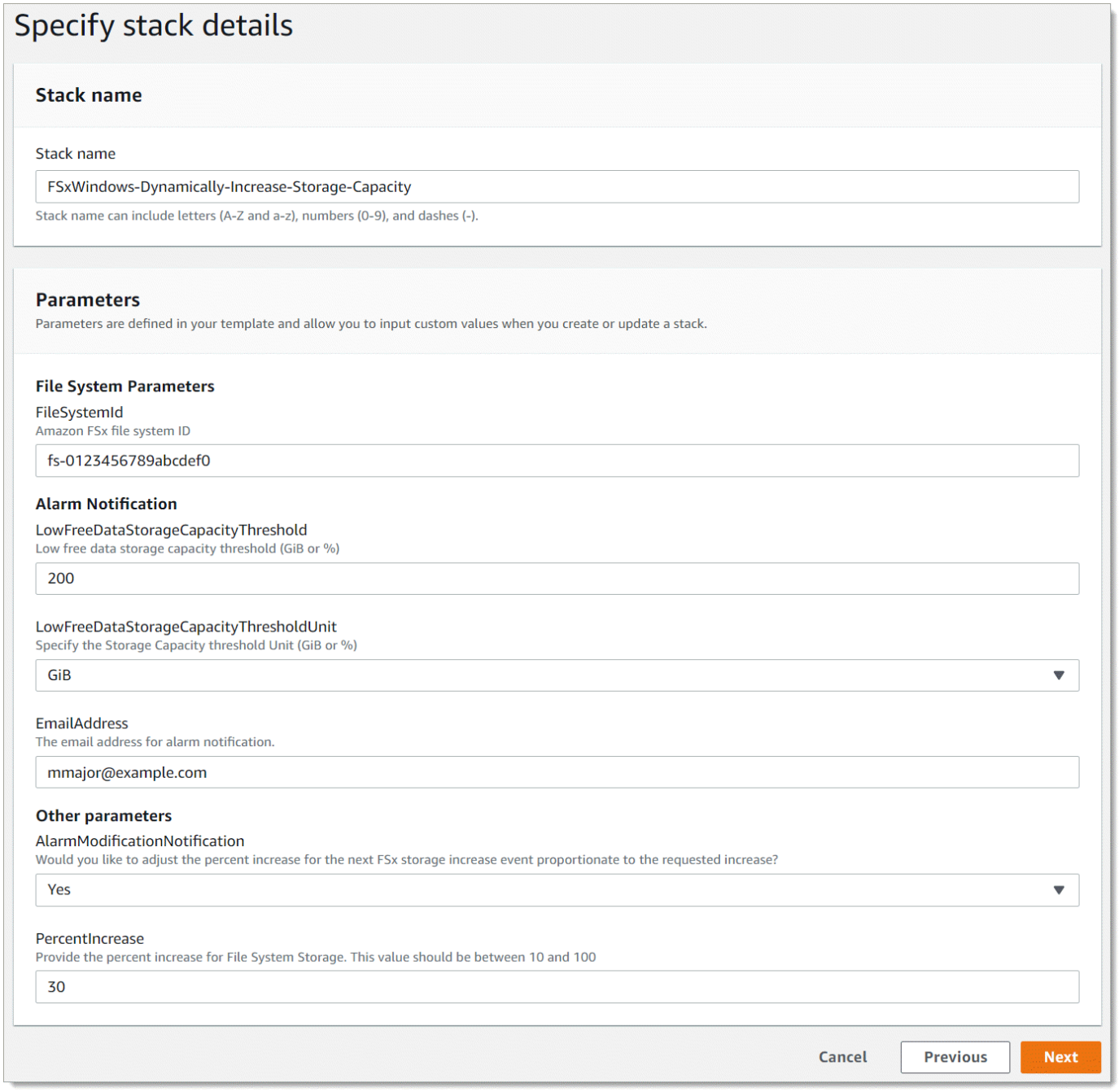
在开始之前，您的 Amazon 账户中必须有一个运行于 Amazon Virtual Private Cloud（Amazon VPC）之中的 Amazon FSx 文件系统。有关如何创建 Amazon FSx 资源的更多信息，请参阅开始使用 FSx 适用于 Windows 文件服务器的亚马逊。

启动自动存储容量增加解决方案堆栈

1. 下载 IncreaseFSxSize Amazon CloudFormation 模板。有关如何创建 CloudFormation 堆栈的更多信息，请参阅《Amazon CloudFormation 用户指南》中的在 Amazon CloudFormation 控制台上创建堆栈。

   > **Note**
   >
   > Amazon FSx 目前仅在特定的 Amazon 区域可用。您必须在可以使用 Amazon FSx 的 Amazon 区域启动此解决方案。有关更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon FSx 端点和配额。

2. 在指定堆栈详细信息中，输入自动存储容量增加解决方案的值。



3. 输入堆栈名称。
4. 对于参数，请查看模板的参数并根据文件系统的需求对其进行修改。然后选择下一步。
5. 输入自定义解决方案所需的任何选项设置，然后选择下一步。
6. 对于审核，请审核并确认解决方案设置。必须选择确认模板创建 IAM 资源对应的复选框。
7. 选择创建以部署堆栈。

您可以在 Amazon CloudFormation 控制台的状态列中查看堆栈的状态。您应该在大约 5 分钟内看到 CREATE_COMPLETE 状态。

更新堆栈

创建堆栈后，您可以使用相同的模板并为参数提供新值，从而对其进行更新。有关更多信息，请参阅《Amazon CloudFormation 用户指南》中的直接更新堆栈。

更新 FSx for Windows 文件系统的存储类型

可以将使用 HDD 存储的文件系统的存储类型更改为使用 SSD 存储。您可以按照以下过程所述，使用 Amazon FSx 控制台、Amazon CLI 或 Amazon FSx API 更改文件系统的存储类型。有关更多信息，请参阅 管理文件系统存储类型。

更新文件系统的存储类型（控制台）

1. 通过以下网址打开 Amazon FSx 控制台：https://console.aws.amazon.com/fsx/。
2. 导航到文件系统，然后选择要为其更新存储类型的 Windows 文件系统。
3. 在操作下，选择更新存储类型。或者，在摘要面板中，选择 HDD 旁边的更新按钮。此时将显示更新存储类型窗口。
4. 对于所需存储类型，选择 SSD。选择更新，启动存储类型更新。

   您可以使用控制台和 CLI 监控存储类型的更新进度。

更新文件系统的存储类型（CLI）

要更新 FSx for Windows File Server 文件系统的存储类型，请使用 Amazon CLI 命令 update-file-system。设置以下参数：

- 将 `--file-system-id` 设置为要更新的文件系统的 ID。
- 将 `--storage-type` 设置为 SSD。无法从 SSD 存储类型切换为 HDD 存储类型。

您可以使用 Amazon CLI 命令 describe-file-systems 来监控更新进度。在输出中，查找 `administrative-actions`。

有关更多信息，请参阅 AdministrativeAction。

监控存储类型更新

将文件系统的存储类型从 HDD 存储更新为 SSD 存储后，可以使用 Amazon FSx 控制台、Amazon CLI 或 API 监控存储类型更新进度，如以下过程所述。

在控制台中监控文件系统更新

在文件系统详细信息窗口的更新选项卡中，您可以查看每种更新类型的 10 个最近更新。

对于存储类型更新，可以查看以下信息。

更新类型

可能的值为存储类型。

目标值

SSD

状态

当前更新状态。对于存储类型更新，可能的值如下：

- 待处理 – Amazon FSx 已收到更新请求，但尚未开始处理。
- 正在进行中 – Amazon FSx 正在处理更新请求。
- 已更新；正在优化 – SSD 存储性能可用于写入操作。更新将进入已更新；正在优化状态，该状态通常持续几个小时，在此期间，读取操作的性能级别将介于 HDD 和 SSD 之间。更新操作完成后，新的 SSD 性能即可用于读取和写入。
- 已完成 – 存储类型更新成功完成。
- 失败 – 存储类型更新失败。选择问号（？）可查看详细信息。

进度百分比

以完成百分比的形式显示存储优化流程的进度。

请求时间

Amazon FSx 收到更新操作请求的时间。

通过 Amazon CLI 和 API 监控更新

您可以使用 describe-file-systems Amazon CLI 命令和 DescribeFileSystems API 操作查看和监控文件系统存储类型更新请求。`AdministrativeActions` 数组列出每

种管理操作类型的 10 个最近更新操作。增加文件系统的 SSD IOPS 时，会生成两个 `AdministrativeActions`：`FILE_SYSTEM_UPDATE` 操作和 `STORAGE_TYPE_OPTIMIZATION` 操作。

更新文件系统的 SSD IOPS

对于配置了 SSD 存储的文件系统，预置 SSD IOPS 的级别决定了文件系统从磁盘读取数据以及向磁盘写入数据时的可用磁盘 I/O 数量，而不是读取或写入缓存中的数据。您可以按照以下过程所述，使用 Amazon FSx 控制台、Amazon CLI 或 Amazon FSx API 更新文件系统的 SSD IOPS。有关管理 SSD IOPS 的更多信息，请参阅 管理 SSD IOPS。

更新文件系统的 SSD IOPS（控制台）

1. 通过以下网址打开 Amazon FSx 控制台：https://console.aws.amazon.com/fsx/。
2. 导航到文件系统，然后选择要更新 SSD IOPS 的 Windows 文件系统。
3. 在操作下，选择更新 SSD IOPS。或者，在摘要面板中，选择更新预置的 SSD IOPS 旁边的更新按钮。将会打开更新 IOPS 预调配窗口。
4. 在模式中，选择自动或用户预置。如果您选择自动，Amazon FSx 会自动为您的文件系统预置每 GiB 存储容量 3 IOPS。如果您选择用户预置，请输入 96– 400,000 之间的任意整数。
5. 选择更新，启动预置的 SSD IOPS 更新。
6. 可以通过文件系统详细信息页面的更新选项卡来监控更新进度。

更新文件系统的 SSD IOPS（CLI）

要更新 FSx for Windows File Server 文件系统的 SSD IOPS，请使用 `--windows-configuration DiskIopsConfiguration` 属性。此属性有 `Iops` 和 `Mode` 两个参数：

- 如果您想要指定 SSD IOPS 的数量，请使用 `Iops=`*`number_of_IOPS`*，在支持的 Amazon 区域和 `Mode=USER_PROVISIONED` 中最高为 40 万。
- 如果您希望 Amazon FSx 自动提高 SSD IOPS，请使用 `Mode=AUTOMATIC`，且不要使用 `Iops` 参数。Amazon FSx 会在您的文件系统上自动保持每 GiB 存储容量 3 SSD IOPS，在支持的 Amazon 区域最多可保持 40 万 SSD IOPS。

您可以使用 Amazon CLI 命令 describe-file-systems 来监控更新进度。在输出中，查找 `administrative-actions`。

有关更多信息，请参阅 AdministrativeAction。

监控预置的 SSD IOPS 更新

在您更新文件系统的预置 SSD IOPS 数量后，可按照以下过程所述使用 Amazon FSx 控制台、Amazon CLI 和 API，以监控 SSD IOPS 更新的进度。

在控制台中监控更新

在文件系统详细信息窗口的更新选项卡中，您可以查看每种更新类型的 10 个最近更新。

有关预置的 SSD IOPS 更新，您可以查看以下信息。

更新类型

可能的值为 IOPS 模式和 SSD IOPS。

目标值

将文件系统的 IOPS 模式和 SSD IOPS 更新为所需的值。

状态

当前更新状态。对于 SSD IOPS 更新，可能的值如下：

- 待处理 – Amazon FSx 已收到更新请求，但尚未开始处理。
- 正在进行中 – Amazon FSx 正在处理更新请求。
- 已更新；正在优化 – 新 IOPS 级别可用于工作负载的写入操作。您的更新进入已更新；正在优化状态，该状态通常持续几个小时，在此期间，工作负载读取操作的 IOPS 级别将介于旧级别和新级别之间。更新操作完成后，新的 IOPS 性能即可用于读取和写入。
- 已完成 – SSD IOPS 更新成功完成。
- 失败 – SSD IOPS 更新失败。选择问号（？）可查看关于存储容量更新失败原因的详细信息。

进度百分比

以完成百分比的形式显示存储优化流程的进度。

请求时间

Amazon FSx 收到更新操作请求的时间。

通过 Amazon CLI 和 API 监控更新

您可以使用 describe-file-systems Amazon CLI 命令和 DescribeFileSystems API 操作查看和监控文件系统 SSD IOPS 更新请求。`AdministrativeActions` 数组列出每

种管理操作类型的 10 个最近更新操作。增加文件系统的 SSD IOPS 时，会生成两个 `AdministrativeActions`：`FILE_SYSTEM_UPDATE` 操作和 `IOPS_OPTIMIZATION` 操作。

管理重复数据删除

您可以使用 Amazon FSx CLI for Remote Management on PowerShell 管理文件系统的重复数据删除设置。有关使用 Amazon FSx CLI Remote Management on PowerShell 的更多信息，请参阅 将 Amazon FSx CLI 用于 PowerShell。

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删除。启用重复数据删除时，系统会默认在重复数据删除后启用数据压缩。
Disable-FSxDedup	在文件共享上禁用重复数据删除。
Get-FSxDedupConfiguration	检索重复数据删除的配置信息，包括用于优化的最小文件大小和期限、压缩设置以及已排除的文件类型和文件夹。
Set-FSxDedupConfiguration	更改重复数据删除的配置设置，包括用于优化的最小文件大小和期限、压缩设置以及已排除的文件类型和文件夹。
Get-FSxDedupStatus	检索重复数据删除状态，并包含描述文件系统的优化节省量和状态的只读属性、时间，以及文件系统上最后一个重复数据删除作业的完成状态。
Get-FSxDedupMetadata	检索重复数据删除的优化元数据。
Update-FSxDedupStatus	计算和检索更新后的重复数据删除节省量信息。
Measure-FSxDedupFileMetadata	衡量和检索在删除一组文件夹后能够在文件系统上回收的潜在存储空间。文件中通常包含与其他文件夹共享的数据块，重复数据删除引擎会计算出哪些是将被删除的唯一数据块。
Get-FSxDedupSchedule	检索当前已定义的重复数据删除计划。
New-FSxDedupSchedule	创建和自定义重复数据删除计划。

重复数据删除命令	描述
Set-FSxDedupSchedule	更改现有重复数据删除计划的配置设置。
Remove-FSxDedupSchedule	删除重复数据删除计划。
Get-FSxDedupJob	获取所有当前正在运行或排队的重复数据删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删除作业。

每个命令的联机帮助中都提供所有命令选项的参考信息。要访问此帮助，请运行包含 -? 的命令，例如 Enable-FSxDedup -?。

启用重复数据删除

您可以使用命令 `Enable-FSxDedup` 在适用于 Windows File Server 的 Amazon FSx 文件共享上启用重复数据删除，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，系统将创建默认计划和配置。您可以使用以下命令创建、修改和删除计划和配置。

您可以使用命令 `Disable-FSxDedup` 在文件系统上完全禁用重复数据删除。

创建重复数据删除计划

尽管在大多数情况下默认计划都能够运行良好，但您可以使用 `New-FsxDedupSchedule` 命令创建新的重复数据删除计划，如下所示。重复数据删除计划将使用 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
}
```

此命令会创建一个名为 `CustomOptimization` 的计划，该计划将在星期一、星期三和星期六运行，每天上午 8:00（UTC）开始作业，最长持续时间为 7 小时，到时即使未完成运行也会停止作业。

请注意，创建新的自定义重复数据删除作业计划不会覆盖或删除现有的默认计划。在创建自定义重复数据删除任务之前，您可能需要禁用不需要的默认作业。

您可以使用 Set-FsxDedupSchedule 命令禁用默认的重复数据删除计划，如下所示。

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com
 -ConfigurationName FSxRemoteAdmin -ScriptBlock {Set-FSxDedupSchedule -Name
 “BackgroundOptimization” -Enabled $false}
```

您可以使用 Remove-FSxDedupSchedule -Name "ScheduleName" 命令删除重复数据删除计划。请注意，您无法修改或删除默认的 BackgroundOptimization 重复数据删除计划，所以需要将其禁用。

修改重复数据删除计划

您可以使用 Set-FsxDedupSchedule 命令修改现有的重复数据删除计划，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
}
```

此命令会将现有的 CustomOptimization 计划修改为在星期一至星期三以及星期六运行，每天上午 9:00（UTC）开始作业，最长持续时间为 9 小时，到时即使未完成运行也会停止作业。

要在优化设置之前修改最小文件期限，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删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**
>
> 命令响应中显示的以下参数的值并不可靠，因此不应使用这些值：“Capacity”、“FreeSpace”、“usedSpace”、“unOptimizedSize”和“SavingSrate”。

重复数据删除问题排查

使用以下信息帮助排查配置和使用重复数据删除时产生的一些常见问题。

主题

重复数据删除不起作用

要查看重复数据删除的当前状态，请运行 `Get-FSxDedupStatus` PowerShell 命令查看最新重复数据删除作业的完成状态。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。

重复数据删除作业失败的最常见原因是内存不足。

- Microsoft 建议最好每 1 TB 的逻辑数据有 1 GB 的内存（或者每 1 TB 的逻辑数据至少有 350 MB 的内存）。使用 Amazon FSx 性能表来确定与文件系统的吞吐能力关联的内存，并确保内存资源足以容纳您的数据大小。如果不够，则需要提高文件系统的吞吐能力，使其满足每 1 TB 逻辑数据提供 1 GB 内存的要求。
- 重复数据删除作业使用 Windows 推荐的默认 25% 内存分配配置，这意味着对于具有 32 GB 内存的文件系统，8 GB 可用于重复数据删除。内存分配是可配置的（使用带 `-Memory` 参数的 `Set-FSxDedupSchedule` 命令）。请注意，为重复数据删除使用较高的内存分配可能会影响文件系统的性能。
- 您可以修改重复数据删除作业的配置，以降低内存需求量。例如，您可以将优化限制为针对特定文件类型或文件夹运行，或者设置优化的最小文件大小和期限。我们还建议将重复数据删除作业配置为在文件系统负载最小的空闲期间运行。

如果重复数据删除作业没有足够的时间完成，也可能会出错。您可能需要更改作业的最长持续时间，如修改重复数据删除计划 中所述。

如果重复数据删除作业已经失败了很长时间，并且在此期间文件系统上的数据发生了变化，那么后续的重复数据删除作业可能需要更多资源才能首次成功完成。

重复数据删除值意外设置为 0

对于已配置重复数据删除的文件系统，SavedSpace 和 OptimizedFilesSavingsRate 的值意外设为 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当前的重复数据删除作业，该过程会将数据从旧磁盘迁移到更大的新磁盘。存储优化作业完成后，Amazon FSx 将恢复文件系统的重复数据删除。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。

删除文件后，文件系统上的空间未被释放

重复数据删除的预期行为是，如果删除的数据是重复数据删除节省空间的内容，那么文件系统上的空间实际上要在垃圾回收作业运行后才会释放。

您可能会发现，将计划设置为在删除大量文件后立即运行垃圾回收作业很有用。垃圾回收作业完成后，您可以将垃圾回收计划恢复回其原始设置。这便可以确保您能立即快速查看删除内容释放的空间。

按照以下步骤将垃圾回收作业设置为 5 分钟后运行。

1. 要验证是否启用了重复数据删除，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。
2. 按照以下步骤将计划设置为垃圾回收作业在从现在起 5 分钟后运行。

```
$FiveMinutesFromNowUTC = ((get-date).AddMinutes(5)).ToUniversalTime()
$DayOfWeek = $FiveMinutesFromNowUTC.DayOfWeek
$Time = $FiveMinutesFromNowUTC.ToString("HH:mm")

Invoke-Command -ComputerName ${RPS_ENDPOINT} -ConfigurationName FSxRemoteAdmin -
ScriptBlock {
    Set-FSxDedupSchedule -Name "WeeklyGarbageCollection" -Days $Using:DayOfWeek -
Start $Using:Time -DurationHours 9
}
```

3. 在运行垃圾回收作业并释放空间后，将计划恢复回其原始设置。

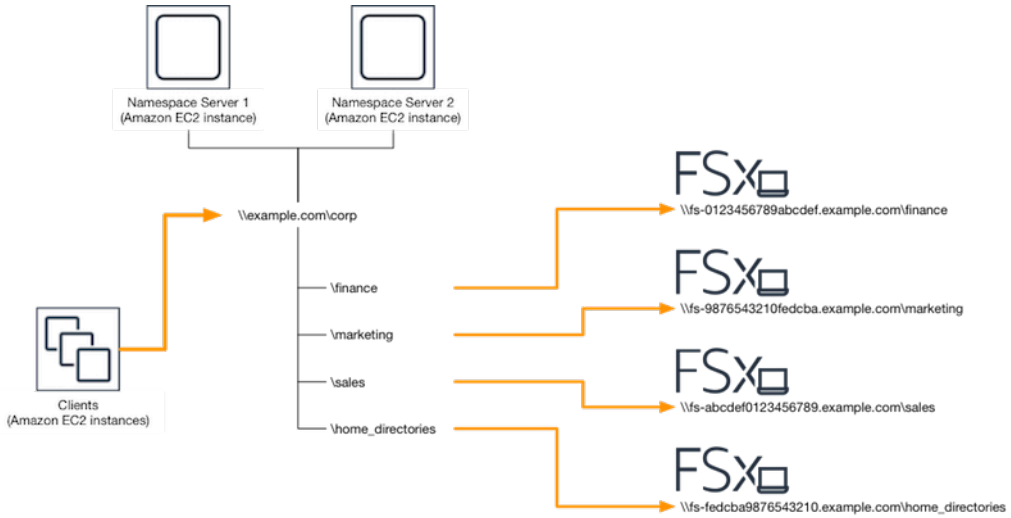
使用 DFS 命名空间

DFS 命名空间是一项 Windows Server 角色服务，用于将不同服务器上的共享文件夹分组为一个或多个逻辑结构化的命名空间。这样就可以为用户提供共享文件夹的虚拟视图，多个文件系统中的文件通过单个路径即可到达，如下图所示。除了整理和统一跨多个文件系统的文件共享访问外，

使用 DFS 命名空间为多个 FSx for Windows File Server 文件系统分组

可以使用 Microsoft 的分布式文件系统 (DFS) 命名空间将多个 FSx for Windows File Server 文件系统上的文件共享分组到一个公共文件夹结构或命名空间。使用 DFS 命名空间，就可以将大型文件数据集的文件存储扩展至单个文件系统的最大存储容量 (64 TiB) 之外，最高可达数百 PB。本节将展示如何在多个 FSx for Windows File Server 文件系统上设置 DFS 命名空间。

DFS 命名空间是一项 Windows Server 角色服务，用于将不同服务器上的共享文件夹分组为一个或多个逻辑结构化的命名空间。这样就可以为用户提供共享文件夹的虚拟视图，多个文件系统中的文件通过单个路径即可到达，如下图所示。除了整理和统一跨多个文件系统的文件共享访问外，



有关使用 DFS 命名空间对适用于 FSx for Windows 文件系统进行分组的分步过程，请参阅 将多个文件系统分组到单个命名空间中。

通过分片提高性能

Amazon FSx for Windows File Server 支持使用 Microsoft 分布式文件系统（DFS）。通过使用 DFS 命名空间，您可以将文件数据分布到多个 Amazon FSx 文件系统，从而横向扩展性能（读取和写入），以处理 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。此解决方案包括将文件数据划分为较小的数据集或分片，然后将其存储在不同的文件系统中。从多个实例访问您的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平性能。

可以使用 使用 DFS 命名空间进行数据分片以横向扩展性能 中提供的解决方案将数据读/写访问权限均匀分布在多个 FSx for Windows File Server 数据文件系统中。

将多个文件系统分组到单个命名空间中

在此过程中，您将在两个命名空间服务器上创建单个基于域的命名空间 (`example.com\corp`)，以合并多个 FSx for Windows 文件系统（财务、营销、销售、home_directories）上存储的文件共享。您还可以在命名空间下设置四个文件共享，每个文件共享都会以透明方式将用户重定向到托管在单独的 FSx for Windows 文件系统上的共享。这样用户就能使用公共命名空间来访问文件共享，而不必为托管文件共享的每个文件系统指定 DNS 名称。

> **Note**
>
> 无法将 Amazon FSx 添加到 DFS 共享路径的根目录。

将多个文件系统分组到一个公共 DFS 命名空间

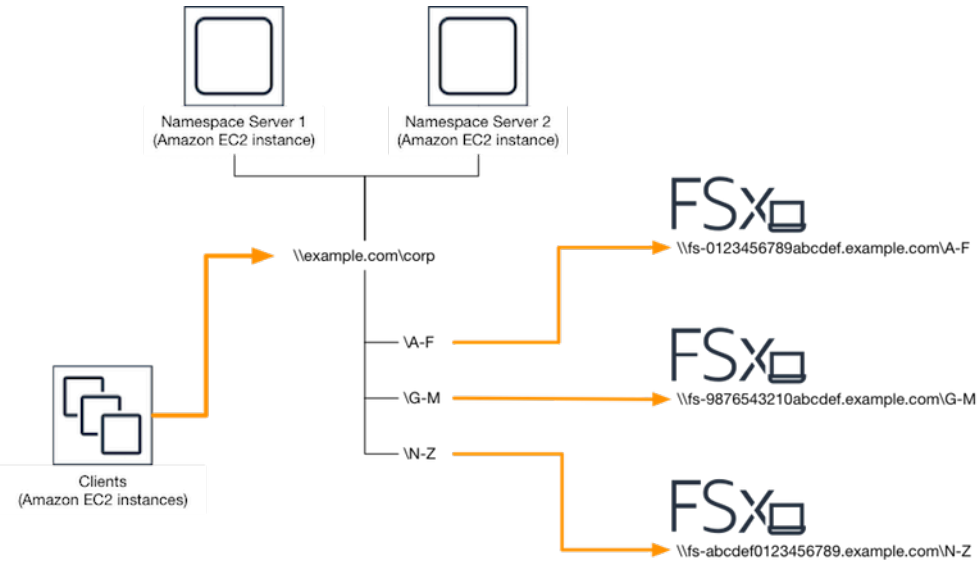
1. 如果您尚未运行 DFS 命名空间服务器，则可以使用 setup-DFSN-servers.template Amazon CloudFormation 模板来启动一对高度可用的 DFS 命名空间服务器。有关创建 Amazon CloudFormation 堆栈的更多信息，请参阅《Amazon CloudFormation 用户指南》中的在 Amazon CloudFormation 控制台上创建堆栈。
2. 以 Amazon 委派的管理员组中用户的身份连接到在上一步中启动的 DFS 命名空间服务器之一。有关详细信息，请参阅《Amazon EC2 用户指南》中的 Connecting to Your Windows Instance。
3. 通过打开操作访问 DFS 管理控制台。打开开始菜单，然后运行 dfsmgmt.msc。此操作将打开 DFS Management GUI 工具。
4. 依次选择操作、新命名空间，输入您为服务器启动的第一个 DFS 命名空间服务器的计算机名称，然后选择下一步。
5. 在名称中输入您要创建的命名空间（例如 corp）。
6. 选择编辑设置，然后根据您的需求设置相应权限。选择下一步。
7. 保持选中默认的基于域的命名空间选项，保持选中启用 Windows Server 2008 模式选项，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. 检查命名空间的设置，然后选择创建。
9. 在导航栏的命名空间下选择新创建的命名空间后，选择操作，然后选择添加命名空间服务器。
10. 在命名空间服务器中输入您已启动的第二个 DFS 命名空间服务器的计算机名称。
11. 选择编辑设置，然后根据您的需求设置相应权限，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，键入文件夹名称（例如，在名称中选择 `finance`），然后选择确定。
13. 在文件夹目标路径中以 UNC 格式键入您希望 DFS 命名空间文件夹指向的文件共享的 DNS 名称（例如 `\\fs-0123456789abcdef0.example.com\finance`），然后选择确定。
14. 如果共享不存在：
    a. 选择是进行创建。
    b. 在创建共享对话框中选择浏览。
    c. 选择现有文件夹，或在 D$ 下创建一个新文件夹，然后选择确定。
    d. 设置相应的共享权限，然后选择确定。
15. 在新文件夹对话框中，选择确定。此操作将在命名空间下创建新文件夹。
16. 对要共享到相同命名空间下的其他文件夹重复最后四个步骤。

使用 DFS 命名空间进行数据分片以横向扩展性能

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* 命名空间中的数据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，您应该决定如何以最佳方式在多个文件共享之间对数据进行分片。选择一种分片约定，在计划使用的所有文件共享中均匀分布 I/O。请记住，每个命名空间总共支持多达 5 万个文件共享和数百 PB 的存储容量。



设置 DFS 命名空间以横向扩展性能

1. 如果您尚未运行 DFS 命名空间服务器，则可以使用 setup-DFSN-servers.template Amazon CloudFormation 模板来启动一对高度可用的 DFS 命名空间服务器。有关创建 Amazon CloudFormation 堆栈的更多信息，请参阅《Amazon CloudFormation 用户指南》中的在 Amazon CloudFormation 控制台上创建堆栈。
2. 以 Amazon 委派的管理员组中用户的身份连接到在上一步中启动的 DFS 命名空间服务器之一。有关详细信息，请参阅《Amazon EC2 用户指南》中的 Connecting to Your Windows Instance。
3. 访问 DFS 管理控制台。打开开始菜单，然后运行 dfsmgmt.msc。此操作将打开 DFS Management GUI 工具。
4. 依次选择操作、新命名空间，输入您为服务器启动的第一个 DFS 命名空间服务器的计算机名称，然后选择下一步。
5. 在名称中输入您要创建的命名空间（例如 corp）。
6. 选择编辑设置，然后根据您的需求设置相应权限。选择下一步。
7. 保持选中默认的基于域的命名空间选项，保持选中启用 Windows Server 2008 模式选项，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. 检查命名空间的设置，然后选择创建。
9. 在导航栏的命名空间下选择新创建的命名空间后，选择操作，然后选择添加命名空间服务器。

10. 在命名空间服务器中输入您已启动的第二个 DFS 命名空间服务器的计算机名称。
11. 选择编辑设置，然后根据您的需求设置相应权限，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，输入第一个分片的文件夹名称（例如，名称选择 A-F），然后选择添加。
13. 在文件夹目标路径中以 UNC 格式（例如 `\\fs-0123456789abcdef0.example.com\A-F`）键入托管此分片的文件共享的 DNS 名称，然后选择确定。
14. 如果共享不存在：

    a. 选择是进行创建。

    b. 在创建共享对话框中选择浏览。

    c. 选择现有文件夹，或在 D$ 下创建一个新文件夹，然后选择确定。

    d. 设置相应的共享权限，然后选择确定。
15. 现在已为分片添加文件夹目标，接下来选择确定。
16. 对要添加到相同命名空间的其他分片重复最后四个步骤。

管理吞吐能力

您可以随时提高和降低文件系统的吞吐能力，以便管理其性能。吞吐能力是决定托管 FSx for Windows File Server 文件系统的文件服务器提供数据的速度的一个因素。吞吐能力的级别越高，文件服务器上缓存数据的每秒 I/O 操作次数（IOPS）和缓存内存容量也就越高。有关更多信息，请参阅 FSx for Windows File Server 性能。

主题

- 吞吐量扩展的运作方式
- 知道何时修改吞吐能力
- 修改吞吐能力
- 监控吞吐能力更新

吞吐量扩展的运作方式

当您修改文件系统的吞吐能力时，Amazon FSx 会在后台将文件系统的文件服务器切换为吞吐量更高或更低的服务器。对于多可用区文件系统，当 Amazon FSx 关闭首选文件服务器和辅助文件服务器时，切换至新文件服务器会触发自动失效转移和失效自动恢复。在扩展吞吐能力期间切换文件服务器时，单可用区文件系统将有几分钟不可用。您的文件系统可以使用新的吞吐能力量后，就会向您收取费用。

> **Note**
>
> 在后端维护操作期间，系统修改（包括对吞吐能力的修改）可能会出现延迟。维护操作会导致排队处理系统修改工作。

对于多可用区文件系统，当 Amazon FSx 关闭首选文件服务器和辅助文件服务器时，吞吐能力扩展会自动进行失效转移和失效自动恢复。在文件服务器更换期间（在吞吐能力扩展、文件系统维护和计划外服务中断期间发生），文件系统的所有持续流量都将由剩余的文件服务器进行处理。当更换的文件服务器恢复在线时，FSx for Windows 将运行重新同步作业，以确保数据同步回更换的新文件服务器。

FSx for Windows 旨在最大限度地减少这种重新同步活动对应用程序和用户的影响。但是，重新同步进程涉及同步大块数据。这意味着，即使只有一小部分数据进行了更新，也可能需要同步大块数据。因此，重新同步作业量不仅取决于数据更新量，还取决于文件系统上数据更新的性质。如果您的工作负载写入量大和 IOPS 量大，则数据同步进程可能需要更长时间，并且需要额外的性能资源。

您的文件系统在此期间将继续可用，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时段修改吞吐能力。我们还建议确保文件系统具有足够的吞吐能力，不仅能够满足工作负载的需要，还能够运行同步作业，以缩短数据同步的持续时间。最后，我们建议在文件系统负载较小时测试失效转移的影响。

知道何时修改吞吐能力

Amazon FSx 与 Amazon CloudWatch 集成，可帮助您监控文件系统的持续吞吐量使用水平。除了文件系统的吞吐能力、存储容量和存储类型外，您可以通过文件系统驱动的性能（吞吐量和 IOPS）还取决于特定工作负载的特征。您可以使用 CloudWatch 指标来确定为了提高性能需要更改的维度有哪些。有关更多信息，请参阅 使用 Amazon CloudWatch 监控。

FSx for Windows File Server 在 Amazon FSx 控制台中“文件系统详细信息”页面的“监控和性能”控制面板中，根据文件系统的 CloudWatch 指标值提供性能警报。这包括吞吐能力以及可以从提高吞吐能力中受益的其他文件系统指标。有关更多信息，请参阅 性能警告和建议。

为文件系统配置足够的吞吐能力，不仅要满足工作负载的预期流量，还需额外预留性能资源以支持在文件系统上启用的各项功能。例如，如果您正在运行重复数据删除，则您选择的吞吐能力必须提供足够的内存，以便根据您拥有的存储空间运行重复数据删除。如果您使用的是影子副本，请将吞吐能力增加到至少为工作负载预期驱动值的三倍，以避免 Windows Server 删除影子副本。有关更多信息，请参阅 吞吐能力对性能的影响。

修改吞吐能力

您可以按照以下过程所述使用 Amazon FSx 控制台、Amazon Command Line Interface（Amazon CLI）或 Amazon FSx API，提高或降低文件系统的吞吐能力。

修改文件系统的吞吐能力（控制台）

1. 通过以下网址打开 Amazon FSx 控制台：https://console.aws.amazon.com/fsx/。
2. 导航到文件系统，然后选择要增加其吞吐能力的 Windows 文件系统。
3. 在操作中，选择更新吞吐量。

   或者，在摘要面板中，选择文件系统吞吐能力旁边的更新。

   此时将显示更新吞吐能力窗口。
4. 从列表中选择吞吐能力的新值。
5. 选择更新，启动吞吐能力更新。

   > **Note**
   >
   > 对于多可用区文件系统，在更新吞吐量扩展时，失效转移和失效自动恢复功能完全可用。对于单可用区系统，在更新期间，可能会在非常短的一段时间内不可用。

6. 可以在文件系统详细信息页面的更新选项卡上监控更新进度。

   您可以使用 Amazon FSx 控制台、Amazon CLI 和 API 来监控更新进度。有关更多信息，请参阅监控吞吐能力更新。

修改文件系统的吞吐能力（CLI）

要提高或降低文件系统的吞吐能力，请使用 Amazon CLI 命令 update-file-system。设置以下参数：

- 将 `--file-system-id` 设置为要更新的文件系统的 ID。
- 将 `ThroughputCapacity` 设置为所需值；有效值为 8、16、32、64、128、256、512、1024、2048、4608、6144、9216、12288MBps。

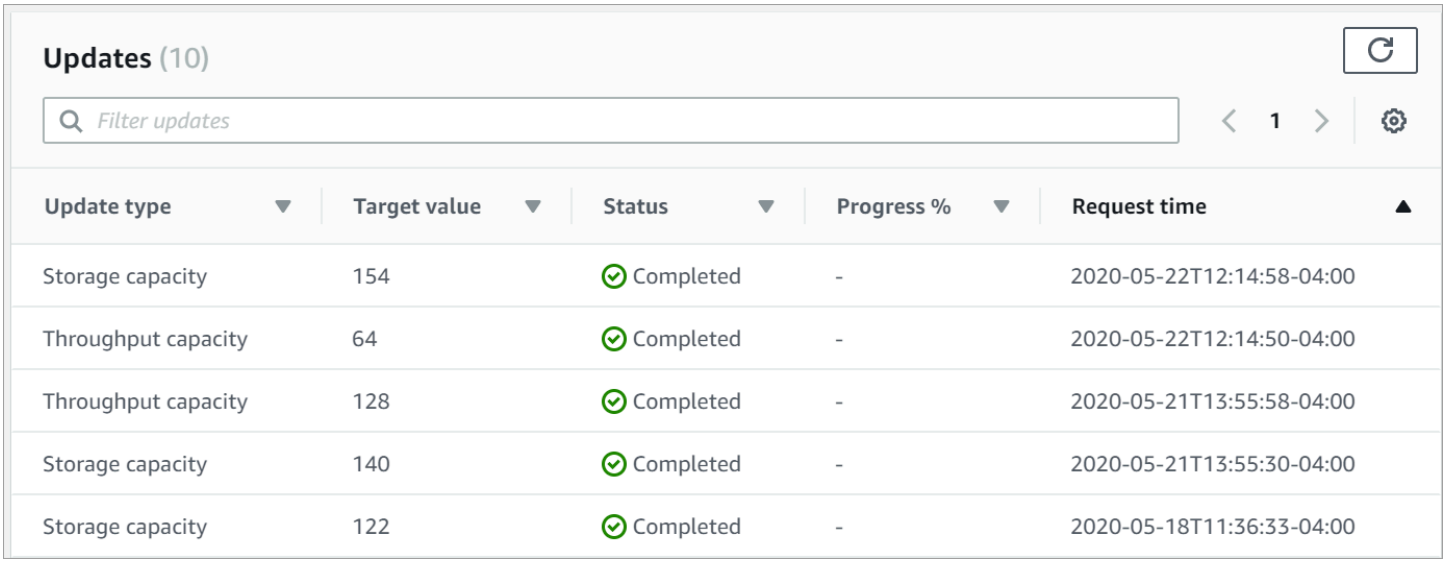
您可以使用 Amazon FSx 控制台、Amazon CLI 和 API 来监控更新进度。有关更多信息，请参阅 监控吞吐能力更新。

监控吞吐能力更新

您可以使用 Amazon FSx 控制台、API 和 Amazon CLI 监控吞吐能力的修改进度。

在控制台中监控吞吐能力更改

在文件系统详细信息窗口的更新选项卡中，您可以查看每种更新操作类型的 10 个最近更新操作。



您可以查看关于吞吐能力更新操作的以下信息。

更新类型

可能的值为吞吐能力。

目标值

要将文件系统的吞吐能力更改为的所需值。

状态

当前更新状态。对于吞吐能力更新，可能出现如下值：

- 待处理 – Amazon FSx 已收到更新请求，但尚未开始处理。
- 正在进行中 – Amazon FSx 正在处理更新请求。
- 已更新；正在优化 – Amazon FSx 已更新文件系统的网络 I/O、CPU 和内存资源。新的磁盘 I/O 性能级别可用于写入操作。对于读取操作，将看到磁盘 I/O 性能介于上一级别和新级别之间，直到您的文件系统不再处于此状态。
- 已完成 – 吞吐能力更新已成功完成。
- 失败 – 吞吐能力更新失败。选择问号（？）可查看关于吞吐量更新失败原因的详细信息。

请求时间

Amazon FSx 收到更新请求的时间。

通过 Amazon CLI 和 API 监控更改

您可以使用 CLI 命令 describe-file-systems 和 API 操作 DescribeFileSystems 查看和监控文件系统吞吐能力修改请求。`AdministrativeActions` 数组列出每种管理操作类型的 10 个最近更新操作。修改文件系统的吞吐能力时，会生成 `FILE_SYSTEM_UPDATE` 管理操作。

以下示例显示了 CLI 命令 `describe-file-systems` 的响应摘录。文件系统的吞吐能力为 8 MBps，目标吞吐能力为 256MBps。

```
.
.
.
    "ThroughputCapacity": 8,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "PENDING",
        "TargetFileSystemValues": {
          "WindowsConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

Amazon FSx 成功完成处理该操作后，状态将变为 `COMPLETED`。文件系统即可使用新的吞吐能力，并在 `ThroughputCapacity` 属性中显示。如以下 CLI 命令 describe-file-systems 的响应摘录中所示。

```
.
.
.
    "ThroughputCapacity": 256,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "COMPLETED",
```

```
        "TargetFileSystemValues": {
          "WindowsConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

如果吞吐能力修改失败，状态将更改为 FAILED 且 FailureDetails 属性中会显示关于失败的信息。有关对失败操作进行问题排查的信息，请参阅存储或吞吐能力更新失败。

管理网络类型

创建 FSx for Windows 文件系统时，必须指定网络类型，该类型必须为以下选项之一：

- IPv4 允许文件系统使用仅互联网协议版本 4（IPv4）进行通信。
- Dual-stack 允许文件系统同时使用互联网协议版本 6（IPv6）和 IPv4 进行通信。

您可以随时使用 Amazon FSx 管理控制台、Amazon CLI、Amazon API 或其中一个 Amazon SDK，以更改现有 FSx for Windows 文件系统的网络类型。例如，如果您的子网同时支持 IPv4 和 IPv6 寻址，则可以将现有文件系统从仅 IPv4 模式更新为双堆栈模式，也可以将双堆栈文件系统更新为仅 IPv4。

使用双堆栈模式

如果您需要从 IPv6 客户端本地访问和管理 Amazon FSx 文件系统，则应使用双堆栈模式。通过将您的 Amazon FSx 文件系统配置为使用双堆栈寻址，您可以从 IPv6 客户端以及 IPv4 客户端在同一 Amazon VPC、另一个 Amazon Web Services 账户 的 VPC 或本地网络中访问您的文件数据。例如，借助已配置为使用双堆栈的 Amazon FSx 文件系统，可让现有 IPv4 客户端和新的 IPv6 客户端访问存储在文件系统上的文件数据。

默认情况下，Amazon FSx 和 Amazon VPC 使用 IPv4 寻址协议。因此，作为使用 IPv6 的先决条件，您必须首先为您的 VPC 和子网分配 Amazon 提供的 IPv6 无类域间范围（CIDR）数据块，然后才能将 IPv6 与 Amazon FSx 文件系统一起使用。有关为 VPC 启用 IPv6 的信息，请参阅《Amazon Virtual Private Cloud 用户指南》中的为 VPC 添加 IPv6 支持。

更改网络类型

您可以使用 Amazon FSx 控制台、Amazon Command Line Interface（Amazon CLI）或 Amazon FSx API 修改文件系统的网络类型。

更改文件系统的网络类型（控制台）

1. 通过以下网址打开 Amazon FSx 控制台：https://console.aws.amazon.com/fsx/。
2. 导航到文件系统，然后选择要为其更改网络类型的 FSx for Windows 文件系统。
3. 对于操作，选择更新网络类型。或者，在网络和安全面板中，选择文件系统的网络类型旁边的管理。

   此时将显示更新网络类型窗口。
4. 对于所需的网络类型，选择 IPv4 或双堆栈。

   - 如果选择 `IPv4`，则无需作进一步配置。
   - 如果选择 `Dual-stack`，则指定文件系统端点将使用的 IPv6 地址范围：
     - 未从 VPC 分配 IPv6 地址范围：Amazon FSx 从 VPC 的 IPv6 CIDR 范围中选择可用的 /118 个 IP 地址作为文件系统的端点 IPv6 地址范围。
5. 选择更新。

修改文件系统的网络类型（CLI）

- 要修改文件系统的网络类型，请使用 CLI 命令 update-file-system（或等效的 UpdateFileSystem API 操作），如下例所示。

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --network-type DUAL
```

为 Amazon FSx 资源贴标签

为帮助您管理文件系统和其他 FSx for Windows File Server 资源，您可以通过标签的形式为每个资源分配您自己的元数据。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

- 标记资源所需的权限

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 FSx for Windows File Server 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《添加标签最佳实践》。

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 FSx for Windows File Server API、Amazon CLI 或 Amazon SDK，则可以使用 `TagResource` API 操作向现有资源应用标签。此外，某些资源创建操作让您可以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。

标记您的资源

您可以标记您账户中已存在的 FSx for Windows File Server 资源。如果您使用的是 Amazon FSx 控制台，您可以使用相关资源屏幕上的“标签”选项卡向资源应用标签。创建资源时，您可以应用带有值的“名称”键，也可以在创建新文件系统时应用您选择的标签。控制台可能根据“名称”标签对资源进行组织，但此标签对 FSx for Windows File Server 服务没有任何语义意义。

对于支持在创建时进行标记的 FSx for Windows File Server 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。

此外，您还可以在 IAM 策略中对 `TagResource` 和 `UntagResource` FSx for Windows File Server API 操作应用资源级权限，从而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）
- 允许在 FSx for Windows File Server 标签中使用的字符包括：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，而必须指定资源标识符。例如，要删除您使用名为 `DeleteMe` 的标签键标记的文件系统，您必须将 `DeleteFileSystem` 操作与文件系统的资源标识符（如 fs-1234567890abcdef0）结合使用。

当您为公有或共享资源添加标签时，您分配的标签仅对您的 Amazon Web Services 账户 可用；其他 Amazon Web Services 账户 无权访问这些标签。为了对共享资源进行基于标签的访问控制，每个 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。

标记资源所需的权限

有关在创建时标记 Amazon FSx 资源所需权限的更多信息，请参阅在创建过程中授予标记资源的权限。有关如何在 IAM 策略中使用标签限制对 Amazon FSx 资源的访问权限的更多信息，请参阅使用标签控制对您的 Amazon FSx 资源的访问权限。

使用 Amazon CLI 更新文件系统

您可以使用本演练中的步骤更新三个元素。对于文件系统中可更新的所有其他元素，您可以从控制台执行此操作。这些过程假定您已在本地计算机上安装和配置 Amazon CLI。有关更多信息，请参阅《Amazon Command Line Interface 用户指南》中的安装和配置。

- AutomaticBackupRetentionDays – 文件系统自动备份的保留天数。

- DailyAutomaticBackupStartTime – 以协调世界时（UTC）设置您希望每日自动备份时段开始的时间。时段为从该指定时间开始的 30 分钟。此时段不能与每周维护备份时段重叠。
- WeeklyMaintenanceStartTime – 维护时段在一周中开始的时间。第 1 天是星期一，第 2 天是星期二，依此类推。时段为从该指定时间开始的 30 分钟。此时段不能与每日自动备份时段重叠。

以下过程概述了如何使用 Amazon CLI 更新文件系统。

更新文件系统的自动备份保留时长

1. 在本地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 替换为您的文件系统的 ID 以及自动备份的保留天数。

```
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时段

1. 在本地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 替换为您的文件系统的 ID，并将时间替换为时段开始的时间。

```
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. 在本地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 替换为您文件系统的 ID，并将日期和时间替换为时段开始的时间。

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-
configuration WeeklyMaintenanceStartTime=1:01:30
```

通过备份、影子副本和计划复制来保护您的数据

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

- Amazon 原生 FSx 备份支持您在亚马逊内部的备份保留和合规需求 FSx。
- Amazon Backup Amazon FSx 文件系统的备份是云端和本地 Amazon 服务的集中式自动备份解决方案的一部分。
- 用户可通过 Windows 影子副本轻松撤消文件更改并通过将文件恢复到早期版本来比较文件版本。
- Amazon DataSync 按计划将您的 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

使用备份保护您的数据。

您可以通过定期备份文件系统来保护 FSx 适用于 Windows File Server 的文件系统上的数据。Amazon FSx 为您提供多种备份文件系统的选项。您可以使用每日自动备份进行每天备份。您可以随时对文件系统进行用户启动的备份。您也可以 Amazon Backup 将其用作 Amazon 资源集中备份解决方案的一部分。这些备份解决方案有助于满足数据留存、业务和合规性需求。

我们建议您使用文件系统默认启用的每日自动备份，并使用 Amazon Backup 集中备份解决方案 Amazon Web Services 服务。 Amazon Backup 允许您配置具有不同频率（例如，一天、每天或每周多次）和保留期的其他备份计划。

使用 Amazon FSx，备份非常 file-system-consistent耐用，而且是增量的。每个备份都包含创建新文件系统所需的所有信息，从而有效地恢复文件系统的 point-in-time快照。为了确保文件系统的一致性，亚马逊在微软 Windows 中 FSx 使用卷影复制服务 (VSS)。为了确保高耐久性，亚马逊将备份 FSx 存储在亚马逊简单存储服务 (Amazon S3) Service 中。

无论是使用每日自动 FSx 备份还是用户启动的备份功能生成，Amazon 备份都是增量备份。这意味着仅保存在最新备份后更改的文件系统数据。由于无需复制数据，这将更大限度地缩短创建备份所需的时间和节省存储成本。

在备份过程中的某个时候，存储 I/O 可能会短暂暂暂停下来，通常会暂停几秒钟。由于 VSS 服务需要将所有缓存的写入内容刷新到磁盘才能恢复 I/O，因此，如果您的工作负载每秒有大量写入操作，则暂停时间可能会更长（`DataWriteOperations`）。大多数最终用户和应用程序都会在短暂的 I/O 暂停中经历这种暂 I/O 停。应用程序对超时设置的敏感度可能有所不同，具体取决于其配置方式。

为您的文件系统创建定期备份是一种最佳实践，它补充了 Amazon FSx for Windows 文件服务器对您的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需求。无论是创建 FSx 备份、复制备份、从备份中恢复文件系统还是删除备份，使用 Amazon 备份都非常简单。请注意，要查看单个文件系统备份的使用情况，您需要启用该特定备份的标签并启用基于标签的账单报告。

主题

使用每日自动备份

默认情况下，Amaz FSx on 会对您的文件系统进行每日自动备份。这些每日自动备份在您创建文件系统时建立的每日备份时段内进行。在选择每日备份时段时，我们建议您为使用文件系统的应用程序选择一天中正常运行时间之外的方便时间。我们还建议选择维护时段之外的备份时段，因为如果持续进行文件系统维护，则可能无法进行自动备份。

每日自动备份会保留一段时间，称为保留期。在 Amazon FSx 控制台中创建文件系统时，默认的每日自动备份保留期为 30 天。亚马逊 FSx API 和 CLI 的默认保留期不同。您可以将保留期设置为 0 到 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 天意味着文件系统永远不会自动备份。我们强烈建议您对具有任何关键功能级别的文件系统使用每日自动备份。

您可以使用 Amazon CLI 或其中一个 Amazon SDKs 来更改文件系统的备份窗口和备份保留期。使用 `UpdateFileSystem` API 操作或 `update-file-system` CLI 命令。有关更多信息，请参阅 使用 Amazon CLI 更新文件系统。

> **Important**
>
> 缩短每日自动备份的保留期将导致超出新保留时段的备份被永久删除。继续操作之前，确保不再需要这些较旧的备份。

使用用户启动备份

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) 来执行此操作。用户启动的 Amazon FSx 文件系统备份永远不会过期，只要您想保留这些备份，它们就可用。即使您删除了已备份的文件系统，用户启动备份也会保留。您只能使用亚马逊 FSx 控制台、API 或 CLI 删除用户启动的备份。它们永远不会被亚马逊自动删除 FSx。有关更多信息，请参阅 删除备份。

如果备份是在修改文件系统时（例如在更新吞吐能力期间或文件系统维护期间）启动，则备份请求将排队并在活动完成后恢复。

要了解如何对文件系统进行用户启动的备份，请参阅 创建用户启动备份。

在 Amazon Amazon Backup 上使用 FSx

Amazon Backup 是一种通过备份 Amazon FSx 文件系统来保护数据的简单且经济实惠的方法。Amazon Backup 是一项统一的备份服务，旨在简化备份的创建、复制、恢复和删除，同时提供更好的报告和审计。 Amazon Backup 可以更轻松地为法律、监管和专业合规制定集中备份策略。 Amazon Backup 还提供了一个可以执行以下操作的中心位置，从而简化了对 Amazon 存储卷、数据库和文件系统的保护：

- 配置和审核要备份的 Amazon 资源。
- 计划自动备份。

- 设置保留策略。
- 跨 Amazon 地区和跨 Amazon 账户复制备份。
- 监控所有最近的备份、复制和还原活动。

Amazon Backup 使用 Amazon 的内置备份功能 FSx。从 Amazon Backup 控制台获取的备份与通过 Amazon 控制 FSx 台进行的备份具有相同级别的文件系统一致性和性能，以及相同的还原选项。与您创建的任何其他 Amazon 备份相比，从中获取的 FSx 备份 Amazon Backup 是增量备份，无论是用户启动的备份还是自动备份。

如果您使用 Amazon Backup 管理这些备份，则可以获得其他功能，例如无限的保留选项，以及能够像每小时一样频繁地创建定时备份。此外，即使在源文件系统被删除之后，也会 Amazon Backup 保留不可变的备份。这样可以防止意外或恶意删除。

执行的备份 Amazon Backup 被视为用户启动的备份，它们计入用户启动的 Amazon 备份配额。 FSx 您可以在 Amazon FSx 控制台、CLI 和 API Amazon Backup 中查看和还原所做的备份。但是，您无法删除在 Amazon FSx 控制台、CLI 或 API Amazon Backup 中拍摄的备份。有关 Amazon Backup 如何使用备份您的亚马逊 FSx 文件系统的更多信息，请参阅《Amazon Backup 开发人员指南》中的 “使用亚马逊 FSx 文件系统”。

复制备份

您可以使用 Amazon FSx 将同一 Amazon 账户内的备份手动复制到另一个 Amazon 区域（跨区域副本）或同一区域内的备份（ Amazon 区域内副本）。您只能在同一 Amazon 分区内制作跨区域副本。您可以使用 Amazon FSx 控制台或 API 创建用户启动的备份副本。 Amazon CLI创建用户启动备份副本时，其类型为 `USER_INITIATED`。

您还可以 Amazon Backup 使用跨 Amazon 区域和跨 Amazon 账户复制备份。 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价值。您可以备份并将其复制到另一个 Amazon 区域，这样在主 Amazon 区域发生灾难时，您可以从备份中恢复并快速恢复另一个 Amazon 区域的可用性。您也可以使用备份副本将文件数据集克隆到其他 Amazon 区域或同一 Amazon 区域内。您可以使用亚马逊 FSx 控制台或 Amazon API 在同一个 Amazon 账户（跨区域或区域内）内制作备份副本。 Amazon CLI FSx 您还可以使用 Amazon Backup 按需或基于策略执行备份副本。

跨账户备份副本对于满足将备份复制到隔离账户的监管合规要求非常重要。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、证书丢失或 Amazon KMS 密钥泄露。跨账户备份支持扇

入（将备份从多个主账户复制到一个隔离的备份副本账户）和扇出（将备份从一个主账户复制到多个隔离的备份副本账户）。

您可以通过使用 Amazon Backup Amazon Organizations 支持来制作跨账户备份副本。跨账户副本的账户界限由 Amazon Organizations 政策定义。有关使用 Amazon Backup 制作跨账户备份副本的更多信息，请参阅Amazon Backup 开发者指南 Amazon Web Services 账户中的跨账户创建备份副本。

备份副本限制

复制备份时，存在以下一些限制：

- 仅支持任意两个商业区域之间、中国（北京）和中国（宁夏） Amazon 区域之间，以及（美国东部）和 Amazon GovCloud Amazon GovCloud （美国西部）区域之间的跨区域备份副本，但不支持跨这两组区域。
- 选择加入区域不支持跨区域备份副本。
- 您可以在任何 Amazon 区域内制作区域内备份副本。
- 源备份的状态必须为 `AVAILABLE`，然后才能进行复制。
- 如果源备份正在复制，则无法将其删除。在目标备份变为可用和允许删除源备份之间可能会有短暂的延迟。如果您重试删除源备份，则应注意这种延迟。
- 每个账户最多可以向一个目标 Amazon 区域提交五个备份副本请求。

跨区域备份副本的权限

您可以使用 IAM 策略声明来授予执行备份复制操作的权限。要与源 Amazon 区域通信以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。

您可以使用该策略授予 `CopyBackup` 备份复制操作权限。您可以在策略的 `Action` 字段中指定该操作，并在策略的 `Resource` 字段中指定资源值，如下面的示例所示。

JSON

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

```
        }
    ]
}
```

有关 IAM 策略的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略与权限。

完整和增量拷贝

将备份复制到与源备份不同的目标 Amazon 区域或目标 Amazon 帐户时，即使您使用相同的 KMS 密钥对备份的源副本和目标副本进行加密，第一个副本也是完整备份副本。

在第一次备份副本之后，同一 Amazon 账户中同一目标区域的所有后续备份副本均为增量备份，前提是您尚未删除该区域中所有先前复制的备份并且一直在使用相同的 Amazon KMS 密钥。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。

要了解如何复制文件系统备份，请参阅 同一账户内复制备份。

将备份还原至新文件系统

您可以使用可用备份来创建新的文件系统，从而有效地恢复另一个文件系统的 point-in-time快照。您可以使用控制台 Amazon CLI、或其中一个来恢复备份 Amazon SDKs。将备份恢复到新文件系统所需的时间与创建新文件系统所需的时间相同。从备份中恢复的数据会延迟加载到文件系统中，在此期间会经历较高延迟。

为确保用户可以继续访问已还原的文件系统，请确保还原文件系统的关联 Active Directory 域与原始文件系统的 Active Directory 域相同，或者受原始文件系统的 Active Directory 域信任。有关 Active Directory 的更多信息，请参阅 使用 Microsoft Active Directory。

要了解如何将备份还原到新 FSx 的 Windows 文件系统，请参阅将备份还原至新文件系统。

> **Note**
>
> 您只能将文件系统备份还原到与原始部署类型和存储容量相同的新文件系统。您可以在新文件系统可用后增加其存储容量。有关更多信息，请参阅 管理存储容量。

将备份还原至新文件系统时，可以更改以下任何文件系统设置：

- 存储类型

- 吞吐能力
- 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
- 每周维护窗口

创建用户启动备份

除了每日自动备份文件系统外，您还可以随时使用 Amazon FSx 控制台创建用户启动的文件系统备份，如以下过程所述。

创建用户启动文件系统备份

1. 打开 Amazon FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 从控制台控制面板中，选择要备份的文件系统的名称。
3. 在操作中，选择创建备份。
4. 在打开的创建备份对话框中，为备份提供一个名称。备份名称最多可以包含 256 个 Unicode 字符，以及字母、空格、数字和特殊字符 . + - = _ : /
5. 选择创建备份。

现在，您已经创建了文件系统备份。在左侧导航栏中选择 “备份”，即可在 Amazon FSx 控制台中找到所有备份的表。用户启动的新备份的类型为 `USER_INITIATED`，其状态为 `CREATING`，直到变成 `AVAILABLE`。有关更多信息，请参阅 使用用户启动备份。

删除备份

您可以使用 Amazon FSx 控制台、CLI 或 API 删除文件系统的所有用户启动和每日自动备份，如以下过程所述。要删除由 Amazon Backup（类型为 Backup）的Amazon 备份，必须使用 Amazon Backup 控制台、CLI 或 API。删除备份是一项永久性且不可恢复的操作。删除的备份中的所有数据也会被删除。除非您确定将来不再需要该备份，否则不要删除该备份。

删除备份（控制台）

1. 打开 Amazon FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 在控制台控制面板的左侧导航窗格中选择备份。
3. 选择备份表中您要删除的备份，然后选择删除备份。
4. 在打开的删除备份对话框中，确认备份 ID 与要删除的备份 ID 一致。
5. 确认已选中要删除的备份对应的复选框。
6. 选择删除备份。

您的备份和所有包含的数据现已永久删除且不可恢复。

备份大小

备份大小由文件系统中已用存储空间（而不是总预置存储容量）来确定。备份大小将取决于已用存储容量以及文件系统上的数据流失量。根据数据在文件系统存储卷中的分配方式及其更改频率，总备份使用量可能会大于或小于已用存储容量。删除备份时，仅会删除该备份特有的数据。

为了提供持久的增量备份，Amazon 在块级别 FSx 备份数据。 file-system-consistent文件系统存储卷上的数据可以存储在多个块中，具体取决于数据被写入或覆盖的模式。因此，备份使用量的总大小可能与文件系统上文件和目录的确切大小不匹配。您的总体备份使用量和成本可以在 Amazon Billing 控制面板中找到，或者 Amazon Cost Management Console。

使用标签来整理 Amazon 账单，以反映您自己的成本结构。为此，请注册以获取包含标签键值的 Amazon Web Services 账户 账单。然后，如需查看组合资源的成本，请按有同样标签键值的资源组织您的账单信息。例如，您可以将特定的应用程序名称用作几个资源的标签，然后组织账单信息，以查看在数个服务中的使用该应用程序的总成本。有关更多信息，请参阅《Amazon Billing 用户指南》中的使用成本分配标签。

> **Note**
>
> 增加存储容量时，将数据从旧存储磁盘组迁移到新的大容量存储磁盘组的过程可能导致备份使用量暂时增加，直到与旧存储磁盘集关联的备份被删除为止。如果在增加存储容量之前，文件系统的存储空间仅部分使用，则需迁移到新磁盘的数据大小可能大于原始存储磁盘上的实际数据大小。这可能导致备份使用量增加至新的存储容量级别。您应考虑增加存储容量对备份计划产生的影响。

同一账户内复制备份

您可以使用 Amazon Web Services 管理控制台 和 Amazon CLI 通过以下步骤将同一 Amazon 账户内的备份手动复制到另一个账户 Amazon Web Services 区域 （跨区域副本）或同一账户内的备份 Amazon Web Services 区域 （区域内副本）。

使用控制台在同一账户（跨区域或区域内）内复制备份

1. 打开 Amazon FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 在导航窗格中，选择备份。
3. 选择备份表中您要复制的备份，然后选择复制备份。
4. 在设置部分，执行以下操作：
   - 在目标区域列表中，选择要将备份复制到的目标 Amazon 区域。目的地可以位于其他 Amazon 区域（跨区域副本）或同一 Amazon 区域（区域内副本）。
   - （可选）选择复制标签，将标签从源备份复制到目标备份。如果您在步骤 6 中选择复制标签并添加标签，则会合并所有标签。
5. 对于加密，选择 Amazon KMS 加密密钥来加密复制的备份。
6. 对于标签 – 可选，输入键和值以将标签添加到您复制的备份。如果您此步骤中添加标签，并在步骤 4 中选择复制标签，则会合并所有标签。
7. 选择复制备份。

您的备份将在同一个 Amazon 账户中复制到所选 Amazon 区域。

使用 CLI 在同一账户（跨区域或区域内）内复制备份

- 使用 `copy-backup` CLI 命令或 CopyBackupAPI 操作在同一个 Amazon 账户内复制备份，无论是在一个 Amazon 区域还是在一个 Amazon 区域内。

  以下命令从 `us-east-1` 区域复制 ID 为 `backup-0abc123456789cba7` 的备份。

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

  响应显示了复制备份的描述。

您可以在 Amazon FSx 控制台上查看备份，也可以使用 `describe-backups` CLI 命令或 DescribeBackupsAPI 操作以编程方式查看备份。

将备份还原至新文件系统

您可以使用 Amazon Web Services 管理控制台、CLI 和 API 恢复文件系统备份以创建新的文件系统，如以下过程所述。

从备份中还原文件系统

1. 打开 Amazon FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 在控制台控制面板的左侧导航窗格中选择备份。
3. 选择备份表中您要还原的备份，然后选择还原备份。

   这样做会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，唯一不同的是部署类型和存储容量已设置且无法更改。但是，您可以更改吞吐能力、关联的 VPC，以及其他设置和存储类型。默认情况下，存储类型设置为 SSD，但您可以在以下条件下将其更改为 HDD：

   - 文件系统部署类型为多可用区或单可用区 2。
   - 存储容量至少为 2000 GiB。
4. 按照创建新文件系统时的操作完成向导。
5. 选择审核和创建。
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。

   Amazon FSx 正在创建一个新的文件系统，一旦其状态更改为`AVAILABLE`，您就可以照常使用该文件系统了。

使用影子副本保护您的数据

Microsoft Windows 影子副本是 Windows 文件系统在某个时间点的快照。启用影子副本后，用户可以快速恢复存储在网络上的已删除文件或更改文件，并比较文件版本。存储管理员可以使用 Windows PowerShell 命令轻松安排定期拍摄卷影副本。

影子副本与文件系统的数据一同存储，仅为更改的文件部分消耗文件系统存储容量。存储在文件系统中的所有影子副本都包含在文件系统的备份中。

> **Note**
>
> 默认情况下，Windows 文件服务器不启用卷影副本。 FSx 要使用影子副本保护文件系统上的数据，您必须启用影子副本，并在文件系统上设置影子复制计划。有关更多信息，请参阅 配置影子副本使用默认存储和计划。

> **Warning**
>
> 影子副本不能替代备份。如果启用影子副本，请确保继续执行定期备份。

主题

使用影子副本的最佳实践

您可以为文件系统启用影子副本，以允许最终用户在 Windows 文件资源管理器中查看和恢复早期快照中的单个文件或文件夹。亚马逊 FSx 使用微软 Windows Server 提供的卷影复制功能。使用以下最佳实践创建影子副本：

- 确保您的文件系统有足够的性能资源：Microsoft Windows 使用一种 copy-on-write方法来记录自上次卷影复制点以来的更改，并且此 copy-on-write活动可能导致每个文件写入操作最多 I/O 执行三次操作。
- 使用 SSD 存储并提高吞吐能力：由于 Windows 需要高水平 I/O 性能来维护影子副本，因此我们建议使用 SSD 存储并将吞吐能力提高至预期工作负载的三倍。这有助于确保您的文件系统有足够的资源来避免影子副本被意外删除等问题。
- 仅维护所需数量的影子副本：如果您有大量影子副本（例如，超过 64 个最新影子副本）或者影子副本在单个文件系统上占用大量存储空间（TB 级），则失效转移和失效自动恢复等进程可能需要一些额外时间。这是因为 Windows 需要 FSx 对卷影副本存储进行一致性检查。由于 Windows 需要在维护卷影副本的同时执行 copy-on-write活动，因此您可能还会遇到更高的 I/O 操作延迟。 FSx 要最大限度地减少影子副本对可用性和性能的影响，请手动删除未使用的影子副本，或者配置脚本以自动删除文件系统上的旧影子副本。

> **Note**
>
> 在多可用区文件系统的故障转移事件中， FSx Windows 版会运行一致性检查，要求在新的活动文件服务器上线之前扫描文件系统上的卷影副本存储。一致性检查的持续时间与文件系统上影子副本的数量以及消耗的存储空间有关。为防止失效转移和失效自动恢复事件延迟，我们建议在文件系统上保留的影子副本少于 64 个，并按照以下步骤定期监控和删除最早的影子副本。

设置影子副本

您可以使用 Amazon 定义的 Windows PowerShell 命令在文件系统上启用和安排定期卷影复制 FSx。以下是在你 FSx 的 Windows 文件服务器文件系统上配置卷影副本时的三个主要设置：

- 设置影子副本在文件系统上可以消耗的最大存储量
- （可选）设置可以在文件系统上存储的最大影子副本数。默认值为 20。
- （可选）设置计划，定义创建影子副本的时间和间隔（例如每天、每周和每月）

每个文件系统在任意时间点可以存储最多 500 个影子副本；但为了确保可用性和性能，我们建议在任何时候保持少于 64 个影子副本。当达到此限制时，您获取的下一个影子副本将替换最旧的影子副本。同样，当达到最大影子副本存储量时，系统会删除一个或多个最旧的影子副本，以便为下一个影子副本腾出足够的存储空间。

有关如何使用默认 Amazon FSx 设置快速启用和安排定期卷影复制的信息，请参阅配置影子副本使用默认存储和计划。

分配影子副本存储空间的注意事项

影子副本是自上个影子副本以来所做的文件更改的块级副本。不会复制整个文件，只复制更改部分。因此，以前版本的文件占用的存储空间通常没有当前文件多。用于更改的卷空间量可能因您的工作负载而异。修改文件时，影子副本使用的存储空间取决于您的工作负载。确定分配给影子副本的存储空间时，您应考虑工作负载的文件系统使用模式。

启用影子副本时，您可以指定影子副本在文件系统上可以消耗的最大存储量。默认限制为文件系统的 10%。如果用户经常添加或修改文件，我们建议您增加限制。限制设置得太小可能会导致删除最旧影子副本的频率比用户预期得要高。

您可以将影子副本存储设置为无界（`Set-FsxShadowStorage -Maxsize "UNBOUNDED"`）。但是，无界配置可能会导致大量影子副本消耗文件系统存储空间。这可能会导致存储容量不足以容纳您的工作负载。如果您设置了无界存储，请务必在达到影子副本限制时扩展存储容量。有关将影子副本存储配置为特定大小或无界存储的信息，请参阅设置影子副本的最大存储量。

启用影子副本后，您可以监控影子副本消耗的存储空间量。有关更多信息，请参阅 查看影子副本存储空间。

设置最大影子副本数时的注意事项

启用影子副本时，您可以指定文件系统上存储的最大影子副本数量。默认限制为 20 个，为了最大程度地减少影子副本对可用性和性能的影响，Microsoft 建议将最大影子副本数配置为少于 64 个。由于 Windows 需要较高的 I/O 性能来维护卷影副本，因此我们建议使用 SSD 存储并将吞吐量增加到预期工作负载的三倍。这有助于确保您的文件系统有足够的资源来避免影子副本被意外删除等问题。

您最多可以设置 500 个影子副本。但是，如果您有大量影子副本或者影子副本在单个文件系统中占用了大量存储空间（TB 级），则失效转移和失效自动恢复等过程可能会花费比预期更长的时间。这是因为 Windows 需要对影子副本存储进行一致性检查。由于 Windows 需要在维护卷影副本的同时执行 copy-on-write活动，因此您可能还会遇到更高的 I/O 操作延迟。

影子副本的文件系统建议

以下是使用影子副本的文件系统建议。

- 确保在文件系统上预置足够的性能容量以满足工作负载需求。亚马逊 FSx 提供由微软 Windows Server 提供的影子副本功能。从设计上讲，Microsoft Windows使用一种 copy-on-write方法来记

录自最新卷影复制点以来的更改，此 copy-on-write活动最多可以产生三种I/O operations for every file write operation. If Windows is unable to keep up with the incoming rate of I/O operations per second, it can cause all shadow copies to be deleted because it can no longer maintain the shadow copies via copy-on-write. Therefore, it is important that you provision sufficient I/O performance capacity for your workload needs on your file system (both the throughput capacity dimension that determines the file server I/O performance, and the storage type and capacity that determine the storage I/O性能）。

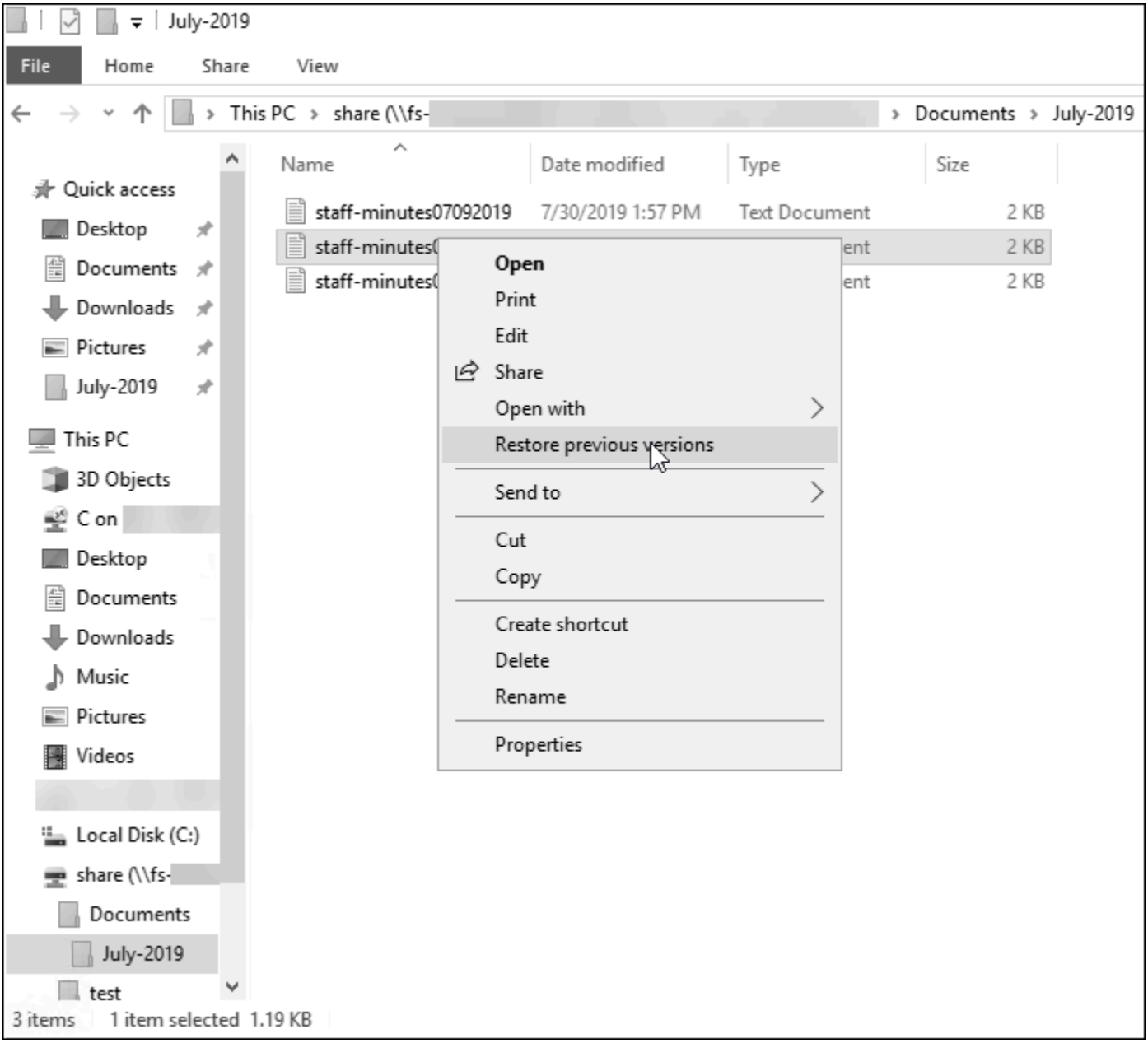
- 我们通常建议您在启用卷影副本时使用配置有 SSD 存储而不是 HDD 存储的文件系统，因为 Windows 维护卷影副本消耗的 I/O 性能更高，而且硬盘存储为 I/O 操作提供的性能容量较低。
- 除了配置的最大影子副本存储量外，您的文件系统还应至少有 320 MB 的可用空间（`MaxSpace`）。例如，如果您为影子副本分配了 5 GB `MaxSpace`，则除了 5 GB `MaxSpace` 之外，您的文件系统应始终至少有 320 MB 的可用空间。

> **Warning**
>
> 配置影子复制计划时，请确保在迁移数据或按计划运行重复数据删除作业时不要安排影子复制。您应该在预计文件系统处于空闲状态时安排影子复制。有关配置自定义影子复制计划的信息，请参阅创建自定义影子副本计划。

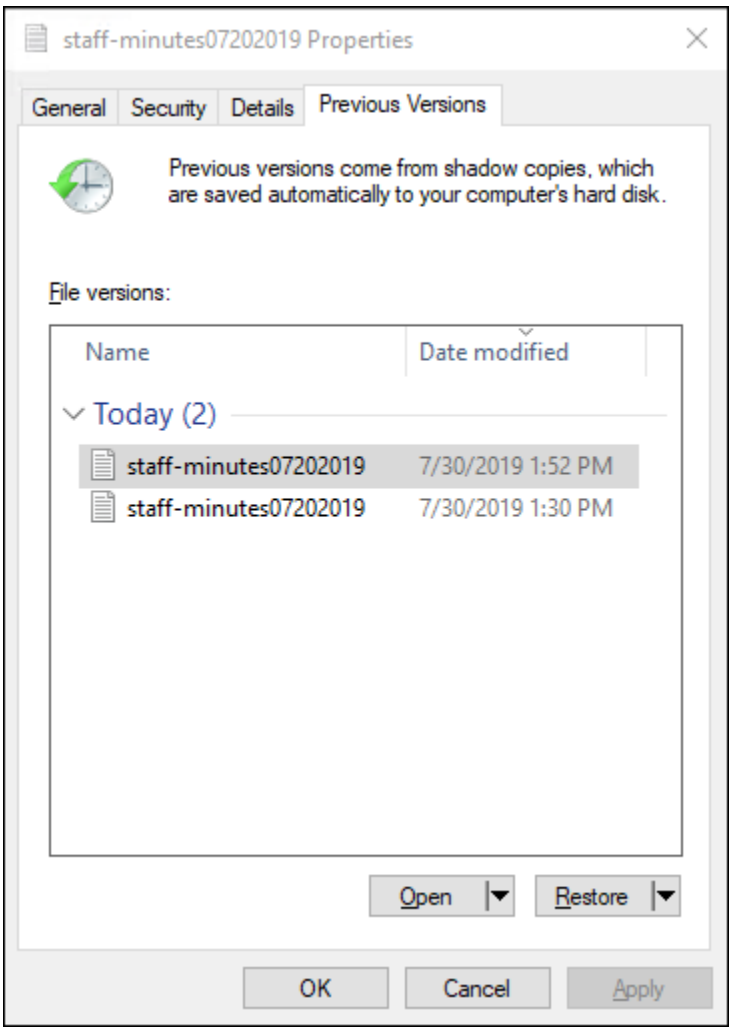
还原单个文件和文件夹

在您的 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，并恢复已删除的文件。

用户可使用常用的 Windows 文件资源管理器界面将文件还原到以前的版本。若要还原文件，您需选择要还原的文件，然后从上下文（右键单击）菜单中选择还原先前版本。



然后，用户就可以从先前版本列表中查看和还原以前的版本。



配置影子副本使用默认存储和计划

您可以使用默认影子副本存储和计划，在文件系统上快速设置影子副本。默认的影子副本存储设置允许影子副本最多消耗文件系统存储容量的 10%。如果您增加文件系统的存储容量，则当前分配的影子副本存储量不会以类似方式增加。

默认计划在 UTC 时间每周一、周二、周三、周四和周五上午 7:00 和中午 12:00 自动获取影子副本。

设置影子副本存储的默认级别

1. 连接到与您的文件系统具有网络连接的 Windows 计算实例。
2. 以文件系统管理员组成员的身份登录 Windows 计算实例。在中 Amazon Managed Microsoft AD，该组是Amazon 授权 FSx 管理员。在自行管理的 Microsoft AD 中，该组是域管理员或是在您创建文件系统时指定的自定义管理组。有关更多信息，请参阅亚马逊 EC2 用户指南中的连接到您的 Windows 实例。

3. 使用以下命令设置默认的影子存储量。*FSxFileSystem-Remote-PowerShell-Endpoint*替换为要管理的文件系统的 Windows 远程 PowerShell 端点。您可以在亚马逊 FSx 控制台、文件系统详细信息屏幕的 “网络和安全” 部分或 `DescribeFileSystem` API 操作的响应中找到 Windows 远程 PowerShell 终端节点。

```
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 MaxShadowCopyNumber
-------------- ---------    -------- ------------------
             0         0 10737418240                 20
```

设置默认影子复制计划

1. 连接到与您的文件系统具有网络连接的 Windows 计算实例。
2. 以文件系统管理员组成员的身份登录 Windows 计算实例。在中 Amazon Managed Microsoft AD，该组是Amazon 授权 FSx 管理员。在自行管理的 Microsoft AD 中，该组是域管理员或是在您创建文件系统时指定的自定义管理组。有关更多信息，请参阅亚马逊 EC2 用户指南中的连接到您的 Windows 实例。
3. 使用以下命令设置默认影子复制计划。

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

系统响应会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影子复制计划，请参阅创建自定义影子副本计划。

设置影子副本的最大存储量

您可以使用Set-FsxShadowStorage自定义 PowerShell 命令定义卷影副本在文件系统上可以消耗的最大存储量。您可以使用 -Maxsize 或 -Default 参数指定影子副本可增大到的最大大小。使用 Default 可以将最大值设置为文件系统存储容量的 10%。您不能在同一个命令中指定 -Maxsize 和 -Default 参数。

使用 -Maxsize，您可以按如下方式定义影子副本存储：

- 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) 或 Set-FsxShadowStorage -Maxsize (2.5GB)
- 占总存储空间的百分比：Set-FsxShadowStorage -Maxsize "20%"
- 设置为无界：Set-FsxShadowStorage -Maxsize "UNBOUNDED"

使用 -Default 将影子存储设置为最多使用文件系统的 10%：Set-FsxShadowStorage -Default。要了解有关使用默认选项的更多信息，请参阅配置影子副本使用默认存储和计划。

在 FSx 适用于 Windows 的文件服务器文件系统上设置卷影副本存储量

1. 以文件系统管理员组成员的用户的身份连接到与您的文件系统具有网络连接的计算实例。在中 Amazon Managed Microsoft AD，该组是Amazon 授权 FSx管理员。在自行管理的 Microsoft AD 中，该组是域管理员或是在您创建文件系统时指定的自定义管理组。有关更多信息，请参阅亚马逊 EC2 用户指南中的连接到您的 Windows 实例。
2. 在计算实例上 PowerShell 打开 Windows 窗口。
3. 使用以下命令在您的 Amazon FSx 文件系统上打开远程 PowerShell 会话。*FSxFileSystem-Remote-PowerShell-Endpoint*替换为要管理的文件系统的 Windows 远程 PowerShell 端点。您可以在亚马逊 FSx 控制台、文件系统详细信息屏幕的 “网络和安全” 部分或 DescribeFileSystem API 操作的响应中找到 Windows 远程 PowerShell 终端节点。

```
PS C:\Users\delegateadmin> enter-pssession -computername FSxFileSystem-Remote-PowerShell-Endpoint -configurationname fsxremoteadmin
```

4. 使用以下命令验证文件系统上是否尚未配置影子副本存储。

```
[fs-1234567890abcef12]: PS>Get-FsxShadowStorage
```

```
No Fsx Shadow Storage Configured
```

5. 使用 -Default 选项将影子存储量设置为卷的 10%，并将最大影子副本数量设置为 20。

```
[fs-1234567890abcef12]: PS>Set-FsxShadowStorage -Default
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
-------------- ---------    -------- ------------------
             0         0 32530536858                 20
```

可以通过使用带 -MaxShadowCopyNumber 参数的 Set-FSxShadowStorage 命令来限制文件系统上允许的最大影子副本数，您可以指定一个介于 1-500 之间的值。根据 Microsoft 对活动工作负载的建议，最大影子副本数默认设置为 20 个。

查看影子副本存储空间

在文件系统的远程 PowerShell 会话中，您可以使用Get-FsxShadowStorage命令查看文件系统上卷影副本当前消耗的存储量。有关在文件系统上启动远程 PowerShell 会话的说明，请参阅将 Amazon FSx CLI 用于 PowerShell。

```
[fs-1234567890abcef12]: PS>PS>Get-fsxshadowstorage
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
-------------- ---------    -------- ------------------
             0         0 10737418240                 20
```

输出会显示影子存储配置，如下所示：

- AllocatedSpace – 文件系统上当前分配给影子副本的存储量（以字节为单位）。该值初始为 0。
- UsedSpace – 影子副本当前使用的存储量（以字节为单位）。该值初始为 0。
- MaxSpace – 影子存储可增大到的最大存储量（以字节为单位）。这是您使用 Set-FsxShadowStorage 命令为影子副本存储设置的值。
- MaxShadowCopyNumber - 文件系统可以拥有的最大影子副本数，介于 1-500 之间。

当 UsedSpace 容量达到配置的最大影子副本存储量 (MaxSpace) 或影子副本数达到配置的最大影子副本数 (MaxShadowCopyNumber) 时，您创建的下一个影子副本将替换掉最早的影子副本。如果您不想

丢掉最早的影子副本，请监控影子副本的存储空间，确保有足够的存储空间来存放新的影子副本。如果您需要更多空间，可以删除现有影子副本或增加影子副本存储的最大存储量。

> **Note**
>
> 自动或手动创建影子副本时，它们会使用您配置的影子副本存储量作为存储限额。卷影副本的大小会随着时间的推移而增长，并利用 CloudWatch `FreeStorageCapacity`指标所显示的可用存储空间，直至配置的最大卷影副本存储量（`MaxSpace`）。

创建自定义影子副本计划

影子副本计划使用 Microsoft Windows 中的计划任务触发器来指定何时自动生成影子副本。影子副本计划可以有多个触发器，为您的计划提供了出色的灵活性。同一时间只能存在一个影子副本计划。在创建影子副本计划之前，必须先设置影子副本存储。

在文件系统上运行 `Set-FsxShadowCopySchedule` 命令时，会覆盖所有现有的影子副本计划。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` 选项为触发器指定时区。如需查看 Windows 时区列表，请参阅 Microsoft 的默认时区文档或在 Windows 命令提示符下运行以下命令：`tzutil /l`。要了解有关 Windows 任务触发器的更多信息，请参阅 Microsoft Windows 开发人员中心文档中的任务触发器。

您还可以使用 `-Default` 选项快速设置默认的影子副本计划。要了解更多信息，请参阅配置影子副本使用默认存储和计划。

创建自定义影子副本计划

1. 创建一组 Windows 计划任务触发器，以定义影子副本计划中创建影子副本的时间。在本地计算机PowerShell上使用中的`new-scheduledTaskTrigger`命令来设置多个触发器。

   以下示例创建了一个自定义影子副本计划，该计划在 UTC 每周一至周五上午 6:00 和下午 6:00 创建影子副本。除非您在创建的 Windows 计划任务触发器中指定时区，否则默认情况下时间均为 UTC。

   ```
   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。该命令会编写一个脚本，使用您刚刚创建的 new-scheduledTaskTrigger 值来设置影子副本计划。*FSxFileSystem-Remote-PowerShell-Endpoint*替换为要管理的文件系统的 Windows 远程 PowerShell 端点。您可以在亚马逊 FSx 控制台、文件系统详细信息屏幕的 “网络和安全” 部分或 DescribeFileSystem API 操作的响应中找到 Windows 远程 PowerShell 终端节点。

```
PS C:\Users\delegateadmin> invoke-command -ComputerName FSxFileSystem-Remote-
PowerShell-Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {
```

3. 在 >> 提示符下输入以下行，使用 set-fsxshadowcopyschedule 命令设置影子副本计划。

```
>> set-fsxshadowcopyschedule -scheduledtasktriggers $Using:trigger1,$Using:trigger2
 -Confirm:$false }
```

响应将显示您在文件系统上配置的影子副本计划。

```
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
```

查看影子副本计划

要查看文件系统上现有的卷影复制时间表，请在文件系统的远程会 PowerShell 话中输入以下命令。有关在文件系统上启动远程 PowerShell 会话的说明，请参阅将 Amazon FSx CLI 用于 PowerShell。

```
[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
```

创建影子副本

要手动创建卷影副本，请在文件系统的远程会 PowerShell 话中输入以下命令。有关在文件系统上启动远程 PowerShell 会话的说明，请参阅将 Amazon FSx CLI 用于 PowerShell。

```
[fs-0123456789abcdef1]PS>New-FsxShadowCopy

Shadow Copy {ABCDEF12-3456-7890-ABCD-EF1234567890} taken successfully
```

查看现有影子副本

要查看文件系统上的现有卷影副本集，请在文件系统的远程会 PowerShell 话中输入以下命令。有关在文件系统上启动远程 PowerShell 会话的说明，请参阅将 Amazon FSx CLI 用于 PowerShell。

```
[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

您可以在文件系统的远程 PowerShell 会话中使用`Remove-FsxShadowCopies`命令删除文件系统中的一个或多个现有卷影副本。有关在文件系统上启动远程 PowerShell 会话的说明，请参阅将 Amazon FSx CLI 用于 PowerShell。

使用以下必选项之一指定要删除的影子副本：

- `-Oldest` 删除最早的影子副本
- `-All` 删除所有现有影子副本
- `-ShadowCopyId` 按 ID 删除特定的影子副本。

您也可以仅使用一个含命令的选项 如果您未指定要删除的卷影副本、指定多个卷影副本 IDs，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，请在文件系统的远程 PowerShell 会话中输入以下命令。

```
[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，请在文件系统的远程会 PowerShell 话中输入以下命令。

```
[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.
```

要在文件系统中删除一定数量的最旧影子副本，请将 -MaxShadowCopyNumber 参数更新为想要保留的所需影子副本数。但是，此种更改只有在拍摄下一个影子副本快照后才会生效，届时系统将自动删除多余的影子副本。在文件系统的远程会 PowerShell 话中使用以下命令。

```
[fs-1234567890abcef12]: PS>Get-fsxshadowstorage
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace MaxSpace    MaxShadowCopyNumber
-------------- --------- ----------- -------------------
     556679168  21659648 10737418240                  50

[fs-1234567890abcef12]: PS>Set-FsxShadowStorage  -MaxShadowCopyNumber 5
Validation
You have 50 shadow copies. Older versions of shadow copies will be deleted, keeping 5
 latest shadow copies on your file system.
Do you want to continue?
[Y] Yes  [N] No  [?] Help (default is "N"): y
FSx Shadow Storage Configuration
```

```
AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
-------------- ---------    -------- -------------------
     556679168  21659648 10737418240                   5
```

删除影子副本计划

要删除文件系统上现有的卷影复制计划，请在文件系统的远程会 PowerShell 话中输入以下命令。有关在文件系统上启动远程 PowerShell 会话的说明，请参阅将 Amazon FSx CLI 用于 PowerShell。

```
[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>
```

删除影子副本的存储空间、计划和所有影子副本

您可以删除影子副本配置（包括所有现有的影子副本）和影子副本计划。同时，您可以释放文件系统上的影子副本存储空间。

为此，请在文件系统的远程会 PowerShell话中输入该`Remove-FsxShadowStorage`命令。有关在文件系统上启动远程 PowerShell 会话的说明，请参阅将 Amazon FSx CLI 用于 PowerShell。

```
[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.
```

卷影副本问题排查

卷影副本丢失或无法访问的潜在原因有很多，详情如下一部分所述。

主题

最早的卷影副本丢失

在以下任一情况下，最早的卷影副本都会被删除：

- 如果您有 500 个卷影副本，则无论为卷影副本分配的剩余存储卷空间如何，下一个卷影副本都会替换最早的卷影副本。
- 如果达到配置的最大卷影副本存储量，则下一个卷影副本将替换一个或多个最早的卷影副本，即使您的卷影副本少于 500 个。

这两个结果都是预期行为。如果为卷影副本分配的存储空间不足，请考虑增加分配的存储空间。

我所有的卷影副本都丢失了

文件系统的 I/O 性能容量不足（例如，因为您使用的是硬盘存储、HDD 存储空间已用完突发容量或吞吐容量不足）可能会导致 Windows Server 删除所有卷影副本，因为它无法使用可用 I/O 性能容量维护卷影副本。请考虑以下建议，帮助防止出现此问题：

- 如果您使用的是硬盘存储，请使用亚马逊 FSx 控制台或亚马逊 FSx API 切换到使用 SSD 存储。有关更多信息，请参阅 管理文件系统存储类型。
- 将文件系统的吞吐能力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，还应确保您的文件系统至少有 320 MB 的可用空间。
- 在预计文件系统处于空闲状态时安排卷影副本。

有关更多信息，请参阅 影子副本的文件系统建议。

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

这是预料之中的行为。Amazon 在最近恢复的文件系统上 FSx 重建卷影副本状态，并且在重建仍在进行时不允许访问卷影副本或备份。

使用计划复制 Amazon DataSync

您可以使用安排定期 Amazon DataSync 将 for Window FSx s 文件服务器文件系统复制到第二个文件系统。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 Amazon DataSync 将现有文件迁移到 FSx for Windows File Server本指南和Amazon DataSync 用户指南中的Amazon 存储服务之间的数据传输。

将 FSx for Windows File Server 与 Microsoft SQL Server 结合使用

高可用性（HA）Microsoft SQL Server 通常部署在 Windows 服务器失效转移集群（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。您可以通过两种方式使用 FSx for Windows File Server 作为高可用性（HA）Microsoft SQL Server 部署的共享存储：用作活动数据文件的存储和用作 SMB 文件共享见证。

> **Note**
>
> 目前，Amazon FSx 不支持 Microsoft SQL Server IFI（即时文件初始化）功能。

SQL Server 建议使用 SSD 存储。SSD 存储专为性能最高、对延迟最敏感的工作负载而设计，包括数据库。

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 Storage 博客上的以下文章：

- Simplify your Microsoft SQL Server high availability deployments using Amazon FSx for Windows File Server
- Optimizing cost for your high availability SQL Server deployments on Amazon
- Simplify SQL Server Always On deployments with Amazon Launch Wizard and Amazon FSx

使用 Amazon FSx 处理 SQL Server 活动数据文件

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应用程序（如 SQL Server）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，无论是否为 HA，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 PowerShell 上使用适用于远程管理的 Amazon FSx CLI 创建 CA 共享。要将共享指定为持续可用的共享，请使用 `New-FSxSmbShare` 将 `-ContinuouslyAvailable` 选项设置为 `$True`。有关更多信息，请参阅 创建持续可用（CA）的共享。

配置 SMB 超时设置

如 故障转移过程 所述，多可用区的失效转移和失效自动恢复可能导致 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有所不同，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能够适应多可用区文件系统失效转移。您可以通过更新文件系统的吞吐能力来测试应用程序在失效转移期间的行为，这将启动自动失效转移和失效自动恢复。

使用 Amazon FSx 作为 SMB 文件共享见证

Windows Server 失效转移群集部署通常会部署 SMB 文件共享见证来维护集群资源仲裁。见证文件共享只需要少量存储空间即可存储仲裁信息。Amazon FSx 文件系统可用作 Windows 服务器失效转移集群部署的 SMB 文件共享见证。

将现有文件存储迁移到 Amazon FSx

Amazon FSx for Windows File Server 的功能、性能和兼容性可帮助您轻松地将企业应用程序直接迁移到 Amazon Web Services Cloud。将本地 Microsoft Windows File Server 存储迁移到 FSx for Windows File Server 的过程包括以下四大步骤：

1. 将文件迁移到 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。
2. 将文件共享配置迁移到 FSx for Windows File Server。有关更多信息，请参阅 将本地文件共享配置迁移到 Amazon FSx。
3. 将现有的 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 Amazon FSx 关联。
4. 割接到 FSx for Windows File Server。有关更多信息，请参阅 将操作割接到 Amazon FSx for Windows File Server。

有关该流程中每个步骤的详细信息，请参阅以下各个部分。

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，我们建议使用 Amazon DataSync，这是一种在线数据传输服务，旨在简化、自动执行和加速与 Amazon 存储服务之间复制大量数据的过程。DataSync 通过互联网或 Amazon Direct Connect 复制数据。作为一项完全托管式服务，DataSync 基本上无需修改应用程序、开发脚本或管理基础设施。有关更多信息，请参阅 使用 Amazon DataSync 将现有文件迁移到 FSx for Windows File Server。

此外，还可以使用 Robust File Copy（又名 Robocopy）解决方案，这是一种适用于 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。

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

要尽可能快速地将大量数据迁移到 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，如果使用硬盘驱动器（HDD）存储的 Amazon FSx 文件系统是最适合您应用程序的解决方案，可以将数据移至 HDD 存储。

要将数据从使用 SSD 存储的 Amazon FSx 文件系统移至 HDD 存储，可以执行以下步骤。（请注意，HDD 文件系统的存储容量至少为 2TB，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 创建用户启动备份。
2. 将备份还原到使用 HDD 存储的文件系统。有关更多信息，请参阅 将备份还原至新文件系统。

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

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 是一种数据传输服务，可以简化、自动执行并加快在本地存储系统与 Amazon 存储服务之间通过互联网或 Amazon Direct Connect 移动和复制数据。DataSync 可以传输您的文件系统数据以及元数据，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），还支持复制文件审计控制信息（也称为 NTFS 系统访问控制列表，SACL），管理员将使用这些信息来控制用户尝试访问文件的审计日志记录。

您可以使用 DataSync 在两个 FSx for Windows File Server 文件系统之间传输文件，也可以将数据移动到另一个 Amazon Web Services 区域 或 Amazon 账户中的文件系统。您可以使用 DataSync 与 FSx for Windows File Server 文件系统执行其他任务。例如，您可以执行一次性数据迁移、定期摄取分布式工作负载的数据以及按计划复制以实现数据保护与恢复。

在 Amazon DataSync 中，FSx for Windows File Server 的位置是 FSx for Windows File Server 的端点。可以在 FSx for Windows File Server 的位置和其他文件系统的位置之间传输文件。有关更多信息，请参阅《Amazon DataSync 用户指南》中的使用位置。

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

先决条件

要将数据迁移至 Amazon FSx for Windows File Server 设置，需要具有满足 DataSync 要求的服务器和网络。要了解更多信息，请参阅《Amazon DataSync 用户指南》中的 DataSync 要求。

如果要执行大型数据迁移或迁移涉及许多小文件，我们建议使用具有 SSD 存储类型的 Amazon FSx 文件系统。这是因为 DataSync 任务涉及扫描文件元数据，这可能会耗尽 HDD 文件系统的磁盘 IOPS 限额，从而导致迁移持续时间长和影响文件系统性能。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。

如果您的数据集主要由小文件组成，文件数以百万计，或者您的可用网络带宽大于单个 DataSync 任务可消耗的带宽，则还可以使用横向扩展架构加速数据传输。有关更多信息，请参阅：How to accelerate your data transfers with Amazon DataSync scale out architectures。

可以使用 FSx 性能指标监控文件系统的磁盘 I/O 利用率。

使用 DataSync 迁移文件的基本步骤

要使用 DataSync 将文件从源位置传输到目标位置，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《Amazon DataSync 用户指南》中的在行管理的存储和 Amazon 之间传输数据、为 SMB 创建位置和为 Amazon FSx for Windows File Server 创建位置。

要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《Amazon DataSync 用户指南》中的将您的代理部署为 Amazon EC2 实例。

在两个 Amazon FSx 文件系统之间迁移

可以使用 DataSync 在两个 Amazon FSx 文件系统之间迁移数据。如果您需要将工作负载从现有文件系统移至具有不同配置的新文件系统（例如从单可用区配置移至多可用区配置），这会很有帮助。此外，也可以使用 DataSync 在两个文件系统之间分配工作负载。

以下是迁移过程的示例概述：

1. 为源和目标文件系统创建 DataSync 位置。请注意，源和目标必须属于同一个 Active Directory（AD）域，或者各自的域之间必须具有 AD 信任关系。
2. 创建并运行 DataSync 任务，将数据从源位置传输到目标位置。可以将该任务作为一次性实例运行，也可以将该任务设置为按配置的计划自动运行。

3. 任务成功完成后，目标文件系统中的数据将是源文件系统的精确副本。请注意，您需要暂时暂停源文件系统上的任何写入活动或文件更新才能完成该任务。然后，可以割接到目标文件系统并删除源文件系统。

在从生产文件系统迁移之前，可以在从最近备份还原的文件系统上测试迁移过程。这样，可以估计数据传输过程所需的时间，并提前排查 DataSync 错误。

为了最大限度地缩短割接时间，可以提前运行 DataSync 任务，将大部分数据从源文件系统移至目标文件系统。停止传输到源文件系统的流量后，可以运行最后一次任务传输，以同步自停止流量以来新更新的任何数据，然后割接到目标文件系统。

可以将 DataSync 任务配置为仅在某些目录中运行，也可以配置为包含或排除某些路径。如果并行运行多个任务，或者要迁移部分数据，这会非常有用。

可以在目标文件系统上创建与源文件系统的 DNS 名称相同的 DNS 别名。这样，您的终端用户和应用程序可以继续使用源文件系统的 DNS 名称访问文件数据。有关如何设置 DNS 别名的更多信息，请参阅：使用 DNS 别名访问数据。

在执行这种类型的迁移时，我们建议执行以下操作：

- 安排迁移，避免任何文件系统备份、每周维护时段和 `Data Deduplication` 作业。具体而言，如果 `Data Deduplication GarbageCollection` 作业与您的计划迁移同时执行，我们建议禁用该作业。
- 对源文件系统和目标文件系统使用 SSD 存储类型。可以通过从备份还原，在 HDD 和 SSD 存储类型之间切换。有关更多信息，请参阅：将现有文件存储迁移到 FSx for Windows File Server。
- 为源文件系统和目标文件系统配置足够的吞吐能力，以便能够处理需要传输的数据量。在 DataSync 任务过程中，监控源文件系统和目标文件系统的性能利用率。有关更多信息，请参阅：使用 Amazon CloudWatch 监控。
- 设置 DataSync 监控以帮助您了解正在进行的任务的进度。也可以将 DataSync 日志发送到 Amazon CloudWatch Logs 组，以便在遇到任何错误时帮助您调试任务。

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

Amazon FSx for Windows File Server 构建于 Microsoft Windows Server 之上，使您能够将现有数据集完全迁移到 Amazon FSx 文件系统。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）、所有者信息和审计信息。在这种全面迁移支持下，Amazon FSx 可以将依赖这些文件数据集且基于 Windows 的工作负载和应用程序迁移到 Amazon Web Services Cloud。

使用以下主题引导您完成复制现有文件数据的过程。执行此复制时，将保留本地数据中心或 Amazon EC2 上自行管理的文件服务器的所有文件元数据。

使用 Robocopy 进行文件迁移的先决条件

在开始之前，请确保完成了以下操作：

- 在本地 Active Directory 与要在其中创建 Amazon FSx 文件系统的 VPC 之间建立网络连接（使用 Amazon Direct Connect 或 VPN）。
- 在 Active Directory 上创建具有将计算机加入域的委派权限的服务账户。有关更多信息，请参阅《Amazon Directory Service 管理指南》中的向您的服务账户委派权限。
- 创建一个 Amazon FSx 文件系统，并将其加入了自行管理的（本地）Microsoft AD 目录。
- 记下包含要传输到 Amazon FSx 的现有文件的文件共享（位于本地或 Amazon 中）的位置（例如 `\\Source\Share`）。
- 记下要将现有文件传输到的 Amazon FSx 文件系统上文件共享的位置（例如 `\\Target\Share`）。

下表汇总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。

迁移用户访问模式	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/写权限模式	用户至少需要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）。
覆盖访问权限的备份/还原权限模式	用户需要是本地 Active Directory 中备份操作员组的成员，并在 RoboCopy 中使用 /b 标志。	用户需要是 Amazon FSx 文件系统管理员组*的成员，并在 RoboCopy 中使用 /b 标志。
覆盖访问权限的域管理员（完全）权限模式	用户需要是本地 Active Directory 中域管理员组的成员。	用户需要是 Amazon FSx 文件系统管理员组*的成员，并在 RoboCopy 中使用 /b 标志。

> **Note**
>
> * 对于加入 Amazon Managed Microsoft AD 的文件系统，Amazon FSx 文件系统管理员组是 Amazon 委派的 FSx 管理员。在自行管理的 Microsoft AD 中，Amazon FSx 文件系统管理员组是域管理员或是在您创建文件系统时为管理指定的自定义组。

使用 Robocopy 迁移文件

可以使用以下过程，将现有文件从本地文件系统迁移到 FSx for Windows File Server 文件系统。

使用 Robocopy 将现有文件迁移到 Amazon FSx

1. 在 Amazon FSx 文件系统所在的 Amazon VPC 中启动 Windows Server 2016 Amazon EC2 实例。
2. 连接到 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》中的连接到 Windows 实例。
3. 打开命令提示符，将现有文件服务器（位于本地或 Amazon 中）上的源文件共享映射到驱动器盘符（例如 *Y*:），如下所示。在此操作过程中，您需要为本地 Active Directory 域管理员组的成员提供凭证。

   ```
   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 Amazon EC2 实例上的不同驱动器盘符（例如 *Z*:），如下所示。在此操作过程中，您需要属于本地 Active Directory 域管理员组和 Amazon FSx 文件系统管理员组成员的用户账户提供凭证。对于加入 Amazon Managed Microsoft AD 的文件系统，该组是 **Amazon Delegated FSx Administrators**。在自行管理的 Microsoft AD 中，该组是 **Domain Admins** 或是在您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 使用 Robocopy 进行文件迁移的先决条件 中的源文件系统和目标文件系统可访问性要求表。

   ```
   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. 从上下文菜单中选择以管理员身份运行。以管理员身份打开命令提示符或 Windows PowerShell，然后运行以下 Robocopy 命令，将文件从源共享复制到目标共享。

   ROBOCOPY 命令是一个灵活的文件传输实用程序，具有多个用于控制数据传输进程的选项。执行此 ROBOCOPY 命令进程后，源共享中的所有文件和目录都将复制到 Amazon FSx 目标共享。该复制将保留文件和文件夹的 NTFS ACL、属性、时间戳、所有者信息和审计信息。

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

   上面的示例命令使用了以下元素和选项：

   - Y – 指的是位于本地 Active Directory 林 mydata.com 中的源共享。
   - Z – 指的是 Amazon FSx 上的目标共享 \\amznfsxabcdef1.mydata.com\share。
   - /copy – 指定要复制的以下文件属性：
     - D – 数据
     - A – 属性
     - T – 时间戳
     - S – NTFS ACL
     - O – 所有者信息
     - U – 审计信息。
   - /secfix – 修复所有文件的文件安全性，甚至包括跳过的文件。
   - /e – 复制子目录，包括空目录。
   - /b – 使用 Windows 中的备份和还原权限复制文件，即使其 NTFS ACL 拒绝向当前用户授予权限。
   - /MT:8 – 指定用于执行多线程复制的线程数。

> **Note**
>
> 如果要通过慢速或不可靠的连接复制大型文件，可以在 robocopy 中使用 /zb 选项代替 /b 选项，启用可重启模式。在可重启模式下，如果大型文件的传输中断，则可以在传输过程中继续

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。

将本地文件共享配置迁移到 Amazon FSx

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。

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

1. 在源文件服务器上，从上下文菜单中选择以管理员身份运行。以管理员身份打开 Windows PowerShell。
2. 在 PowerShell 中运行以下命令，将源文件服务器的文件共享导出到名为 `SmbShares.xml` 的文件中。将该示例中的 F: 替换为要从中导出文件共享的文件服务器上的驱动器盘符。

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

3. 编辑 `SmbShares.xml` 文件，将对 F:（您的驱动器盘符）的所有引用替换为 D:\share，因为 Amazon FSx 文件系统位于 D:\share 上。
4. 将现有文件共享配置导入到 FSx for Windows File Server。在可以访问您的目标 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。然后，使用以下命令将其导入到一个变量中。

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

5. 使用以下方法之一，准备在 FSx for Windows File Server 文件服务器上创建文件共享所需的凭证对象。

   要以交互方式生成凭证对象，请使用以下命令。

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

要使用 Amazon Secrets Manager 资源生成凭证对象，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 }
}
```

将本地 DNS 配置迁移到 FSx for Windows File Server

FSx for Windows File Server 为每个文件系统提供了一个默认域名系统（DNS）名称，可以用于访问文件系统上的数据。还可以通过将备用 DNS 名称配置为 Amazon FSx 文件系统的 DNS 别名，使用所选择的任何 DNS 名称访问您的文件系统。

使用 DNS 别名，在将文件系统存储从本地迁移到 Amazon FSx 时，可以继续使用现有 DNS 名称访问存储在 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 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，可以将 DNS 别名与现有 FSx for Windows File Server 相关联。每次最多可以将 50 个 DNS 别名与一个文件系统关联。有关更多信息，请参阅 管理 DNS 别名。

DNS 别名必须满足以下要求：

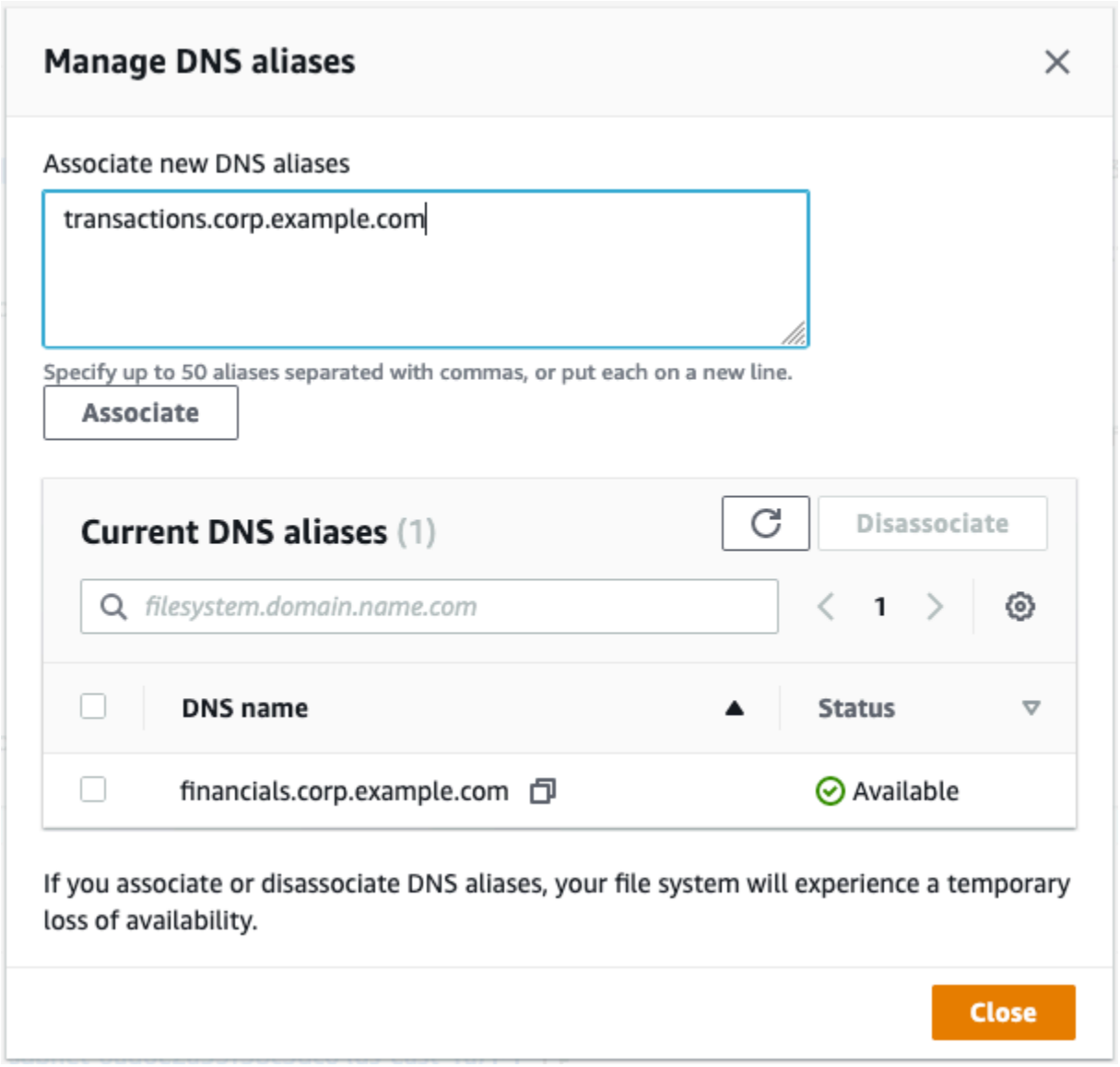
- 必须采用完全限定域名（FQDN）格式，例如 `accounting.example.com`。
- 可以包含字母数字字符和连字符（-）。
- 不得以连字符开头或结尾。
- 可以使用数字开头。

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。

以下过程介绍了如何使用 Amazon FSx 控制台、CLI 和 API 将 DNS 别名与现有的 FSx for Windows File Server 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 别名的更多信息，请参阅 将 DNS 别名与文件系统相关联。

将 DNS 别名与现有文件系统关联（控制台）

1. 通过以下网址打开 Amazon FSx 控制台：https://console.aws.amazon.com/fsx/。
2. 导航到文件系统，然后选择要与 DNS 别名关联的 Windows 文件系统。
3. 在网络与安全选项卡上，选择 DNS 别名对应的管理以打开管理 DNS 别名对话框。



4. 在关联新的别名框中，输入要关联的 DNS 别名。
5. 选择关联，将别名添加到文件系统。

   可以在当前别名列表中监控刚刚关联的别名的状态。当状态显示为可用时，别名已与文件系统关联（此过程可能需要长达 2.5 分钟）。

将 DNS 别名与现有文件系统关联（CLI）

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

  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
```

响应显示了 Amazon FSx 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 CLI 命令 `describe-file-system-aliases`（等效的 API 操作为 DescribeFileSystemAliases）。当别名的 `Lifecycle` 值为 AVAILABLE 时，便可以使用该别名访问文件系统了（此过程可能需要长达 2.5 分钟）。

将操作割接到 Amazon FSx for Windows File Server

迁移本地文件存储、文件共享配置和 DNS 配置后，下一步是将操作割接到 FSx for Windows File Server 文件系统。要割接到 FSx for Windows File Server 文件系统，请执行以下步骤：

- 准备割接。
  - 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 Amazon FSx 文件系统。

以下各部分介绍了执行每个步骤的过程。

主题

准备割接到 Amazon FSx

要为割接到 Amazon FSx 文件系统做准备，必须执行以下操作：

- 将所有写入原始文件系统的客户端断开连接。
- 使用 Amazon DataSync 或 Robocopy 执行最终文件同步。有关更多信息，请参阅 将现有文件存储迁移到 FSx for Windows File Server。
- 执行最终的文件共享配置同步。有关更多信息，请参阅 将本地文件共享配置迁移到 Amazon FSx。

为 Kerberos 身份验证配置 SPN

我们建议对 Amazon FSx 使用基于 Kerberos 的身份验证和传输中加密。Kerberos 能够为访问文件系统的客户端提供最安全的身份验证。要对使用 DNS 别名访问 Amazon FSx 的客户端启用 Kerberos 身份验证，必须在 Amazon FSx 文件系统的 Active Directory 计算机对象上添加与 DNS 别名对应的服务主体名称（SPN）。

Kerberos 身份验证需要两个 SPN。

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

例如，如果别名是 `finance.domain.com`，则两个必需的 SPN 如下。

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

一个 SPN 一次只能与一个 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 名称具有现有 SPN，则在为 Amazon FSx 文件系统创建 SPN 之前，必须先将其删除。

以下过程介绍了如何查找任何现有 SPN、将其删除以及为 Amazon FSx 文件系统的 Active Directory 计算机对象创建新的 SPN。

安装所需的 PowerShell Active Directory 模块

1. 登录已加入您的 Amazon FSx 文件系统所加入的 Active Directory 的 Windows 实例。
2. 以管理员身份打开 PowerShell。
3. 使用以下命令安装 PowerShell Active Directory 模块。

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

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

1. 使用以下命令查找所有现有 SPN。将 *alias_fqdn* 替换为在 将本地 DNS 配置迁移到 FSx for Windows File Server 中与文件系统关联的 DNS 别名。

```
## 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。

   - 将 *alias_fqdn* 替换为在 将本地 DNS 配置迁移到 FSx for Windows File Server 中与文件系统关联的完整 DNS 别名。
   - 将 *file_system_DNS_name* 替换为原始文件系统的 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. 对在 将本地 DNS 配置迁移到 FSx for Windows File Server 中与文件系统关联的每个 DNS 别名重复这些步骤。

为 Amazon FSx 文件系统的 Active Directory 计算机对象设置 SPN

1. 运行以下命令，为 Amazon FSx 文件系统设置新的 SPN。

   - 将 *file_system_DNS_name* 替换为 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。选择文件系统详细信息页面中的网络与安全窗格。您也可以在 API 操作 DescribeFileSystems 的响应中找到 DNS 名称。

   - 将 *alias_fqdn* 替换为在 将本地 DNS 配置迁移到 FSx for Windows File Server 中与文件系统关联的完整 DNS 别名。

```
## 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 AD 计算机对象中存在 DNS 别名的 SPN，则为 Amazon FSx 文件系统设置 SPN 将失败。有关查找并删除现有 SPN 的信息，请参阅查找并删除原始文件系统 Active Directory 计算机对象上的现有 DNS 别名 SPN。

2. 使用以下示例脚本验证是否为 DNS 别名配置了新 SPN。确保响应包括两个 HOST SPN：HOST/*alias* 和 HOST/*alias_fqdn*。

   将 *file_system_DNS_name* 替换为 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，然后选择文件系统详细页面上的网络与安全窗格。

   您也可以在 API 操作 DescribeFileSystems 的响应中找到 DNS 名称。

```
## 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. 对在 将本地 DNS 配置迁移到 FSx for Windows File Server 中与文件系统关联的每个 DNS 别名重复上述步骤。

> **Note**
>
> 可以通过在 Active Directory 中设置以下组策略对象（GPO），强制对使用 DNS 别名连接到文件系统的客户端执行 Kerberos 身份验证和传输中加密：
>
> - 限制 NTLM：远程服务器的传出 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“演练 5：使用 DNS 别名访问文件系统”中的使用组策略对象（GPO）强制执行 Kerberos 身份验证。

更新 Amazon FSx 文件系统的 DNS CNAME 记录

为文件系统正确配置 SPN 后，可以通过以下方式割接到 Amazon FSx：将解析为原始文件系统的每个 DNS 记录替换为解析为 Amazon FSx 文件系统默认 DNS 名称的 DNS 记录。

安装所需的 PowerShell cmdlet

1. 以具有 DNS 管理权限的组（对于 Amazon 托管 Microsoft Active Directory，为 Amazon 委派的域名系统管理员；对于自行管理的 Active Directory，为域管理员或您已委派 DNS 管理权限的其他组）的成员用户身份登录到已加入您的 Amazon FSx 文件系统所加入的 Active Directory 的 Windows 实例

   有关详细信息，请参阅《Amazon EC2 用户指南》中的连接到 Windows 实例。
2. 以管理员身份打开 PowerShell。
3. 按照此过程中的说明操作需要 PowerShell DNS 服务器模块。使用以下命令安装该模块。

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

更新现有的 DNS CNAME 记录

1. 以下脚本将 *alias_fqdn* 的所有现有 DNS CNAME 记录更新到 Amazon FSx 文件系统的计算机对象。如果未找到任何记录，将为 DNS 别名 *alias_fqdn* 创建一个新的 DNS CNAME 记录，该记录将解析为 Amazon FSx 文件系统的默认 DNS 名称。

   要运行脚本，请执行以下操作：

   - 将 *alias_fqdn* 替换为与文件系统关联的 DNS 别名。
   - 将 *file_system_DNS_name* 替换为 Amazon FSx 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. 对在 将本地 DNS 配置迁移到 FSx for Windows File Server 中与文件系统关联的每个 DNS 别名重复上述步骤。

监控 FSx for Windows File Server 文件系统

监控是保持 FSx for Windows File Server 和 Amazon 解决方案可靠性、可用性和性能的重要方面。您应从 Amazon 解决方案的所有部分收集监控数据，以便更轻松地调试出现的故障。不过，在开始监控 FSx for Windows File Server 之前，您应制定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？

有关 FSx for Windows File Server 中的日志记录和监控的更多信息，请参阅以下主题。

主题

自动和手动监控

Amazon 提供多种可用于监控 FSx for Windows File Server 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，以监控 FSx for Windows File Server，并在出现错误时报告：

- Amazon CloudWatch 警报：按您指定的时间段观察单个指标，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。具体操作是将一条通知已发送到某个 Amazon Simple Notification Service（Amazon SNS）主题或 Amazon EC2 Auto Scaling 策略。CloudWatch 告警不调用操作，因为这些操作处于特定状态；状态必须改变并保持指定时间。有关更多信息，请参阅 使用 Amazon CloudWatch 监控。

- Amazon CloudWatch Logs：监控、存储和访问来自 Amazon CloudTrail 或其他来源的日志文件。如需了解更多信息，请参阅 Amazon CloudWatch Logs 用户指南中的什么是 Amazon CloudWatch Logs？
- Amazon CloudTrail 日志监控：在账户间共享日志文件，通过将 CloudTrail 日志文件发送到 CloudWatch Logs 来进行实时监控，用 Java 编写日志处理应用程序，验证 CloudTrail 提供的日志文件未发生更改。有关更多信息，请参见《Amazon CloudTrail 用户指南》的使用 CloudTrail 日志文件。

手动监控工具

监控 FSx for Windows File Server 的另一重要环节是手动监控 Amazon CloudWatch 警报未涵盖的那些项目。FSx for Windows File Server、CloudWatch 和其他 Amazon 控制台控制面板提供 Amazon 环境状态的概览视图。

Amazon FSx 监控和性能控制面板显示：

- 当前警告和 CloudWatch 警报
- 文件系统活动摘要
- 文件系统存储容量和利用率
- 文件服务器和存储卷性能
- CloudWatch 警报

Amazon CloudWatch 控制面板显示：

- 当前警报和状态
- 告警和资源图表
- 服务运行状况

此外，还可以使用 CloudWatch 执行以下操作：

- 创建自定义控制面板以监控您使用的服务。
- 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。
- 创建和编辑警报以接收有关问题的通知。

有关 Amazon FSx 监控和性能控制面板的更多信息，请参阅使用文件系统指标。

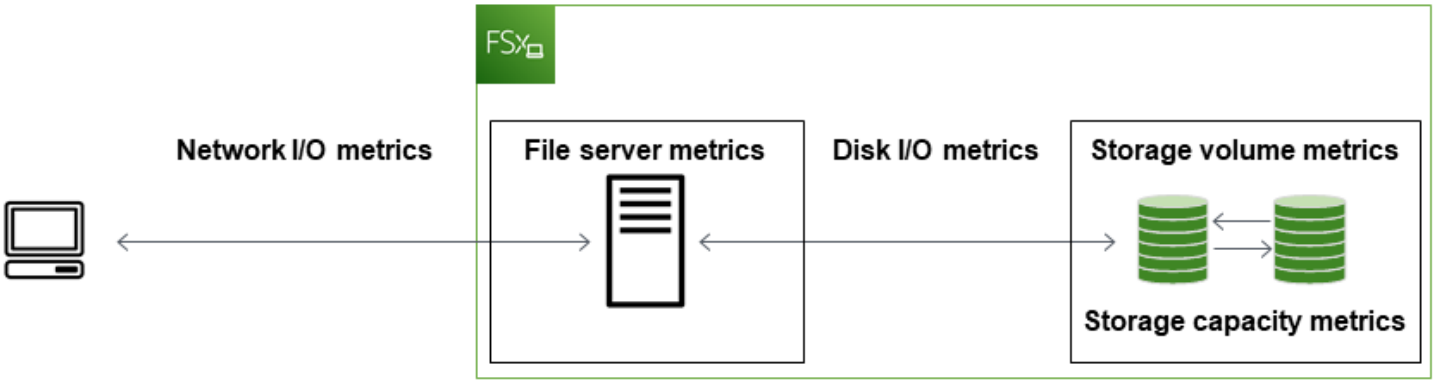
使用 Amazon CloudWatch 监控

Amazon CloudWatch 监控 FSx for Windows File Server 文件系统的原始数据，并将数据处理为可读且近乎实时的指标。这些统计数据会保存 15 个月，从而使您能够访问历史信息，以帮助您了解工作流程或文件系统的执行情况。

FSx for Windows File Server 发布以下领域的 CloudWatch 指标：

- 网络 I/O 指标衡量访问文件系统的客户端和文件服务器之间的活动。
- 文件服务器指标衡量网络吞吐量利用率、文件服务器 CPU 和内存，以及文件服务器磁盘吞吐量和 IOPS 利用率。
- 磁盘 I/O 指标衡量文件服务器和存储卷之间的活动。
- 存储卷指标衡量 HDD 存储卷的磁盘吞吐量利用率和 SSD 存储卷的 IOPS 利用率。
- 存储容量指标衡量存储使用量，包括重复数据删除带来的存储节省。

下图说明了 FSx for Windows File Server 文件系统、其组件和指标领域。



默认情况下，适用于 Windows File Server 的 Amazon FSx 会以 1 分钟为间隔将指标数据发送到 CloudWatch，但以下项以 5 分钟为间隔发出：

- `FileServerDiskThroughputBalance`
- `FileServerDiskIopsBalance`

有关 CloudWatch 的更多信息，请参阅《Amazon CloudWatch 用户指南》中的什么是 Amazon CloudWatch？。

对于单可用区文件系统，在文件系统维护或基础设施组件更换期间，可能不会发布指标；对于多可用区文件系统，在主文件服务器和辅助文件服务器之间进行失效转移和失效自动恢复期间，可能不会发布指标。

一些 Amazon FSx CloudWatch 指标以原始字节的形式进行报告。字节数不会舍入到十进制或二进制单位倍数。

主题

CloudWatch 指标和维度

FSx for Windows File Server 将所有文件系统的以下指标发布到 Amazon CloudWatch 的 `AWS/FSx` 命名空间中：

- `DataReadBytes`
- `DataWriteBytes`
- `DataReadOperations`
- `DataWriteOperations`
- `MetadataOperations`
- `FreeStorageCapacity`

FSx for Windows File Server 将吞吐能力至少配置为 32 MBps 的文件系统的以下部分所述指标发布到 Amazon CloudWatch 的 `AWS/FSx` 命名空间中。

网络 I/O 指标

`AWS/FSx` 命名空间包括以下网络 I/O 指标。

指标	描述
`DataReadBytes`	访问文件系统的客户端的读取操作字节数。

指标	描述
	单位：字节 有效统计数据：Sum
DataWriteBytes	访问文件系统的客户端的写入操作字节数。 单位：字节 有效统计数据：Sum
DataReadOperations	访问文件系统的客户端的读取操作数。 单位：计数 有效统计数据：Sum
DataWriteOperations	访问文件系统的客户端的写入操作数。 单位：计数 有效统计数据：Sum
MetadataOperations	访问文件系统的客户端的元数据操作数。 单位：计数 有效统计数据：Sum
ClientConnections	客户端与文件服务器之间的活动连接数。 单位：计数

文件服务器指标

AWS/FSx 命名空间包括以下文件服务器指标。

指标	描述
NetworkThroughputUtilization	访问文件系统的客户端的网络吞吐量，表示为预调配限制的百分比。 单位：百分比
CPUUtilization	文件服务器 CPU 资源的利用率百分比。 单位：百分比
MemoryUtilization	文件服务器内存资源的利用率百分比。 单位：百分比
FileServerDiskThroughputUtilization	文件服务器与其存储卷之间的磁盘吞吐量，表示为由吞吐能力决定的预调配限制的百分比。 单位：百分比
FileServerDiskThroughputBalance	文件服务器与其存储卷之间磁盘吞吐量的可用突增点数百分比。适用于预调配的吞吐能力不高于 256Mbps 的文件系统。 单位：百分比
FileServerDiskIopsUtilization	文件服务器与存储卷之间的磁盘 IOPS，表示为由吞吐能力决定的预调配限制的百分比。 单位：百分比
FileServerDiskIopsBalance	文件服务器与其存储卷之间磁盘 IOPS 的可用突增点数百分比。适用于预调配的吞吐能力不高于 256Mbps 的文件系统。 单位：百分比

磁盘 I/O 指标

AWS/FSx 命名空间包括以下磁盘 I/O 指标。

指标	描述
DiskReadBytes	访问存储卷的读取操作字节数。 单位：字节 有效统计数据：Sum
DiskWriteBytes	访问存储卷的写入操作字节数。 单位：字节 有效统计数据：Sum
DiskReadOperations	访问存储卷的文件服务器的读取操作数。 单位：计数 有效统计数据：Sum
DiskWriteOperations	访问存储卷的文件服务器的写入操作数。 单位：计数 有效统计数据：Sum

FSx for Windows 存储卷指标

AWS/FSx 命名空间包括以下存储卷指标。

指标	描述
DiskThroughputUtilization	（仅限 HDD）文件服务器与其存储卷之间的磁盘吞吐量，表示为由存储卷决定的预调配限制的百分比。 单位：百分比
DiskThroughputBalance	（仅限 HDD）存储卷磁盘吞吐量和磁盘 IOPS 的可用突增点数百分比。

指标	描述
	单位：百分比
DiskIopsUtilization	（仅限 SSD）文件服务器与存储卷之间的磁盘 IOPS，表示为由存储卷决定的预调配 IOPS 的百分比。 单位：百分比

存储容量指标

AWS/FSx 命名空间包括以下存储容量指标。

指标	描述
FreeStorageCapacity	可用存储容量的大小。 单位：字节 有效统计数据：Average、Minimum
StorageCapacityUtilization	已用物理存储容量，表示为总存储容量的百分比。 单位：百分比
DeduplicationSavedStorage	启用了重复数据删除时节省的存储空间量。 单位：字节

FSx for Windows File Server 指标的命名空间和维度

FSx for Windows File Server 指标使用 FSx 命名空间，并且为单个维度 FileSystemId 提供指标。可以使用 describe-file-systems Amazon CLI 命令或 DescribeFileSystems API 命令查找文件系统的 ID。文件系统 ID 采用 *fs-0123456789abcdef0* 形式。

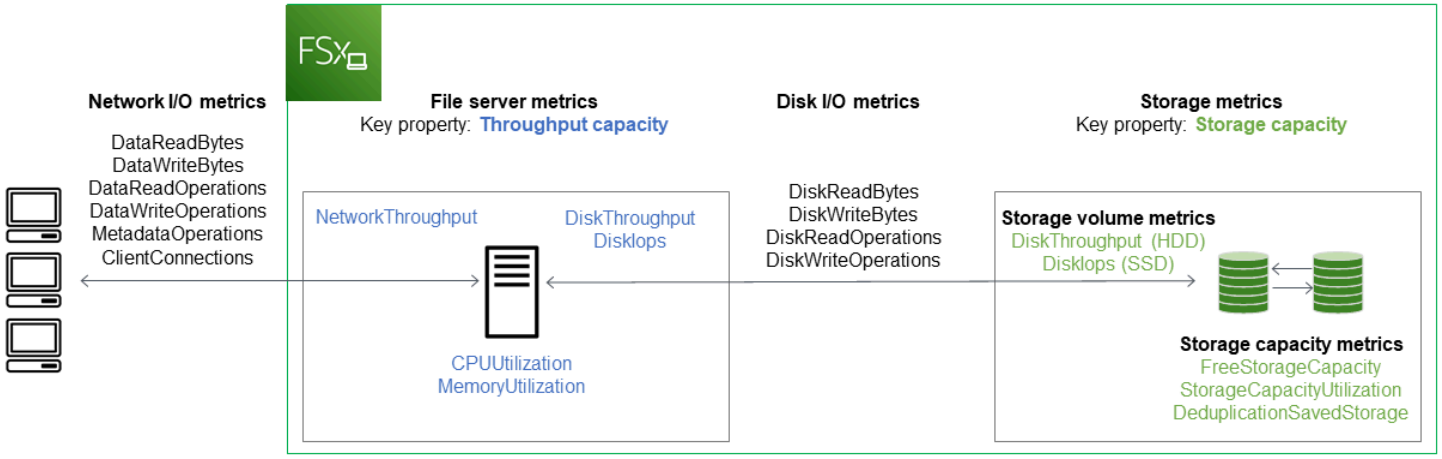
使用文件系统指标

每个 Amazon FSx 文件系统都有两个主要的架构组件：

- 文件服务器，用于为访问文件系统的客户端提供数据。

- 存储卷，用于托管文件系统中的数据。

FSx for Windows File Server 在 CloudWatch 中报告指标，这些指标可跟踪文件系统的文件服务器和存储卷的性能和资源利用率。下图说明了 Amazon FSx 文件系统及其架构组件，以及可用于监控的性能和资源 CloudWatch 指标。针对一组指标显示的关键属性是文件系统属性，用于确定这些指标的容量。调整该属性会修改该组指标的文件系统性能。



可以使用 Amazon FSx 控制台中的监控和性能面板查看下表中所述的 FSx for Windows File Server CloudWatch 指标。

“监控和性能”面板	如何...	图表	相关指标
摘要	...确定文件系统的总 IOPS？	总 IOPS	总和（DataReadOperations + DataWriteOperations + MetadataOperations）/周期（以秒为单位）
	...确定文件系统的总吞吐量？	总吞吐量	总和（DataReadBytes + DataWriteBytes）/周期（以秒为单位）
	...确定文件系统上的可用存储容量大小？	可用存储容量	FreeStorageCapacity

“监控和性能”面板	如何...	图表	相关指标
存储	...客户端与文件服务器之间建立的连接数？	客户端连接	ClientConnections
	...确定已用物理磁盘空间量（表示为文件系统总存储容量的百分比）？	存储容量利用率	StorageCapacityUtilization
	...确定通过重复数据删除节省的物理磁盘空间量？	通过重复数据删除节省的存储容量	DeduplicationSavedStorage
性能 – 文件服务器	...确定访问文件系统的客户端的网络吞吐量（表示为文件系统预调配吞吐量的百分比）？	网络吞吐量利用率	NetworkThroughputUtilization [1]
	...确定文件服务器与其存储卷之间的磁盘吞吐量（表示为由吞吐能力决定的预调配限制的百分比）？	磁盘吞吐量利用率	FileServerDiskThroughputUtilization [1]
	...确定文件服务器与其存储卷之间磁盘吞吐量的可用突增点数百分比？	磁盘吞吐量突增平衡	FileServerDiskThroughputBalance
	...确定文件服务器与存储卷之间的磁盘 IOPS（表示为由吞吐能力决定的预调配限制的百分比）？	磁盘 IOPS 利用率	FileServerDiskIopsUtilization
	...确定文件服务器与存储卷之间磁盘 IOPS 的可用突增点数百分比？	磁盘 IOPS 突增平衡	FileServerDiskIopsBalance
	...确定文件服务器的 CPU 利用率百分比？	CPU 使用率	CPUUtilization

“监控和性能”面板	如何...	图表	相关指标
	...确定文件服务器的内存利用率百分比？	内存利用率	`MemoryUtilization`
性能 – 存储卷	...确定访问存储卷的操作吞吐量（表示为由 HDD 存储容量决定的预调配限制的百分比）？	磁盘吞吐量利用率（HDD）	`DiskThroughputUtilization`
	...确定访问 HDD 存储卷的操作可用吞吐量和 IOPS 突增点数百分比？	磁盘吞吐量突增平衡（HDD）	`DiskThroughputBalance` [2]
	...确定访问存储卷的操作 IOPS（表示为由 HDD 存储容量决定的预调配限制的百分比）？	磁盘 IOPS 利用率（HDD）	SUM（`DiskReadOperations` + `DiskWriteOperations`）/ `Period`（秒）/（12 * 预置 HDD 存储容量（TiB））
	...确定访问存储卷的操作 IOPS（表示为由 SSD 存储容量决定的预调配限制的百分比）？	磁盘 IOPS 利用率（SSD）	`DiskIopsUtilization`

Note

[1]我们建议您将平均吞吐能力利用率保持在 50% 以下，以确保有足够的备用吞吐能力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、重复数据删除或影子复制）。

[2]根据工作负载，HDD 存储卷可能会出现显著的性能差异。IOPS 或吞吐量突然激增可能导致磁盘性能下降。有关更多信息，请参阅 HDD 突增性能。

性能警告和建议

FSx for Windows 针对吞吐能力至少配置为 32Mbps 的文件系统提供了性能警告。每当 CloudWatch 指标中的某一个指标接近或超过多个连续数据点的预定阈值时，Amazon FSx 就会显示警告。这些警告会为您提供切实可行的建议，您可以使用这些建议来优化文件系统的性能。

可以在监控和性能控制面板的多个区域内访问警告。监控和性能面板的摘要部分中会显示所有活动或近期的 Amazon FSx 性能警告，以及为处于“警报”状态的文件系统配置的所有 CloudWatch 警报。仪表板中显示指标图表的部分也会显示警告。

您可以为任意 Amazon FSx 指标创建 CloudWatch 警报。有关更多信息，请参阅 创建 CloudWatch 警报。

使用性能警告提高文件系统的性能

Amazon FSx 会为您提供切实可行的建议，您可以使用这些建议来优化文件系统的性能。这些建议介绍了如何解决潜在的性能瓶颈。如果您希望继续进行活动，或者该活动对文件系统的性能造成了影响，您可以采取建议的操作。根据触发警告的指标，您可以通过增加文件系统的吞吐能力或存储容量来解决警告，如下表所述。

如果有针对此指标的警告	请执行该操作
网络吞吐量 – 利用率	增加吞吐能力
文件服务器 > 磁盘 IOPS – 利用率	
文件服务器 > 磁盘吞吐量 – 利用率	
文件服务器 > 磁盘 IOPS – 突增余额	
文件服务器 > 磁盘吞吐量 – 突增余额	
存储容量利用率	增加存储容量
存储卷 > 磁盘吞吐量 – 利用率（HDD）	增加存储容量或切换到 SDD 存储类型
存储卷 > 磁盘吞吐量 – 突增余额（HDD）	
存储卷 > 磁盘 IOPS – 利用率（SSD）	提高 SSD IOPS

> **Note**
>
> 某些文件系统事件可能会消耗磁盘 I/O 性能资源，并可能触发性能警告。例如：
>
> - 存储容量扩展的优化阶段会增加磁盘吞吐量，如 增加存储容量并提升文件系统性能 中所述
> - 对于多可用区文件系统，吞吐能力扩展、硬件更换或可用区中断等事件会导致自动失效转移和失效自动恢复事件。在此期间发生的任何数据更改都需要在主文件服务器和辅助文件服务器之间进行同步，Windows Server 运行的数据同步作业可能会消耗磁盘 I/O 资源。有关更多信息，请参阅 管理吞吐能力。

有关文件系统性能的更多信息，请参阅 FSx for Windows File Server 性能。

访问文件系统指标

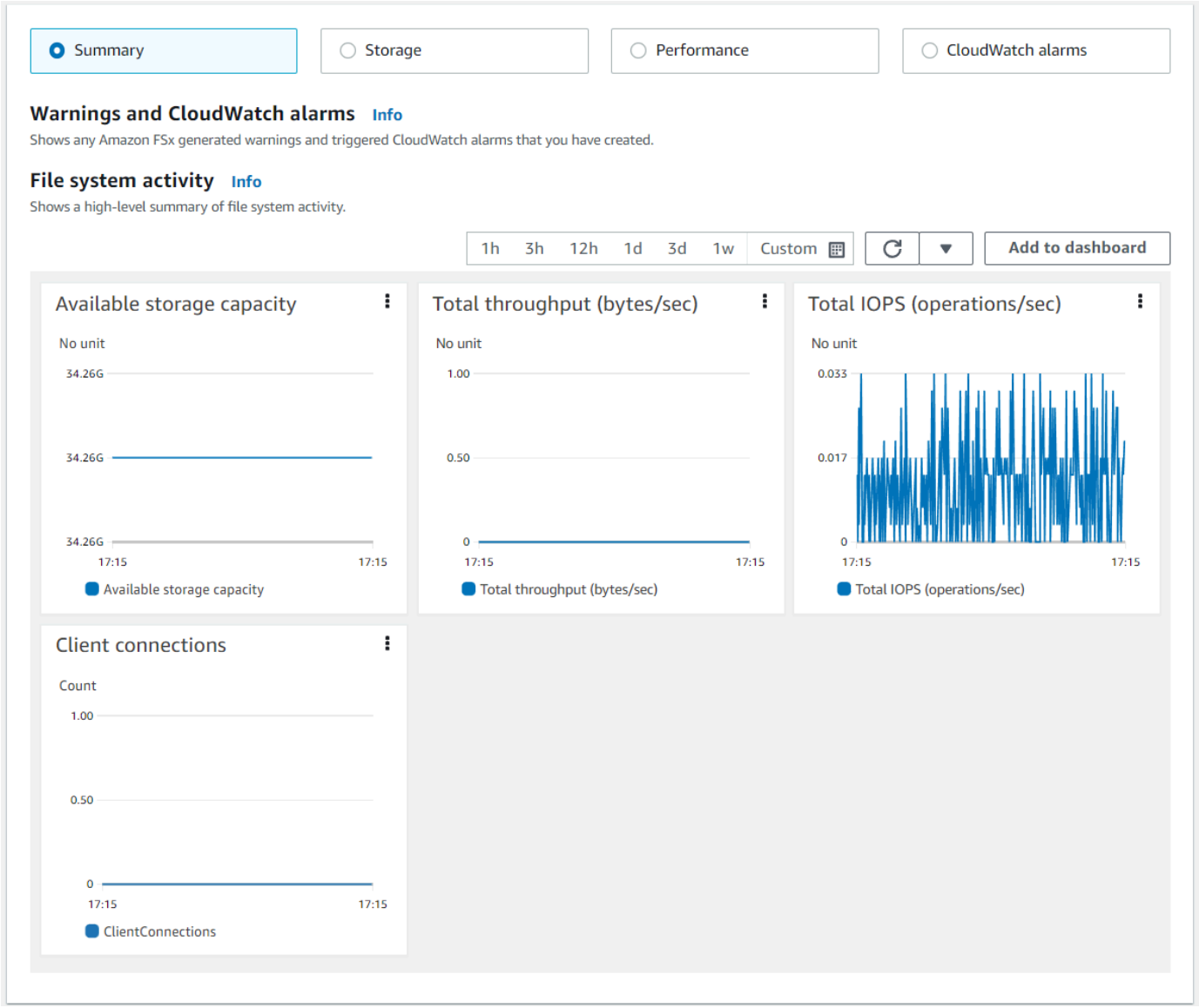
您可以通过以下方式查看 CloudWatch 的 Amazon FSx 指标。

- Amazon FSx 控制台
- CloudWatch 控制台
- CloudWatch CLI
- CloudWatch API

以下过程介绍了如何使用这些不同的工具访问文件系统的指标。

使用 Amazon FSx 控制台查看文件系统指标

1. 通过以下网址打开 Amazon FSx 控制台：https://console.aws.amazon.com/fsx/。
2. 要显示文件系统详细信息页面，请在导航窗格中选择文件系统。
3. 选择要查看其指标的文件系统。
4. 要查看文件系统指标图表，请在第二个面板上选择监控和性能。

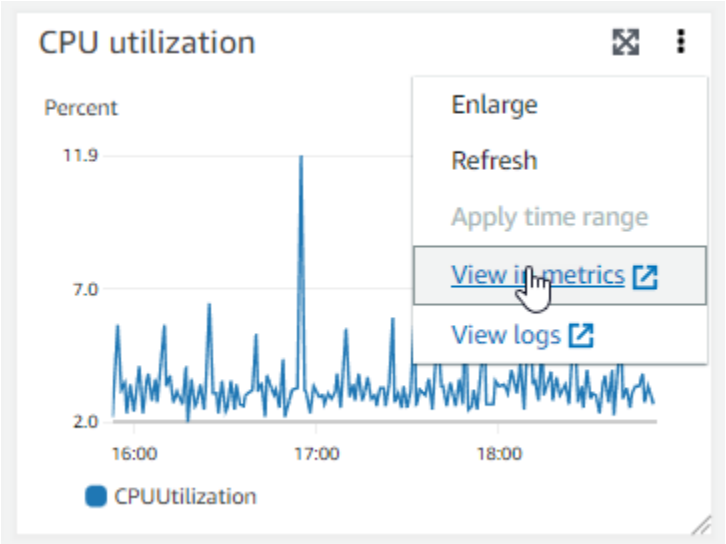


- 摘要指标默认显示，其中显示了所有活动警告、CloudWatch 警报以及文件系统活动指标。
- 选择存储可查看存储容量和利用率指标。
- 选择性能可查看文件服务器和存储性能指标。
- 选择 CloudWatch 警报可查看为文件系统配置的所有警报的图表。

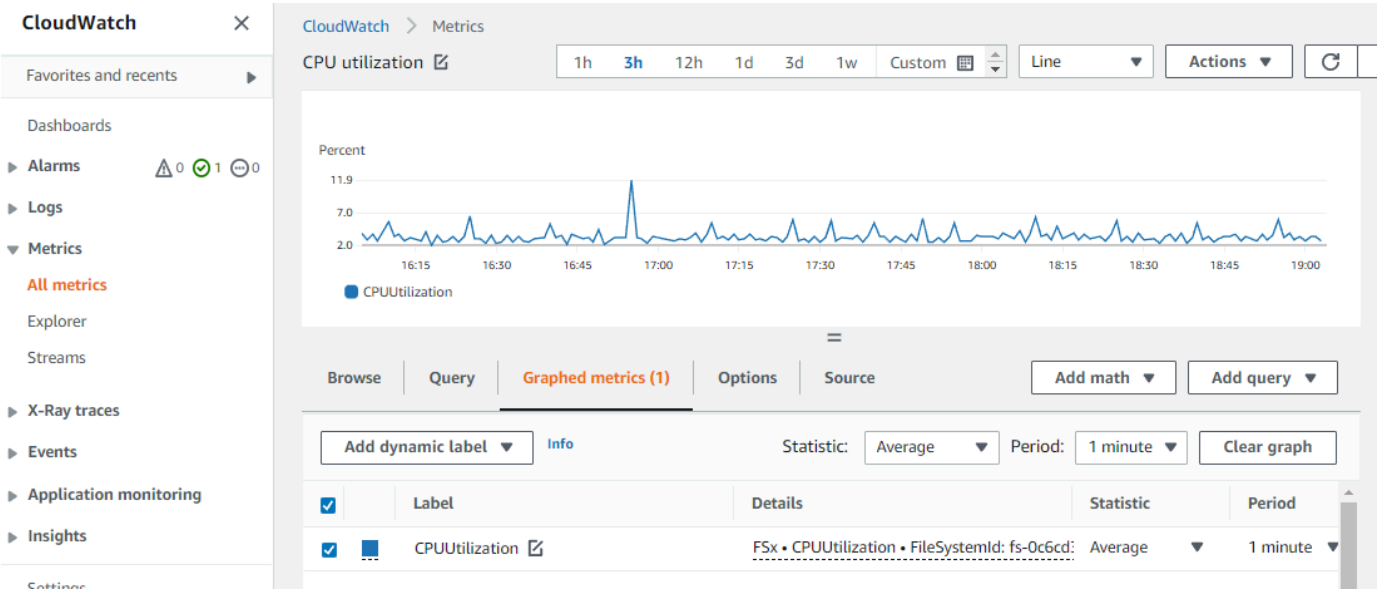
有关更多信息，请参阅 使用文件系统指标。

在 CloudWatch 控制台中查看指标

1. 要在 Amazon CloudWatch 控制台的指标页面中查看文件系统指标，请在 Amazon FSx 控制台的监控和性能面板中导航到该指标。
2. 从指标图表右上角的操作菜单中选择在指标中查看，如下图所示。



这将在 CloudWatch 控制台中打开指标页面，显示指标图表，如下图所示。



将指标添加到 CloudWatch 控制面板

1. 要将一组 FSx for Windows 文件系统指标添加到 CloudWatch 控制台中的控制面板，请在 Amazon FSx 控制台的监控和性能面板中选择这组指标（摘要、存储或性能）。

2. 选择面板右上角的添加到控制面板，这将打开 CloudWatch 控制台。
3. 从列表中选择一个现有的 CloudWatch 控制面板，或者创建一个新的控制面板。有关更多信息，请参阅《Amazon CloudWatch 用户指南》中的使用 Amazon CloudWatch 控制面板。

从 Amazon CLI 访问指标

- 使用带有 `--namespace "AWS/FSx"` 命名空间的 `list-metrics` 命令。有关更多信息，请参阅 Amazon CLI 命令参考。

```
$ aws cloudwatch list-metrics --namespace "AWS/FSx"
aws cloudwatch list-metrics --namespace "AWS/FSx"
{
    "Metrics": [
        {
            "Namespace": "AWS/FSx",
            "MetricName": "DataWriteOperationTime",
            "Dimensions": [
                {
                    "Name": "FileSystemId",
                    "Value": "fs-09a106ebc3a0bb087"
                }
            ]
        },
        {
            "Namespace": "AWS/FSx",
            "MetricName": "CapacityPoolWriteBytes",
            "Dimensions": [
                {
                    "Name": "VolumeId",
                    "Value": "fsvol-0cb2281509f5db3c2"
                },
                {
                    "Name": "FileSystemId",
                    "Value": "fs-09a106ebc3a0bb087"
                }
            ]
        },
        {
            "Namespace": "AWS/FSx",
            "MetricName": "DiskReadBytes",
            "Dimensions": [
                {
```

```
                    "Name": "FileSystemId",
                    "Value": "fs-09a106ebc3a0bb087"
                }
            ]
        },
        {
            "Namespace": "AWS/FSx",
            "MetricName": "CompressionRatio",
            "Dimensions": [
                {
                    "Name": "FileSystemId",
                    "Value": "fs-0f84c9a176a4d7c92"
                }
            ]
        },
.
.
.
}
```

使用 CloudWatch API

从 CloudWatch API 访问指标

- 调用 GetMetricStatistics。有关更多信息，请参阅 Amazon CloudWatch API 参考。

创建 CloudWatch 警报

可以创建 CloudWatch 告警，在告警改变状态时发送 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 主题或自动扩缩策略的通知。

告警仅为持续状态更改调用操作。CloudWatch 警报不会仅仅因为处于特定状态就调用操作；状态必须已改变并在指定的若干个时间段内保持不变。您可以通过 Amazon FSx 控制台或 CloudWatch 控制台创建警报。

以下过程介绍了如何使用控制台、Amazon CLI 和 API 为 Amazon FSx 创建警报。

设置 CloudWatch 警报（控制台）

1. 通过以下网址打开 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. 在摘要页面上，选择监控和性能。
5. 选择 CloudWatch 警报。
6. 选择创建 CloudWatch 警报。随后您将被重定向至 CloudWatch 控制台。
7. 选择选择指标，然后选择下一步。
8. 在指标部分中，选择 FSx。
9. 选择文件系统指标，选中要为其创建警报的指标，然后选择选择指标。
10. 在条件部分中，选择您希望用于该警报的条件，然后选择下一步。

> **Note**
>
> 对于单可用区文件系统，在文件系统维护期间，可能不会发布指标；对于多可用区文件系统，在主文件服务器和辅助文件服务器之间进行失效转移和失效自动恢复期间，可能不会发布指标。为了防止不必要和误导性的警报条件更改，以及为了配置警报以使其能够应对缺失的数据点，请参阅《Amazon CloudWatch 用户指南》中的配置 CloudWatch 警报处理缺失数据的方式。

11. 如果您希望 CloudWatch 在警报状态触发操作时向您发送电子邮件或 SNS 通知，请选择每当此警报状态为警报状态。

    对于选择 SNS 主题，选择一个现有的 SNS 主题。如果您选择创建主题，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。选择下一步。

> **Note**
>
> 如果您使用创建主题创建了一个新的 Amazon SNS 主题，那么电子邮件地址在接收通知之前必须通过验证。当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。

12. 填写指标的名称、描述和每当值，然后选择下一步。
13. 在预览和创建页面上，查看您即将创建的警报，然后选择创建警报。

使用 CloudWatch 控制台设置警报

1. 登录到 Amazon Web Services 管理控制台 并通过以下网址打开 CloudWatch 控制台：https://console.aws.amazon.com/cloudwatch/。
2. 选择创建警报以启动创建警报向导。
3. 选择 FSx 指标并滚动浏览 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。选择要为其创建警报的指标，然后选择下一步。
4. 填写指标的名称、描述和每当值。
5. 如果您希望 CloudWatch 在达到警报状态时向您发送一封电子邮件，对于 Whenever this alarm（每当此警报），请选择 State is ALARM（状态为“警报”）。对于发送通知到，选择一个现有 SNS 主题。如果您选择创建主题，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**
   >
   > 如果您使用创建主题创建了一个新的 Amazon SNS 主题，那么电子邮件地址在接收通知之前必须通过验证。当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，可在警报预览区域预览即将创建的警报。选择创建警报。

设置 CloudWatch 警报（CLI）

- 调用 `put-metric-alarm`。有关更多信息，请参阅 Amazon CLI Command Reference。

设置警报（API）

- 调用 `PutMetricAlarm`。有关更多信息，请参阅 Amazon CloudWatch API 参考。

使用 Amazon CloudTrail 记录 Amazon FSx for Windows File Server 的 API 调用日志

Amazon FSx for Windows File Server 与 Amazon CloudTrail 集成，后者是在 Amazon FSx 中提供用户、角色或 Amazon 服务所采取操作的记录的服务。CloudTrail 以事件形式捕获 Amazon FSx 的所有 API 调用。捕获的调用包含来自 Amazon FSx 控制台的调用以及对 Amazon FSx API 操作的代

码调用。如果您创建跟踪，则可以使 CloudTrail 事件持续传送到 Amazon S3 桶（包括 Amazon FSx 的事件）。如果您不配置跟踪，则仍可在 CloudTrail 控制台中的事件历史记录中查看最新事件。使用 CloudTrail 收集的信息，您可以确定向 Amazon FSx 发出了什么请求、发出请求的 IP 地址、何人发出的请求、请求的发出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 Web Services 账户 时，将在该账户上启用 CloudTrail。当 Amazon FSx 中发生活动时，该活动将记录在 CloudTrail 事件中，并与其他 Amazon 服务事件一同保存在事件历史记录中。您可以在 Amazon Web Services 账户中查看、搜索和下载最新事件。有关更多信息，请参阅使用 CloudTrail 事件历史记录查看事件。

对于 Amazon Web Services 账户 中的事件的持续记录（包括 Amazon FSx 的事件），请创建跟踪记录。通过跟踪记录，CloudTrail 可将日志文件传送至 Amazon S3 存储桶。预设情况下，在控制台中创建跟踪记录时，此跟踪记录应用于所有Amazon Web Services 区域。此跟踪记录在 Amazon 分区中记录所有区域中的事件，并将日志文件传送至您指定的 Amazon S3 存储桶。此外，您可以配置其他 Amazon 服务，进一步分析在 CloudTrail 日志中收集的事件数据并采取行动。有关更多信息，请参阅下列内容：

- 创建跟踪记录概述
- CloudTrail 支持的服务和集成
- Configuring Amazon SNS notifications for CloudTrail
- 从多个区域接收 CloudTrail 日志文件和从多个账户接收 CloudTrail 日志文件

所有 Amazon FSx 操作均由 CloudTrail 记录并记载到 Amazon FSx API 参考中。例如，对 `CreateFileSystem`、`CreateBackup` 和 `TagResource` 操作的调用会在 CloudTrail 日志文件中生成条目。

每个事件或日志条目都包含有关生成请求的人员信息。身份信息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用户的临时安全凭证发出的。
- 请求是否由其他 Amazon 服务发出。

有关更多信息，请参阅 CloudTrail userIdentity 元素。

了解 Amazon FSx 日志文件条目

跟踪记录是一种配置，可用于将事件作为日志文件传送到您指定的 Amazon S3 桶。CloudTrail 日志文件包含一个或多个日记账条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序显示。

以下示例显示了一个 CloudTrail 日志条目，该条目演示了从控制台为文件系统创建标签时的 `TagResource` 操作。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
        "principalId": “111122223333”,
        "arn": "arn:aws:sts::111122223333:root”,
        "accountId": “111122223333”,
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE”,
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-14T22:36:07Z"
            }
        }
    },
    "eventTime": "2018-11-14T22:36:07Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "TagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": “192.0.2.0”,
    "userAgent": “console.amazonaws.com”,
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789”
    },
    "responseElements": null,
    "requestID": “aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51”,
    "eventID": “bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p”,
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": “111122223333”
}
```

以下示例显示了一个 CloudTrail 日志条目，该条目演示了从控制台删除文件系统标签时的 UntagResource 操作。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
        "principalId": "111122223333",
        "arn": "arn:aws:sts::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-14T23:40:54Z"
            }
        }
    },
    "eventTime": "2018-11-14T23:40:54Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "UntagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789"
    },
    "responseElements": null,
    "requestID": "aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51",
    "eventID": "bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p",
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": "111122223333"
}
```

Amazon 的安全 FSx

云安全 Amazon 是重中之重。作为 Amazon 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方共同承担 Amazon 的责任。责任共担模式将其描述为云的 安全性和云中 的安全性：

- 云安全 — Amazon 负责保护在 Amazon Web Services 云中运行 Amazon 服务的基础设施。Amazon 还为您提供可以安全使用的服务。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 FSx 适用于亚马逊 Windows 文件服务器的合规计划，请参阅合规计划范围内的Amazon 服务。
- 云端安全-您的责任由您使用的 Amazon 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

本文档可帮助您了解在使用 Amazon FSx for Windows 文件服务器时如何应用分担责任模型。以下主题向您展示如何配置 Amazon f FSx or Windows 文件服务器以满足您的安全与合规目标。您还将学习如何使用其他 Amazon 服务来帮助您监控和保护您的 Amazon f FSx or Windows 文件服务器资源。

主题

适用于 Windows File Server 的 Amazon FSx 中的数据保护

对于适用于 Windows File Server 的 Amazon FSx 中的数据保护，Amazon 责任共担模式适用。如该模式中所述，Amazon 负责保护运行所有 Amazon Web Services 云 的全球基础结构。您负责维护对托管在此基础结构上的内容的控制。您还负责您所使用的 Amazon Web Services 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。

出于数据保护目的，建议您保护 Amazon Web Services 账户 凭证并使用 Amazon IAM Identity Center 或 Amazon Identity and Access Management（IAM）设置单个用户。这样，每个用户只获得履行其工作职责所需的权限。还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证（MFA）。
- 使用 SSL/TLS 与 Amazon 资源进行通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用 Amazon CloudTrail 设置 API 和用户活动日记账记录。有关使用 CloudTrail 跟踪来捕获 Amazon 活动的信息，请参阅《Amazon CloudTrail 用户指南》中的使用 CloudTrail 跟踪。
- 使用 Amazon 加密解决方案以及 Amazon Web Services 服务中的所有默认安全控制。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果在通过命令行界面或 API 访问 Amazon 时需要经过 FIPS 140-3 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-3 版》。

强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括使用控制台、API、Amazon CLI 或 Amazon SDK 处理 FSx for Windows File Server 或其他 Amazon Web Services 服务 时。在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供网址，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

FSx for Windows File Server 中的数据加密

适用于 Windows File Server 的 Amazon FSx 支持静态数据加密和传输中数据加密。创建 Amazon FSx 文件系统时，系统会自动启用静态数据加密。在支持 SMB 协议 3.0 或更高版本的计算实例上映射的文件共享支持传输中数据加密。Amazon FSx 会在您访问文件系统时使用 SMB 加密自动加密传输中数据，而无需修改应用程序。

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。

如果您的组织受到要求对数据和元数据进行静态加密的公司或监管政策的约束，则您的数据会自动进行静态加密。我们还建议您通过对传输中数据进行加密来挂载文件系统，从而对传输中数据进行加密。

静态数据加密

所有 Amazon FSx 文件系统都使用 Amazon Key Management Service（Amazon KMS）管理的密钥进行静态加密。数据在写入文件系统前会自动加密，并在读取时自动解密。这些过程由 Amazon FSx 透明地处理，因此，您不必修改您的应用程序。

Amazon FSx 使用行业标准 AES-256 加密算法对静态 Amazon FSx 数据和元数据进行加密。有关更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的加密基础知识。

> **Note**
>
> 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 FSx 与 Amazon KMS 集成在一起以进行密钥管理。Amazon FSx 使用 Amazon KMS key 来加密您的文件系统。您可以选择用于加密和解密文件系统（包括数据和元数据）的 KMS 密钥。您可以启用、禁用或撤销对该 KMS 密钥的授权。该 KMS 密钥可以是以下两种类型之一：

- Amazon 托管式密钥 – 这是默认 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政策以及为多个用户或服务提供授权。有关创建客户托管式密钥的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的创建密钥。

如果将客户托管式密钥作为您的 KMS 密钥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，对于客户托管式密钥，您可以随时选择何时禁用、重新启用、删除或撤销您的 KMS 密钥访问权限。有关更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的轮换 Amazon KMS keys。

Amazon KMS 的 Amazon FSx 密钥政策

密钥政策是控制对 KMS 密钥访问的主要方法。有关密钥政策的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的使用 Amazon KMS 中的密钥政策。以下列表描述了 Amazon FSx 针对静态加密文件系统支持的所有 Amazon KMS 相关权限：

- kms:Encrypt –（可选）将明文加密为加密文字。该权限包含在默认密钥策略中。
- kms:Decrypt –（必需）解密密文。密文是以前加密的明文。该权限包含在默认密钥策略中。

- kms:ReEncrypt – (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:GenerateDataKeyWithoutPlaintext – (必需) 返回在 KMS 密钥下加密的数据加密密钥。该权限包含在默认密钥政策中的 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。授权是密钥政策的替代权限机制。有关授权的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的使用授权。该权限包含在默认密钥策略中。
- kms:DescribeKey – (必需) 提供有关所指定 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。在使用控制台创建加密的文件系统时，该权限将填充 KMS 密钥列表。我们建议您使用该权限以提供最佳的用户体验。该权限包含在默认密钥策略中。

传输中数据加密

在支持 SMB 协议 3.0 或更高版本的计算实例上映射的文件共享支持传输中数据加密。这包括从 Windows Server 2012 和 Windows 8 开始的所有 Windows 版本，以及所有 Samba 客户端版本 4.2 或更高版本的 Linux 客户端。适用于 Windows File Server 的 Amazon FSx 会在您访问文件系统时使用 SMB 加密自动加密传输中数据，而无需修改应用程序。

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，同时通过使用 SMB Kerberos 会话密钥进行签名来提供数据完整性。使用 AES-128-GCM 可以提高性能，例如，通过加密的 SMB 连接复制大文件时，性能最多可提高 2 倍。

为了满足始终对传输中数据进行加密的合规性要求，您可以将文件系统的访问权限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。这允许您在同一个文件系统上混合使用加密和未加密的文件共享。

管理传输中加密

您可以使用一组自定义 PowerShell 命令来控制在 FSx for Windows File Server 文件系统和客户端之间的传输中数据加密。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，以保持传输中数据始终处于加密状态。启用强制执行传输中数据加密后，使用不支持 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。

您还可以在文件共享级别而不是文件服务器级别控制传输中数据加密。如果您想对某些包含敏感数据的文件共享强制执行传输中加密，并允许所有用户访问某些其他文件共享，则可以使用文件共享级别的加

密控制，以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别的加密。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 for Remote Management on PowerShell 管理文件系统上的传输中加密。要了解如何使用此 CLI，请参阅将 Amazon FSx CLI 用于 PowerShell。

如下所列为可用于管理文件系统上的用户传输中加密的命令。

传输中加密命令	描述
Get-FSxSmbServerConfiguration	检索服务器消息块（SMB）服务器配置。在系统响应中，可以根据 `EncryptData` 和 `RejectUnencryptedAccess` 属性的值确定文件系统的传输中加密设置。
Set-FSxSmbServerConfiguration	此命令提供两个选项，用于在文件系统上全局配置传输中加密： • `-EncryptData $True\|$False` - 将此参数设置为 `True` 可开启传输中数据加密。将此参数设置为 `False` 可关闭传输中数据加密。 • `-RejectUnencryptedAccess $True\|$False` - 将此参数设置为 `True` 禁止不支持加密的客户端访问文件系统。将此参数设置为 `False` 允许不支持加密的客户端访问文件系统。
Set-FSxSmbShare -name ***name*** -EncryptData $True	将此参数设置为 `True`，以开启共享的传输中数据加密。将此参数设置为 `False`，以关闭共享的传输中数据加密。

每个命令的联机帮助中都提供所有命令选项的参考信息。要访问此帮助，请运行包含 -? 的命令，例如 Get-FSxSmbServerConfiguration -?。

使用 Windows 进行文件和文件夹级别的访问控制 ACLs

亚马逊版 FSx Windows 文件服务器支持通过微软 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，使管理员和用户能够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账户。要了解有关 Amazon 活动目录支持的更多信息 FSx，请参阅使用 Microsoft Active Directory。

您的加入域的计算实例可以使用 Active Directory 凭证访问亚马逊 FSx 文件共享。您可以使用标准的 Windows 访问控制列表 (ACLs) 进行精细的文件级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证，以强制执行这些 Windows ACLs。

每个亚马逊 FSx 文件系统都附带一个名为的默认 Windows 文件共享`share`。此共享文件夹 ACLs 的 Windows 已配置为允许域用户进行 read/write 访问。它们还允许完全控制 Active Directory 中受委托对文件系统执行管理操作的委派的管理员组。如果您要将文件系统与 Amazon 托管 Microsoft AD 集成，则此组为 Amazon 委派 FSx 管理员。如果您要将文件系统与自行管理的 Microsoft AD 设置集成，则该组可以是域管理员。也可以是您在创建文件系统时指定的自定义委派的管理员组。要更改 ACLs，您可以将共享映射为委派管理员组成员的用户。

> **Warning**
>
> Amazon FSx 要求系统用户对您的文件系统中的所有文件夹拥有完全控制 NTFS ACL 权限。请勿更改此用户在您的文件夹上的 NTFS ACL 权限。这样做会使您的文件共享无法访问，并使文件系统备份无法使用。

相关链接

- 什么是 Amazon Directory Service？ 在《 Amazon Directory Service 管理指南》中。
- 在《AmazonAmazon Directory Service 管理指南》中创建你的 Microsoft AD 托管目录。
- 《Amazon Directory Service 管理指南》中的何时创建信任关系。
- 步骤 1：设置 Active Directory.

使用 Amazon VPC 进行文件系统访问控制

您可以通过弹性网络 interface 访问您的亚马逊 FSx 文件系统。该网络接口位于虚拟私有云（VPC）中，基于您与文件系统关联的 Amazon Virtual Private Cloud（Amazon VPC）服务。您可以通过其域名服务 (DNS) 名称连接到您的 Amazon FSx 文件系统。DNS 名称映射到 VPC 中文件系统弹性网络接口的私有 IP 地址。只有关联 VPC 内的资源、通过 Amazon Direct Connect 或 VPN 与关联 VPC 连接的资源或对等体内的资源 VPCs 才能访问文件系统的网络接口。有关更多信息，请参阅《Amazon VPC 用户指南》中的什么是 Amazon VPC？。

> **Warning**
>
> 不得修改或删除与您的文件系统关联的弹性网络接口。修改或删除该网络接口可能会导致永久丢失您的 VPC 和文件系统之间的连接。

FSx 适用于 Windows 文件服务器支持 VPC 共享，这使您能够查看、创建、修改和删除其他 Amazon 账户拥有的 VPC 中共享子网中的资源。有关更多信息，请参阅 Amazon VPC 用户指南 VPCs中的使用共享。

Amazon VPC 安全组

为了进一步控制通过 VPC 内文件系统弹性网络接口的网络流量，请使用安全组来限制对文件系统的访问。安全组是一种状态防火墙，用于控制进出其关联网络接口的流量。在这种情况下，关联的资源就是文件系统的网络接口。

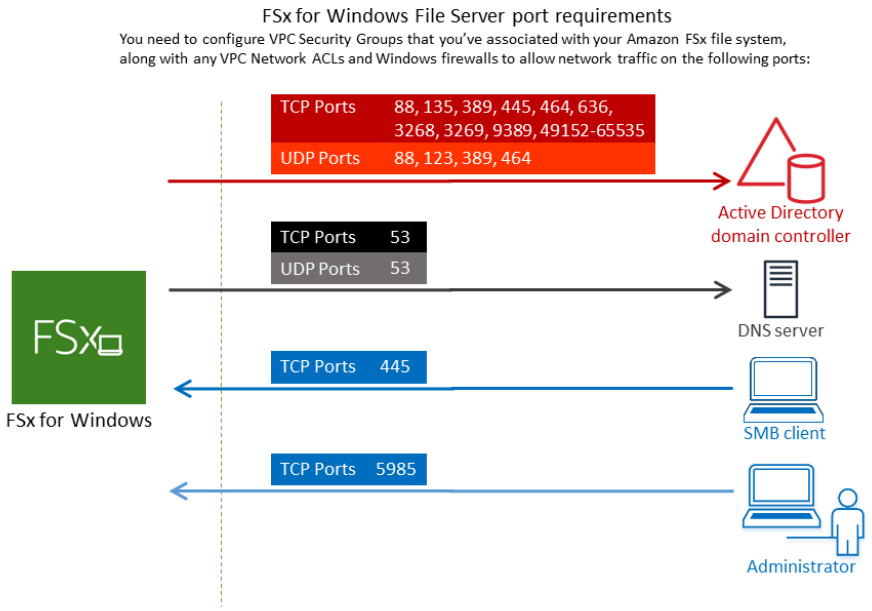
要使用安全组控制对您的 Amazon FSx 文件系统的访问，请添加入站和出站规则。入站规则控制传入的流量，出站规则控制从文件系统传出的流量。确保您的安全组中有正确的网络流量规则，可以将 Amazon FSx 文件系统的文件共享映射到支持的计算实例上的文件夹。

有关安全组规则的更多信息，请参阅 Amazon EC2 用户指南中的安全组规则。

为 Amazon 创建安全组 FSx

1. 在 https://console.aws.amazon.com/ec2 上打开亚马逊 EC2 控制台。
2. 在导航窗格中，选择 Security Groups（安全组）。
3. 选择创建安全组。
4. 为安全组指定名称和描述。
5. 对于 VPC，请选择与您的文件系统关联的 Amazon VPC 以在该 VPC 中创建安全组。
6. 添加以下规则以允许以下端口上的出站网络流量：

   a. 对于 VPC 安全组，用于您的默认 Amazon VPC 的默认安全组已添加到控制台中的文件系统。请确保您创建 FSx 文件系统的子网的安全组和 VPC 网络 ACLs 允许以下图所示的端口和方向上的流量。



下表确定了每个端口的作用。

协议	端口	角色
TCP/UDP	53	域名系统（DNS）
TCP/UDP	88	Kerberos 身份验证
TCP/UDP	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	轻量级目录访问协议 TLS/SSL (LDAPS)
TCP	3268	Microsoft 全局目录

协议	端口	角色
TCP	3269	基于 SSL 的 Microsoft 全局目录
TCP	5985	WinRM 2.0（Microsoft Windows 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到适用于每个 AD 域控制器、DNS 服务器、 FSx 客户端和管理员的防火墙上。 FSx

> **Important**
>
> 虽然 Amazon VPC 安全组要求仅在网络流量启动的方向上打开端口，但大多数 Windows 防火墙和 VPC 网络都 ACLs 要求双向打开端口。

> **Note**
>
> 如果您定义了 Active Directory 站点，则必须确保与 Amazon FSx 文件系统关联的 VPC 中的子网是在活动目录站点中定义的，并且您的 VPC 中的子网与其他站点中的子网之间不存在冲突。您可以使用 Active Directory Sites and Services MMC 管理单元查看和更改这些设置。

> **Note**
>
> 在某些情况下，您可能已经修改了 Amazon Managed Microsoft AD 安全组规则的默认设置。如果是，请确保此安全组具有允许来自您的 Amazon FSx 文件系统的流量所需的入

站规则。有关必需的入站规则的更多信息，请参阅《Amazon Directory Service 管理指南》中的Amazon Managed Microsoft AD 先决条件。

现在，您已经创建了安全组，可以将其与 Amazon FSx 文件系统的弹性网络接口相关联。

将安全组与您的 Amazon FSx 文件系统关联

1. 打开 Amazon FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 在控制面板上，选择您的文件系统以查看其详细信息。
3. 在网络与安全选项卡上，选择文件系统的网络接口；例如，ENI-01234567890123456。对于单可用区文件系统，您将看到单个网络接口。对于多可用区文件系统，您将在首选子网和备用子网中分别看到一个网络接口。
4. 对于每个网络接口，选择网络接口，然后在操作中选择更改安全组。
5. 在更改安全组对话框中，选择要使用的安全组，然后选择保存。

禁止访问文件系统

要暂时禁止所有客户端通过网络访问您的文件系统，您可以删除与文件系统的 elastic network interface 关联的所有安全组，然后将其替换为没有 inbound/outbound 规则的组。

亚马逊 VPC 网络 ACLs

保护对您的 VPC 内文件系统的访问的另一种选择是建立网络访问控制列表（网络 ACLs）。网络与安全组 ACLs 是分开的，但具有类似的功能，可以为您的 VPC 中的资源添加额外的安全层。有关网络的更多信息 ACLs，请参阅 Amazon VPC 用户指南 ACLs中的网络。

使用文件访问审计记录最终用户的访问

Amazon FSx for Windows 文件服务器支持审核最终用户对文件、文件夹和文件共享的访问权限。您可以选择将文件系统的审计事件日志发送到提供丰富功能集的其他 Amazon 服务。这些服务包括实现查询、处理、存储和存档日志、发出通知和触发操作，以进一步推进安全性和合规性目标。

有关使用文件访问审计来深入了解访问模式和实施最终用户活动安全通知的更多信息，请参阅文件存储访问模式见解和实施最终用户活动安全通知。

> **Note**
>
> 只有吞吐量为 32 MBps 或更大 FSx 的 Windows 文件系统才支持文件访问审计。您可以修改现有文件系统的吞吐能力。有关更多信息，请参阅 管理吞吐能力。

文件访问审计能让您根据您定义的审核控制措施记录最终用户对单个文件、文件夹和文件共享的访问。审计控制也称为 NTFS 系统访问控制列表 (SACLs)。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计。

Amazon FSx 支持以下 Windows 审核事件，用于访问文件、文件夹和文件共享：

- 对于文件访问，它支持：全部、遍历文件夹/执行文件、列出文件夹/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：连接到文件共享。

在文件、文件夹和文件共享访问中，Amazon FSx 支持记录成功尝试（例如拥有足够权限的用户成功访问文件或文件共享）、失败的尝试或两者兼而有之。

您可以配置是只想对文件和文件夹进行访问审核，还是只对文件共享进行访问审核，或者都进行审核。您也可以配置应记录哪些类型的访问（仅成功尝试、仅失败尝试或同时记录两者）。您还可以随时关闭文件访问审计。

> **Note**
>
> 文件访问审计仅记录启用后的最终用户访问数据。也就是说，文件访问审计不会生成在启用文件访问审核前发生的最终用户文件、文件夹和文件共享访问活动的审计事件日志。

支持的访问审核事件最大速率为每秒 5000 个事件。访问审核事件不针对每个文件读取和写入操作生成，而是每个文件元数据操作生成一次，例如用户创建、打开或删除文件时。

主题

- 设置文件和文件夹审计控制
- 管理文件访问审计

审核事件日志目标

启用文件访问审计时，必须配置 Amazon 向其 FSx 发送审核事件日志的 Amazon 服务。您可以将审计事件日志发送到日志组中的 Amazon CloudWatch 日志流或 Amazon Data CloudWatch Firehose 传输流。您可以在创建 Amazon FSx for Windows 文件服务器文件系统时选择审核事件日志目标，也可以在更新现有文件系统之后随时选择审计事件日志目标。有关更多信息，请参阅 管理文件访问审计。

以下是一些可以帮助您决定如何选择审核事件日志目标的建议：

- 如果您想在 Amazon CloudWatch 控制台中存储、查看和搜索审计事件日志，使用 Logs Insights 对日志进行查询，以及触发 CloudWatch 警报或 Lambda 函数，请选择 CloudWatch CloudWatch 日志。
- 如果您想持续将事件流式传输到亚马逊 S3 中的存储、亚马逊 Redshift 中的数据库、亚马逊服务或合作伙伴解决方案（例如 Splunk 或 Datadog）进行进一步分析， Amazon 请选择 OpenSearch Amazon Data Firehose。

默认情况下，Amazon FSx 将在您的账户中创建并使用默认 CloudWatch 日志组作为审计事件日志目标。如果要使用自定义 CloudWatch 日志组或使用 Firehose 作为审核事件日志目标，则对审计事件日志目标的名称和位置要求如下：

- CloudWatch 日志日志组的名称必须以`/aws/fsx/`前缀开头。如果您在控制台上创建或更新文件系统时没有现有的 CloudWatch 日志日志组，Amazon FSx 可以在日志组中创建和使用默认 CloudWatch `/aws/fsx/windows`日志流。如果您不想使用默认日志组，则配置用户界面允许您在控制台上创建或更新文件系统时创建 CloudWatch 日志日志组。
- Firehose 传输流的名称必须以 `aws-fsx-` 为前缀。如果您没有现有的 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 Firehose 传输流配置为以 `Direct PUT` 作为其来源。不得使用现有的 Kinesis 数据流作为传输流的数据来源。
- 目标（ CloudWatch 日志日志组或 Firehose 传输流）必须与您的亚马逊 FSx 文件系统位于同一个 Amazon 分区 Amazon Web Services 区域、和 Amazon Web Services 账户 中。

您可以随时更改审核事件日志的目标（例如，从 Lo CloudWatch gs 更改为 Firehose）。更改后，新的审核事件日志便只会发送到新的目标。

最大努力审核事件日志传送

通常，审核事件日志记录传输至目标只需要几分钟，但有时可能会需要更长的时间。在极少数情况下，审核事件日志记录可能会有遗漏。如果您的使用案例需要特定的语义（例如，确保不遗漏任何审核事件），我们建议您在设计工作流程时对遗漏的事件进行说明。您可以通过扫描文件系统上的文件和文件夹结构来审核遗漏的事件。

迁移审核控制措施

如果您已经对现有文件数据设置了审计控制 (SACLs)，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 来传输数据以及与您的 Amazon FSx 文件系统关联 SACLs 的。此外，您还可以使用 Robocopy（Robust File Copy）。有关更多信息，请参阅 将现有文件存储迁移到 Amazon FSx。

查看事件日志

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

- 要查看 CloudWatch 日志日志，请进入 CloudWatch 控制台，选择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 Amazon Logs 用户指南中的查看发送到 CloudWatch CloudWatch 日志的日志数据。

  您可以使用 CloudWatch Logs 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 Amazon Logs 用户指南中的使用 CloudWatch 日志见解分析 CloudWatch 日志数据。

  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《亚马逊日志用户指南》中的将日志数据导出到 Amazon CloudWatch S3。
- 您无法在 Firehose 上查看审核事件日志。但是，您可以将 Firehose 配置为将日志转发到您可以读取的目标。目的地包括亚马逊 S3、亚马逊 Redshift、亚马逊 OpenSearch 服务以及 Splunk 和 Datadog 等合作伙伴解决方案。有关更多信息，请参阅亚马逊 Dat a Firehose 开发者指南中的选择目的地。

审核事件字段

本节介绍审核事件日志中的信息描述以及审核事件示例。

以下是对 Windows 审核事件中重要字段的描述。

- EventID 指 Microsoft 定义的 Windows 事件日志事件 ID。有关文件系统事件和文件共享事件的信息，请参阅 Microsoft 文档。
- SubjectUserName指执行访问权限的用户。
- ObjectName指访问的目标文件、文件夹或文件共享。
- ShareName适用于为文件共享访问而生成的事件。例如，`EventID 5140` 在访问网络共享对象时生成。
- IpAddress指启动文件共享事件的客户端。
- Keywords（如有）指明文件访问成功还是失败。如果是成功的访问，该值为 `0x8020000000000000`。如果是失败的访问，该值为 `0x8010000000000000`。
- TimeCreated SystemTime指事件在系统中生成并以 <YYYY-MM--: mm : ss.s>Z 格式显示的时间。DDThh
- 计算机是指文件系统 Windows 远程 PowerShell 端点的 DNS 名称，可用于识别文件系统。
- AccessMask，如果可用，则指所执行的文件访问类型（例如 ReadData、 WriteData）。
- AccessList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 中）。

访问类型	访问掩码	值
读取数据或列出目录	0x1	%%4416
写入数据或添加文件	0x2	%%4417
追加数据或添加子目录	0x4	%%4418
读取扩展属性	0x8	%%4419
写入扩展属性	0x10	%%4420
执行/遍历	0x20	%%4421
删除子	0x40	%%4422
读取属性	0x80	%%4423
写入属性	0x100	%%4424

访问类型	访问掩码	值
删除	0x10000	%%1537
读取 ACL	0x20000	%%1538
写入 ACL	0x40000	%%1539
写入所有者	0x80000	%1540
同步	0x100000	%1541
访问安全 ACL	0x1000000	%%1542

以下是一些关键事件和示例。请注意，对 XML 设置了格式以便于阅读。

删除对象时会记录事件 ID 4660。

```
<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>
```

请求删除文件时会记录事件 ID 4659。

```
<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>
```

为对象执行特定操作时会记录事件 ID 4663。以下示例显示了从文件中读取数据，这些数据可以通过 AccessList %%4416 进行解读。

```
<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>
```

以下示例显示了文件中的 write/append 数据，可以从中解释`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 表示已请求对某个对象请求特定访问权限。在以下示例中，读取请求是 ObjectName 为 “permtest” 发起的，但尝试失败，如关键字值所示。`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>
```

更改对象权限时会记录事件 ID 4670。以下示例显示用户 “管理员” 修改了 “permtest” 的权限，以向 SID “S-1-5-21-65 ObjectName 8495921-4185342820-3824891517-1113” 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>
```

每次访问文件共享时都会记录事件 ID 5140。

```
<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>
```

在文件共享级别拒绝访问时会记录事件 ID 5145。以下示例显示了对 ShareName “demoshare01” 的访问被拒绝。

```
<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 Lo CloudWatch gs Insights 搜索日志数据，则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/
```

- 查询与特定文件名匹配的所有事件：

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

有关 Lo CloudWatch gs Insights 查询语言的更多信息，请参阅 Amazon Logs 用户指南中的使用 CloudWatch CloudWatch 日志见解分析日志数据。

设置文件和文件夹审计控制

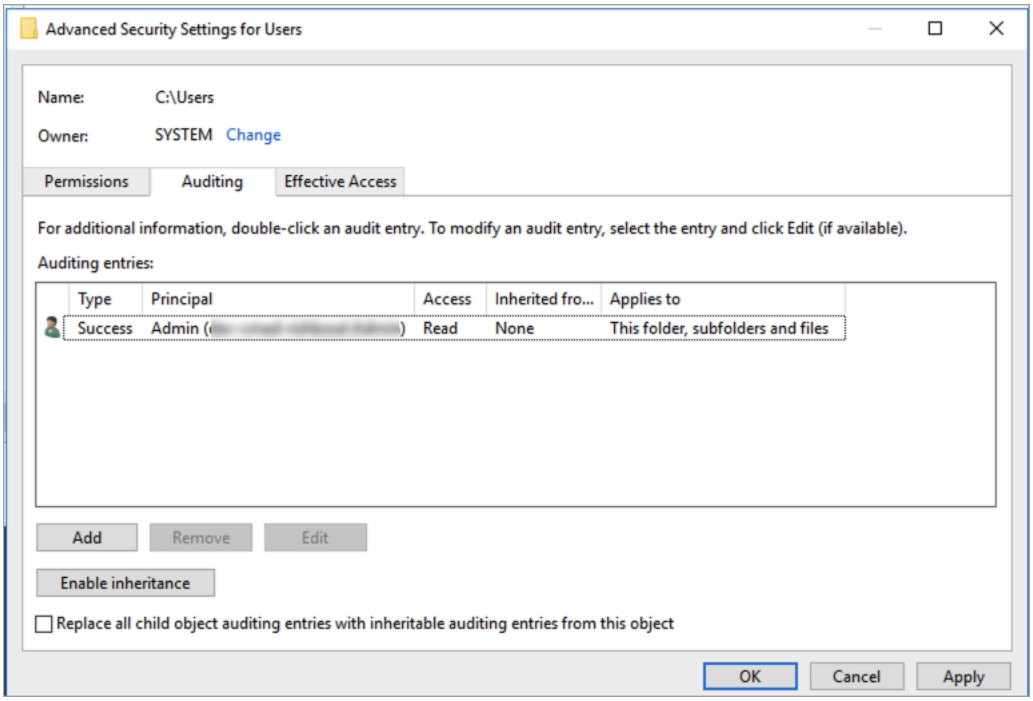
您需要为要审核用户访问尝试的文件和文件夹设置审核控制措施。审计控制也称为 NTFS 系统访问控制列表 (SACLs)。

您可以使用 Windows 原生 GUI 界面或使用 Windows 命令以编程方式配置审计控制。 PowerShell 如果启用继承，则通常只需要对要记录访问日志的顶级文件夹设置审核控制措施。

使用 Windows GUI 设置审核访问

要使用 GUI 对文件和文件夹设置审核控制措施，请使用 Windows 文件资源管理器。在给定文件或文件夹上，打开 Windows 文件资源管理器，然后选择属性 > 安全 > 高级 > 审核选项卡。

以下审核控制措施示例审核文件夹的成功事件。每当管理员用户成功打开该句柄进行读取时，就会发出一个 Windows 事件日志条目。



类型字段指示您要审核的操作。将此字段设置为成功可审核成功的尝试，将此字段设置为失败可审核失败的尝试，将此字段设置为全部可审核成功的尝试和失败的尝试。

有关审核输入字段的更多信息，请参阅 Microsoft 文档中的对文件或文件夹应用基本审核策略。

使用 PowerShell 命令设置审核访问权限

您可以使用 Microsoft Windows `Set-Acl` 命令对任何文件或文件夹设置审核 SACL。有关此命令的更多信息，请参阅 Microsoft Set-Acl 文档。

以下是使用一系列 PowerShell 命令和变量为成功尝试设置审核访问权限的示例。您可以调整这些示例命令，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

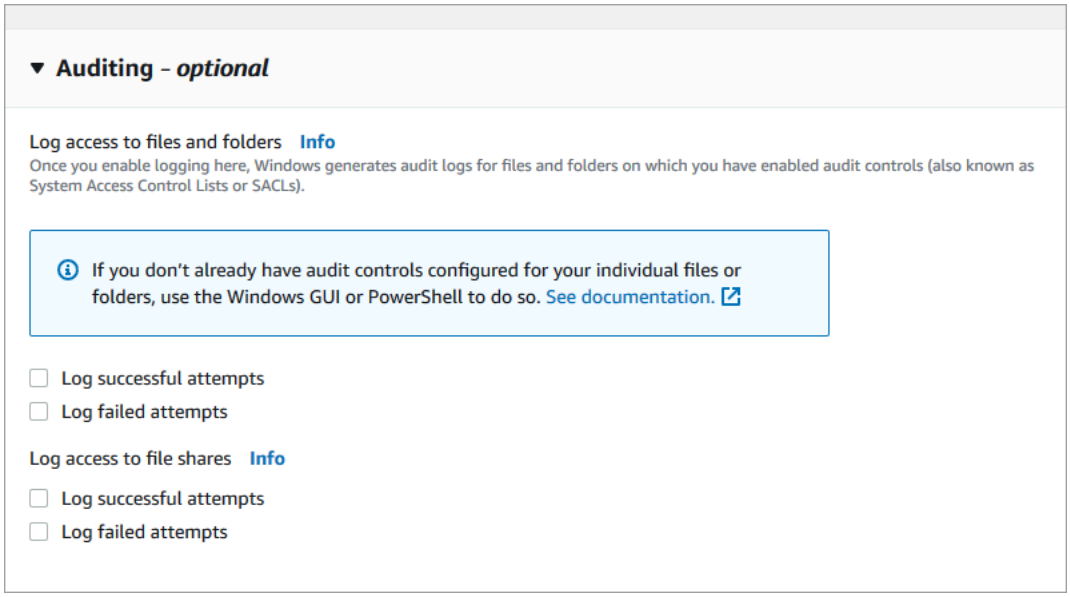
在创建新的 Amazon FSx for Windows 文件服务器文件系统时，您可以启用文件访问审计。当您通过 Amazon FSx 控制台创建文件系统时，文件访问审计默认处于关闭状态。

在启用了文件访问审计的现有文件系统上，您可以更改文件访问审计设置，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 控制台或 API 执行这些任务。Amazon CLI

> **Note**
>
> 只有吞吐量为 32 MBps 或更大 FSx 的 Windows 文件服务器文件系统的 Amazon 支持文件访问审计。 MBps 如果启用了文件访问审计，则无法创建或更新吞吐量小于 32 的文件系统。创建文件系统后，您可以随时修改吞吐能力。有关更多信息，请参阅 管理吞吐能力。

创建文件系统时启用文件访问审计（控制台）

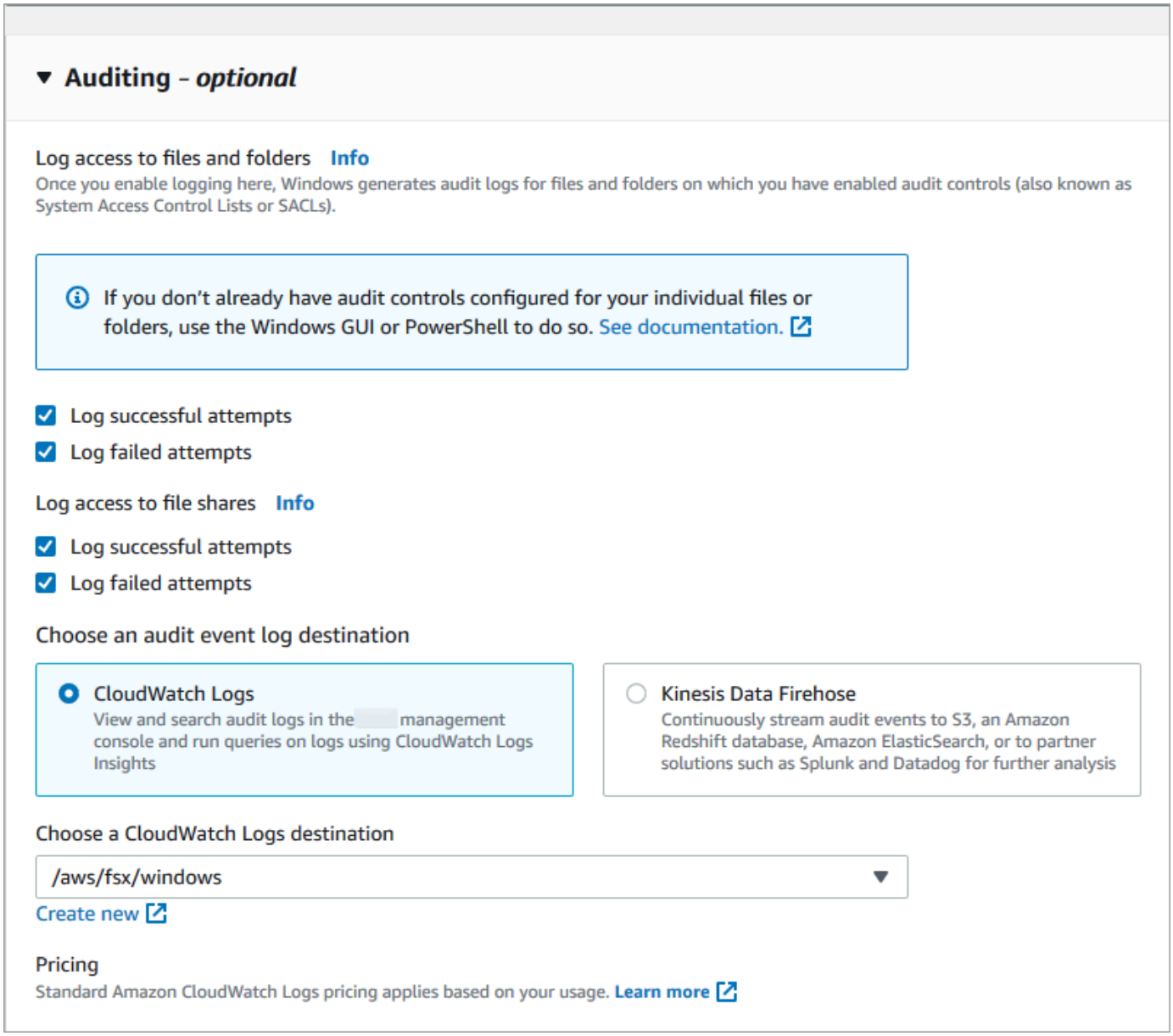
1. 打开亚马逊 FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 按照“入门”部分的步骤 5。创建文件系统中所述的步骤创建新文件系统。
3. 打开审核 – 可选部分。默认情况下，文件访问审计处于禁用状态。



4. 要启用和配置文件访问审计，请执行以下操作。

   - 在 “记录对文件和文件夹的访问权限” 中，选择记录成功 and/or 失败的尝试。如果未做出选择，则会禁用文件和文件夹的日志记录。
   - 要记录对文件共享的访问权限，请选择记录成功 and/or 失败的尝试。如果未做出选择，则会禁用文件共享的日志记录。
   - 在 “选择审核事件日志目标” 中，选择 “CloudWatch 日志” 或 “Fire hose”。然后选择现有日志或传输流，或者创建新的日志或传输流。对于 CloudWatch 日志，Amazon FSx 可以在日志组中创建和使用默认 CloudWatch `/aws/fsx/windows`日志流。

   以下是文件访问审计配置的示例，该配置将审核最终用户成功和失败的文件、文件夹和文件共享访问尝试。审核事件日志将发送到默认的 CloudWatch 日志`/aws/fsx/windows`日志组目标。



5. 继续执行文件系统创建向导的下一部分。

当文件系统处于可用状态时，将启用文件访问审计功能。

在创建文件系统时启用文件访问审计（CLI）

1. 创建新文件系统时，请将`AuditLogConfiguration`属性与 CreateFileSystemAPI 操作配合使用，为新文件系统启用文件访问审计。

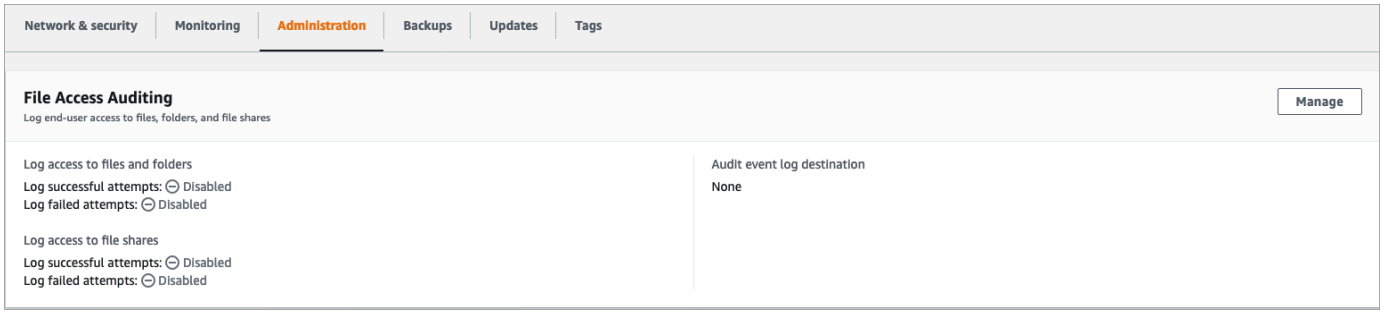
```
aws fsx create-file-system \
  --file-system-type WINDOWS \
```

```
  --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"}'
```

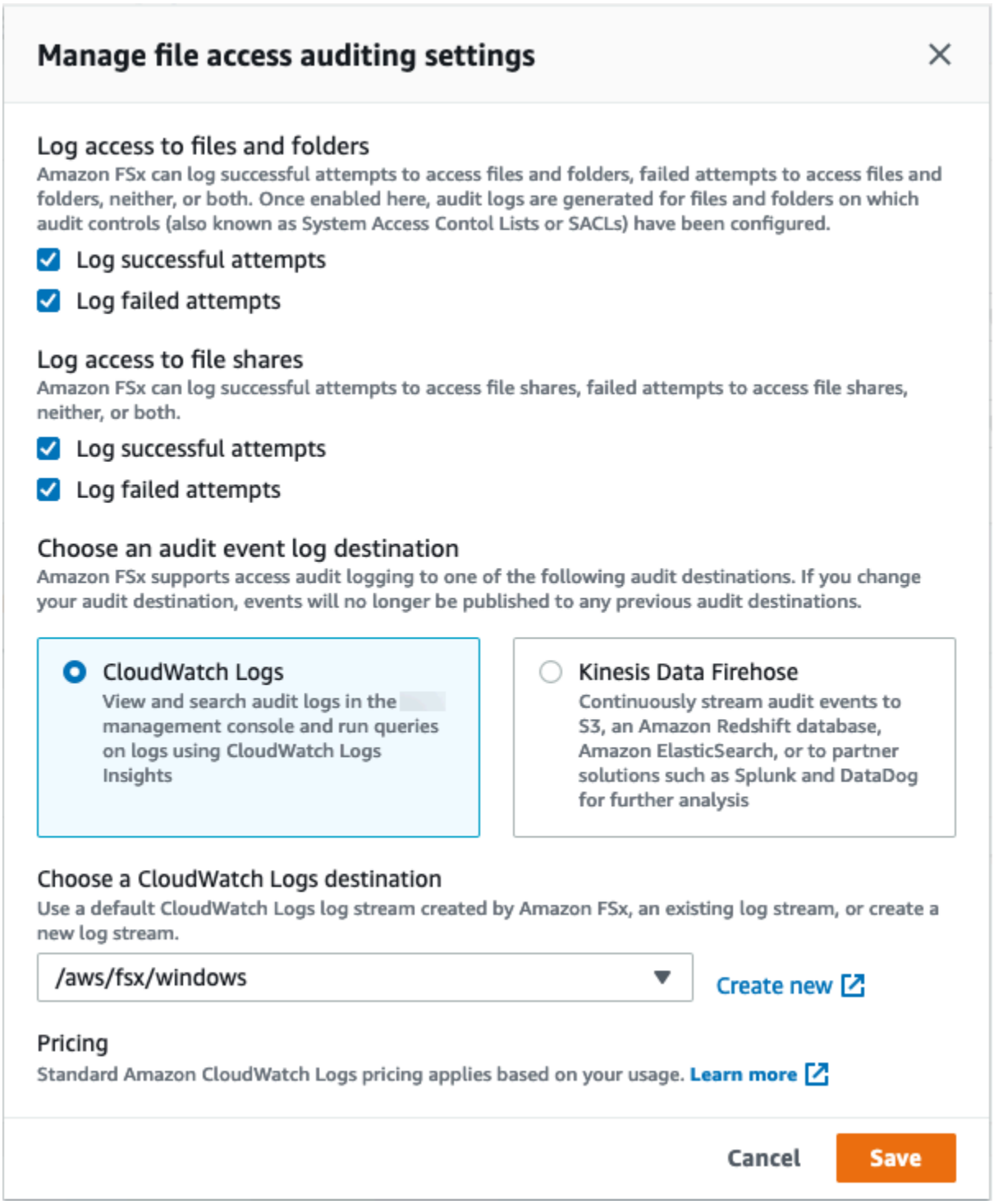
2. 当文件系统处于可用状态时，将启用文件访问审计功能。

更改文件访问审计配置（控制台）

1. 打开亚马逊 FSx 控制台，网址为https://console.aws.amazon.com/fsx/。
2. 导航到文件系统，然后选择要管理文件访问审计的 Windows 文件系统。
3. 选择管理选项卡。
4. 在文件访问审计面板上，选择管理。



5. 在管理文件访问审计设置对话框中，更改所需的设置。



- 在 “记录对文件和文件夹的访问权限” 中，选择记录成功 and/or 失败的尝试。如果未做出选择，则会禁用文件和文件夹的日志记录。
- 要记录对文件共享的访问权限，请选择记录成功 and/or 失败的尝试。如果未做出选择，则会禁用文件共享的日志记录。

- 在 “选择审核事件日志目标” 中，选择 “CloudWatch 日志” 或 “Fire hose”。然后选择现有日志或传输流，或者创建新的日志或传输流。

6. 选择保存。

更改文件访问审计配置（CLI）

- 使用 update-file-system CLI 命令或等效 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"}'
```

适用于 Windows 文件服务器 FSx 的亚马逊身份和访问管理

Amazon Identity and Access Management (IAM) Amazon Web Services 服务 可帮助管理员安全地控制对 Amazon 资源的访问权限。IAM 管理员控制谁可以通过 Windows 文件服务器资源进行身份验证（登录）和授权（拥有权限）。 FSx 您可以使用 IAM Amazon Web Services 服务 ，无需支付额外费用。

主题

- 受众
- 使用身份进行身份验证
- 使用策略管理访问
- FSx 适用于 Windows 的 Amazon 文件服务器如何与 IAM 配合使用
- FSx 适用于亚马逊 Windows 文件服务器的基于身份的策略示例
- Amazon 适用于 Windows 文件服务器 FSx 的亚马逊托管策略
- 对适用 FSx 于 Windows 的 Amazon 文件服务器身份和访问权限进行故障排除
- 在 Amazon 上使用标签 FSx
- 使用适用于 Windows 文件服务器 FSx 的服务相关角色

受众

您的使用方式 Amazon Identity and Access Management (IAM) 因您的角色而异：

- 服务用户 - 如果您无法访问功能，请向管理员申请权限（请参阅对适用 FSx 于 Windows 的 Amazon 文件服务器身份和访问权限进行故障排除）
- 服务管理员 - 确定用户访问权限并提交权限请求（请参阅 FSx 适用于 Windows 的 Amazon 文件服务器如何与 IAM 配合使用）
- IAM 管理员 - 编写用于管理访问权限的策略（请参阅 FSx 适用于亚马逊 Windows 文件服务器的基于身份的策略示例）

使用身份进行身份验证

身份验证是您 Amazon 使用身份凭证登录的方式。您必须以 IAM 用户身份进行身份验证 Amazon Web Services 账户根用户，或者通过担任 IAM 角色进行身份验证。

对于编程访问， Amazon 提供 SDK 和 CLI 来对请求进行加密签名。有关更多信息，请参阅《IAM 用户指南》中的适用于 API 请求的Amazon 签名版本 4。

Amazon Web Services 账户 root 用户

创建时 Amazon Web Services 账户，首先会有一个名为 Amazon Web Services 账户 root 用户的登录身份，该身份可以完全访问所有资源 Amazon Web Services 服务 和资源。我们强烈建议不要使用根用户进行日常任务。有关需要根用户凭证的任务，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

联合身份

作为最佳实践，要求人类用户使用与身份提供商的联合身份验证才能 Amazon Web Services 服务 使用临时证书进行访问。

联合身份是指来自您的企业目录、Web 身份提供商的用户 Amazon Directory Service ，或者 Amazon Web Services 服务 使用来自身份源的凭据进行访问的用户。联合身份代入可提供临时凭证的角色。

IAM 用户和群组

IAM 用户是对单个人员或应用程序具有特定权限的一个身份。建议使用临时凭证，而非具有长期凭证的 IAM 用户。有关更多信息，请参阅 IAM 用户指南中的要求人类用户使用身份提供商的联合身份验证才能 Amazon 使用临时证书进行访问。

IAM 组指定一组 IAM 用户，便于更轻松地对大量用户进行权限管理。有关更多信息，请参阅《IAM 用户指南》中的 IAM 用户的使用案例。

IAM 角色

IAM 角色是具有特定权限的身份，可提供临时凭证。您可以通过从用户切换到 IAM 角色（控制台）或调用 Amazon CLI 或 Amazon API 操作来代入角色。有关更多信息，请参阅《IAM 用户指南》中的担任角色的方法。

IAM 角色对于联合用户访问、临时 IAM 用户权限、跨账户访问、跨服务访问以及在 Amazon 上运行的应用程序非常有用。 EC2有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

使用策略管理访问

您可以 Amazon 通过创建策略并将其附加到 Amazon 身份或资源来控制中的访问权限。策略定义了与身份或资源关联时的权限。 Amazon 在委托人提出请求时评估这些政策。大多数策略都以 JSON 文档的 Amazon 形式存储在中。有关 JSON 策略文档的更多信息，请参阅《IAM 用户指南》中的 JSON 策略概述。

管理员使用策略，通过定义哪个主体可以对什么资源以及在什么条件下执行操作，来指定谁有权访问什么内容。

默认情况下，用户和角色没有权限。IAM 管理员创建 IAM 策略并将其添加到角色中，然后用户可以代入这些角色。IAM 策略定义权限，而不考虑您使用哪种方法来执行操作。

基于身份的策略

基于身份的策略是您附加到身份（用户、组或角色）的 JSON 权限策略文档。这些策略控制身份可在何种条件下对哪些资源执行什么操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户管理型策略定义自定义 IAM 权限。

基于身份的策略可以是内联策略（直接嵌入到单个身份中）或托管策略（附加到多个身份的独立策略）。要了解如何在托管策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管策略与内联策略之间进行选择。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。您必须在基于资源的策略中指定主体。

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

其他策略类型

Amazon 支持其他策略类型，这些策略类型可以设置更常见的策略类型授予的最大权限：

- 权限边界 – 设置基于身份的策略可以授予 IAM 实体的最大权限。有关更多信息，请参阅《 IAM 用户指南》中的 IAM 实体的权限边界。
- 服务控制策略 (SCPs)-在中指定组织或组织单位的最大权限 Amazon Organizations。有关更多信息，请参阅《Amazon Organizations 用户指南》中的服务控制策略。
- 资源控制策略 (RCPs)-设置账户中资源的最大可用权限。有关更多信息，请参阅《Amazon Organizations 用户指南》中的资源控制策略 (RCPs)。
- 会话策略 – 在为角色或联合用户创建临时会话时，作为参数传递的高级策略。有关更多信息，请参阅《IAM 用户指南》中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 Amazon 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

FSx 适用于 Windows 的 Amazon 文件服务器如何与 IAM 配合使用

在使用 IAM 管理 Windows 文件服务器 FSx 的访问权限之前，请先了解哪些可用 FSx 于 Windows 文件服务器的 IAM 功能。

你可以在 Windows 版亚马逊文件服务器上使用 FSx 的 IAM 功能

IAM 功能	FSx 支持
基于身份的策略	是
基于资源的策略	否
策略操作	是
策略资源	是

IAM 功能	FSx 支持
策略条件键（特定于服务）	是
ACLs	否
ABAC（策略中的标签）	是
临时凭证	是
转发访问会话	是
服务角色	否
服务关联角色	是

要全面了解 FSx 以及其他 Amazon 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中的与 IAM 配合使用的Amazon 服务。

基于身份的策略 FSx

支持基于身份的策略：是

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

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

基于身份的策略示例 FSx

要查看基 FSx 于 Windows 文件服务器身份的策略的示例，请参阅。FSx 适用于亚马逊 Windows 文件服务器的基于身份的策略示例

内部基于资源的政策 FSx

支持基于资源的策略：否

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定

资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 Amazon Web Services 服务。

要启用跨账户访问，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的主体。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

的政策行动 FSx

支持策略操作：是

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。在策略中包含操作以授予执行关联操作的权限。

要查看 FSx 操作列表，请参阅《服务授权参考》中的 Amazon FSx 为 Windows 文件服务器定义的操作。

正在执行的策略操作在操作前 FSx 使用以下前缀：

```
fsx
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
      "fsx:action1",
      "fsx:action2"
         ]
```

要查看基 FSx 于 Windows 文件服务器身份的策略的示例，请参阅。 FSx 适用于亚马逊 Windows 文件服务器的基于身份的策略示例

的政策资源 FSx

支持策略资源：是

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

`Resource` JSON 策略元素指定要向其应用操作的一个或多个对象。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于不支持资源级权限的操作，请使用通配符 (*) 指示语句应用于所有资源。

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

要查看 FSx 资源类型及其列表 ARNs，请参阅《服务授权参考》中的 Amazon FSx 为 Windows 文件服务器定义的资源。要了解您可以使用哪些操作来指定每种资源的 ARN，请参阅亚马逊为 Windows 文件服务器定义 FSx 的操作。

要查看基 FSx 于 Windows 文件服务器身份的策略的示例，请参阅。 FSx 适用于亚马逊 Windows 文件服务器的基于身份的策略示例

的策略条件密钥 FSx

支持特定于服务的策略条件键：是

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

`Condition` 元素指定语句何时根据定义的标准执行。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。要查看所有 Amazon 全局条件键，请参阅 IAM 用户指南中的Amazon 全局条件上下文密钥。

要查看 FSx 条件密钥列表，请参阅《服务授权参考》中的 Amazon FSx for Windows 文件服务器的条件密钥。要了解您可以使用条件键的操作和资源，请参阅 Amazon 为 Windows 文件服务器定义 FSx 的操作。

要查看基 FSx 于 Windows 文件服务器身份的策略的示例，请参阅。 FSx 适用于亚马逊 Windows 文件服务器的基于身份的策略示例

ACLs in FSx

支持 ACLs：否

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

ABAC with FSx

支持 ABAC（策略中的标签）：是

基于属性的访问权限控制（ABAC）是一种授权策略，该策略基于称为标签的属性来定义权限。您可以将标签附加到 IAM 实体和 Amazon 资源，然后设计 ABAC 策略以允许在委托人的标签与资源上的标签匹配时进行操作。

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

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

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权定义权限。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问权限控制（ABAC）。

将临时证书与 FSx

支持临时凭证：是

临时证书提供对 Amazon 资源的短期访问权限，并且是在您使用联合身份或切换角色时自动创建的。Amazon 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的临时安全凭证和使用 IAM 的。Amazon Web Services 服务

转发访问会话 FSx

支持转发访问会话（FAS）：是

转发访问会话 (FAS) 使用调用主体的权限 Amazon Web Services 服务，再加上 Amazon Web Services 服务 向下游服务发出请求的请求。有关发出 FAS 请求时的策略详细信息，请参阅转发访问会话。

FSx 的服务角色

支持服务角色：否

服务角色是由一项服务担任、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 Amazon Web Services 服务委派权限的角色。

> **Warning**
>
> 更改服务角色的权限可能会中断 FSx 功能。只有在 FSx 提供操作指导时才编辑服务角色。

的服务相关角色 FSx

支持服务关联角色：是

服务相关角色是一种与服务相关联的 Amazon Web Services 服务服务角色。服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 Amazon Web Services 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务关联角色的权限。

有关创建或管理 FSx Windows 文件服务器服务相关角色的详细信息，请参阅使用适用于 Windows 文件服务器 FSx 的服务相关角色。

FSx 适用于亚马逊 Windows 文件服务器的基于身份的策略示例

默认情况下，用户和角色无权创建或修改 Window FSx s 文件服务器资源。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。

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

有关由 FSx定义的操作和资源类型（包括每种资源类型的格式）的详细信息，请参阅《服务授权参考》中的 Amazon FSx for Windows 文件服务器的操作、资源和条件密钥。 ARNs

主题

- 策略最佳实践
- 使用 FSx 控制台
- 允许用户查看他们自己的权限

策略最佳实践

基于身份的策略决定了是否有人可以在你的账户中创建、访问或删除 FSx Windows 文件服务器资源。这些操作可能会使 Amazon Web Services 账户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- 开始使用 Amazon 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的Amazon 托管策略。它们在你的版本中可用 Amazon Web Services 账户。我们建议您通过定义针对您的用例的 Amazon 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 Amazon 托管策略或工作职能的Amazon 托管策略。
- 应用最低权限：在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM 策略中的条件进一步限制访问权限：您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 Amazon Web Services 服务，例如 Amazon CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性：IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言（JSON）和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM Access Analyzer 验证策略。
- 需要多重身份验证 (MFA)-如果 Amazon Web Services 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的使用 MFA 保护 API 访问。

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

使用 FSx 控制台

要访问 FSx 适用于 Windows 的 Amazon 文件服务器控制台，您必须拥有一组最低权限。这些权限必须允许您列出和查看有关您的 FSx Windows 文件服务器资源的详细信息 Amazon Web Services 账户。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于仅调用 Amazon CLI 或 Amazon API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

为确保用户和角色仍然可以使用 FSx 控制台，还要将 FSx `AmazonFSxConsoleReadOnlyAccess` Amazon 托管策略附加到实体。有关更多信息，请参阅《IAM 用户指南》中的为用户添加权限。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上或使用 Amazon CLI 或 Amazon API 以编程方式完成此操作的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Amazon 适用于 Windows 文件服务器 FSx 的亚马逊托管策略

Amazon 托管策略是由创建和管理的独立策略 Amazon。 Amazon 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住， Amazon 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 Amazon 客户使用。我们建议通过定义特定于使用案例的客户管理型策略来进一步减少权限。

您无法更改 Amazon 托管策略中定义的权限。如果 Amazon 更新 Amazon 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。 Amazon 最有可能在启动新的 API 或现有服务可以使用新 Amazon Web Services 服务 的 API 操作时更新 Amazon 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 Amazon 托管式策略。

Amazon FSx ServiceRolePolicy

允许 FSx Amazon 代表您管理 Amazon 资源。请参阅 使用适用于 Windows 文件服务器 FSx 的服务相关角色，了解更多信息。

Amazon 托管策略：Amazon FSx DeleteServiceLinkedRoleAccess

您不能将 AmazonFSxDeleteServiceLinkedRoleAccess 附加到自己的 IAM 实体。该策略关联到服务，仅用于该服务的服务关联角色。您不能附加、分离、修改或删除此策略。有关更多信息，请参阅使用适用于 Windows 文件服务器 FSx 的服务相关角色。

该策略授予管理权限，允许亚马逊 FSx 删除其对 Amazon S3 访问权限的服务关联角色，该角色仅 FSx 供亚马逊用于 Lustre。

权限详细信息

此策略包括iam允许亚马逊 FSx 查看、删除和查看 Amazon S3 FSx 服务关联角色访问权限的删除状态的权限。

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

Amazon 托管策略：Amazon FSx FullAccess

您可以将 Amazon 附加FSxFullAccess 到您的 IAM 实体。亚马逊 FSx 还将此政策附加到允许亚马逊 FSx 代表您执行操作的服务角色。

提供对 Amazon 的完全访问权限 FSx 和相关 Amazon 服务的访问权限。

权限详细信息

该策略包含以下权限。

- fsx— 允许委托人具有执行所有 Amazon FSx 操作的完全访问权限，但以下操作除外。BypassSnaplockEnterpriseRetention
- ds— 允许委托人查看有关 Amazon Directory Service 目录的信息。

- ec2
  - 允许主体在指定的条件下创建标签。
  - 为可以与 VPC 配合使用的所有安全组提供增强的安全组验证。
- iam— 允许原则代表用户创建 Amazon FSx 服务关联角色。这是必需的，这样 Amazon FSx 才能代表用户管理 Amazon 资源。
- firehose：允许主体将记录写入 Amazon Data Firehose。这是必需的，这样用户才能通过向 Firehose 发送审核访问日志来监控 FSx Windows 文件服务器文件系统的访问权限。
- logs：允许主体创建日志组、日志流并将事件写入日志流。这是必需的，这样用户才能通过向日志发送审核访问日志来监控 FSx Windows 文件服务器文件系统的访问权限。 CloudWatch

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

Amazon 托管策略：Amazon FSx ConsoleFullAccess

您可以将 AmazonFSxConsoleFullAccess 策略附加到 IAM 身份。

此政策授予管理权限，允许用户完全访问亚马逊 FSx 并通过访问相关 Amazon 服务 Amazon Web Services 管理控制台。

权限详细信息

该策略包含以下权限。

- fsx— 允许委托人在 Amazon FSx 管理控制台中执行所有操作，但以下操作除外。BypassSnaplockEnterpriseRetention
- cloudwatch— 允许委托人在 Amazon FSx 管理控制台中查看 CloudWatch 警报和指标。
- ds— 允许委托人列出有关 Amazon Directory Service 目录的信息。
- ec2
  - 允许委托人在路由表上创建标签，列出网络接口、路由表、安全组、子网和与 Amazon FSx 文件系统关联的 VPC。
  - 允许主体为可与 VPC 配合使用的所有安全组提供增强的安全组验证。
  - 允许委托人查看与 Amazon FSx 文件系统关联的弹性网络接口。
- kms— 允许委托人列出密钥的别名。 Amazon Key Management Service
- s3：允许主体列出 Amazon S3 桶中的部分或全部对象（最多 1000 个）。

- `secretsmanager`— 允许委托人列出 Amazon Secrets Manager 用于选择域加入服务帐户凭据的密码。
- `iam`— 授予创建服务关联角色的权限，该角色允许 Amazon FSx 代表用户执行操作。

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

Amazon 托管策略：Amazon FSx ConsoleReadOnlyAccess

您可以将 `AmazonFSxConsoleReadOnlyAccess` 策略附加到 IAM 身份。

此政策向 Amazon FSx 和相关 Amazon 服务授予只读权限，以便用户可以在中查看有关这些服务的信息 Amazon Web Services 管理控制台。

权限详细信息

该策略包含以下权限。

- `fsx`— 允许委托人在 Amazon FSx 管理控制台中查看有关亚马逊 FSx 文件系统的信息，包括所有标签。
- `cloudwatch`— 允许委托人在 Amazon FSx 管理控制台中查看 CloudWatch 警报和指标。
- `ds`— 允许委托人在 Amazon FSx 管理控制台中查看有关 Amazon Directory Service 目录的信息。
- `ec2`
  - 允许委托人在 Amazon FSx 管理控制台中查看网络接口、安全组、子网和与 Amazon FSx 文件系统关联的 VPC。
  - 允许主体为可与 VPC 配合使用的所有安全组提供增强的安全组验证。
  - 允许委托人查看与 Amazon FSx 文件系统关联的弹性网络接口。
- `kms`— 允许委托人在 Amazon FSx 管理控制台中查看 Amazon Key Management Service 密钥的别名。
- `log`— 允许委托人描述与提出请求的账户关联的 Amazon Logs CloudWatch 日志组。这是必需的，这样委托人才能查看适用于 Windows 文件服务器的文件系统的现有文件访问审核配置。 FSx
- `secretsmanager`— 允许委托人列出 Amazon Secrets Manager 用于选择域加入服务帐户凭据的密码。
- `firehose`：允许主体描述与发出请求的账户关联的 Amazon Data Firehose 传输流。这是必需的，这样委托人才能查看适用于 Windows 文件服务器的文件系统的现有文件访问审核配置。 FSx

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

Amazon 托管策略：Amazon FSx ReadOnlyAccess

您可以将 AmazonFSxReadOnlyAccess 策略附加到 IAM 身份。

- fsx— 允许委托人在 Amazon FSx 管理控制台中查看有关亚马逊 FSx 文件系统的信息，包括所有标签。
- ec2：为可以与 VPC 配合使用的所有安全组提供增强的安全组验证。

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

亚马逊 FSx 更新了托 Amazon 管政策

查看 FSx 自该服务开始跟踪这些变更以来亚马逊 Amazon 托管政策更新的详细信息。要获取有关此页面变更的自动提醒，请订阅 Amazon FSx 文档历史记录 页面上的 RSS 提要。

更改	描述	日期
亚马逊 FSx ConsoleFullAccess-对现有政策的更新	Amazon FSx 添加了一项新权限secretsmanager:ListSecrets ，允许委托人列出 Amazon Secrets Manager 用于选择域名加入服务账户凭证的密码。	2025 年 11 月 5 日
亚马逊 FSx ConsoleReadOnlyAccess-对现有政策的更新	Amazon FSx 添加了一项新权限secretsmanager:ListSecrets ，允许委托人列出 Amazon Secrets Manager 用于选择域名加入服务账户凭证的密码。	2025 年 11 月 3 日
亚马逊 FSx ServiceRolePolicy-对现有政策的更新	Amazon FSx 添加了一项新权限ec2:AssignIpv6Addresses ，允许委托人为带有AmazonFSx.FileSyst	2025 年 7 月 22 日

更改	描述	日期
	emId 标签的客户网络接口分配 IPv6 地址。	
亚马逊 FSx ServiceRolePolicy-对现有政策的更新	Amazon FSx 添加了一项新权限ec2:UnassignIpv6Addresses ，允许委托人取消分配 IPv6 带有标签的客户网络接口的地址。AmazonFSx.FileSystemId	2025 年 7 月 22 日
亚马逊 FSx ConsoleFullAccess-对现有政策的更新	Amazon FSx 添加了一项新权限fsx:CreateAndAttachS3AccessPoint ，允许委托人创建 S3 接入点并将其连接到 FSx 卷。	2025 年 6 月 25 日
亚马逊 FSx ConsoleFullAccess-对现有政策的更新	Amazon FSx 添加了一项新权限fsx:DescribeS3AccessPointAttachments ，允许委托人列出所有 S3 接 Amazon Web Services 账户入 Amazon Web Services 区域点。	2025 年 6 月 25 日
亚马逊 FSx ConsoleFullAccess-对现有政策的更新	Amazon FSx 添加了一项新权限fsx:DetachAndDeleteS3AccessPoint ，允许委托人删除 S3 接入点。	2025 年 6 月 25 日
亚马逊 FSx FullAccess-对现有政策的更新	Amazon FSx 添加了一项新权限fsx:CreateAndAttachS3AccessPoint ，允许委托人创建 S3 接入点并将其连接到 FSx 卷。	2025 年 6 月 25 日

更改	描述	日期
亚马逊 FSx FullAccess-对现有政策的更新	Amazon FSx 添加了一项新权限`fsx:DescribeS3AccessPointAttachments`，允许委托人列出所有 S3 接入点。	2025 年 6 月 25 日
亚马逊 FSx FullAccess-对现有政策的更新	Amazon FSx 添加了一项新权限`fsx:DetachAndDeleteS3AccessPoint`，允许委托人删除 S3 接入点。	2025 年 6 月 25 日
亚马逊 FSx ConsoleReadOnlyAccess-对现有政策的更新	Amazon FSx 增加了新权限`ec2:DescribeNetworkInterfaces`，允许委托人查看与其文件系统关联的弹性网络接口。	2025 年 2 月 25 日
亚马逊 FSx ConsoleFullAccess-对现有政策的更新	Amazon FSx 增加了新权限`ec2:DescribeNetworkInterfaces`，允许委托人查看与其文件系统关联的弹性网络接口。	2025 年 2 月 7 日
亚马逊 FSx ServiceRolePolicy-对现有政策的更新	Amazon FSx 增加了新权限`ec2:GetSecurityGroupsForVpc`，允许委托人对可用于 VPC 的所有安全组提供增强的安全组验证。	2024 年 1 月 9 日
亚马逊 FSx ReadOnlyAccess-对现有政策的更新	Amazon FSx 增加了新权限`ec2:GetSecurityGroupsForVpc`，允许委托人对可用于 VPC 的所有安全组提供增强的安全组验证。	2024 年 1 月 9 日

更改	描述	日期
亚马逊 FSx ConsoleReadOnlyAccess-对现有政策的更新	Amazon FSx 增加了新权限`ec2:GetSecurityGroupsForVpc`，允许委托人对可用于 VPC 的所有安全组提供增强的安全组验证。	2024 年 1 月 9 日
亚马逊 FSx FullAccess-对现有政策的更新	Amazon FSx 增加了新权限`ec2:GetSecurityGroupsForVpc`，允许委托人对可用于 VPC 的所有安全组提供增强的安全组验证。	2024 年 1 月 9 日
亚马逊 FSx ConsoleFullAccess-对现有政策的更新	Amazon FSx 增加了新权限`ec2:GetSecurityGroupsForVpc`，允许委托人对可用于 VPC 的所有安全组提供增强的安全组验证。	2024 年 1 月 9 日
亚马逊 FSx FullAccess-对现有政策的更新	亚马逊 FSx 增加了新的权限，允许用户对 OpenZFS 文件系统执行跨区域和跨账户数据复制。 FSx	2023 年 12 月 20 日
亚马逊 FSx ConsoleFullAccess-对现有政策的更新	亚马逊 FSx 增加了新的权限，允许用户对 OpenZFS 文件系统执行跨区域和跨账户数据复制。 FSx	2023 年 12 月 20 日
亚马逊 FSx FullAccess-对现有政策的更新	Amazon FSx 增加了新的权限，允许用户按需复制 OpenZFS 文件系统的卷。 FSx	2023 年 11 月 26 日
亚马逊 FSx ConsoleFullAccess-对现有政策的更新	Amazon FSx 增加了新的权限，允许用户按需复制 OpenZFS 文件系统的卷。 FSx	2023 年 11 月 26 日

更改	描述	日期
亚马逊 FSx FullAccess-对现有政策的更新	Amazon FSx 添加了新的权限，使用户能够查看、启用和禁用 ONTAP 多可用区文件 FSx 系统的共享 VPC 支持。	2023 年 11 月 14 日
亚马逊 FSx ConsoleFullAccess-对现有政策的更新	Amazon FSx 添加了新的权限，使用户能够查看、启用和禁用 ONTAP 多可用区文件 FSx 系统的共享 VPC 支持。	2023 年 11 月 14 日
亚马逊 FSx FullAccess-对现有政策的更新	亚马逊 FSx 增加了新的权限，FSx 允许亚马逊管理 OpenZFS 多可用区文件系统的网络配置。 FSx	2023 年 8 月 9 日
Amazon 托管策略：Amazon FSx ServiceRolePolicy — 更新现有政策	亚马逊 FSx 修改了现有`cloudwatch:PutMetricData` 权限，以便亚马逊将 CloudWatch 指标 FSx 发布到`Amazon/FSx` 命名空间。	2023 年 7 月 24 日
亚马逊 FSx FullAccess-对现有政策的更新	Amazon FSx 更新了政策，删除了`fsx:*`权限并添加了具体`fsx`操作。	2023 年 7 月 13 日
亚马逊 FSx ConsoleFullAccess-对现有政策的更新	Amazon FSx 更新了政策，删除了`fsx:*`权限并添加了具体`fsx`操作。	2023 年 7 月 13 日
亚马逊 FSx ConsoleReadOnlyAccess-对现有政策的更新	亚马逊 FSx 增加了新的权限，使用户能够在亚马逊 FSx 控制台中查看 Windows 文件服务器文件系统的增强性能指标和建议的操作。 FSx	2022 年 9 月 21 日

更改	描述	日期
亚马逊 FSx ConsoleFullAccess-对现有政策的更新	亚马逊 FSx 增加了新的权限，使用户能够在亚马逊 FSx 控制台中查看 Windows 文件服务器文件系统的增强性能指标和建议的操作。 FSx	2022 年 9 月 21 日
亚马逊 FSx ReadOnlyAccess-已开始追踪政策	该政策授予对所有 Amazon FSx 资源以及与之关联的任何标签的只读访问权限。	2022 年 2 月 4 日
亚马逊 FSx DeleteServiceLinkedRoleAccess-已开始追踪政策	此策略授予管理权限， FSx 允许亚马逊删除其对 Amazon S3 访问权限的服务关联角色。	2022 年 1 月 7 日
亚马逊 FSx ServiceRolePolicy-对现有政策的更新	亚马逊 FSx 增加了新的权限， FSx 允许亚马逊管理适用 FSx 于 NetApp ONTAP 文件系统的亚马逊网络配置。	2021 年 9 月 2 日
亚马逊 FSx FullAccess-对现有政策的更新	亚马逊 FSx 添加了新的权限， FSx 允许亚马逊在 EC2 路由表上为限定范围的呼叫创建标签。	2021 年 9 月 2 日
亚马逊 FSx ConsoleFullAccess-对现有政策的更新	亚马逊 FSx 添加了新的权限， FSx 允许亚马逊为 NetApp ONTAP 多可用区文件系统创建亚马逊 FSx 。	2021 年 9 月 2 日
亚马逊 FSx ConsoleFullAccess-对现有政策的更新	亚马逊 FSx 添加了新的权限， FSx 允许亚马逊在 EC2 路由表上为限定范围的呼叫创建标签。	2021 年 9 月 2 日

更改	描述	日期
亚马逊 FSx ServiceRolePolicy-对现有政策的更新	亚马逊 FSx 增加了新的权限，FSx 允许亚马逊描述和写入 CloudWatch 日志流。 这是必需的，这样用户才能使用日志查看 Windows 文件服务器文件系统的文件访问审核 CloudWatch 日志。 FSx	2021 年 6 月 8 日
亚马逊 FSx ServiceRolePolicy-对现有政策的更新	亚马逊 FSx 增加了新的权限，允许亚马逊描述和写 FSx 入亚马逊 Data Firehose 传送流。 这是必需的，这样用户才能使用 Amazon Data Firehose 查看 FSx 适用于 Windows 文件服务器的文件系统的文件访问审核日志。	2021 年 6 月 8 日
亚马逊 FSx FullAccess-对现有政策的更新	Amazon FSx 增加了新的权限，允许委托人描述和创建 CloudWatch 日志组、日志流以及将事件写入日志流。 这是必需的，这样委托人才能使用日志查看 Windows 文件服务器文件系统的文件访问审核 CloudWatch 日志。 FSx	2021 年 6 月 8 日

更改	描述	日期
亚马逊 FSx FullAccess-对现有政策的更新	亚马逊 FSx 增加了新的权限，允许委托人向亚马逊数据 Firehose 描述和写入记录。 这是必需的，这样用户才能使用 Amazon Data Firehose 查看 FSx 适用于 Windows 文件服务器的文件系统的文件访问审核日志。	2021 年 6 月 8 日
亚马逊 FSx ConsoleFullAccess-对现有政策的更新	Amazon FSx 增加了新的权限，允许委托人描述与提出请求的账户关联的 Amazon Logs CloudWatch 日志组。 这是必需的，这样委托人才能在为 Windows 文件服务器文件系统配置文件访问审计时选择现有的 CloudWatch 日志日志组。 FSx	2021 年 6 月 8 日
亚马逊 FSx ConsoleFullAccess-对现有政策的更新	亚马逊 FSx 增加了新的权限，允许委托人描述与提出请求的账户关联的 Amazon Data Firehose 传输流。 这是必需的，这样委托人才能在为 Windows 文件服务器文件系统配置文件访问审计时选择现有的 Fire FSx hose 传送流。	2021 年 6 月 8 日

更改	描述	日期
亚马逊 FSx ConsoleReadOnlyAccess-对现有政策的更新	Amazon FSx 增加了新的权限，允许委托人描述与提出请求的账户关联的 Amazon Logs CloudWatch 日志组。 这是必需的，这样委托人才能查看适用于 Windows 文件服务器的文件系统的现有文件访问审核配置。 FSx	2021 年 6 月 8 日
亚马逊 FSx ConsoleReadOnlyAccess-对现有政策的更新	亚马逊 FSx 增加了新的权限，允许委托人描述与提出请求的账户关联的 Amazon Data Firehose 传输流。 这是必需的，这样委托人才能查看适用于 Windows 文件服务器的文件系统的现有文件访问审核配置。 FSx	2021 年 6 月 8 日
亚马逊 FSx 开始追踪变更	Amazon FSx 开始跟踪其 Amazon 托管政策的变更。	2021 年 6 月 8 日

对适用 FSx 于 Windows 的 Amazon 文件服务器身份和访问权限进行故障排除

使用以下信息来帮助您诊断和修复在使用 Windows 文件服务器和 IAM 时可能遇到 FSx 的常见问题。

主题

- 我无权在以下位置执行操作 FSx
- 我无权执行 iam：PassRole
- 我想允许我以外的人 Amazon Web Services 账户 访问我的 FSx 资源

我无权在以下位置执行操作 FSx

如果您收到错误提示，指明您无权执行某个操作，则必须更新策略以允许执行该操作。

当 mateojackson IAM 用户尝试使用控制台查看有关虚构 *my-example-widget* 资源的详细信息，但不拥有虚构 fsx:*GetWidget* 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 fsx:GetWidget on resource: my-example-widget
```

在此情况下，必须更新 mateojackson 用户的策略，以允许使用 fsx:*GetWidget* 操作访问 *my-example-widget* 资源。

如果您需要帮助，请联系您的 Amazon 管理员。您的管理员是提供登录凭证的人。

我无权执行 iam：PassRole

如果您收到一条错误消息，提示您无权执行该iam:PassRole操作，则必须更新您的策略以允许您将角色传递给 Windows File Server。 FSx

有些 Amazon Web Services 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为的 IAM 用户marymajor尝试使用控制台在 Windows 文件服务器中 FSx 执行操作时，会出现以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 iam:PassRole 操作。

如果您需要帮助，请联系您的 Amazon 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人 Amazon Web Services 账户 访问我的 FSx 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以代入角色。对于支持基于资源的策略或访问控制列表 (ACLs) 的服务，您可以使用这些策略向人们授予访问您的资源的权限。

要了解更多信息，请参阅以下内容：

- 要了解 Window FSx s 文件服务器是否支持这些功能，请参阅 FSx 适用于 Windows 的 Amazon 文件服务器如何与 IAM 配合使用。
- 要了解如何提供对您拥有的资源的访问权限 Amazon Web Services 账户 ，请参阅 IAM 用户指南中的向您拥有 Amazon Web Services 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 Amazon Web Services 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 Amazon Web Services 账户
- 要了解如何通过身份联合验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（身份联合验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

在 Amazon 上使用标签 FSx

您可以使用标签来控制对 Amazon FSx 资源的访问权限并实现基于属性的访问控制 (ABAC)。用户需要有权在创建期间对 Amazon FSx 资源应用标签。

在创建过程中授予标记资源的权限

一些 FSx 为 Windows 文件服务器创建资源的 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权限控制（ABAC）。有关更多信息，请参阅《IAM 用户指南》中的什么是适用于 Amazon的 ABAC？。

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。

以下示例演示了一个策略，该策略允许用户在特定文件系统中创建文件系统并在创建文件系统时将标签应用于文件系统 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，并在创建备份的过程中向备份应用任何标签。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateBackup"
      ],
      "Resource": "arn:aws:fsx:region:account-id:file-system/file-system-id*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:region:account-id:backup/*"
    }
  ]
}
```

仅当用户在资源创建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。

有关为 Amazon FSx 资源添加标签的更多信息，请参阅为 Amazon FSx 资源贴标签。有关使用标签控制 FSx 资源访问权限的更多信息，请参阅使用标签控制对您的 Amazon FSx 资源的访问权限。

使用标签控制对您的 Amazon FSx 资源的访问权限

要控制对 Amazon FSx 资源和操作的访问权限，您可以使用基于标签的 Amazon Identity and Access Management (IAM) 策略。您可以使用两种方法提供控制：

1. 根据这些 FSx 资源上的标签控制对 Amazon 资源的访问权限。

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 Amazon 资源访问的信息，请参阅 IAM 用户指南中的使用标签控制访问权限。有关在创建 Amazon FSx 资源时标记 Amazon 资源的更多信息，请参阅在创建过程中授予标记资源的权限。有关标记资源的更多信息，请参阅为 Amazon FSx 资源贴标签。

根据资源上的标签控制访问权限

要控制用户或角色可以对 Amazon FSx 资源执行的操作，您可以在资源上使用标签。例如，您可能希望根据文件系统资源上的标签的键/值对允许或拒绝对该资源执行特定的 API 操作。

Example 策略 – 提供特定标签时在其上创建文件系统

只有当用户使用特定标签键值对标记文件系统时，此策略才允许用户创建文件系统，在本示例中为 `key=Department, value=Finance`。

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

Example 策略 — 仅创建带有特定标签的 Amazon FSx 文件系统的备份

此策略允许用户仅在标有键值对 `key=Department, value=Finance` 的文件系统上创建备份，并且将使用该 `Deparment=Finance` 标签创建备份。

JSON

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

```
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource",
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example 策略 – 通过带有特定标签的备份创建带有特定标签的文件系统

此策略允许用户仅通过带有 Department=Finance 标签的备份创建带有 Department=Finance 标签的文件系统。

JSON

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

```
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateFileSystemFromBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example 策略 – 删除带有特定标签的文件系统

此策略允许用户删除带有 Department=Finance 标签的文件系统。如果他们创建了最终备份，则必须使用 Department=Finance 标记。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteFileSystem"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:file-system/*",
            "Condition": {
                "StringEquals": {
```

```
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

使用适用于 Windows 文件服务器 FSx 的服务相关角色

FSx 适用于 Windows 的 Amazon 文件服务器使用 Amazon Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种独特的 IAM 角色类型，直接链接到 Window FSx s 文件服务器。服务相关角色由 FSx Windows File Server 预定义，包括该服务代表你调用其他 Amazon 服务所需的所有权限。

服务相关角色可以更轻松地设置 FSx Windows 文件服务器，因为您不必手动添加必要的权限。 FSx 对于 Windows 文件服务器定义其服务相关角色的权限，除非另行定义，否则只有 FSx Windows 文件服务器可以担任其角色。定义的权限包括信任策略和权限策略，以及不能附加到任何其他 IAM 实体的权限策略。

只有在首先删除相关资源后，您才能删除服务关联角色。这可以保护你 FSx 的 Windows 文件服务器资源，因为你不能无意中删除访问这些资源的权限。

有关支持服务相关角色的其他服务的信息，请参阅使用 IAM 的Amazon 服务并查找服务相关角色列中显示为是的服务。选择是和链接，查看该服务的服务关联角色文档。

Windows 文件服务器 FSx 的服务相关角色权限

FSx 适用于 Windows File Server 使用名为 `AWSServiceRoleForAmazonFSx` — 的服务相关角色在您的账户中执行某些操作，例如在 VPC 中为文件系统创建弹性网络接口。

角色权限策略允许 FSx Windows 文件服务器对所有适用 Amazon 资源完成以下操作：

您不能将 Amazon 附加FSxServiceRolePolicy 到您的 IAM 实体。此策略附加到服务相关角色， FSx 允许您代表您管理 Amazon 资源。有关更多信息，请参阅 使用适用于 Windows 文件服务器 FSx 的服务相关角色。

有关此策略的更新，请参阅 Amazon FSx ServiceRolePolicy。

此策略授予管理权限， FSx 允许代表用户管理 Amazon 资源。

权限详细信息

亚马逊FSxServiceRolePolicy 角色权限由亚马逊FSxServiceRolePolicy Amazon 托管策略定义。Amazon FSx ServiceRolePolicy 拥有以下权限：

> **Note**
>
> 所有亚马逊 FSx 文件系统类型FSxServiceRolePolicy 都使用亚马逊；列出的某些权限可能不适用 FSx 于 Windows。

- ds— FSx 允许查看、授权和取消对 Amazon Directory Service 目录中的应用程序的授权。
- ec2— FSx 允许执行以下操作：
  - 查看、创建和取消关联与 Amazon FSx 文件系统关联的网络接口。
  - 查看与 Amazon FSx 文件系统关联的一个或多个弹性 IP 地址。
  - 查看与亚马逊 FSx 文件系统关联的亚马逊 VPCs、安全组和子网。
  - 为带有`AmazonFSx.FileSystemId`标签的客户网络接口分配 IPv6 地址。
  - 取消分配 IPv6 带有`AmazonFSx.FileSystemId`标签的客户网络接口的地址。
  - 为可以与 VPC 配合使用的所有安全组提供增强的安全组验证。
  - 为获得 Amazon授权的用户创建在网络接口上执行某些操作的权限。
- `cloudwatch`— FSx 允许将指标数据点发布到 Amazon/FSx 命名空间 CloudWatch 下。
- `route53`— 允许 FSx 将 Amazon VPC 与私有托管区域关联。
- `logs`— FSx 允许描述和写入 CloudWatch 日志日志流。这样，用户就可以将 Windows 文件服务器文件系统的文件访问审核日志发送到 CloudWatch 日志流。 FSx
- `firehose`— FSx 允许描述和写入 Amazon Data Firehose 的传输流。这样，用户就可以将适用于 Windows 文件服务器的文件系统的文件访问审核日志发布到 Amazon Data Firehose 传输流。 FSx

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CreateFileSystem",
            "Effect": "Allow",
            "Action": [
                "ds:AuthorizeApplication",
                "ds:GetAuthorizedApplicationDetails",
                "ds:UnauthorizeApplication",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeAddresses",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVPCs",
                "ec2:DisassociateAddress",
                "ec2:GetSecurityGroupsForVpc",
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PutMetrics",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/FSx"
                }
            }
        },
```

```
        {
            "Sid": "TagResourceNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "AmazonFSx.FileSystemId"
                }
            }
        },
        {
            "Sid": "ManageNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonFSx.FileSystemId": "false"
                }
            }
        },
        {
            "Sid": "ManageRouteTable",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateRoute",
                "ec2:ReplaceRoute",
                "ec2:DeleteRoute"
            ],
```

```
            "Resource": [
                "arn:aws:ec2:*:*:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/AmazonFSx": "ManagedByAmazonFSx"
                }
            }
        },
        {
            "Sid": "PutCloudWatchLogs",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/fsx/*"
        },
        {
            "Sid": "ManageAuditLogs",
            "Effect": "Allow",
            "Action": [
                "firehose:DescribeDeliveryStream",
                "firehose:PutRecord",
                "firehose:PutRecordBatch"
            ],
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
        }
    ]
}
```

亚马逊 FSx 更新了托 Amazon 管政策 中介绍了本政策的所有更新。

您必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务关联角色。有关更多信息，请参阅《IAM 用户指南》中的服务关联角色权限。

为 Windows 文件服务器创建服务相关角色 FSx

您无需手动创建服务关联角色。当你在中创建文件系统时 Amazon Web Services 管理控制台，FSx 适用于 Windows 文件服务器的 IAM CLI 或 IAM API 会为你创建服务相关角色。

> **Important**
>
> 如果您在其他使用此角色支持的功能的服务中完成某个操作，此服务关联角色可以出现在您的账户中。要了解更多信息，请参阅我的 IAM 账户中的新角色。

如果您删除该服务关联角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。创建文件系统时， FSx Windows 文件服务器会再次为您创建服务相关角色。

编辑 Windows 文件服务器 FSx 的服务相关角色

FSx Windows 文件服务器不允许您编辑服务相关角色。创建服务关联角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。但是可以使用 IAM 编辑角色描述。有关更多信息，请参阅《IAM 用户指南》中的编辑服务关联角色。

删除 Windows 文件服务器 FSx 的服务相关角色

如果不再需要使用某个需要服务关联角色的功能或服务，我们建议您删除该角色。这样就没有未被主动监控或维护的未使用实体。但是，您必须先删除所有文件系统和备份，然后才能手动删除服务关联角色。

> **Note**
>
> 如果您尝试删除资源时， FSx 适用于 Windows 的文件服务器的服务正在使用该角色，则删除可能会失败。如果发生这种情况，请等待几分钟后重试。

使用 IAM 手动删除服务关联角色

使用 IAM 控制台、IAM CLI 或 IAM API 删除服务关联角色。有关更多信息，请参阅《IAM 用户指南》中的删除服务关联角色。

Windows 文件服务器服务相关角色支持的区域 FSx

FSx Windows File Server 支持在提供服务的所有区域中使用服务相关角色。有关更多信息，请参阅 Amazon 区域和端点。

适用于 Windows File Server 的 Amazon FSx 合规性验证

要了解某个 Amazon Web Services 服务是否在特定合规性计划范围内，请参阅合规性计划范围内的 Amazon Web Services 服务，然后选择您感兴趣的合规性计划。有关常规信息，请参阅 、、Amazon Web Services 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、在 Amazon Artifact 中下载报告。

您在使用 Amazon Web Services 服务 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。有关您在使用 Amazon Web Services 服务时的合规责任的更多信息，请参阅 Amazon 安全性文档。

适用于 Windows File Server 的 Amazon FSx 和接口 VPC 端点

您可以将 Amazon FSx 配置为使用接口 VPC 端点以改善 VPC 的安全状况。接口 VPC 端点由 Amazon PrivateLink 提供支持，该技术支持您通过私密方式访问 Amazon FSx API，而无需采用互联网网关、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 端点均由子网中的一个或多个弹性网络接口表示。网络接口提供一个私有 IP 地址，此地址可用作指向 Amazon FSx API 的流量的入口点。Amazon FSx 支持使用仅 IPv4 和双堆栈（IPv4 和 IPv6）IP 地址类型配置的 VPC 端点。有关更多信息，请参阅《Amazon VPC 用户指南》中的创建接口 VPC 端点。

Amazon FSx 接口 VPC 端点注意事项

请务必先查看《Amazon VPC 用户指南》中的接口 VPC 端点属性和限制，然后再为 Amazon FSx 设置接口 VPC 端点。

您可以从 VPC 调用任何 Amazon FSx API 操作。例如，您可以通过从 VPC 中调用 CreateFileSystem API 来创建 FSx for Windows File Server 文件系统。有关 Amazon FSx API 的完整列表，请参阅 Amazon FSx API 参考中的操作。

VPC 对等连接注意事项

可通过 VPC 对等连接，将其他 VPC 连接到有接口 VPC 端点的 VPC。VPC 对等连接是两个 VPC 之间的网络连接。您可以在自己的两个 VPC 之间建立 VPC 对等连接，或者与其他 Amazon Web

Services 账户 中的 VPC 之间建立此连接。VPC 也可以位于两个不同的 Amazon Web Services 区域中。

对等 VPC 之间的流量保留在 Amazon 网络上，不会穿越公共互联网。建立对等 VPC 连接后，两个 VPC 中的资源，如 Amazon Elastic Compute Cloud（Amazon EC2）实例，可以通过在其中一个 VPC 中创建的接口 VPC 端点访问 Amazon FSx API。

为 Amazon FSx API 创建接口 VPC 端点

您可以使用 Amazon VPC 控制台或 Amazon Command Line Interface（Amazon CLI）为 Amazon FSx API 创建 VPC 端点。有关更多信息，请参阅《Amazon VPC 用户指南》中的创建接口 VPC 端点。

要为 Amazon FSx 创建接口 VPC 端点，请执行以下操作之一：

- **com.amazonaws.*region*.fsx** – 为 Amazon FSx API 操作创建端点。
- **com.amazonaws.*region*.fsx-fips** – 为 Amazon FSx API 创建符合美国联邦信息处理标准（FIPS）140-2 的端点。

要使用私有 DNS 选项，您必须设置 VPC 的 `enableDnsHostnames` 和 `enableDnsSupport` 属性。有关更多信息，请参阅《Amazon VPC 用户指南》中的查看和更新 VPC 的 DNS 支持。

除中国的 Amazon Web Services 区域 外，如果您为端点启用私有 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`），从而通过 VPC 端点向 Amazon FSx 发出 API 请求。对于中国（北京）和中国（宁夏）Amazon Web Services 区域，您可以通过 VPC 端点分别使用 `fsx-api.cn-north-1.amazonaws.com.cn` 和 `fsx-api.cn-northwest-1.amazonaws.com.cn` 发出 API 请求。

有关更多信息，请参阅《Amazon VPC 用户指南》中的通过接口 VPC 端点访问服务。

为 Amazon FSx 创建 VPC 端点策略

要进一步控制对 Amazon FSx API 的访问，您可以选择向 VPC 端点附加 Amazon Identity and Access Management（IAM）policy。此策略指定以下内容：

- 可执行操作的主体。
- 可执行的操作。
- 可对其执行操作的资源。

有关更多信息，请参阅《Amazon VPC 用户指南》中的使用 VPC 端点控制对服务的访问。

使用其他服务

除了 Amazon 之外 CloudWatch Amazon Identity and Access Management Amazon CloudTrail， FSx 适用于 Windows 文件服务器的 Amazon DataSync、和，还集成了以下功能 Amazon Web Services 服务：

- Amazon A WorkSpaces WorkSpaces pplications — Applications — Applications 是一项完全托管的应用程序流服务，用户可以随时随地即时访问其桌面应用程序 WorkSpaces 应用程序管理托管和运行应用程序所需的 Amazon 资源，自动扩展，并按需向用户提供访问权限。了解如何使用 WorkSpaces 应用程序为个人用户创建永久存储，以及如何在 Windows File Server 文件系统上 FSx 为多个用户共享存储。有关更多信息，请参阅 将亚马逊 FSx 与亚马逊 WorkSpaces 应用程序配合使用。
- Amazon Kendra - Amazon Kendra 是一项智能搜索服务，它使用自然语言处理和高级机器学习算法，从您的数据中返回搜索问题的特定答案。借助 Amazon Kendra，您可以通过将多个数据存储库连接到索引，以及提取和爬取文档来创建统一的搜索体验。有关将 Amazon Kendra 与 Windows 文件服务器配合使用的 FSx 更多信息，请参阅。 FSx 用于搭载 Amazon Kendra 的 Windows 文件服务器

主题

将亚马逊 FSx 与亚马逊 WorkSpaces 应用程序配合使用

通过支持服务器消息块 (SMB) 协议，Amazon FSx for Windows 文件服务器支持从亚马逊 EC2、VMware Cloud on、Amazon Amazon和亚马逊 WorkSpaces WorkSpaces 应用程序实例访问您的文件系统。 WorkSpaces 应用程序是一项完全托管的应用程序流媒体服务。您可以在 “应用程序” 上集中管理桌面 WorkSpaces 应用程序，并将它们安全地传送到任何计算机上的浏览器。有关 WorkSpaces 应用程序的更多信息，请参阅《Amazon WorkSpaces 应用程序管理指南》。有关如何简化亚马逊 WorkSpaces 应用程序映像和队列管理的说明，请参阅 Amazon 博客文章自动创建自定义 AppStream 2.0 Windows 映像。

以下过程向您展示如何使用 Amazon FSx with A WorkSpaces pplications 为每位用户提供个人永久存储空间，以及如何提供共享文件夹，以便多个用户可以访问公共文件。

为每位用户提供个人永久存储

您可以使用 Amazon FSx 在 WorkSpaces 应用程序流式传输会话中为组织中的每位用户提供一个独特的存储驱动器。用户将仅有权访问其文件夹。驱动器会在流会话开始时自动装载，并且在流会话之间自动保留在驱动器中添加或更新的文件。

要完成此任务，您需要执行三个过程。

使用 Amazon 为域用户创建主文件夹 FSx

1. 创建 Amazon FSx 文件系统。有关更多信息，请参阅 开始使用 FSx 适用于 Windows 文件服务器的亚马逊。
2. 文件系统可用后，在您的 Amazon 文件系统中为每个域 WorkSpaces 应用程序用户创建一个 FSx 文件夹。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 `%username%` 来轻松生成文件共享的 UNC 名称以进行映射。
3. 将这些文件夹都共享为共享文件夹。有关更多信息，请参阅 创建、更新、删除文件共享。

启动已加入域的应用程序映像生成器 WorkSpaces

1. 登录 WorkSpaces 应用程序控制台：https://console.aws.amazon.com/appstream2
2. 从导航菜单中选择目录配置然后创建一个目录配置对象。有关更多信息，请参阅《亚马逊应用程序管理指南》中的将 Active Directory 与 WorkSpaces WorkSpaces 应用程序配合使用。
3. 选择图像、映像生成器，然后启动新的图像生成器。
4. 选择之前在映像生成器启动向导中创建的目录配置对象，将映像生成器加入 Active Directory 域。
5. 在与您的 Amazon FSx 文件系统相同的 VPC 中启动映像生成器。请务必将映像生成器与您的 Amazon FSx 文件系统加入的同一 Amazon Managed Microsoft AD 目录相关联。您与映像生成器关联的 VPC 安全组必须允许访问您的 Amazon FSx 文件系统。
6. 映像生成器可用后，请连接到映像生成器并使用您的域管理员账户登录。
7. 安装应用程序。

将 Amazon FSx 文件共享与 WorkSpaces 应用程序关联

1. 在映像生成器中，使用以下命令创建批处理脚本并将其存储在已知的文件位置（例如：C:\Scripts\map-fs.bat）。以下示例使用 S: 作为驱动器号来映射您的 Amazon FSx 文件系统上的共享文件夹。在此脚本中，您可以使用 Amazon FSx 文件系统的 DNS 名称或与文件系统关联的 DNS 别名，您可以从亚马逊 FSx 控制台的文件系统详细信息视图中获取该别名。

使用文件系统的 DNS 名称时：

```
@echo off
net use S: /delete
net use S: \\file-system-DNS-name\users\%username%
```

使用与文件系统关联的 DNS 别名时：

```
@echo off
net use S: /delete
net use S: \\fqdn-DNS-alias\users\%username%
```

2. 打开 PowerShell 提示符并运行`gpedit.msc`。
3. 在用户配置中选择 Windows 设置，然后选择登录。
4. 导航到您在此过程的第一步中创建的批处理脚本，然后选中此脚本。
5. 在计算机配置下，依次选择 Windows 管理模板、系统，然后选择组策略。
6. 选择策略配置登录脚本延迟。启用该策略并将延迟时间缩短至 0。此设置有助于确保在用户启动流会话时立即执行用户登录脚本。
7. 创建您的映像并将其分配给 WorkSpaces 应用程序队列。确保您也将 WorkSpaces 应用程序队列加入到用于映像生成器的同一 Active Directory 域中。在您的 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 安全组必须提供对您的 Amazon FSx 文件系统的访问权限。
8. 使用 SAML SSO 启动流会话。要连接到已加入 Active Directory 的实例集，请使用 SAML 提供商来配置单点登录联合身份验证。有关更多信息，请参阅《亚马逊 WorkSpaces 应用程序管理指南》中的 “使用 SAML 2.0 单点登录访问 2.0”。 AppStream
9. 在直播会话中，您的 Amazon FSx 文件共享将映射到 S: 驱动器号。

提供用户间提供共享文件夹

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通用文件（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 创建共享文件夹 FSx

1. 创建 Amazon FSx 文件系统。有关更多信息，请参阅 开始使用 FSx 适用于 Windows 文件服务器的亚马逊。
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*file-system-DNS-name*\ share 访问该文件夹，如果您使用的是 DNS 别名，则可以使用*fqdn-DNS-alias*\\\ share 地址访问该文件夹。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 创建、更新、删除文件共享。

启动 WorkSpaces 应用程序映像生成器

1. 在 WorkSpaces 应用程序控制台中，启动新的映像生成器或连接到现有的映像生成器。在您的 Amazon FSx 文件系统使用的同一 VPC 中启动映像生成器。您与映像生成器关联的 VPC 安全组必须允许访问您的 Amazon FSx 文件系统。
2. 映像生成器可用后，请以“管理员”用户身份连接到映像生成器。
3. 以“管理员”身份安装或更新应用程序。

将共享文件夹与 WorkSpaces 应用程序链接

1. 按照前面的步骤说明创建批处理脚本，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 控制台中的文件系统详情视图中获取），以及访问共享文件夹的凭证。

   使用文件系统的 DNS 名称时：

   ```
   @echo off
   net use S: /delete
   net use S: \\file-system-DNS-name\share /user:username password
   ```

   使用与文件系统关联的 DNS 别名时：

   ```
   @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。您可以按照上一节中介绍的相同说明操作。

3. 创建您的映像并将其分配给实例集。
4. 启动流会话。现在，您应该会看到共享文件夹已自动映射到驱动器盘符。

FSx 用于搭载 Amazon Kendra 的 Windows 文件服务器

Amazon Kendra 是一项高度准确和智能的搜索服务。 FSx 适用于 Windows 文件服务器的文件系统可用作 Amazon Kendra 的数据源，允许您对存储在文件系统中的文档中包含的信息进行索引和智能搜索。

- 有关 Amazon Kendra 的更多信息，请参阅《Amazon Kendra 开发人员指南》https://docs.amazonaws.cn/kendra/latest/dg/what-is-kendra.html中的什么是 Amazon Kendra。
- 有关如何将您的文件系统添加为 Amazon Kendra 数据源的更多信息，请参阅 Amazon K endra 开发者指南中的亚马逊 FSx 数据源（控制台）入门。
- 关于 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 Machine Learning 博客上的 Machine Learning Blog 上使用适用于 FSx 亚马逊 Windows 文件服务器的 Amazon Kendra 连接器安全搜索 Windows 文件系统上的非结构化数据。Amazon

文件系统性能

当您添加 FSx 适用于 Windows 文件服务器的文件系统作为数据源时，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。）此类发自 Amazon Kendra 的文件访问活动会消耗文件系统资源，与使用您自己的工作负载访问文件系统的活动类似。

确保已为您的文件系统配置了足够的资源，这样您的工作负载性能就不会受到影响。具体而言，如果您计划索引大量文件，我们建议使用具有 SSD 存储类型的文件系统，这样可以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。

限额

接下来，您将了解使用适用于 Windows File Server 的 Amazon FSx 时的限额。

主题

您可以增加的限额

以下是您可以提高的每个 Amazon Web Services 账户、每个 Amazon Web Services 区域 的适用于 Windows File Server 的 Amazon FSx 的配额。

资源	默认值	描述
Windows 文件系统	100	您可以在此账户中创建的最大 Amazon FSx for Windows Server 文件系统数量。
Windows 吞吐能力	10240	此账户中所有 Amazon FSx for Windows 文件系统允许的吞吐能力总量（以 MBps 计）。
Windows HDD 存储容量	524288	此账户中所有适用于 Windows File Server 的 Amazon FSx 文件系统允许的最大 HDD 存储容量（以 GiB 计）。
Windows SSD 存储容量	524288	此账户中所有适用于 Windows File Server 的 Amazon FSx 文件系统允许的最大 SSD 存储容量（以 GiB 计）。

资源	默认值	描述
Windows 的 SSD IOPS 总量	500,000	此账户中所有适用于 Windows File Server 的 Amazon FSx 文件系统允许的 SSD IOPS 总量。
Windows 备份	500	您可以在此账户中拥有的所有适用于 Windows File Server 的 Amazon FSx 文件系统的最大用户启动备份数量。

要请求提高限额

1. 打开 Amazon Support 中心页面，登录（如有必要），然后选择创建案例。
2. 在创建案例中选择账户和账单支持。
3. 在案例详细信息面板中输入以下条目：
   - 对于类型，选择账户。
   - 对于类别，选择其他账户问题。
   - 对于主题，请输入 **`FSx for Windows File Server service limit increase request`**。
   - 提供您申请的详细描述，包括：
     - 您想要增加的 FSx 限额以及您希望增加到的值（如果已知）。
     - 您申请增加限额的原因。
     - 您申请增加限额的每个文件系统的文件系统 ID 和区域。
4. 提供您的首选联系选项，然后选择提交。

每个文件系统的资源限额

以下是同一 Amazon Web Services 区域 中的适用于 Windows File Server 的 Amazon FSx 上每个文件系统的资源限额。

资源	每个文件系统的限额
最大标签数	50
自动备份的最长保留期	90 天
每个账户可向单个目标区域提出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）	2,000 GiB
最大存储容量，SSD 和 HDD	64 TiB
最小 SSD IOPS	96
最大 SSD IOPS	400,000
最低吞吐能力	8 MBps
最大吞吐能力	12,288 MBps
最大文件共享数	100000

其他注意事项

此外，请注意以下情况：

- 每个 Amazon Key Management Service（Amazon KMS）密钥最多可以用于 125 个 Amazon FSx 文件系统。
- 有关可以创建文件系统的 Amazon Web Services 区域 中位置的列表，请参阅《Amazon Web Services 一般参考》中的 Amazon FSx 端点和限额。
- 您可以使用文件共享的域名服务（DNS）名称将文件共享从 Amazon EC2 实例映射到虚拟私有云（VPC）。

Microsoft Windows 的特有限额

有关更多信息，请参阅 Microsoft Windows 开发人员中心的 NTFS 限额。

对亚马逊进行故障排除 FSx

使用以下部分来帮助解决您在使用Amazon时遇到的问题 FSx。

如果您在使用亚马逊时遇到以下未列出的问题 FSx，请尝试在亚马逊 FSx 论坛中提问。

主题

您无法访问您的文件系统

导致无法访问您的文件系统的潜在原因有很多，每种原因都有自己的解决方案，如下所示。

主题

文件系统弹性网络接口已修改或删除

您不得修改或删除文件系统的弹性网络接口。修改或删除该网络接口可能会导致永久丢失您的 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 e FSx lastic 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。

连接到文件系统弹性网络接口的弹性 IP 地址已删除

Amazon FSx 不支持从公共互联网访问文件系统。Amazon FSx 会自动分离附加到文件系统弹性网络接口的任何弹性 IP 地址，即可从互联网访问的公有 IP 地址。有关更多信息，请参阅 访问您的数据。

文件系统安全组缺少所需的入站或出站规则。

查看 Amazon VPC 安全组 中指定的入站规则，并确保文件系统的关联安全组具有相应的入站规则。

计算实例的安全组缺少所需的出站规则

查看 Amazon VPC 安全组 中指定的出站规则，并确保计算实例的关联安全组具有相应的出站规则。

计算实例未加入 Active Directory

您的计算实例可能无法正确加入以下两种类型的 Active Directory：

- 您的文件系统所连接的 Amazon Managed Microsoft AD 目录。
- 与 Amazon Managed Microsoft AD 目录建立了单向林信任关系的 Microsoft Active Directory 目录。

确保您的计算实例已加入两种类型的目录之一。一种类型是您的文件系统所连接的 Amazon Managed Microsoft AD 目录。另一种类型是 Microsoft Active Directory 目录，该目录与该 Amazon Managed Microsoft AD 目录建立了单向林信任关系。有关更多信息，请参阅 将 Amazon FSx 与 Amazon Directory Service for Microsoft Active Directory 结合使用。

文件共享不存在

您尝试访问的 Microsoft Windows 文件共享不存在。

如果您使用的是现有文件共享，请务必正确指定文件系统 DNS 名称和共享名称。要管理您的文件共享，请参阅创建、更新、删除文件共享。

Active Directory 用户缺少所需权限

您访问文件共享的 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 (ACLs) 允许需要访问该文件夹的 Active Directory 用户进行访问。

移除了允许完全控制 NTFS ACL 权限

如果您移除 SYSTEM 用户对您共享的文件夹的允许完全控制 NTFS ACL 权限，则该共享可能无法访问，并且从那时起进行的任何文件系统备份都可能无法使用。

您将需要重新创建受影响的文件共享。有关更多信息，请参阅 创建、更新、删除文件共享。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

您使用 Amazon Direct Connect 或 VPN 在本地使用您的 Amazon FSx 文件系统，而本地客户端使用的是非私有 IP 地址范围。

Amazon FSx 仅支持使用非私有 IP 地址的本地客户端访问 2020 年 12 月 17 日之后创建的文件系统。

如果您需要使用非私有 IP 地址范围访问 2020 年 12 月 17 日之前创建的 Windows File Server 文件系统，则可以通过恢复文件系统的备份来创建新的文件系统。 FSx 有关更多信息，请参阅 使用备份保护您的数据。。

新文件系统未在 DNS 中注册

对于加入自我管理的 Active Directory 的文件系统，亚马逊在创建文件系统 DNS 时并 FSx 未对其进行注册，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，则亚马逊 FSx 不会在 DNS 中注册文件系统。您必须为您的 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，则需要添加两个 DNS A 条目。按照以下过程获取文件系统 IP 地址或在手动添加 DNS A 条目时要使用的地址。

1. 在中 https://console.aws.amazon.com/fsx/，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. 在网络与安全选项卡中，执行以下任一操作：

- 对于单可用区 1 文件系统：
  - 在 “子网” 面板中，选择 “网络接口” 下方显示的 elastic 网络接口，打开 Amazon 中的 “网络接口” 页面 EC2 。
  - 要使用的单可用区 1 文件系统的 IP 地址显示在主私 IPv4 有 IP 列中。
- 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 “网络接口” 下方显示的 elastic 网络接口，打开 Amazon 中的 “网络接口” 页面 EC2 。
  - 要使用的首选子网的 IP 地址显示在 “辅助私 IPv4 有 IP” 列中。
  - 在 Amazon FSx 待机子网面板中，选择网络接口下显示的弹性网络接口，在亚马逊 EC2 控制台中打开网络接口页面。
  - 备用子网要使用的 IP 地址显示在 “辅助私 IPv4 有 IP” 列中。

无法使用 DNS 别名访问文件系统

如果使用 DNS 别名无法访问文件系统，请按照以下过程对问题进行排查。

1. 执行以下任一步骤，验证别名是否与文件系统关联：

   a. 使用 Amazon FSx 控制台-选择您要访问的文件系统。在文件系统详细信息页面上，DNS 别名显示在网络与安全选项卡上。

   b. 使用 CLI 或 API-使用 `describe-file-system-aliases`CLI 命令或 DescribeFileSystemAliasesAPI 操作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。
3. 如果 DNS 别名与文件系统关联，请确认您也配置了以下必填项：

   - 已创建与您的亚马逊 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 (SPNs)。

     有关更多信息，请参阅 为 Kerberos 配置服务主体名称（SPN）。
   - 为 DNS 别名创建了 DNS 别名记录，该记录可解析为亚马逊 FSx 文件系统的默认 DNS 名称。

     有关更多信息，请参阅 更新或创建 DNS CNAME 记录。
4. 如果您创建了有效的 DNS 别名记录 SPNs 和 DNS 别名记录，请验证客户机的 DNS CNAME 记录是否可以解析到正确的文件系统。

a. 运行 nslookup 以确认该记录存在且可解析为文件系统的默认 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，加快该过程。

```
ipconfig /flushdns
```

5. 如果 DNS CNAME 记录解析为 Amazon FSx 文件系统的默认 DNS，但客户端仍然无法访问文件系统，您无法访问您的文件系统 请参阅了解其他故障排除步骤。

无法使用 IP 地址访问文件系统

如果您无法使用 IP 地址访问文件系统，请尝试改用 DNS 名称或关联的 DNS 别名。

您可以通过选择 Windows 文件服务器、网络和安全，在亚马逊 FSx 控制台上找到文件系统的 DNS 名称和任何关联的 DNS 别名。或者，您可以在 CreateFileSystem 或 DescribeFileSystems API 操作的响应中找到它们。有关使用 DNS 别名的更多信息，请参阅管理 DNS 别名。

- 对于加入 Amazon 托管 Microsoft 活动目录的单可用区文件系统，DNS 名称如下所示。

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

- 加入自行管理的 Active Directory 的所有多可用区文件系统以及单可用区文件系统的 DNS 名称如下所示。

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

创建新的 Amazon FSx 文件系统失败

文件系统创建请求失败的原因有很多，如以下部分所述。

主题

- VPC 安全组和网络配置错误 ACLs
- 文件系统管理员组名重复
- 无法访问 DNS 服务器或域控制器
- 无效服务账户凭证
- 亚马逊 FSx 无法访问您的 Active Directory 服务账户证书 Amazon Secrets Manager

- 服务账号权限不足
- 服务账户容量已超限
- 亚马逊 FSx 无法访问组织单位 (OU)
- 服务账户无法访问管理员组
- 亚马逊在域中 FSx 断了连接
- 服务账户没有适当的权限
- 创建参数中使用了 Unicode 字符
- 恢复备份时将存储类型切换到 HDD 失败

VPC 安全组和网络配置错误 ACLs

确保使用推荐的安全组配置配置 VPC 安全组和网络 ACLs 。有关更多信息，请参阅创建安全组。

文件系统管理员组名重复

创建加入自行管理的 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 apply your Microsoft Active
 Directory configuration with the
specified file system administrators group. Please ensure that your Active Directory
 does not contain multiple domain
groups with the name: domain_group.
```

Amazon 之所以 FSx 没有创建文件系统，是因为该域中有多个同名的管理员组。

如果您未指定群组名称，Amazon FSx 将尝试使用默认值 “域管理员” 作为管理员群组。如果有多个群组使用默认的“域管理员”名称，请求将失败。

按照以下步骤解决问题。

1. 查看将文件系统加入自行管理的 Active Directory 的先决条件。
2. 在创建加入自我管理的 A ct FSx ive Directory 的 Windows 文件服务器文件系统之前，请使用 Amazon Active Directory 验证工具验证您的自我管理的 Active Directory 配置。 FSx
3. 使用 Amazon Web Services 管理控制台 或创建新的文件系统 Amazon CLI。有关更多信息，请参阅 将亚马逊 FSx 文件系统加入自我管理的 Microsoft Active Directory 域。
4. 为文件系统管理员组提供一个在自行管理的 Active Directory 域中唯一的名称。

无法访问 DNS 服务器或域控制器

创建加入自行管理的 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.
```

按照以下步骤排查并解决问题。

1. 确认您符合在创建 Amazon FSx 文件系统的子网和自行管理的 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 先决条件。

   使用 Amazon Act FSx ive Directory 验证工具测试和验证这些网络设置。

   > **Note**
   >
   > 如果您定义了多个 Active Directory 站点，请确保与 Amazon FSx 文件系统关联的 VPC 中的子网在 Active Directory 站点中定义，并且您的 VPC 中的子网与其他站点中的子网之间不存在 IP 冲突。您可以使用 Active Directory Sites and Services 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 ACLs配置为允许所有端口上的出站网络流量。

   > **Note**
   >
   > 如果要实施最低权限，则可以只允许与 Active Directory 域控制器通信所需的特定端口支持出站流量。有关更多信息，请参阅 Microsoft Active Directory 文档。

3. 确认 Microsoft Windows 文件服务器或网络管理属性的值不包含非 Lat-1 字符。例如，如果您使用 `Domänen-Admins` 作为文件系统管理员组的名称，那么文件系统创建就会失败。
4. 确认 Active Directory 域的 DNS 服务器和域控制器是否处于活动状态，且能够响应对所提供域的请求。

5. 确保 Active Directory 域的功能级别为 Windows Server 2008 R2 或更高版本。
6. 确保您的 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 Active Directory 文档。

无效服务账户凭证

创建加入自行管理的 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.
```

按照以下步骤排查并解决问题。

案例 1：如果您使用 Amazon Secrets Manager 密钥来存储您的活动目录凭证

1. 审核 使用存储活动目录凭证 Amazon Secrets Manager。
2. 密钥 ARN 正确的情况下，遵循正确的格式：`arn:aws:secretsmanager:region:account-id:secret:secret-name-6chars`。
3. 验证密钥是否包含两个非空值的必填字段：
   - `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME`：AD 服务账号用户名。
   - `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD`：AD 服务账户密码。
4. 验证密钥和密钥是否具有基于资源的策略，该策略授予 Amazon FSx 服务主体检索机密值的`fsx.amazonaws.com`权限。

案例 2：如果您使用纯文本凭证加入 Active Directory

1. 确认您只输入了用户名作为服务账户用户名，例如在自行管理的 Active Directory 配置中输入 `ServiceAcct`。

> **Important**
>
> 输入服务账户用户名时，请勿包含域前缀（`corp.com\ServiceAcct`）或域后缀（`ServiceAcct@corp.com`）。

输入服务帐户用户名（CN= ServiceAcct、ou=Example、dc=Corp、dc=Corp、dc=com）时，请勿使用可分辨名称 (DN)。

2. 确认 Active Directory 域中是否有您提供的服务账户。
3. 确保您已向提供的服务账户授予所需的权限。服务账户必须能在文件系统加入的域的 OU 中创建和删除计算机对象。服务账户还必须至少有权执行以下操作：

   - 重置密码
   - 限制账户读取和写入数据
   - 验证写入 DNS 主机名的能力
   - 验证写入服务主体名称的能力

   有关如何创建具有正确权限的服务账户的更多信息，请参阅 亚马逊 FSx 服务账户。

亚马逊 FSx 无法访问您的 Active Directory 服务账户证书 Amazon Secrets Manager

以下各节描述常见问题及其解决方法。

加入自行管理的 Active Directory 的文件系统失败，并显示以下错误消息：

```
You can't provide both username/password and a domain join service account
secret to connect to your Active Directory. Provide only one set of
credentials.
```

要解决此问题

1. 选择是提供存储在 Secrets Manager 密钥中的凭证，还是提供以纯文本形式存储的凭证。
2. 加入 Active Directory 时，仅提供其中一个参数，不能同时提供两个参数。

加入自行管理的 Active Directory 的文件系统失败，并显示以下错误消息：

```
The domain join service account secret ARN format you entered isn't
valid. Use the format: arn:partition:secretsmanager:region:account-
id:secret:secret-name-6chars
```

要解决此问题

1. 审核 使用存储活动目录凭证 Amazon Secrets Manager。
2. 验证您输入的 ARN 格式是否正确。正确的格式示例为 `arn:aws:secretsmanager:us-east-1:123456789012:secret:MyDatabaseSecret-Ab3d5f`。

加入自行管理的 Active Directory 的文件系统失败，并显示以下错误消息：

```
Amazon FSx can't access the domain join service account secret [ARN]. Add a resource permission to the secret that grants the FSx service principal (fsx.amazonaws.com) permission to access it.
```

要解决此问题

1. 审核 使用存储活动目录凭证 Amazon Secrets Manager。
2. 验证您提供的 Secrets Manager 密钥是否具有 FSx 允许亚马逊使用该密钥的正确策略。

加入自行管理的 Active Directory 的文件系统失败，并显示以下错误消息：

```
You don't have permission to access the domain join service account secret [ARN]. A resource permission needs to be added to the secret to grant you access.
```

要解决此问题

- Secrets Manager 密钥所有者或管理员需要向您的账户授予使用该密钥的访问权限。有关更多信息，请参阅基于身份的策略。

加入自行管理的 Active Directory 的文件系统失败，并显示以下错误消息：

```
The domain join service account secret format or content isn't valid. Make sure the secret includes both CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME and CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD fields with non-empty values.
```

要解决此问题

1. 审核 使用存储活动目录凭证 Amazon Secrets Manager。
2. 验证您提供的 Secrets Manager 密钥是否同时包含两个必填字段。

服务账号权限不足

创建加入自行管理的 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.
```

按照以下程序排查并解决问题。

- 确保您已向提供的服务账户授予所需的权限。服务账户必须能在文件系统加入的域的 OU 中创建和删除计算机对象。服务账户还必须至少有权执行以下操作：
  - 重置密码
  - 限制账户读取和写入数据
  - 验证写入 DNS 主机名的能力
  - 验证写入服务主体名称的能力

  有关如何创建具有正确权限的服务账户的更多信息，请参阅 亚马逊 FSx 服务账户。

服务账户容量已超限

创建加入自行管理的 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，请确认您提供的服务账户是否已达到可以加入域的最大计算机数量。如果已达到最大限制，请创建一个具有正确权限的新服务账户。使用新的服务账户并创建新的文件系统。有关更多信息，请参阅 亚马逊 FSx 服务账户。

亚马逊 FSx 无法访问组织单位 (OU)

创建加入自行管理的 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.
```

按照以下步骤排查并解决问题。

1. 确认 Active Directory 域中是否有您提供的 OU。
2. 确保您已向提供的服务账户授予所需的权限。服务账户必须能在文件系统加入的域的 OU 中创建和删除计算机对象。服务账户还必须至少有权执行以下操作：

   - 重置密码
   - 限制账户读取和写入数据
   - 验证写入 DNS 主机名的能力
   - 验证写入服务主体名称的能力
   - 被授予创建和删除计算机对象的控制权
   - 验证读取和写入账户限制的能力

   有关如何创建具有正确权限的服务账户的更多信息，请参阅 亚马逊 FSx 服务账户。

服务账户无法访问管理员组

创建加入自行管理的 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.
```

按照以下步骤排查并解决问题。

1. 确保您只提供组名称作为管理员组参数的字符串。

   > **Important**
   >
   > 提供组名称参数时，请勿包含域前缀（`corp.com\FSxAdmins`）或域后缀（`FSxAdmins@corp.com`）。
   > 请勿使用该组的可分辨名称（DN）。可分辨名称的一个例子是 CN= FSx Admins、ou=Example、dc=Corp、dc=com。

2. 确保提供的管理员组与您要加入文件系统的管理员组位于同一 Active Directory 域中。
3. 如果您未提供管理员组参数，Amazon 会 FSx 尝试在您的 Active Directory 域中使用该`Builtin Domain Admins`组。如果此组的名称已更改，或者您使用其他组进行域管理，则必须在为该组提供该名称。

亚马逊在域中 FSx 断了连接

创建加入自行管理的 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.
```

在创建您的文件系统时，亚马逊能够访问您 FSx 的 Active Directory 域的 DNS 服务器和域控制器，并将文件系统成功加入您的 Active Directory 域。但是，在完成文件系统创建时，Amazon FSx 失去了与您的域的连接或您的域名成员资格。按照以下步骤排查并解决问题。

1. 确保您的亚马逊 FSx 文件系统和活动目录之间继续存在网络连接。而且，使用路由规则、VPC 安全组规则、VPC 网络和域控制器防火墙规则，确保它们之间继续允许网络 ACLs流量。
2. 确保亚马逊 FSx 为您的 Active Directory 域中的文件系统创建的计算机对象仍处于活动状态，且未被删除或以其他方式操作。

服务账户没有适当的权限

创建加入自行管理的 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.
```

确保您已向提供的服务账户授予所需的权限。按照以下步骤排查并解决问题。

服务账户至少需要具有以下权限：

- 被授予创建和删除加入文件系统的 OU 中的计算机对象的控制权
- 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
  - 验证写入 DNS 主机名的能力
  - 验证写入服务主体名称的能力
  - 能够（经委派）创建和删除计算机对象
  - 验证读取和写入账户限制的能力
  - 能够修改权限

  有关如何创建具有正确权限的服务账户的更多信息，请参阅 亚马逊 FSx 服务账户。

创建参数中使用了 Unicode 字符

创建加入自行管理的 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 FSx for ONTAP User Guide.
```

亚马逊 FSx 不支持 Unicode 字符。确认所有创建参数都没有 Unicode 字符，例如重音符号。这包括可以留空的参数，其默认值会自动填写。确保 Active Directory 中相应的默认值也不包含 Unicode 字符。

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，并显示以下错误消息：

```
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.
```

恢复备份并且您已将存储类型从 SSD 更改为 HDD 时会出现此问题。从备份恢复失败，因为您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。在增加请求之前，文件系统的 SSD 存储容量低于创建 HDD 文件系统所需的最低存储容量 2000 GiB。

要解决此问题，请执行以下步骤：

1. 等待存储容量增加请求完成，文件系统至少具有 2000 GiB 的 SSD 存储容量。有关更多信息，请参阅 监控存储容量增加。
2. 对文件系统进行用户发起的备份。有关更多信息，请参阅 使用用户启动备份。
3. 将用户发起的备份还原到使用 HDD 存储的文件系统。有关更多信息，请参阅 将备份还原至新文件系统。

文件系统处于配置错误状态

由于您 FSx 的 Active Directory 环境发生了变化，适用于 Windows 文件服务器的文件系统可能会进入配置错误的状态。在这种状态下，您的文件系统当前不可用，或者有失去可用性的风险，并且有可能会备份失败。

配置错误状态包括一条错误消息和建议的更正措施，您可以使用 Amazon FSx 控制台、API 或 Amazon CLI访问这些错误消息和建议的更正措施。采取纠正措施后，请确认文件系统的状态是否已更改为 `Available` – 请注意，此更改可能需要几分钟才能完成。

由于多种原因，您的文件系统可能会进入配置错误状态，例如：

- DNS 服务器 IP 地址失效。
- 服务账户凭证失效，或者缺少所需权限。
- 由于网络连接问题（例如 VPC 安全组无效、VPC 网络 ACL 或路由表配置或者域控制器防火墙设置），无法访问 Active Directory 域控制器。

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

（有关 Active Directory 要求的完整列表，请参阅先决条件。 您还可以使用 Amazon Active Directory 验证工具验证您的 FSx 活动目录环境是否已正确配置以满足这些要求。）

解决其中一些问题需要直接更新文件系统 Active Directory 配置的一个或多个参数，例如更改 DNS 服务器 IP 地址或更改服务账户的用户名或密码。在这些情况下，您的纠正措施必然涉及使用亚马逊 FSx 控制台、API 或 Amazon CLI 更新所需的配置参数。

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，您需要采取进一步措施才能使文件系统 `Available`。确保 Active Directory 环境配置正确后，在亚马逊 FSx 控制台中选择 “配置错误” 状态旁边的 “尝试恢复” 按钮，或者在亚马逊 FSx 控制台、API 或 Amazon CLI中使用该`StartMisconfiguredStateRecovery`命令。

主题

- 文件系统配置错误：Amazon FSx 无法访问您的域名的 DNS 服务器或域控制器。
- 文件系统配置错误：服务账户凭证无效
- 文件系统配置错误：密钥或 KMS Amazon Secrets Manager 密钥配置不正确
- 文件系统配置错误：提供的服务账户无权将文件系统加入域中
- 文件系统配置错误：服务账户无法再将任何计算机加入域中
- 文件系统配置错误：服务账户无权访问 OU

文件系统配置错误：Amazon FSx 无法访问您的域名的 DNS 服务器或域控制器。

当亚马逊 FSx无法与你的 Microsoft Active Directory 域控制器或控制器通信时，文件系统将进入一种`Misconfigured`状态。

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 Amazon Act FSx ive Directory 验证工具测试和验证您自行管理的 Active Directory 的网络设置。有关更多信息，请参阅 使用自行管理的 Microsoft Active Directory。

3. 在亚马逊 FSx 控制台中查看文件系统的自我管理活动目录配置。
4. 要更新文件系统的自我管理 Active Directory 配置，您可以使用亚马逊 FSx 控制台。

   a. 在导航窗格上，选择文件系统，然后选择要更新的文件系统；随即显示文件系统详细信息页面。

   b. 在文件系统详细信息页面上，选择联网与安全选项卡上的更新。

   您也可以使用 Amazon FSx CLI `update-file-system` 命令或 API 操作UpdateFileSystem。

文件系统配置错误：服务账户凭证无效

亚马逊 FSx 无法与你的 Microsoft Active Directory 域控制器或控制器建立连接。这是因为提供的服务账户凭证无效。有关更多信息，请参阅 使用自行管理的 Microsoft Active Directory。

要解决配置错误问题，请执行以下操作：

1. 确认您使用的是正确的服务账户，以及该账户的正确凭证。
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. 在导航窗格上，选择文件系统，然后选择要更新的配置错误的文件系统。

   b. 在文件系统详细信息页面上，选择联网与安全选项卡中的更新。

   您也可以使用亚马逊 FSx API 操作`update-file-system`。要了解更多信息，请参阅 Amazon FSx API 参考UpdateFileSystem中的。

文件系统配置错误：密钥或 KMS Amazon Secrets Manager 密钥配置不正确

亚马逊 FSx 无法与你的 Microsoft Active Directory 域控制器或控制器建立连接。这是因为您的 Amazon Secrets Manager 密钥或配置不 Amazon KMS key 正确。有关更多信息，请参阅 使用存储活动目录凭证 Amazon Secrets Manager。

要解决配置错误问题，请执行以下操作：

1. 验证密钥 ARN 是否正确且是否遵循正确的格式：`arn:aws:secretsmanager:region:account-id:secret:secret-name-6chars`。
2. 验证密钥是否包含两个非空值的必填字段：

- CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME：AD 服务账号用户名。
- CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD：AD 服务账户密码。
- 验证密钥和密钥是否具有基于资源的策略，该策略授予 Amazon FSx 服务主体检索机密值的fsx.amazonaws.com权限。

文件系统配置错误：提供的服务账户无权将文件系统加入域中

亚马逊 FSx 无法与你的微软 Active Directory 域控制器建立连接。这是因为提供的服务账户无权将文件系统加入具有指定 OU 的域中

要解决配置错误问题，请执行以下操作：

1. 向 Amazon FSx 服务账户添加所需权限，或创建具有所需权限的新服务账户。有关此操作的更多信息，请参阅亚马逊 FSx 服务账户。
2. 然后使用新的服务账户凭证更新文件系统自行管理的 Active Directory 配置。要更新配置，您可以使用 Amazon FSx 控制台。

   a. 在导航窗格上，选择文件系统，然后选择要更新的文件系统；随即显示文件系统详细信息页面。

   b. 在文件系统详细信息页面上，选择联网与安全选项卡上的更新。

   您也可以使用亚马逊 FSx API 操作update-file-system。要了解更多信息，请参阅 Amazon FSx API 参考UpdateFileSystem中的。

文件系统配置错误：服务账户无法再将任何计算机加入域中

亚马逊 FSx 无法与你的微软 Active Directory 域控制器建立连接。这种情况是因为提供的服务账户已达到可以加入域的最大计算机数量。

要解决配置错误问题，请执行以下操作：

1. 识别其他服务账户或创建可以将新计算机加入域的新服务账户。
2. 然后使用亚马逊 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. 在导航窗格上，选择文件系统，然后选择要更新的文件系统；随即显示文件系统详细信息页面。

b. 在文件系统详细信息页面上，选择联网与安全选项卡上的更新。

您也可以使用亚马逊 FSx API 操作`update-file-system`。要了解更多信息，请参阅 Amazon FSx API 参考UpdateFileSystem中的。

文件系统配置错误：服务账户无权访问 OU

亚马逊 FSx 无法与你的 Microsoft Active Directory 域控制器建立连接，因为提供的服务账户无权访问指定的 OU。

要解决配置错误问题，请执行以下操作：

1. 识别其他服务账户或创建可以访问 OU 的新服务账户。
2. 然后使用新的服务账户凭证更新文件系统自行管理的 Active Directory 配置。

a. 在导航窗格上，选择文件系统，然后选择要更新的文件系统；随即显示文件系统详细信息页面。

b. 在文件系统详细信息页面上，选择联网与安全选项卡上的更新。

您也可以使用亚马逊 FSx API 操作`update-file-system`。要了解更多信息，请参阅 Amazon FSx API 参考UpdateFileSystem中的。

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）。

多可用区文件系统经过本地配置，可在多个访问区之间实现冗余。使用多可用区部署类型跨多个可用区获得高可用性。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。

存储或吞吐能力更新失败

许多潜在原因会导致文件系统存储和吞吐能力更新请求失败，每种原因都有自己的解决方案。

存储容量增加失败，因为 Amazon FSx 无法访问文件系统的 Amazon KMS key

存储容量增加请求失败，因为 Amazon FSx 无法访问用于加密文件系统的 KMS 密钥。

您需要确保 Amazon FSx 有权访问用于加密文件系统的 KMS 密钥才能运行管理操作。使用以下信息解决密钥访问问题。

- 如果 KMS 密钥已被删除，文件系统及其使用已删除 KMS 密钥的任何备份都无法恢复。有关更多信息，请参阅《 Amazon Key Management Service 开发者指南》中的删除 Amazon KMS key。
- 如果 KMS 密钥已禁用，而这是客户管理的密钥，您需要重新启用密钥，然后重新尝试存储容量增加请求。有关更多信息，请参阅《 Amazon Key Management Service 开发人员指南》中的启用和禁用密钥。
- 如果密钥因为待删除而无效，则必须在密钥仍处于 `PendingDeletion` 状态时取消删除密钥。您可以在 KMS 密钥 `Enabled` 后重新尝试请求。
- 如果密钥因待导入无效，则必须等待导入完成，然后才能重新尝试增加存储空间的请求。
- 如果已超过密钥的授权限制，则必须请求增加密钥授权的数量。有关更多信息，请参阅《 Amazon Key Management Service 开发人员指南》中的资源配额。批准增加配额后，请重新尝试增加存储空间的请求。

由于自行管理的 Active Directory 配置错误，存储容量或吞吐能力更新失败

因为文件系统自行管理的 Active Directory 处于配置错误状态，存储容量或吞吐能力更新请求失败。

要解决特定的配置错误状态，请参阅文件系统处于配置错误状态。

由于吞吐能力不足，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 MBps。

将文件系统的吞吐容量至少增加到 16 MBps，然后重试请求。有关更多信息，请参阅 管理吞吐能力。

吞吐量容量更新为 8 MBps 失败

将文件系统的吞吐容量修改为 8 的请求 MBps 失败。

当存储容量增加请求待处理或正在处理时，可能会发生这种情况。增加存储容量需要的最低吞吐量为 16 MBps。请等待存储容量增加请求完成，然后重新尝试吞吐能力修改请求。

文档历史记录

- API 版本：2018-03-01
- 文档最新更新时间：2025 年 9 月 30 日

下表描述了亚马逊 FSx Windows 用户指南的重要更改。如需有关文档更新的通知，您可以订阅 RSS 源。

变更	说明	日期
为 Amazon Secrets Manager 集成新增了 Support	Amazon FSx 现已与集成，Amazon Secrets Manager 以增强对活动目录凭证的管理。有关更多信息，请参阅使用 Amazon Secrets Manager存储 Active Directory 凭证。	2025 年 11 月 5 日
亚马逊 FSx ConsoleFullAccess-更新现有政策	Amazon FSx 添加了一项新权限`secretsmanager:ListSecrets` ，允许委托人列出 Amazon Secrets Manager 用于选择域名加入服务账户凭证的密码。有关更多信息，请参阅Amazon 托管策略：Amazon FSx FullAccess。	2025 年 11 月 5 日
增加了对互联网协议版本 6 的支持 (IPv6)	FSx 适用于 Windows File Server 的文件系统现在支持两种网络类型选项： IPv4仅限和双堆栈（同时适用于 IPv4 和 IPv6）。创建文件系统时，您必须指定其中一种选项。您可以随时更改现有 Window FSx s 文件服务器文件系统的网络类型。有关更多信息，请参阅管理网络类型。	2025 年 9 月 30 日

亚马逊 FSx 更新了亚马逊FSx ServiceRolePolicy Amazon 托管政策	亚马逊向亚马逊 FSx 添加了`ec2:AssignIpv6Addresses` 和`ec2:UnassignIpv6Addresses` 权限FSxServiceRolePolicy。有关更多信息，请参阅 Amazon FSx ServiceRolePolicy。	2025 年 7 月 22 日
亚马逊 FSx 更新了亚马逊FSx FullAccess Amazon 托管政策	A mazon FSx FullAccess 托管政策已更新`fsx:CreateAndAttachS3AccessPoint` ，添加了`fsx:DescribeS3AccessPointAttachments` 、和`fsx:DetachAndDeleteS3AccessPoint` 权限。	2025 年 6 月 25 日
亚马逊 FSx 更新了亚马逊FSx ConsoleFullAccess Amazon 托管政策	A mazon FSx ConsoleFullAccess 托管政策已更新`fsx:CreateAndAttachS3AccessPoint` ，添加了`fsx:DescribeS3AccessPointAttachments` 、和`fsx:DetachAndDeleteS3AccessPoint` 权限。	2025 年 6 月 25 日
亚马逊 FSx 更新了亚马逊FSx ConsoleReadOnlyAccess Amazon 托管政策	亚马逊 FSx 更新了亚马逊 FSxConsoleReadOnlyAccess 政策以添加`ec2:DescribeNetworkInterfaces` 权限。有关更多信息，请参阅 Amazon FSx ConsoleReadOnlyAccess 政策。	2025 年 2 月 25 日

增加了对亚马逊双栈 VPC 接口终端节点的支持 FSx	现在，您可以使用 IPv6 IP 地址 IPv4 和 DNS 名称为 Amazon FSx 创建双栈 VPC 接口终端节点。有关更多信息，FSx 请参阅 Windows 文件服务器和接口 VPC 终端节点。	2025 年 2 月 7 日
添加了对双堆栈 API 端点的支持	用于创建和管理文件系统的亚马逊 FSx 服务 API 具有新的双堆栈终端节点。有关更多信息，请参阅《亚马逊 API 参考》中的 FSx API 终端节点。	2025 年 2 月 7 日
亚马逊 FSx 更新了亚马逊FSx ConsoleFullAccess Amazon 托管政策	亚马逊 FSx 更新了亚马逊FSx ConsoleFullAccess 政策以添加`ec2:DescribeNetworkInterfaces` 权限。有关更多信息，请参阅 Amazon FSx ConsoleFullAccess 政策。	2025 年 2 月 7 日
FSx 适用于 Windows 文件服务器的 Active Directory 验证工具的更新版本	FSx 适用于 Windows 文件服务器的 Active Directory 验证工具的更新版本现已推出。有关更多信息，请参阅验证您的 Active Directory 配置	2024 年 11 月 6 日

在吞吐量为 4 GBps 及更高的文件系统上增加了对更高 IOPS 级别的支持	FSx Windows File Server 将吞吐量为 4 GBps 或更高的文件系统的最大 IOPS 从 130K 提高到 150K，吞吐容量为 6 GBps 或更高的文件系统从 17.5K 提高到 200 K，吞吐容量为 9 GBps 或更高的文件系统从 260 万增加到 300 K，吞吐容量为 12 或更高的文件系统从 35K 提高到 400K。 GBps 有关更多信息，FSx 请参阅 Windows 文件服务器性能。	2024 年 1 月 17 日
亚马逊 FSx 更新了亚马逊 FSxFullAccess、亚马逊 FSxConsoleFullAccess、亚马逊FSxReadOnlyAccesFSxConsoleReadOnlyAccess、亚马逊和亚马逊FSxServiceRolePolicy Amazon 托管政策	亚马逊 FSx 更新了亚马逊FSx FullAccessFSxConsoleFullAccess、亚马逊FSxReadOnlyAccess、亚马逊FSxConsoleReadOnlyAccess、亚马逊和亚马逊FSxServiceRolePolicy 政策以添加`ec2:GetSecurityGroupsForVpc` 权限。有关更多信息，请参阅 Amazon 对 Amazon 托管策略的 FSx 更新。	2024 年 1 月 9 日
亚马逊 FSx 更新了亚马逊FSx FullAccess 和亚马逊FSxConsoleFullAccess Amazon 托管政策	亚马逊 FSx 更新了亚马逊FSx FullAccess 和亚马逊FSxConsoleFullAccess 政策以添加该`ManageCrossAccountDataReplication` 操作。有关更多信息，请参阅 Amazon 对 Amazon 托管策略的 FSx 更新。	2023 年 12 月 20 日

亚马逊 FSx 更新了亚马逊FSx FullAccess 和亚马逊FSxConsoleFullAccess Amazon 托管政策	亚马逊 FSx 更新了亚马逊FSx FullAccess 和亚马逊FSxConsoleFullAccess 政策以添加`fsx:CopySnapshotAndUpdateVolume` 权限。有关更多信息，请参阅 Amazon 对 Amazon 托管策略的 FSx 更新。	2023 年 11 月 26 日
亚马逊 FSx 更新了亚马逊FSx FullAccess 和亚马逊FSxConsoleFullAccess Amazon 托管政策	亚马逊 FSx 更新了亚马逊FSxFullAccess 和亚马逊的FSxConsoleFullAccess 政策，增加了`fsx:DescribeSharedVPCConfiguration` 和`fsx:UpdateSharedVPCConfiguration` 权限。有关更多信息，请参阅 Amazon 对 Amazon 托管策略的 FSx 更新。	2023 年 11 月 14 日
添加了对更新文件系统存储类型的支持	FSx 适用于 Windows 文件服务器的文件系统现在支持从硬盘存储类型更新到固态硬盘存储类型。有关更多信息，请参阅管理存储类型。	2023 年 8 月 9 日
添加了对提高最大吞吐能力的支持	FSx 适用于 Windows 文件服务器的文件系统现在最多支持 12 个 GBps 吞吐容量。有关更多信息，FSx 请参阅 Windows 文件服务器性能。	2023 年 8 月 9 日

添加了对 SSD IOPS 预置的支持	FSx 适用于 Windows 文件服务器的文件系统现在支持独立于存储容量配置固态硬盘 IOPS，最高可达 350,000 IOPS。有关更多信息，请参阅管理 SSD IOPS。	2023 年 8 月 9 日
亚马逊 FSx 更新了亚马逊FSx ServiceRolePolicy Amazon 托管政策	亚马逊 FSx 更新了亚马逊中的`cloudwatch:PutMetricData` 权限FSxServiceRolePolicy。有关更多信息，请参阅 Amazon FSx ServiceRolePolicy。	2023 年 7 月 24 日
亚马逊 FSx 更新了亚马逊FSx FullAccess Amazon 托管政策	亚马逊 FSx 更新了亚马逊 FSxFullAccess 政策，删除了`fsx:*`权限并添加了具体`fsx`操作。有关更多信息，请参阅 Amazon FSx FullAccess 政策。	2023 年 7 月 13 日
亚马逊 FSx 更新了亚马逊FSx ConsoleFullAccess Amazon 托管政策	亚马逊 FSx 更新了亚马逊 FSxConsoleFullAccess 政策，删除了`fsx:*`权限并添加了具体`fsx`操作。有关更多信息，请参阅 Amazon FSx ConsoleFullAccess 政策。	2023 年 7 月 13 日
增加了对亚马逊 Windows 文件服务器 FSx 版新 CloudWatch 指标的支持	FSx Windows File Server 现在提供了其他 CloudWatch 指标，用于监控文件服务器和存储卷的性能和容量使用情况。有关更多信息，请参阅指标和维度。	2022 年 9 月 22 日

添加了对文件系统性能警告的支持	FSx 现在，当一组指标中的任何一个接近或超过这些 CloudWatch 指标的预定阈值时，Amazon 会在 “性能和监控” 窗口中提供警告。每条警告还会提供可行建议，用于提高文件系统的性能。有关更多信息，请参阅性能警告和建议。	2022 年 9 月 22 日
添加了对增强文件系统性能监控的支持	适用 FSx 于 Windows 文件服务器文件系统的亚马逊 FSx 控制台文件系统监控控制面板包括新的摘要、存储和性能部分。这些部分显示了新 CloudWatch 指标的图表，这些指标可为您提供增强的性能监控。有关更多信息，请参阅使用监控指标 CloudWatch。	2022 年 9 月 22 日
为 Amazon PrivateLink 接口 VPC 终端节点添加了 Support。	现在，您可以使用接口 VPC 终端节点从您的 VPC 访问 Amazon FSx API，而无需通过互联网发送流量。有关更多信息，请参阅 Amazon FSx 和接口 VPC 终端节点。	2022 年 4 月 5 日
添加了对 Amazon Kendra 的支持	现在，您可以使用 FSx 适用于 Windows 的文件服务器文件系统作为 Amazon Kendra 的数据源，从而可以索引和搜索存储在文件系统中的文档中包含的信息。有关更多信息，请参阅在 Amazon Kendra 上使用适用 FSx 于 Windows 文件服务器。	2022 年 3 月 26 日

添加了对文件访问审计的支持	现在，您可以启用对最终用户对文件、文件夹和文件共享的访问权限的审计。您可以选择向亚马逊日志或亚马逊数据 Firehose 服务发送审核事件 CloudWatch 日志。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支持	现在，您可以使用 Amazon 将同一 Amazon 账户内的备份复制 FSx 到另一个账户 Amazon Web Services 区域（跨区域副本）或同一账户内的备份 Amazon Web Services 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	使用 Amazon开发的可自定义 Amazon CloudFormation 模板在文件系统的容量达到您指定的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
添加了对使用非私有 IP 地址进行客户端访问的支持	您可以使用非私有 IP 地址通过本地客户端访问 FSx Windows 文件服务器文件系统。有关更多信息，请参阅支持的环境。你可以加入 FSx Windows 文件服务器文件系统的自我管理的 Microsoft Active Directory，该目录包含使用非私有 IP 地址的 DNS 服务器和 AD 域控制器。有关更多信息，请参阅将亚马逊 FSx 与自行管理的 Microsoft Active Directory 配合使用。	2020 年 12 月 17 日

添加了对使用 DNS 别名的支持	现在，您可以将 DNS 别名与您 FSx 的 Windows 文件服务器文件系统相关联，您可以使用这些文件系统访问文件系统中的数据。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
添加了对 Amazon Elastic Container Service 的支持	现在，您可以使用带有 Amazon ECS 的 Windows 文件服务器。 FSx 有关更多信息，请参阅支持的客户端。	2020 年 11 月 9 日
亚马逊 FSx 现已与 Amazon Backup	现在， Amazon Backup 除了使用 Amazon 原生备份外，您还可以使用 FSx 备份和恢复 FSx 文件系统。有关更多信息，请参阅在 Amazon Amazon Backup 上使用 FSx。	2020 年 11 月 9 日
添加了对吞吐能力扩展的支持	现在，您可以随着吞吐量要求的变化修改现有 FSx Windows 文件服务器文件系统的吞吐容量。有关更多信息，请参阅管理吞吐能力。	2020 年 6 月 1 日
添加了对存储容量扩展的支持	现在，您可以随着存储需求的变化增加现有 FSx 的 Windows 文件服务器文件系统的存储容量。有关更多信息，请参阅管理存储容量。	2020 年 6 月 1 日
添加了对硬盘驱动器（HDD）存储的支持	用 FSx 于 Windows 文件服务器时，硬盘存储可为您提供价格和性能上的灵活性。有关更多信息，请参阅使用 Amazon 优化成本 FSx。	2020 年 3 月 26 日

添加了 Support 对使用文件传输的支持 Amazon DataSync	现在 Amazon DataSync ，您可以使用在 Windows 文件服务器之间 FSx 来回传输文件。有关更多信息，请参阅使用 Windows 文件服务器将文件迁移到亚马逊 FSx Amazon DataSync。	2020 年 2 月 4 日
FSx 适用于 Windows 文件服务器的版本支持其他 Windows 文件系统管理任务	现在，您可以使用 Amazon FSx CLI 进行远程管理，管理和管理文件共享、重复数据删除、存储配额和文件共享传输中的加密。 PowerShell有关更多信息，请参阅管理文件系统。	2019 年 11 月 20 日
FSx 适用于 Windows 文件服务器发布原生多可用区支持	您可以使用适用于 Windows File Server FSx 的多可用区部署，更轻松地创建跨多个可用区的具有高可用性的文件系统（AZs）。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 适用于 Windows File Server 发布了对管理用户会话和打开文件的支持	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 FSx 的 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的文件。	2019 年 10 月 17 日

亚马逊 FSx 发布对微软 Windows 卷影副本的支持	现在，你可以在你的 Windows 文件服务器文件系统上配置 Windows 卷影副本。 FSx 影子副本使用户可以轻松撤消文件更改并通过将文件恢复到早期版本来比较文件版本。有关更多信息，请参阅使用影子副本。	2019 年 7 月 31 日
亚马逊 FSx 发布共享的微软 Active Directory 支持	现在，您可以 FSx 将 Windows 文件服务器文件系统加入位于不同 VPC 或与文件系统不同的 Amazon Managed Microsoft AD Amazon Web Services 账户 目录。有关更多信息，请参阅 Active Directory 支持。	2019 年 6 月 25 日
亚马逊 FSx 发布增强版微软 Active Directory 支持	现在，你可以将 Windows 文件服务器文件系统加入 FSx 你自行管理的 Microsoft Active Directory 域，无论是在本地还是在云中。有关更多信息，请参阅 Active Directory 支持。	2019 年 6 月 24 日
亚马逊 FSx 符合 SOC 认证	亚马逊 FSx 已被评估为符合 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
增加了有关 Amazon Direct Connect VPN 和区域间 VPC 对等连接支持的澄清说明	2019 年 2 月 22 日之后创建的亚马逊 FSx 文件系统可使用 VPN 和跨区域 VPC 对等互连进行 Amazon Direct Connect 访问。有关更多信息，请参阅支持的访问方法。	2019 年 2 月 25 日

增加了Amazon Direct Connect、VPN 和区域间 VPC 对等连接支持	现在，您可以从本地资源和其他 Amazon VPC 中的资源访问 FSx 适用于 Windows 的亚马逊文件服务器文件系统，或者 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 现已正式上市	亚马逊 FSx 版 Windows 文件服务器提供完全托管的微软 Windows 文件服务器，由完全原生 Windows 文件系统提供支持。Amazon FSx for Windows File Server 提供的功能、性能和兼容性使企业应用程序可以轻松升级和迁移到其中 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。